An Efficient Framework for Data Dissemination in Multi-UAV Ad hoc Networks

A Thesis

submitted in partial fulfillment of the requirements for the award of the degree of

Doctor of Philosophy

in

Computer Science and Engineering Department

by

Mohd. Abuzar Sayeed
Reg No: 901503014

Under the supervision of
Dr. Rajesh Kumar

Thapar Institute of Engineering and Technology
Patiala-147004, Punjab, India
March 2021

Candidate Declaration

I hereby certify that the work, which is being presented in the thesis, entitled **An Efficient Framework for Data Dissemination in Multi-UAV Ad hoc Networks**, in partial fulfillment of the requirements for the award of the degree of **Doctor of Philosophy** and submitted to Thapar Institute of Engineering and Technology is an authentic record of my own work carried out during the period **July 2015** to **March 2021** under the supervision of **Dr. Rajesh Kumar**.

The matter presented in this thesis has not been submitted elsewhere for the award of any other degree or diploma from any institution.

Date: 05/08/2021

Mohd. Abuzar Sayeed
Candidate

This is to certify that the above statement made by the candidate is correct to the best of our knowledge.

Date: 05/08/2021

Dr. Rajesh Kumar
Professor, CSED
Supervisor

Acknowledgements

First, I would like to express my deep gratitude to my supervisor **Dr. Rajesh Kumar**, Computer Science and Engineering Department, Thapar Institute of Engineering and Technology, for his invaluable advice and encouragement at every step of my PhD program. Dr Kumar was always there to provide academic, philosophical, emotional and motivation support. Without his unfailing support and belief in me, this thesis would not have been possible. His contribution to this thesis goes well beyond his role as an academic supervisor and includes constant support on a personal level without which this journey may never have been completed. And for this, I am truly grateful. The role and contribution he had in past 5 years of my life, I can only express by acknowledging that he is a mentor for Life.

An overwhelming gratitude and complements to my friend and mentor **Dr. Vishal Sharma**, Assistant Professor, EEECS, Queen's University, Belfast, for his constant motivation and encouragement. Without his expertise and ability to examine and evaluate intensively and aggressively, this thesis would not have been visualized. Dr Sharma's ability to allow more and more time and efforts towards every single step, and technical details of the subject is something of a lesson forever and a quality I would like to keep with me. His commitment towards his job and motivation to beat the benchmarks has left me inspired and I would like to work alongside him in times to come

I would like to express my gratitude to Professor & Head, Computer Science and Engineering Department **Dr. Maninder Singh**, and Professor & Dean-RSP **Dr. Rafat Siddiqui** for their constant motivation and encouragement. I would like to thank **Dr. Sushma Jain**, PhD Coordinator for making my PhD a smooth and easy going affair. I would like to thank **Dr. Ravinder Kumar** for his support.

I would like to give special acknowledgements to my fellow M. Tech and Ph.D scholars Ms. Farhat Un Nisa, Mr. Gurpreet Pal Singh Mehta, Mr. Neeshu Agarwal, Mr. Ayush Gupta, Mr. Savidh Khan, Mr. Sachin Jaidka, Ms. Tripti Choudhary, Ms. Akanksha Kotwal, Ms. Bhawna Jangid, Ms. Chaavi Tewatia and Mr. Rahul Sharma for their support and motivation.

Finally, I would like to express my sincere and deep gratitude to my parents and brothers for supporting me at every step.

Mohd. Abuzar Sayeed

Abstract

Unmanned aerial vehicles (UAVs) are self abundant flying robots, which provide efficient, low-complex, critical connectivity and concordance coverage. Multiple UAVs form an autonomous connected communication network which has revolutionized both civilian and military aviation and paved in towards unprecedented innovations in the area of infrastructure less connectivity. UAVs are sometimes interpreted as and are equated to mobile connected devices, however, UAVs demand extra features and advance planning towards network formations, transmission scheduling, data dissemination, trajectory and velocity planning and Quality of Service (QoS) requirements.

It is copiously acknowledged and proved with simulations, real time research and industry modelings that aerial and ground networks can come together and perform complex tasks uplifting the barriers of energy, environment, geography and trajectory. The works presented in this thesis target data dissemination is multi UAV ad hoc networks. Both transmission scheduling and aerial mobility aspects of data dissemination are presented. Initially, an efficient data dissemination scheme for multi-UAV assisted Wireless Sensor Networks (WSN) is presented. The WSN network formations constantly suffer from depleting charge forcing the topology into constant reconfiguration. On account of rapidly depleting and re-configuring ground nodes a data dissemination framework is presented. In order to facilitate data aggregation and transmission a virtual topology is constructed by exploiting aerial network formation and Software Defined Networks (SDN). The topology is constantly monitored and reconfigured when required. An effective and efficient sleep timer and back-off counter is also proposed on accord of depleting energy.

Building upon the transmission scheduling framework, two UAV Mobility/Trajectory frameworks for enhanced coverage and data dissemination in multi-UAV ad hoc networks are presented. First, a novel mobility framework for multi-UAV assisted WSNs is proposed which takes into account average transmission densities of the underlying topology/geography. The underlying network is classified dense or scarce based on the derived attraction factor, the classification is further processed to generate UAV waypoints. Second, an SDN based mobility framework for communication and coordination among aerial and ground nodes is introduced. The SDN controller provides the opportunity to update flows on the move, thus, adapting to the dynamic topology. This helps updating the legal moves through re-configurable flow tables.

A QoS enhancement mechanism for multi UAV ground ad hoc networks is presented in form of a throughput maximization approach which involves minimizing delay and packet

loss through UAV trajectory optimization, reinforcing the congested nodes and transmission channels. A position-aware graph neural network (GNN) is used for characterization, prediction, and dynamic UAV trajectory enhancement. The aggressive reinforcement policy is achieved by characterizing nodes, links, and overall topology through delay, loss, throughput, and distance.

The coordination between aerial and ground nodes has enhanced the versatility and quality of the traditional networks but if unaddressed, it also exposes the overall networked infrastructure. The conceptualization of attacks on UAV systems is as inherent as the exciting possibilities and future that comes along Unmanned Aerial Systems (UAS). The thesis presents a study of possible threats, vulnerabilities and attacks mounted on the connected UAS and presents a framework for safeguarding UAS against malicious attackers and recovering the rogue UAVs. Recurrent neural networks and multivariate component analysis is used for detecting outliers and abnormalities in the aerial networked environment.

Table of Contents

List of Figures

List of Tables

List of Abbreviations

3GPP	Third Generation Partnership Project
AKA	Authentication and Key Agreement
CBRN	Chemical, Biological, Radiological, and Nuclear
CE	Control Element
CNN	Convolutional Neural Network
CONOPS	Civilian Concepts of Operations
CSAT	Cooperation, Search, Acquisition and Tracking
DCAN	Developed Control of ATM Networks
DSN	Deep Space Network
FANET	Flying Ad hoc Network
FE	Forwarding Element
FIB	Forwarding Information Base
GNN	Graph Neural Networks
HAP	High Altitude Platform
IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet of Things
IP	Internet Protocol
LOS	Line of Sight
LSTM	Long Short Term Memory
LTE	Long term Evolution
MANET	Mobile Ad hoc Network
MIMO	Multiple Input Multiple Output
NCA	Network Control Applications
NE	Network Element
NETCONF	Network Configuration
NIB	Network Information Base
NSA	Network Control Server
OBU	On Board Unit
OFA	Open Flow Agent
OFC	Open Flow Controller
ONF	Open Networking Foundation
OPENSIG	Open Signaling
RAP	Routing Application Proxy
RF	Radio Frequency

RIB	Routing Information Base
RSU	Road Side Unit
SDN	Software defined Network
TCP	Transmission Control Protocol
TE	Traffic Engineering
UAS	Unmanned Aerial System
UAV	Unmanned Aerial Vehicle
VANET	Vehicular Ad hoc Network
VTN	Virtual Tenant Networks
WMN	Wireless Mesh Network
WSN	Wireless Sensor Network

Chapter 1

Introduction

Wireless communication defines a paradigm shift from electrical to electromagnetic transfer of information between two or more end points which are not necessarily connected to electrical conductors. The propagation distance of wireless communication can range from, somewhere between a few meters as is the case of IEEE 802.15.1 Bluetooth to millions of kilometers as is the case of NASA's Deep Space Network (DSN). Wireless communication networks are designed to support portable, fixed, mobile, temporary and permanent connections and can be generalized to scalable technological advancements of non confined nature which have revolutionized the connectivity down till the most fundamental aspects of data communication. Up against the wired counterparts wireless technology provides cost deficit independent low complex connectivity with varying degree of scalability alongside the non-negotiable advantage of mobility. The mobile flexibility offered by the wireless networks prompt the user to access data anytime from anywhere without connecting to the infrastructure backbone and offer reachability among the nodes to communicate easily [1, 2, 3, 4].

Institute of Electrical and Electronics Engineers (IEEE) has classified wireless networks into Infrastructure-based wireless networks and infrastructure-less wireless networks or ad hoc networks. The infrastructure-less wireless ad hoc networks are further reclassified as Wireless Sensor Networks (WSNs), Wireless Mesh Networks (WMNs), and Mobile Ad hoc Networks (MANETs). Further MANETs are grouped into Vehicular Ad hoc Networks (VANETs) and Flying Ad hoc Networks (FANETS) [5, 6, 7].

1.1 Background

Self-organizing topologies of temporal nature which are scalable to any number of nodes given an efficient compromise between the number of nodes and available bandwidth serves as the basic definition of ad hoc networks. The fundamental feature which segregates ad hoc configuration from that of infrastructure based classifications is that the nodes can communicate and manage the overall topology without fixed connectivity. The technological revolution has resulted in the evolution of this basic definition of ad hoc

networks and today every existing topology is in one or the other ad hoc deployment. The offered flexibility, reduced deployment cost, inherent fault tolerance and robustness, dynamic and instantaneous scalability, ability to facilitate both direct and indirect communications and versatile deployment characteristics (virtually anywhere) has made this breed of wireless communication the topic of interest, particularly in the research community. Yet the deployment arrives with its own set of requirements and issues. Slow data rate, noise, interference, medium access control, routing, dynamic topology and packet error rate contribute towards the paramount complexity of the wireless ad hoc networks. Alongside these issues, the existing protocols and standards cannot fit in directly when it comes to ad hoc networks [1, 5, 6].

Ad hoc networks are comprehensively allocated into Mobile Ad hoc Networks (MANETs), Vehicular Ad hoc Networks (VANETs) and Flying Ad hoc Networks (FANETS). MANETs are specialized unpredictable typologies characterized by slow randomized movements. MANET nodes themselves act as routing junctions and facilitate to-and-fro communications unlike infrastructure based wireless networks that employ access points or fixed infrastructure routers for communications. MANET nodes follow the principle of auto-configuration with random connections and disconnections being an inherent property. MANETs are a self configured and a self organized network where nodes can communicate anytime at will in any direction and random connections are established automatically.

VANETs are high speed sub classification of MANETs. In harmony with MANETs, VANETs themselves are a multi-hopping network comprising of mobile nodes. In contrast to MANETs, VANET nodes are highly mobile and tend to create a diminishing topology as a result of constant disconnections and volatile topological constraints. Put simply, VANETs constitute a spontaneously created wireless network of mobile devices – in the vehicular domain. Indispensably, VANETs are a network of vehicles: stationary, relative or, high speed. It consists of a fixed infrastructure road side unit (RSU) which communicates with vehicles and also facilitates communication between two vehicles. The moving vehicles are equipped with an on board unit (OBU). The RSU is further connected to other RSUs or the backbone network. VANETS are designed with the main purpose of improving security on the road, vehicular collision prevention, safety, blind crossing, dynamic route scheduling and real-time traffic condition monitoring. Facilitating internet connectivity to the on road vehicles is another added advantage of VANETs [8, 9].

FANETs are a subset of VANETs which in turn, are classified MANETs. FANETs are very high speed unmanned aerial nodes (UAV) which by default and deployment

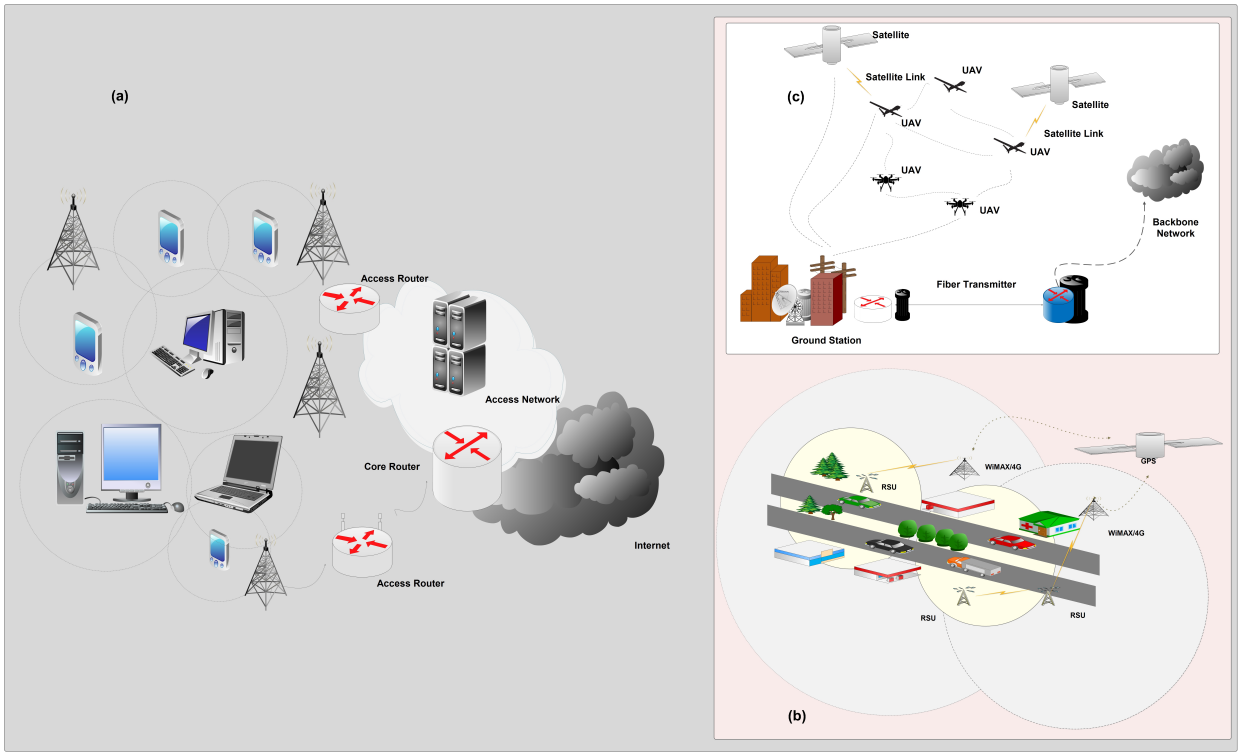


Figure 1.1: Ad hoc Network Classification: (a) MANETs, (b) VANETs, (c) FANETs.

Table 1.1: Comparison Among Ad hoc Networks.

PARAMETERS	MANETs	VANETs	FANETs
Node Mobility	2-D Low Compactness	2-D Medium Compactness	3-D High Compactness
Mobility Model	Random	Regular	Predetermined
Node Density	Low	Medium/High	Low
Node Velocity	Low	Medium/High	High
Topology Change	Slow	Average	Rapid
Line of Sight	Not Available	Scenario Specific	Available
Power Consumption	Low	Vehicle Dependent	High
Computational Power	Limited	Average	High
Localization	GPS	GPS, AGPS, DGPS	GPS, AGPS, DGPS, IMU
Network Lifetime	Low	High	High

characteristics form a star topology with the ground control and mesh topology among themselves. Unmanned Aerial Vehicles (UAVs) are autonomous flying robots, with or without payload, which provide efficient low-complex connectivity and comprehensive encyclopedic coverage. UAV's degree of autonomy depends on the flight and mission characteristics. They are either under control of a remote human operator, onboard micro controller and computers or managed in turn, by an autonomous robot. The major difference between UAV and other mobile networks is broadly dictated by node mobility, node density, topology change, radio propagation model, power consumption and network lifetime, computational power and localization. Figure 1.1 and Table 1.1 detail the MANET classification and present a comparative study of MANETs, VANETs and FANETs.

The exponential developments in UAV technology and varying applicability of small to large scale UAV deployments has paved the road map towards reliable and budget wireless communication solutions. UAVs can be deployed as temporary aerial base station to provide reliable low cost network connectivity to the desired areas. UAVs can be deployed alongside ground vehicles for military, search and rescue operations. And along side sensor nodes at harsh geographical locations, serving as data sinks. UAVs can also serve as user equipment (UEs), called the cellular-connected UAVs, alongside ground nodes for delivery purposes [1].

The UAV applications range from weather forecasting and remote sensing, disaster relief and supply operation, military operations and surveillance, geographical monitoring, monitoring of inhabitable area, UAV guided cooperative systems, terrestrial movement tracking, aircraft tracking system, civilian services, information relaying, hotspots and access points, agricultural support and monitoring systems, defense against aerial threats, journalism, commercial surveillance and filming, law enforcement, scientific research, conservation, pollution monitoring, archaeology, cargo transport, disease spread patterns and spy systems. Wireless networks can take advantage of the versatility of UAV deployments for spearheading Collaborative Flying Ad Hoc Networks. Collaborative FANETs are formed by coordinating different ad hoc networks with varied operational environments and characteristics. Coordination between two simultaneously operating yet different ad hoc networks enhances scalability with budget operational costs. Collaborative network formations can easily uplift the complexities of complex tasks such as cooperative search, tracking, and data acquisition. In this thesis work, collaborative networks are formed between wireless sensor networks (WSN), ground ad hoc networks and the unmanned aerial networks.

1.2 Multi-UAV Networks

The range of applicability and environment independent deployment alongside the coordination and guiding capabilities towards existing and legacy network formations have paved a broad entry-exit scenario for UAV networks. UAVs have achieved substantial exposure towards both single and multi-UAV deployments and have shown tremendous growth both in research and applications. UAVs are capable of supporting a wide range of civilian and military applications as a result of their flexible movements and ease of configurations. UAVs can further be deployed to form collaborative networks with the ground nodes [10, 11, 12, 13]. The collaboration among ground and aerial nodes has resulted in significant gains in data dissemination, monitoring, and control over strategic locations. UAVs play a significant role when it comes to data gathering from inaccessible

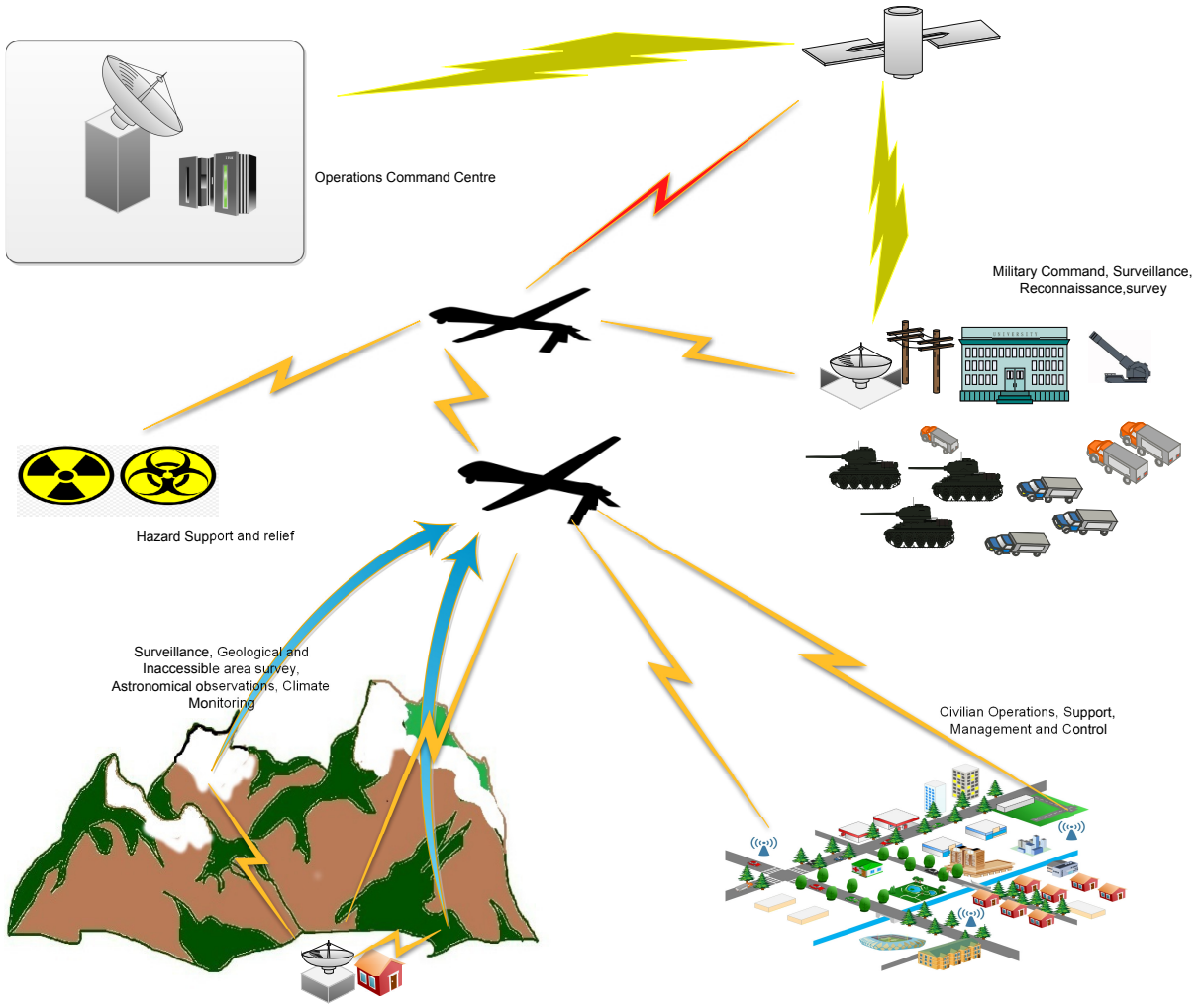


Figure 1.2: An Illustration of Multi-UAV Network Formation.

and sensitive geographical locations. Multiple UAVs can form self-abundant networks which can form a collaborative system with existing ground networks, elevating the issues of coverage, scalability, and efficiency of existing network formations. The multi-UAV deployments can readily integrate with existing network formations in order to navigate ground nodes [5, 14].

Multi-UAV collaborate to achieve common objectives or achieve different mission parameters. It has been abundantly noted and tested in application that collaborative UAV and ground networks together can perform complex-critical tasks. With both environment and energy as targets, the cooperative network is expected to traverse the geography or archive the mission essentials with satisfactory constraints. Cooperation, Search, Acquisition and Tracking (CSAT), Cognitive Mapping, Topological Organizing Maps and Self-healing neural models are proposed for Multi-UAV and ground ad hoc collaborative models [5, 15, 16, 17, 18, 19, 20]. Figure 1.2 gives an insight into the exemplary scenario

of UAV cooperative networks.

Cooperative ad hoc networks have led the civilian and military applications to a new level. When interfaced together, these networks provide an efficient backdrop to surveillance, disaster management, reconnaissance, and other applications. There is a history of unmanned aerial vehicles (UAVs) deployed for military applications, but the recent advances in wireless technologies have shifted the attention towards the Civilian Concepts of Operations (CONOPS) that were initially driven by the purpose of homeland security. High radio frequency (RF) coverage, high altitude, high throughput, heavy payload, operating time, ease of use, low cost are the basic requirements of UAV-CONOPS. CBRN (Chemical, Biological, Radiological, and Nuclear Reconnaissance)-CONOPS whose major purpose is the containment of hazards are also turning towards UAV networks. Cellular network based air-to-ground links and UAS-backbone systems, communication aware sensor distribution etc. are some of the promising aspects of the UAV systems [21, 22].

The cooperation between aerial and ground networks is essentially a collaborative network formation between unmanned aerial nodes and static or mobile ground nodes. Mobile ground nodes can range anywhere from traditional or military vehicles loaded with transceiver and processing units to VANETs themselves. Static nodes are typical wireless sensor motes. Until stated otherwise this thesis address WSN nodes as the underlying ground network. WSNs are random and spatially distributed networks of nodes. The nodes consist of transceiver, battery, storage, and processing power. The WSNs operate in areas that are generally not accessible on a frequent basis. The motes in WSNs function as recording and transmitting agents. The WSNs consist of a base station, manager nodes, and sensor motes. The major issue with WSNs is depleting battery power, which in turn, is not easy to replace.

The cooperation between WSNs and UAV networks can achieve many goals related to weather forecasting and remote sensing, military operations and surveillance, monitoring of inhabited areas, cooperative systems, information relaying, agricultural support, disaster relief, archaeology, pollution control [23, 24]. The application of UAVs can help elevate a lot of problems such as energy, transmission delays, better coverage, etc. The major issue at hand is the formation of this collaborative network itself, which requires focusing on topology, UAV paths, relaying and energy efficiency [25]. In addition to these, UAVs can be used to perform remote diagnosis of WSN's field that otherwise is tedious because of its remoteness and diversity. As an example, UAVs-WSNs coordination can be used to track land mines while allowing safe passages for the soldiers in military scenarios. Moreover, UAVs-WSNs can be used to identify disoriented devices and support as rescue equipment in natural disasters.

1.2.1 Multi-UAV Networks: Characteristics

The crucial step towards UAV networks is the development of sustainable Multi-UAV environments. The network characteristics of UAV follow a cause and effect pattern. UAVs inherit from MANETs, VANETs, and traditional WSNs but due to high dimensionality of aerial networks some characterizes are specific to aerial networks that differ from others while others are effected by fast speed and volatility. This section lists the network specific characteristics of aerial networks.

i. *Radio propagation:* UAV enabled communication systems rely massively on the radio channel models, configurations, aerial and ground node densities, node movement characteristics and associated network conditions. Network paradigm dictates a good communication channel between the aerial node and ground nodes alongside LoS connection to at least one base station. Another fundamental characteristic of UAV communication is that a particular ground node must have good communication corridor with at least one aerial node. Both aerial and ground nodes employ different communication channels and due to the aforementioned independence the radio propagation model and conditions differ significantly

ii. *Power consumption and network lifetime:* UAVs generally employ hybrid power units. A hybrid power unit is capable of processing on liquid/gas fuel, fuel cell, battery, solar cells, and super-capacitor. Legacy and traditional wireless network nodes have always operated within power constraints. Efficient battery utilization and prolonging the network lifetime has always been an important concern. The usage of UAVs and collaborative network formations to increase the operational duration of the wireless devices has revolutionized the infrastructure less wireless networks. The added constraint is that aerial nodes themselves suffer from high energy depletion rates.

iii. *High Data Rate:* The improved connectivity resulting from larger equipments and LoS connectivity facilitates reduced network latency and higher accuracy. The latency can be broadly established as the motivation towards higher packed delivery ratios as well.

iv. *Computational limitations:* UAVs can gather information on demand irrespective of underlying geography and environment of interest. UAVs have changed the era of information transfer by establishing an easy, cost effective and fast solution for data acquisition. UAVs don't necessarily suffer from computational limitation but computing power and equipment weight are directly proportional to the power consumption and aerial network lifetime. Also the data transfer rates achieved by

multi-UAV systems lifts the computational burden from the ground nodes as data can be easily transferred to ground control for pre-processing.

v. *Adaptability:* Multi-UAVs together achieve a dynamic autonomous network formation and are capable of achieving mission objectives without human intervention. UAV networks are capable of self-configuration, and are able to maintain and monitor the network independently.

vi. *Deployment:* UAVs are platform and communication technology independent nodes. The overall adaptability of aerial nodes makes it easy to deploy, upgrade and redeploy nodes without any restrictions of technology or geography.

vii. *Connectivity:* Aerial nodes suffer from no to minimal connectivity issues. 3-dimensional movement and node elevation provides with direct LoS connectivity. Also the hybrid power utilization and ability to operate independent of geography and communication technology further enhances connectivity of the aerial networks.

viii. *Node failures:* Failure of an aerial node doesn't effect entire collaborative topology. The topology can be slightly reconfigured and the network continues to operate with comparable performance levels. With this ease of deployment, without tampering the overall mission objectives a faulty node can also be replaced, upgraded or redeployed.

ix. *Flight path and mobility:* Mobility and flight path of the aerial nodes can be managed, maintained and modified dynamically during the lifetime of the network. UAV nodes possess the flexibility of pre-programmed static routes, mission specific dynamic mobility, adaptive mobility, statistical mobility or random mobility. Maneuvers of the aerial nodes can be controlled effectively and efficiently without overlapping way-points.

x. *Mission environment:* The greatest contribution of aerial nodes towards communication networks is environment, communication and mission independence. UAV application can differ in terms of number of aerial nodes, communication technology, geographical size, topological requirements, payload and flight time, mobility or autonomy.

xi. *Scalability:* UAV networks are scalable to any size, topological or mission requirements with an added constraint. An efficient compromise between the data rate and the number of nodes is required to maintain consistent system performance levels. Increasing data rates without changing the number of nodes or increasing the number of nodes without improving the data rate leads to a gradual decline in

system performance.

1.2.2 Multi-UAV Networks: Key Challenges and Research Gaps

Based on the findings of literature survey, following areas have been identified that require significant research contributions:

i. *Radio propagation:* UAV nodes are mandated to have a good connection with at least one on ground base station, but the presence of multiple aerial and ground bases cause interference and resultant performance deficits. This coexistence requires thorough attention and coordination between terrestrial and infrastructure network. Also the 3 dimensional network environment consists of services designed for classical and legacy wireless networks.

ii. *Topology:* Ad hoc networks rely heavily on efficient selection of neighbors and arrangement of nodes within the spatial geometry. Arrangement of nodes in an efficient manner to enhance the performance of the network is one of the major challenges in multi-UAV networks. The choice of topology is extremely important as the sudden topology change in UAV networks make it very difficult to maintain a consistent coordination among the nodes. Therefore in order to maintain a consistent transmission channel, a self-configuring dynamic topology which is inherently decentralized, is required to achieve better flexibility in case of disconnections.. For instance, the mesh topology is inherently self-organizing but the star topology can achieve a distributed control which is important for fast association and infrastructure independence.

iii. *Mobility:* The aerial nodes are subject to high mobility resulting in frequent topological changes and momentary connections among the nodes. Erratic aerial networks cannot be subjected to handshake and traditional data dissemination techniques as the nodes are deployed and re-deployed and every encounter can be first and last. Although the changing dimensions make jamming and other attacks impractical, but sustaining the network itself is a complex task.

iv. *Routing:* Routing has persisted as an in issue whether it is wireless or wired network configuration. An efficient routing mechanism facilitates higher throughput rates while guaranteeing minimal latency during network operations. For UAV networks, more robust and fault-tolerant routing protocols are required which can provide minimum delay during route selection, efficient re-configurations, and higher provisioning for quality of services to end users.

v. *Energy:* Ad hoc networks suffer from higher energy depletion rates. The energy

depletion primitive is applicable to both aerial and ground nodes. Thus, efficient designs and configurations are required that consume lesser energy. Device and topological configurations can be efficiently designed and managed to lower the overall energy consumption of the proposed network deployment.

vi. *Timing Constraints:* The connection time between nodes is volatile, thus requiring message transmission, reception, and authentication in a limited time interval. Also, during the next encounter, a node would have been hacked or any malicious attacker could have cloned the identity, thus imposing short-lived authentications. The added constraint of the safety pushes even harder bound on the timing constraints.

vii. *Network Size:* Network size depends on the area under deployment or the size of the collaborative network. It imposes two fundamental challenges to aerial networks. Firstly, the proposed mechanism must be scalable with the dynamically increasing size of the network. Secondly, different areas might be subjected to different requirements or protocols.

viii. *Real-Time and Topological Awareness:* UAV applications deployed in mission-critical scenarios function on the principle of reply and response. A rogue or inconsiderate aerial node is capable of disrupting routine data dissemination mechanisms that are in place and can escalate the response time of the overall system. Routing and transport is also required to cope with dynamically changing topology and constantly switching aerial nodes.

ix. *Density:* The network is ever evolving as it can be sparse or dense, the interference level keeps shifting from low to high and vice-versa. This density of network is also dependent on area or disaster situation to be surveyed. Altitude also has an impact on the positioning and topology formation as the coverage area of the beacon is dependent on the height of the flight. An efficient data dissemination framework that dictates the tactical movement of UAVs according to the specified terrain is required.

x. *Transmission:* Both the inter node transmission and inter layer transmission are to be taken care of while implementing these networks in order to address the strict deadline and latency issues. Especially when two different kinds of networks come into contact it becomes extremely important to perform route re-distribution and summation. This redistribution and summation not only requires coordination between the layers of the UAV transmission system but also between the different kinds of networks involved.

xi. *Corridor Detection:* The corridor detection and maintenance algorithm need to

evolve as growing urbanization and traffic is making it difficult to determine an efficient and safe corridor. This growing urbanization has also led to the increase in interference and sudden changes in topology and altitude. A framework is required that takes into account all these issues that may happen anytime during the course of the flight.

xii. *Safety and Threat Mitigation:* With the number of possible permutations for compromising operational safety of an aerial network, once, inside the network, the attacker can unleash malicious nodes, with a threat to UAV systems ranging anywhere from confidentiality, integrity, authentication, non-repudiation, and scalability. Attacks on UAV systems are possible at any layer of communication: *Application* (malicious code, repudiation, data corruption, impersonation, authentication), *Transport* (TCP attacks, flooding, session attacks), *Network* (DoS, routing attacks, flooding, resource poisoning, wormhole, Byzantine, information disclosure, packet replication, cache poisoning), *Data Link* (MAC attack, DoS, traffic monitoring), and *Physical* (jamming and DoS). The rudimentary step towards an end-to-end secure UAS is not only safeguarding communication paths but also securing the overall environment which makes up the platform. Communication paths, end devices, base station, packet core, backbone network, and underlying IP networks together constitute the UAS operational environment. The drone should be able to verify the source of transmissions (command/control) it is receiving, and reject those coming from malicious transmitters. Drone operational environment should be built in a way that it is automatically able to detect common attacks such as replay, which use the same principles as a DDoS attack to bombard the target device with commands to disrupt or gain entry.

xiii. *Authentication:* UAS are tightly packed into four communication scenarios: UAV to terrestrial (HAP or Satellite); UAV to UAV; UAV to mobile ground nodes; UAV to the base station. The availability of the above-mentioned communication channel relies on cooperation among the nodes. Secure UAS is a collective of safe wired and wireless communication links with protection against both internal and external adversaries. Authentication primitives on transmissions, if applied, can compromise the overall privacy of the system. An attacker can trick the overall system by taking advantage of an authentication dialogue between a normal aerial node and a compromised aerial node and can use the information in further attacking the overall system. A situation may arise where an eavesdropper listening to the conversation can acquire fake credentials. Once inside the system, an attacker can take advantage of compromised security or jacked nodes to launch a full scale cyber/network attack

on the overall aerial system.

xiv. *Software Defined Networking:* Introduction of SDN and Network Function Virtualization (NFV) had prompted towards achieving dynamic control and on demand arrangement of the network. Another issue that needs to be addressed and involves SDN and NFV is the level of flexibility that can be achieved with the independence of physical, MAC and LLC. A significant level of abstraction which provides interoperability among different types of networks and within the same network consisting of different kind of devices is prime concern.

xv. *4G LTE and 5G:* The currently deployed generation of wireless communication, 4G LTE, is characterized by increased data transfer rates, security and reliability. 5G communication networks are not only an evolution from the current networks but also add new capabilities to the existing 4G/LTE networks. 5G exploits existing setups where the infrastructure is based on SDN and NFV. The standardization of 5G is still in process but 5G networks make use of low, medium, and high bands of communication and are termed as New Radio (NR) air interface. Along with enhanced efficiency the third-generation partnership project (3GPP) also demands the embedding of safety capabilities into the network architecture itself. The technological flexibility, better radio coverage and speed gains alongside safety and security of LTE can open a broad spectrum of developments in the field of UAV networks.

1.3 Objectives of Thesis

On the basis of literature review and research gaps, the following objectives are delineated and how each objective have been accomplished is explained using the following methodology:

(a) *Objective 1: Detailed survey and analysis of the literature for developing a thorough understanding of the problem identified.*

To develop an in-depth understanding of the aerial networks, topological requirements, environmental characteristics, operational parameters and issues associated with the UAV network deployment itself, theoretical and practical review of the available literature and simulators was conducted. The survey included industry standards and deployment white papers alongside articles from journals and magazines, which lead to the identification of research gaps and problem formulation and later defined the scope of this work.

(b) *Objective 2: To design and develop an efficient framework for data dissemination*

in Multi-UAV ad hoc networks.

This objective is accomplished in three phases. In first phase, a transmission scheduling based data dissemination approach is proposed. The framework establishes a virtual topology over the underlying actual topology by means of an SDN controller, while capitalizing on the mobile aerial relays at the same time. The proposed SDN controller monitors, manages, tracks and re-configures the topology according to the data aggregation and distribution demands. The simultaneous communication from aerial nodes towards ground nodes, controller and base station is facilitated by multiple input multiple output (MIMO) antennas. The energy efficiency of the proposed solution comes from the efficient and effective management of sleep states and back-ff counters by the SDN controller.

In second phase, an aerial mobility/trajectory based data dissemination framework is proposed. The proposed framework operates by evaluating the originating transmissions. The transmissions are used to calculate the attraction factor and the UAV way-points are generated accordingly.

In third phase, a framework for safeguarding UAS against malicious attackers and recovering rogue UAVs is proposed. Convolutional Neural Network (CNN) and Long Short Term Memory (LSTM) based predictions are used for detecting abnormality in behavioral, statistical, and mobility patterns. Statistical analysis is employed for detecting outliers in networked aerial environment.

(c) *Objective 3: To achieve QoS enhancement over the proposed data dissemination framework.*

To accomplish the objective, a throughput maximization approach depending on delay and packed loss minimization by adjusting the UAV trajectory is proposed for aerial ground networks. Trajectory of the nodes is adjusted according to the characterizations and predictions made by position aware graph neural network (GNN).

(d) *Objective 4: Testing and validation of proposed framework and QoS approach using simulators.*

For testing and validation, comparative analysis is carried out at every stage of the research has been carried out. The SDN-enabled data dissemination framework is evaluated against clustered hierarchical layouts and hexagonal cell layouts through network simulations. The results suggest significant improvements in the proposed model for various metrics, such as lifetime, delay, latency, delivery ra-

tio, and throughput in comparison with the existing solutions. The proposed UAS safety framework is evaluated with LSTM and CNN. Also a comparative study of the proposed framework against Behavior Rule-Based UAV Intrusion Detection System (BRUIDS) and Hierarchical Detection and Response System (HDRS) is presented. The throughput maximization approach is evaluated against Software-Defined UAVs (U-S) and UAVs as Base Stations (U-B). The proposed approach demonstrates consistency and gains in average throughput while minimizing delay and packet loss. The scalability test of the proposed approach is performed by varying data rates and the number of UAVs.

1.4 Thesis Contributions

Thesis contributions are classified into five major categories: 1. Analysis and classification of related research work, industrial standards, organizational white papers and simulators. 2. SDN-enabled framework for data dissemination in multi-UAV ad hoc networks. 3. Mobility/Trajectory based data dissemination in multi UAV ad hoc networks. 4. UAS safety framework. 5. Efficient mobility model and throughput maximization for UAVs Communication Networks. Details of proposed techniques and contributions are discussed below.

1. *Analysis and Classification of Related Research Work.*

   (a) Identification of research gaps and challenges associated with multi-UAV ad hoc networks.

   (b) Detailed survey of frameworks and models for data dissemination in multi-UAV ad hoc networks proposed in literature.

   (c) Identification of current trends and directions by means of studying global standards, organization specific standards and white papers.

   (d) Testing various open source simulators to understand applicability and design complexities of the problem at hand.

2. *SDN-enabled framework for data dissemination in multi-UAV ad hoc networks:* The proposed technique implements a framework for efficiently scheduling transmissions across the network. The framework is also capable of managing the topology alongside sleep timers and back-off counters for the ground WSN nodes.

   (a) The proposed technique models a simple and effective system model that exploits the gliding capabilities of the UAVs for efficient data dissemination be-

tween UAVs, WSNs, and base station.

(b) The proposed framework also implements an energy model which serves as an input to the SDN controller, which in turn, defines the topology.

(c) SDN controller that evaluates the energy model and runs the reconfiguration algorithm to update the topology. UAVs are equipped with virtual switch on which flow entries are constantly updated by the SDN controller.

(d) Sleep state management for WSNs,which relies on UAV maneuvers for energy efficiency and a back-off counter, which provide non-conflicting random back-off intervals without increasing the waiting time.

3. *Mobility and Trajectory aware data dissemination in in multi-UAV ad hoc networks:* The proposed framework takes into account the topological structure as well as the importance of strategic locations to fix UAV way-points and decides the data transmission paradigm. An extended framework which incorporates an SDN controller for facilitating secure mobility and transmissions in UAV-ground communications is also proposed.

(a) The overall topology is decomposed into densely and scarcely populated regions. This division is on the basis of average transmission densities arising from particular regions. The densely and scarcely populated regions, in turn, serve as the basis for UAV way-point selection.

(b) An implicit self-clustering scheme for data accumulation whenever UAV is not in range. Cluster head swapping mechanism, which provides every node with a direct UAV link in order to maximize transfer rates. The implicit clustering serves as banks for UAV way-points.

(c) A modified version of Dijkstra's Single Source Shortest Path (DSSSP) algorithm where edge weight is calculated not on the basis of region density but on the average transmission density (attraction factor), providing preference to the strategically important locations is presented. A separate mechanism for data dissemination is proposed for ground nodes which lie off the UAV trajectory.

(d) The extended model features an SDN controller. The SDN controller provides with the opportunity to update flows on the move, thus, adapting to the dynamic topology, and also updates the legal moves as well as node authentication by means of pre-installed flow tables.

(e) The controller-generated dynamic way-points prevent UAV from erratic move-

ments as well as any unidentified transmission is discarded based on the flow action rules.

4. *Efficient deployment with throughput maximization for UAVs communication networks.*

   (a) The proposed approach monitors the state of aerial nodes and aerial topology for traffic patterns and link congestion. The aerial nodes and associated links are modeled for traffic characterizations, delay, loss and throughput to estimate the topological re-configurations and capacity predictions.

   (b) The aim of the proposed approach is to place data rates close to the throughput upper bound of UAV assisted ground networks through aerial node repurposing, reinforcing burdened nodes, and links. Throughput enhancement is conceptualized by by pushing data through new routes created by adjusting UAV positions which in turn, minimizes delays and loss.

   (c) Introduction of Graph Neural Networks (GNN) in context of aerial communications.

   (d) The proposed approach can act as an overlay and can accommodate any kind of UAV assisted network configuration. It is feasible to scale the approach to accommodate any number of ground and aerial nodes, given the data rate is evenly matched.

5. *Safeguarding Unmanned Aerial Systems (UAS): An Approach for Identifying Malicious Aerial Nodes.*

   (a) The proposed framework implements a conceptual grid based system layout. The virtual grid is required for centralized monitoring, tracking, and guiding the aerial network. Security paradigms are enforced based on positioning of aerial node concerning the grid. The overall safety of the aerial system is ascertained by periodically shuffling the grid through timeout or whenever any rogue behavior is detected. Every time the grid is shuffled or a node crosses into a different section of the grid, security parameters are re-negotiated.

   (b) Communication channels are secured using public key security and privacy mechanisms. The shuffling grid conceptual layout of the proposed framework elevates the threat of key disclosure from a hijacked UAV, as the security parameters shuffle alongside the system model. The proposed channel security mechanism is low on memory and processing requirements and elevates threats originating from MITM, mobility patterns and statistical analysis.

(c) The proposed framework incorporates UAV behavior prediction using LSTM/CNN and Multivariate statistical analysis using PCA for threat detection, mitigation and recovery. The temporal prediction mechanism with look-back capability keeps track of the overall UAS environment for rogue behavioral, mobility and statistical patterns. Behavior prediction is responsible for re-initiating the conceptual system layout and security paradigms. Multivariate statistical analysis is run in conjunction with behavior prediction for eliminating the outliers from the UAS environment.

1.5 Organization of Thesis

This thesis describes the design of an efficient framework for data dissemination in multi-UAV ad hoc networks, safeguarding the overall aerial-ground network environment and QoS enhancements over the proposed schemes. The thesis is organized into seven chapters as described below:

Chapter 1:
Chapter 1 lays the foundation of UAV, UAS and FANETs. The chapter also discusses classification of wireless networks and outlines the difference between MANETs, VANETs and FANETs. The evolution of UAV from defense specific to consumer and civilian applications is presented in depth. Applications and challenges associated with multi-UAV collaborative networks are presented alongside the identified gaps in present research environment. The chapter also outlines the objective of the thesis and lays the foundation towards the proposed solution.

Chapter 2:
Chapter 2 presents an in depth analysis of thesis objectives alongside the solutions proposed in literature. Industry specific solutions and frameworks by standardization communities are also discussed. The chapter presents a study of data dissemination in multi-UAV ad hoc networks, UAS Safety, Trajectory and QoS enhancement. Software defined Network (SDN) which serve as component to the proposed solution is also discussed with respect to the identified problem.

Chapter 3:
Chapter 3 elaborates on data dissemination in multi-UAV assisted WSNs. Challenges associated with data dissemination in aerial-ground collaborative formations are also outlined. An SDN based data dissemination framework which incorporates data dissemination, back-off and sleep counters and energy management is presented in this chapter.

The system model incorporates efficient and simple movements for UAVs for increasing the flight time and better data transmission/reception. A dynamic, flexible, easy to implement and time efficient mechanism is presented for topology formation. It is energy efficient and avoids disconnections and dead transmissions. The comparative analysis of the proposed approach is performed against Clustered Hierarchical WSNs (CSW) and Traditional Hexagonal Cell (TXC) based WSNs, with UAVs acting as a sink. The scalability analysis of the proposed approach with variable and constant bit rates is also presented.

Chapter 4:
Chapter 4 discusses mobility and trajectory based data dissemination in multi-UAV ad hoc networks. First, a data dissemination model is proposed, which takes into account the attraction factor for setting up the way-points for UAV movements. The model is capable of deciding between the locations which result in more coverage, increased throughput with lesser number of UAVs employed. The comparative analysis of the proposed approach is presented against the entity mobility models i.e., 3D Random Way Point, 3D Random Walk and the Gauss–Markov Mobility Model. The proposed mobility scheme is also compared against traditional techniques of fixed UAV maneuvers. Second, the proposed model is extended to a SDN-based secure approach which takes into account the topological density and restricts the UAV and ground node transmissions to authenticity. Significant gains are observed for throughput, coverage, and latency by establishing a simulated network between multiple UAVs and WSN motes.

Chapter 5:
Chapter 5 presents a technique for throughput maximization for UAVs communication networks (a multi-UAV assisted ground network, where UAVs are deployed as transceivers as well as base stations in a given 3D area). A dynamically re-configurable topology is presented where state information of aerial nodes is generated and updated periodically to keep track of congestion and declining throughput. While multi-UAV trajectory optimization generally focuses on aerial nodes moving in the 2D front parallel plane, this is an atypically simple, special case. The proposed approach considers aerial nodes moving continuously in all 3 dimensions. 2D tracking suffers a steep performance decline when speed and distances increase as overall mapping accuracy is always higher in 3D than in 2D. The proposed approach employs separation and dimensionality to provide more than additive improvements as the aerial nodes packed closely together in a 2D front parallel perspective can be far apart if altitude is considered, and can be mapped accurately in a 3D geography. Moreover, the mapping accuracy improves when aerial nodes are

separated by different altitude planes. For performance analysis, the proposed approach is compared against Software Defined UAVs (U-S) and UAVs as Base Stations (U-B) inspired configurations, respectively. Proof of correctness and scalability analysis of the proposed approach is also presented.

Chapter 6:
Chapter 6 presents a layered centralized framework that safeguards from malicious intruders and incorporates privacy protection mechanisms. The proposed UAS safety framework addresses the threats originating from rogue and inconsiderate UAVs, from within the organizational structure, eavesdroppers and malicious attackers and incorporates privacy protection mechanisms. At the foreground, the framework enforces a grid-based system layout with a dynamically shuffling grid as the baseline defense mechanism against statistical, information monitoring, hijacking, eavesdropping, and mobility pattern threats. Intelligent behavior prediction and statistical analysis runs in the background and keeps track of changes in the overall system behavior and statistics. Statistical and behavioral analysis is important as every time a rogue behavior is detected, the overall system is analyzed and security paradigms are re-initiated to recover the aerial system. The framework is evaluated with LSTM and CNN. Also a comparative study of the proposed framework against BRUIDS and HDRS is presented.

Chapter 7:
This chapter summarizes and concludes with respect to each step taken to achieve the aforementioned objectives. The chapter also highlights the novel contributions made in context of multi-UAV networks. Subsequently, the last section of this chapter covers ways and methods by which this research work can be further extended and meaningful contributions can be made.

Chapter 2

Literature Review

There is a growing technological trend in industry and research to seek synergies and exponential gains through component independent participation in communication networks. Expanding the fundamental concepts of networked infrastructure and scaling towards dynamic collaboration of independent capacities, resource sharing, risk minimization with evolutionary gains in order to inch ahead and exploit the collaborative technology. Aerial networks are one such development that have taken the potential of traditional networks to extraordinary benchmarks. UAVs can be deployed stand alone or in a swarming multi-UAV environment and have revolutionized conventional technologies by means of guided, cooperative and collaborative network formations. Figure 2.1 provides an insight into systematic evolution of UAV networks from single to multi-UAV to coordinated/guided to cooperative to collaborative network formations.

The flexible applicability and ability of unmanned aerial vehicles towards fast, cost-effective, and temporary deployments has opened a broad spectrum of possibilities for future wireless technologies. UAVs can be deployed in virtually every scenario, from cellular base stations to disaster relief and response vehicles. Aerial networks have a line of sight (LoS) advantage and the high altitude deployment itself is a major factor behind improved coverage. UAV-assisted ground networks have already taken cooperative search, acquisition, and tracking (CSAT) to new dimensions. Cooperative ad hoc network formations have led to major advances in civilian and military applications. Aerial and ground communication networks, when laced in conjunction, facilitate an efficient entourage for supervision, catastrophe reassurance, observation, investigation, and supplementary applications [26, 6, 27, 5, 28, 29, 30, 31].

The race of evolution in wireless technology has graduated the use of UAVs from the military to the Civilian Concepts of Operations (CONOPS). Enhanced coverage, throughput maximization, sustainable operating costs, and ease of deployment constitute the fundamental obligations towards UAV-CONOPS. CBRN-CONOPS are focused on hazard containment and mitigation [32, 33, 21, 22]. UAV collaborative networks have paved for a level playing field for data dissemination, broadcast/multi-cast communications.

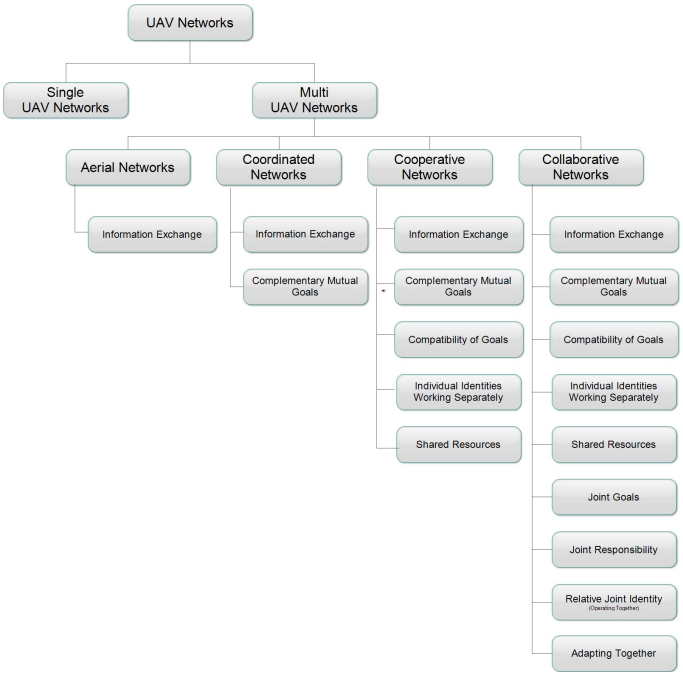


Figure 2.1: Evolution of Multi-UAV Networks.

2.1 Literature Classification

Data dissemination is the collection and distribution of statistical/experimental or any other form of data. UAVs have evolved the data dissemination process and with the advancement in wireless and non-proprietary technology both infrastructure and infrastructure less networks have observed a exponential development at both industry and research levels.

Generally, UAVs act as aerial base stations to support ground communications, be it cellular, sensor, relief, and response or data dissemination and hence hovering altitude or geographical positioning along the (x,y) axis can be jointly or separately optimized to achieve varying levels of performance gains [34, 35, 36, 37, 38]. UAVs can also serve as a middle man for coverage enhancement and boosting capacity [39, 40, 41, 42, 43]. With the emergence of 4G LTE and 5G communication technologies, cost-effective coverage enhancement has been a topic of interest. The issue can be easily resolved by employing UAVs as mobile base stations or temporary relays [44, 45]. The UAV hovering and optimal placement can boost overall capacity and throughput of the Internet of Things (IoT)-communications [46, 47].

There are two prominent characteristics of aerial networks which can be exploited and over which data dissemination paradigms are established. The advancements and enhancements in data dissemination technology are built around transmission scheduling of

the multi-UAV environments and the mobility/trajectory of the aerial node itself. This chapter classifies and discusses literature as aerial components and additional components. Additional components discuss Software Defined Network (SDN) controllers which are deployed extensively in achieving the objectives of the thesis. The aerial components discuss data dissemination and safety of Unmanned Aerial Systems (UAS). The data dissemination techniques are further studied as Transmission Scheduling Centric Frameworks/Techniques/Middlewares/Architectures and Mobility/trajectory Centric Frameworks/Techniques/Middlewares/Architectures. The relatively new field of UAS safety is also introduced in this chapter. Figure 2.2. presents an insight into the literature classification.

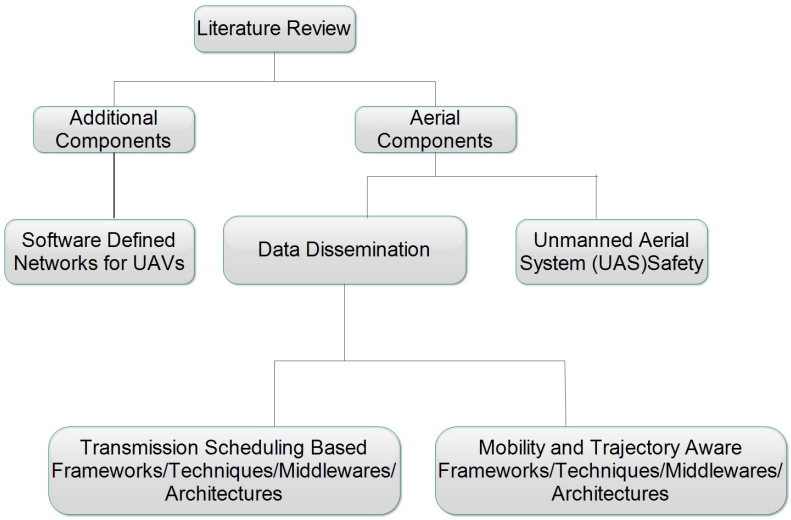


Figure 2.2: Literature Classification.

2.1.1 Data dissemination: Transmission Scheduling Based Frameworks, Techniques, Middlewares and Architectures

Distributed deployment and management of tasks and services have resulted in cooperative frameworks and service-oriented architectures. These frameworks incline towards uplifting the problem of coverage, robustness, deployment costs, interoperability, service integration, control, and scalability. The collaborative sensing, action, communication, and control serve as the breeding grounds for middleware architectures and frameworks. Table 2.1 lists some of the major contributions in multi-UAv assisted data dissemination. The motivation behind these frameworks, techniques, middlewares, and architectures is discussed alongside.

Table 2.1: Data Dissemination: Transmission Scheduling Based Frameworks, Techniques, Middlewares and Architectures.

Approach	Author	Motivation	Components	Features	Pros and Cons	Analysis
Cooperative air and ground surveillance.	Grocholsky et al [48].	Combining broad but less detailed view of UAV with limited resolution view of ground vehicles.	Onboard PC, Avionics, Airframe, Kalman Filter.	1. Target estimation using Kalman Filter. 2. Entropy Based Uncertainty Reduction. 3. Decentralized proactive network sensing. 4. Reactive localization control for improved quality.	1.Reduction in flight time. 2.Better quality estimates of features and targets.	Realtime.
Cooperative framework for multi UAV guided ground Ad hoc networks.	Sharma and Kumar [5].	UAVs help uplifting the problem of coverage, failures, limiting guidance and dead nodes by acting as supervisors.	Extended Kalman Filter, Bayesian Kalman filter, Virtual Concepts, Cognitive Maps, Adaptive resonance theory 2 algorithm, Topological Organising Maps.	1. Kalman filters estimate initial values of ground nodes. 2. Bayesian Kalman filter estimates UAV path and learning rate. 3. UAV waypoints fixed using kalman filter. 4. ART2 algorithm effectively combines coognitive maps generated by the nodes.	1. No of UAVs directly proportional to computation time and inversely proportional to no of computations. 2. No of ground nodes inversely proportinal to number of computations but directly proportional to the computation time. 3. UAVs must be provided with non redundant way points.	NS2 and MatLab.
Service oriented middleware for multi UAV guided ad hoc networks.	Sharma and Kumar [14].	For the sake of robustness, interoperability and flexibility an adaptable and scalable architecture is required.	Topology manager, Component controller, Data/Traffic controller.	1. Node tracking, path discovery and channel selection. 2. Medium access control, routing, service identification and security. 3. Traffic generation and control, Data management.	1. Self Configurable. 2. High level of adaptability. 3. Easy maneuverability. 4. Esay upgrade. . 5. Easy integration with existing systems.	NS2 and MatLab.

Continued on next page

Table 2.1 – continued from previous page

Approach	Author	Motivation	Components	Features	Pros and Cons	Analysis
Distributed component-based framework for unmanned air vehicles.	El-Sayed and ElHelw [49].	A component-centered distributed framework for UAVs which presents the opportunity to incorporate heterogeneous UAV components.	Mission planner, Task executor, World model, DicoCom.	1. Reusable flexible design. 2. Support for distributed Computing. 3.Heterogeneous environment setup. 4. Multiple interaction patterns for communication (Event driven, Server push,query).	1 Seamless and highly robust integration of distributed components. 2. Dico-Script scripting language that provides application developers with design options of Dico components.	Realtime.
A framework for fuzzy logic based UAV navigation and control.	Doitsidis et al [50].	Maneuverability, Control and navigation of small unmanned aerial vehicles.	Altitude fuzzy logic controller, Latitude-Longitude fuzzy logic controller, Error Calculating box.	1. Altitude fuzzy logic controller processes the input and presents with desired elevation and throttle of the UAV. 2. The roll angle of the UAV is provided by Latitude-Longitude controller.	1. Efficient fuzzy logic control for ariel vehicles. 2. Real time flight performance observations are required to correct the oscillations present in flight.	Matlab and Aerosim Aeronautical Simulation Block Set.
A Middleware Architecture for Unmanned Aircraft Avionics.	Lopez et al [51].	Complexity, space, power, computation limit the use of UAVs in civil avionics. New hardware/software systems are required that provide dynamic control of UAV missions.	Service Containers.	1. Service container is responsible for a) Service management. b) Name management provides abstract view to application developer. c) Network management and abstraction. d) Resource management. 2. Data Distribution System Model supports remote procedure calls.	1. Low budget, efficient and rapid deployment. 2. Completely distributed services in form of applications. 3. Abstraction from complex hardware and for application developers.	Avionics use cases.

Continued on next page

Table 2.1 – continued from previous page

Approach	Author	Motivation	Components	Features	Pros and Cons	Analysis
A Service-Oriented middleware for building collaborative UAVs.	Mohamed et al [18].	Distributed environment for application development, deployment, operation and management.	Collaborative UAV Applications, Service-Oriented Middleware, Collaborative Services.	1. UAVs visualized as service providers (intermediate to advanced services). 2. Broker services which have the current and estimated position of UAVs over a given time interval. 3. Synchronized service call and asynchronous messages for local and remote services respectively 4. Collaborative services.	1. Position estimates help invocation of remote services. 2. Transparency and dynamic service deployment. 3. Communication method and heterogeneity abstraction. 4. Self-organizing environment and interoperability.	Service-Oriented middleware technologies
Aerial–ground cooperative vehicular networking architecture.	Zhou et al [26].	Aiding and assisting ground VANETs by deploying serial nodes.	Cooperative aerial-ground network, Onboard control, sensing, processing, diagnosis.	1. Performance improvement in VANETs in tedious communication environment. 2. Multi-UAV assisted VANET prototype. 3. Collaborative services.	1. Effective UAV Scheduling. 2. Adaptive formation planning. 3. Energy efficient network. 4. Multidimensional channel modeling.	Real Time.
On demand UAV positioning.	Galkin et al [40].	UAVs acting as base station/access points for ground users in thick urban environments.	LoS and Non-LoS channel probabilities, Signal fading behavior, UAV Placement, k-means Distance Distribution.	1. Density detection using Nakagami-m fading. 2. Optimal UAV height maintenance for access points.	1. Reduction in channel fading. 2. Minimal radio propagation distance.	Mathematical R simulations.

Continued on next page

Table 2.1 – continued from previous page

Approach	Author	Motivation	Components	Features	Pros and Cons	Analysis
UAV deployment for 5G heterogeneous communications.	Sharma et al [44].	Cost effective deployment of UAV base stations in 5G environments.	Macro Base Station (MBS), Cooperative UAV allocation, Network bargaining.	1. MBS decides UAV placement. 2. UAV network bargaining for serving particular area. 3. Cooperative network formation for load balancing.	1. Enhanced overall throughput. 2. Fifth percentile spectral coherence. 3. Stable network formation and coordination. 4. Coverage boost and better SINR.	Numerical simulations.
TDMA and PFS based aerial ground communication.	Ho and Shimamoto [52].	UAV nodes to remove multi hop WSN communications.	Prioritized Frame Selection (PFS), Time Division Multiple Access (TDMA), Frame based Random Access (FRA).	1. PFS and TDMA used simultaneously. 2. Different modes for classified and non classified transmissions. 3. FRA replaces CDMA for sensor to UAV communications.	1. Optimal UAV altitude. 2. Scenario based optimal packet size. 3. Optimal density of sensor nodes. 4. Improved medium access. 5. Sensor activation and transmission.	Software simulations.
UAV assisted border survellance.	Berrahal et al [53].	Trespasser detection using WSN-UAV collaborative network.	VTail quadcopter, RFID Tags.	1. Detecting and resolving network failures. 2. Network maintenance. 3. Hostage scenario retaliation.	1. Optimal sensor positioning by UAV drops. 2. Transmitting and receiving between isolated geography. 3. Sensor sleep paradigm. 4. Sensor wake-up procedure under threat scenarios.	Real time but simulated environment.

Continued on next page

Table 2.1 – continued from previous page

Approach	Author	Motivation	Components	Features	Pros and Cons	Analysis
Prioritized data gathering in aerial-ground networks.	Say et al [54].	UAV assisted data gathering for improved efficiency in WSN.	Priority-based optimized frame selection (POFS), Priority-based contention window adjustment scheme (PCWAS), Frame selection-based routing protocol (FSRP).	1. Sensor nodes split into frames based on geography. 2. PCWAS prioritizes CSMA/CA MAC. 3. Each frame has embeded transmission priorities. 4. FSRP operates on aforementioned frame selection. 5. transmission distance based routing protocol.	1. Minimized redundant transmission. 2. Energy conservation. 3. Direction independent UAV reception. 4. Reduced relative distance between sender and receiver. 5. Better channel quality.	Software simulations.
Data dissemination in delay tolerant networks.	Reina et al [55].	Adjustment of inter-related parameters for data dissemination in delay tolerant networks.	Non-Dominating Sorting Genetic Algorithm (NSGA-II), Community Resource for Archiving Wireless Data At Dartmouth (CRAWDAD), Mobility traces from University Polytechnic of Bucharest.	1. Probabilistic multi-objective data dissemination in delay tolerant networks. 2. Pareto front for generating non-dominant solution pools. 3. Decision tree based pooling from Pareto front solutions. 4. Social connectivity based result selection.	1. Overall and in-advance estimate of possible solutions. 2. Evaluated solutions for targeted performance levels. 3. Optimized delivery rate and cost. 4. Minimal latency.	MobEmu and Python DEAP
History-based forwarding in delay tolerant networks.	Ciobanu et al [56].	High reachability and proportionate delivery throughout the network.	Jaccard distance, History encountered ration, Eight such mobility traces.	1. Probabilistic transmission methodology based on graphical cut nodes. 2. History-based Jaccard distance.	1. Better performance with limited storage. 2. Optimized delivery with minimized cost. 3. Reduced latency. 4. Reduced overflow of buffers.	Trace emulator.

Continued on next page

Table 2.1 – continued from previous page

Approach	Author	Motivation	Components	Features	Pros and Cons	Analysis
Tactical aerial maneuvers in disaster response.	Sánchez-García et al [57].	Efficient victim assignment for UAVs in disaster situations.	Jaccard distance, Realistic discrete time mobility framework, Simulated annealing algorithm, Hill climbing algorithm, Random walk, Bonn Motion, Manhattan grid model, Disaster area model.	1. Realistic visualization of victim movements. 2. Jaccard based aerial movements to facilitate efficient communication. 3. Comparative decisions on UAV tactical movement.	1. Self deployment of UAVs. 2. Maximized victim service numbers.	Java and Python.
UAV assisted data dissemination in WSNs.	Khan et al [58].	Optimized packet deliver and operational network lifetime.	Randomly deployed nodes, Partitioned sensor field.	1. Temporal data gathering from ground nodes. 2. Virtual grid based low complex approach.	1. Reduced data dissemination cost. 2. Optimal route selection and minimal route readjustment. 3. Optimal data deliver with reduced communication overheads. 4. Energy conservation in ground nodes.	Java and Python.
Behavior evaluation of ground nodes.	Oh et al [59].	Fuzzy decision logic based ground node monitoring.	Trajectory and velocity classification, Extended kalman filtering, Behavior analysis, Target tracking filter, Sensor fusion.	1. Ground vehicle driving mode detection using behavior analysis. 2. String based classification of driving mode history. 3. Fuzzification based classification of behavior into threat or temporal.	1. Significant rate of threat detection. 2. Applicability in ground and marine traffic control.	Numerical simulations.

Continued on next page

Table 2.1 – continued from previous page

Approach	Author	Motivation	Components	Features	Pros and Cons	Analysis
UAV target tracking.	Jensen et al [60, 61].	Cost efficient and time constrained tracking of tagged transmitters.	Fractional Order Potential, Kalman Filter, Monte Carlo Analysis, Radio transmitter implants.	1. Fractional Order Potential for navigating aerial nodes. 2. Kalman filtering to estimate transmitter locations. 3. Monte Carlo Analysis to introduce and compare proposed techniques.	1. Hight target hit rate under noisy signal propagation.	Real time.
Data collection in WSN.	Jawhar et al [62].	Energy efficient extended network lifetime while monitoring monitoring linear infrastructures .	Linear Sensor Networks (LSNs), Relay node clustering.	1. Relay nodes serving as cluster heads. 2. Back and forth aerial movements along linear network. 3. One hop transmission rage of sensor and relay nodes. 4. Three independent network models based on UAV node movements.	1. Reduced energy consumption. 2. Reduced transmission collisions. 3. Reduced hidden node interference.	Software simulations.
Data dissemination in linear wireless networks.	Jawhar et al [63].	Energy efficient data communication in linear wireless networks.	Linear Sensor Networks (LSNs), Relay node clustering.	1. Relay nodes serving as cluster heads. 2. Back and forth aerial movements along linear network. 3. One hop transmission rage of sensor and relay nodes. 4. Three independent network models based on UAV node movements.	1. Reduced energy consumption. 2. Reduced transmission collisions. 3. Reduced hidden node interference.	Software simulations.

Continued on next page

Table 2.1 – continued from previous page

Approach	Author	Motivation	Components	Features	Pros and Cons	Analysis
Coordination and disaster management.	Maza et al [64].	Multi-UAV distributed task allocation.	AWARE platform, TUB-H helicopters.	1. Multi-UAV surveillance. 2. Fire threat confirmation. 3. Distributed task allocation. 4. Conflict resolution.	1. Mission completion statistics: Node deployment, Firemen tracking, Surveillance, Node deployment and fire monitoring, Fire monitoring, Load transportation.	Real time.
Energy efficient data dissemination.	Sharma et al [65].	Energy efficient aerial-ground collaborative data dissemination.	Fire fly optimization algorithm (FFOA), Aerial-ground collaborative system model.	1. Eradication of routing loops. 2. Attraction factor of FFOA is is used for network coordination. 3. Different attraction factor for different communication paradigms.	1. Energy efficient. 2. Continued aerial ground connectivity. 3. Enhanced network lifetime. 4. Better coverage. 5. Increased throughput with minimal delays.	NS2 and MatLab.
Data dissemination in UAV assisted IoT.	Xue et al [66].	Maximized data distribution in geographically dispersed IoT.	Non-convex optimization (mobility and energy constraints), Alternating descent procedure, Concave-convex procedure.	1. UAV flight routines of hovering, climbing and descending for energy conservation. 2. Hovering over closeby nodes. 3. UAV gains altitude for far off nodes.	1. Better data dissemination. 2. Enhanced network lifetime.	Software simulations.
Data dissemination in UAV assisted IoT.	Erman et al [67].	Maximized data distribution in geographically dispersed IoT.	Honeycomb tessellation, Virtual infrastructure highways, Hexagonal cell-based data dissemination (HexDD) protocol.	1. Fault-tolerant data dissemination. 2. Routing holes bypassed.	1. Reduced communication and hot region cost. 2. Reduced energy consumption. 3. High data delivery with minimal latency	NS2.

Continued on next page

Table 2.1 – continued from previous page

Approach	Author	Motivation	Components	Features	Pros and Cons	Analysis
Behavior detection in VANETs.	Sharma et al [68].	UAV assisted vehicle tracking and driver behaviour assessment.	DEMATEL system, Behaviour analysis	1. Novel UAV guided VANETs. 2. Tracking and management of road vehicles. 3. Vehicular tracing and behavior classification. 4. Vehicular assessment for collision prevention. 5. Analysis over both mathematical and real world data.	1. Statistical improvements: Cost, Accuracy, Delay, Scalability, positioning, Trade-off	Real time evaluation.
Multi-UAV enabled data communication.	Zhan and Zeng [69].	Maximum operational time minimization in UAV assisted data collection.	M in–max multiple traveling salesman problem (min–max m-TSP), Convex optimization, Bisection method, Time discretization technique, Karush–Kuhn–Tucker (KKT), Successive convex approximation (SCA)	1. UAV trajectory and sleep schedule optimization. 2. Hovering mode data collection. 3. Continuos data collection by flying mode.	1. Reduced hovering time. 2. Fast convergence. 3. Maximized data collection	Software simulations.
Data dissemination in UAV assisted VANETs.	Fan et al [70].	Delay constrained data delivery in Vehicular Ad hoc Networks.	Multi-edge knapsack maximization problem, Polynomial time approximation, Bisection method, Time discretization technique, Karush–Kuhn–Tucker (KKT), Successive convex approximation (SCA)	1. Cooperative RSU based path selection. 2. Probabilistic UAV selection.	1. Optimized transmission rate. 2. Maximized throughput. 3. Constrained delay. 4. Maximized delivery.	Simulation of Urban Mobility (SUMO).

Continued on next page

Table 2.1 – continued from previous page

Approach	Author	Motivation	Components	Features	Pros and Cons	Analysis
Energy efficient data dissemination.	Al-Habob et al [71].	Minimal energy consumption in UAV assisted data dissemination for IoT devices.	Ant colony optimization (ACO)	1. Selective reception and transmission. 2. Optimized path selection for energy efficiency.	1. Energy conservation	Software simulations.
Data aggregation in multi-UAV environment.	Xiong et al [72].	Energy efficient data aggregation in multi-UAV assisted ground networks.	Store carry forward (SCF) routing, Multi hopping, Single coalition strategy (SCS), Coalition formation strategy (CFS), Coalition game theory.	1. Collaborative data aggregation for UAV transmissions. 2. Energy based dynamic routing choice. 3. Game theoretic aerial collaboration for ferrying and transmitting data.	1. Energy conservation. SCS to be used for small data. 3. CFS to be used for large data.	Software simulations.
Routing protocol for congestion control.	Sharma et al [73].	Fruit fly based routing in multi-UAV assisted ground networks.	OFFRP: Optimized Fruit Fly algorithm, Fruit fly index.	1. Relay selection based on fruit fly index. 2. Route maintenance and periodic updates. 3. Smell index manages contention window. 4. Route rehabilitation maintains congestion free operation.	1. Optimal routing. Congestion control. 3. CFS to be used for large data.	NS2 and MatLab.

Continued on next page

Table 2.1 – continued from previous page

Approach	Author	Motivation	Components	Features	Pros and Cons	Analysis
Rendezvous and task allocation.	Sharma et al [74].	Task allocation and decision making in multi-UAV networks (FANETs).	Hill Myna optimization, Desert sparrow optimization.	1. Myna vocal rage defines radio propagation range. 2. Common dialects form a cluster. 3. Source, destination and route decided on the basis of Myna participation. 4. Desert Sparrow based non redundant task allocation.	1. Statistical improvements: Network cooperation time. Coocgnitive transfer ration. Network latency. Handeled tasks.	Onboard processors, Statistical analysis, NS2 and MatLab.

2.1.2 Data Dissemination: Mobility and Trajectory Aware Frameworks, Techniques, Middlewares and Architectures

The unexplored potential of UAV assisted networks brings certain challenges alongside. Trajectory design, resource allocation, channel allocation, and trade-offs between throughput and delays are a few identified challenges towards maximized data rates in multi-UAV collaborative deployments [21]. UAV-assisted ground networks are due to gain significantly from considering and exploiting the flexible mobility characteristics of aerial nodes. UAV nodes are highly maneuverable and can provide greater opportunities for LoS channel availability and better capacity with on-demand trajectory modifications [75, 76]. The on-demand availability of UAV mobility instead of predetermined paths can alleviate the restrictions incurring from high latency and transmission losses and thus boosting the overall data dissemination process. Table 2.2 presents mobility/trajectory centric approaches, frameworks, techniques, middlewares and architectures for data dissemination in multi-UAV assisted networks.

Table 2.2: Data Dissemination: Mobility and Trajectory Aware Frameworks, Techniques, Middlewares and Architectures.

Approach	Author	Parameters of Interest	Key Components	Ground Network	Aerial Network	Target
Trajectory and transmission design.	Wu et al [77].	Multiuser scheduling. UAV Trajectory. UAV Energy.	Non-convex optimization. Block coordinate descent. Successive convex optimization.	Mobile users.	Multi-UAV.	Maximized throughput.
Trajectory optimization for network edge data delivery.	Chenj et al [78].	End user service. Date rate.	Minimum connection time. Decomposed convex optimization. Iterative component design.	Edge users.	Single-UAV.	Maximized sum rate (MSR).
Trajectory design for time minimization.	Zeng et al [79].	Mission completion time. File recovery probability. UAV speed. UAV path.	Mixed-integer non convex problem. Convex optimization.	Ground terminals.	Single/Multi UAV.	Mission completion time. UAV enabled multicasting.
Energy efficient aerial transmissions.	Zeng et al [80].	Communication throughput. UAV energy requirements. UAV speed and direction.	Optimal UAV flight radius. Optimal UAV speed.	Ground terminals.	Single/Multi UAV.	Energy efficiency.
Trajectory and transmission design for multiple access networks.	Wu et al [81].	Multi-user communication scheduling. UAV trajectory over fixed plane.	Block coordinate descent. Successive convex optimization.	Mobile users.	Multi UAV.	Maximized throughput.

Continued on next page

Table 2.2 – continued from previous page

Approach	Author	Parameters of Interest	Key Components	Ground Network	Aerial Network	target
Energy trade-offs in aerial ground communications.	Yang et al [82].	Optimal ground terminal transmission power. UAV trajectory.	Optimized UAV propulsion energy. Optimal ground node transmission energy.	Ground terminal.	Multi UAV.	Energy tradeoff with straight and circular trajectories.
Wireless power transfer.	Yang et al [83].	Minimum received energy. Speed constraints.	Lagrange dual method. Successive convex optimization.	Energy receivers.	Multi UAV.	Average received power.
Communication design.	Na et al [84].	Average harvested energy. Average achievable rate. UAV trajectory. User scheduling. Sub-carrier and power allocation	Orthogonal Frequency Division Multiplexing (OFDM). Simultaneous Wireless Information and Power Transfer (SWIPT). Non-convex optimization	Ground users.	UAV.	Enhanced convergence.
Power Optimization for UAV Relay.	Zhang et al [85].	UAV trajectory. Power control.	Maximum outrage probability	Mobile devices.	Multi-UAV.	Amplification and relaying.
Trajectory planning for data collection.	Samir et al [86].	UAV flight. Time.	Branch, reduce and bound (BRB) algorithm. Successive convex approximation.	IoT devices.	Multi-UAV.	Displacement and Time deadline.
Trajectory and power modelling.	Cui et al [87].	Secrecy rate. Trajectory. Transmit power.	Block coordinate descent. S-procedure. Successive convex optimization.	Ground receivers.	Multi-UAV.	Average worst case secrecy rate.
Wireless power transfer.	Hu et al [88].	UAV speed. UAV Trajectory.	Lagrange dual method. Successive convex optimization.	Ground devices.	Multi-UAV.	Minimum received energy.
Coarse trajectory design.	Tran et al [89].	UAV path. UAV Velocity.	Heuristic search. Dynamic programming. Traveling salesman problem.	Variable ground devices.	Multi-UAV.	Minimized energy consumption.
Trajectory control algorithm.	Fadlullah et al [90].	Congestion. Average node distance.	Trajectory control algorithm.	Unmanned aerial systems (UAS).	UAS.	Congestion alleviation.
Energy efficient trajectory design.	Sallouha et al [91].	UAV altitude. UAV energy.	Energy-constrained optimization.	Terrestrial anchors.	Multi-UAV.	Minimum localization error.
Communication design.	Li et al [92].	UAV trajectory. UAV Convergence.	Successive convex approximation. Iterating methods.	Ground terminals.	Multi-UAV.	Minimum secrecy rate .

Continued on next page

Table 2.2 – continued from previous page

Approach	Author	Parameters of Interest	Key Components	Ground Network	Aerial Network	target
Secure UAV communications.	Zhang et al [93].	UAV trajectory. UAV transmission power. Uplink and downlink transmissions	Successive convex approximation. Block coordinate descent.	Ground nodes.	Multi-UAV.	Secrecy rate.
Cellular UAV communications.	Zhang et al [94].	UAV trajectory. UAV connectivity. Signal to noise ratio	Successive convex approximation. Block coordinate descent.	Cellular networks.	Multi-UAV.	UAV mission time.
UAV task offloading.	Xiong et al [95].	UAV trajectory. Task offloading. Bit allocation	Alternative optimization.	IoT devices.	Multi-UAV.	Minimal energy consumption.
Surface assisted UAV transmission.	Li et al [96].	Passive beam-forming. UAV trajectory	Successive convex approximation (SCA). Phase-shift solution.	Re-configurable intelligent surfaces.	Multi-UAV.	Average achievable rate.
UAV assisted non-orthogonal multiple access (NOMA) networks.	Zhao et al [97].	NOMA precoding. UAV trajectory	Alternate user scheduling.	Base stations.	Multi-UAV.	Maximal sum rate.
UAV trajectory in maritime environment.	Tang et al [98].	UAV path	Snap trajectory method. Corridor constraint optimization.	Ground nodes.	Multi-UAV.	Average deviation distance.
Secure UAV transmissions.	Zhong et al [99].	UAV trajectory. Communication and Jamming power.	Alternating optimization. Successive convex approximation.	Ground nodes.	Multi-UAV.	Average secrecy rate.
Search time optimization.	Pérez-Carabaza et al [100].	UAV collision. Target detection time. Loss.	Ant colony optimization.	––.	Multi-UAV.	Minimum Time Search (MTS).
UAV enabled secure communication.	Zhou et al [101].	Transmission power. UAV trajectory.	Alternating iterative algorithm. Successive convex approximation.	Information receivers (IRs).	UAV base stations.	Minimum average secrecy rate.
UAV assisted NOMA and IoT.	Zhou et al [102].	UAV trajectory planning. Subslot allocation.	Lagrange Multiplier. Bisection method.	Wireless powered IoT terminals.	Multi-UAV.	Average achievable sum rate of uplink communications.
Age optimal trajectory design.	Liu et al [103].	UAV trajectory planning.	Hamiltonian path. Dynamic programming. Genetic algorithm	Wireless sensor networks (WSN).	Multi-UAV.	Data collection.
Resource allocation design.	Li et al [104].	UAV trajectory. Sub-carrier allocation.	Mixed integer non-convex optimization.	Ground users.	Multi-UAV.	Maximal system throughput.

Continued on next page

Table 2.2 – continued from previous page

Approach	Author	Parameters of Interest	Key Components	Ground Network	Aerial Network	target
3 dimensional trajectory optimization.	You et al [105].	UAV trajectory. UAV communication scheduling.	Block coordinate descent. Successive convex optimization.	Wireless sensor networks(WSN).	Multi-UAV.	Average data collection rate.
UAV assisted IoT.	Na et al [102].	UAV trajectory. Sub-slot allocation. Power allocation	Alternative iteration algorithm.	IoT devices.	Multi-UAV.	Minimum achievable rate.
Trajectory design for resource allocation.	Sun et al [106].	Power consumption. Energy harvesting. Storage capacity. Quality of service requirements	Monotonic optimization. Successive convex optimization.	−−.	Solar powered UAV.	Average system throughput.
UAV enabled wireless power transfer.	Xu et al [107].	UAV mobility. Transferred energy. UAV velocity.	Pareto-boundary energy.	Energy receivers (ERs).	UAV-mounted energy transmitter (ET).	Wireless power transfer (WPT) efficiency.
Decentralized trajectory design.	Hu et al [108].	UAV trajectory. UAV sensing.	Reinforcement learning. Markov chains.	IoT devices.	Multi-UAV.	UAV utility.
UAV enabled radio access.	Zhang et al [109].	UAV trajectory. UAV transmissions.	Block coordinate descent. Successive convex optimization.	Ground users.	Multi-UAV.	UAV flight duration. Mission completion time.
Dual UAV assisted secure transmission.	Cai et al [110].	UAV trajectory. UAV speed. User scheduling. UAV return constraint. UAV collision constraint.	Binary joint optimization algorithm.	Ground users.	Dual UAV.	Minimum worst-case secrecy rate.
Resource allocation in apace-air-ground IoT.	Wang et al [111].	UAV trajectory. Connection scheduling. Power control	Block coordinate descent. Successive convex optimization.	Internet of Remote Things (IoRT).	Multi-UAV.	Overall system capacity.
Joint offloading for mobile edge computing.	Hu et al [112].	UAV trajectory. Offloading ratio. User scheduling. Energy consumption.	Decomposition-based algorithm.	Wireless nodes.	Multi-UAV.	Minimum average delay.
Multi-Hop UAV Relaying.	Zhang et al [113].	UAV trajectory. Transmit power optimization. Collision avoidance.	Alternating maximization. Successive convex optimization.	Wireless nodes.	Multi-UAV.	End-to-end throughput.
Trajectory planning for disaster scenarios.	Demiane et al [114].	UAV trajectory. UAV waypoints.	Received signal strength indicators (RSSI).	Mobile devices.	Multi-UAV.	Localization accuracy of mobile devices.

Continued on next page

Table 2.2 – continued from previous page

Approach	Author	Parameters of Interest	Key Components	Ground Network	Aerial Network	target
Energy efficient trajectory design.	Xu et al [115].	Flight trajectory. Energy consumption.	Linear programming (LP). Successive convex optimization.	Distributed ground terminals.	Multi-UAV.	Throughput threshold.
Multi-UAV trajectory and power control.	Liu et al [116].	Flight trajectory. Power requirements.	Multi-agent Q-learning. Echo state network (ESN).	Mobile ground nodes.	Multi-UAV.	Sum transmit rate. Maximized user rate.
Secrecy of UAV systems.	Pan et al [117].	Received signal-to-noise ratio. Probability density.	Monte Carlo simulations.	Ground receiver.	Multi-UAV.	Secrecy outage performance.
UAV assisted ground relays.	Zeng et al [118].	Transmit power. Relay trajectory.	Successive convex optimization.	Ground relays.	Multi-UAV.	Throughput maximization.
UAV sensing cellular networks.	Zhang et al [119].	UAV sensing. UAV trajectory. UAV transmissions	Successive convex optimization. Differential methods	Base stations.	Multi-UAV.	Maximum energy efficiency.
Trajectory design for UAV assisted WSN networks.	Zhang et al [120].	UAV mobility. UAV trajectory.	Successive convex optimization. Traveling salesman problem	WSN.	Multi-UAV.	Minimal mean square error.
UAV trajectory and protocol design.	Hua et al [121].	Time allocation. UAV trajectory. reflection coefficient.	Successive convex optimization. Block coordinate descent.	Backscatter device (BD).	Multi-UAV.	Maximum system ergodic capacity.
Re-enforcement learning based trajectory design.	Yin et al [122].	Trajectory learning.	Markov decision process. Model-free reinforcement learning. Deterministic policy gradient (DPG)	Multiple ground users.	Multi-UAV.	Maximum expected uplink sum rate.
Multi-UAV trajectory optimization.	Choi et al [123].	UAV Trajectory.	Non-Uniform Rational B-Spline (NURBS) surface fitting.	−−.	Multi-UAV.	Aerial Imaging.
Real time UAV path planning.	Roberge et al [124].	UAV waypoints.	Parallel genetic algorithm. Particle swarm optimization	−−.	Multi-UAV.	Superior aerial trajectory.
Energy efficient mobile edge computing.	Li et al [125].	UAV trajectory. Transmit power. Computation load allocation.	Non convex fractional programming. Dinkelbach algorithm. Successive convex optimization.	Ground users.	Multi-UAV.	UAV energy conservation.
Multiple access for mobile UAV networks.	Cui et al [126].	UAV trajectory. Resource allocation.	Penalty dual-decomposition.	Ground users.	Mobile UAV.	Minimum average rate.

Continued on next page

Table 2.2 – continued from previous page

Approach	Author	Parameters of Interest	Key Components	Ground Network	Aerial Network	target
UAV enabled MAC.	Li et al [127].	UAV trajectory. Resource allocation. Poer. Flight	Lagrange dual decomposition.	Ground users.	Multi-UAV.	Maximum average sum rate.
UAV enabled amplify and forward network.	Jiang et al [128].	UAV trajectory. Source/relay power.	Successive convex optimization. Iterative programming	Ground users.	Multi-UAV.	Maximum end-to-end throughput.
Multi-UAV interference coordination.	Shen et al [129].	UAV trajectory. Transmit power. UAV speed. UAV altitude. Collision avoidance	Successive convex optimization.	Ground wireless networks.	Multi-UAV.	Maximum aggregate sum.
Energy efficient trajectory design.	Zhu et al [130].	UAV trajectory. Transmit power.	Non service tolerant approach.	Massive machine type devices.	Multi-UAV.	Power consumption.
Energy constrained data dissemination.	Gu et al [131].	Trajectory optimization. Transmit power.	IoT devices.	Multi-UAV.	Throughput maximization.	

2.1.3 Unmanned Aerial Systems (UAS) Safety

Unmanned Aerial Vehicles (UAVs) are autonomous flying robots, with or without payload, which provide efficient low-complex connectivity and comprehensive encyclopedic coverage. UAVs are on-demand low altitude alternatives to High Altitude Platforms (HAPs) which come with an advantage of the Line of Sight (LoS). The UAV applications range from aerospace, military, civil, biohazard and emergency scenarios, archaeology, cargo transport, conservation, film making, health care, journalism, law enforcement, UAV swarming and research [5, 132, 133, 134]. UAVs are also used as a relay for mobile devices to receive an uplink from the base station and to amplify and forward it [85]. UAVs, together with HAP and satellite communication systems, form the Unmanned Aerial System (UAS).

In special cases, UAVs are considered equivalent to the devices in the Internet of Things (IoT), however, the procedures are designed by ignoring the fact that UAVs require extra-features for trajectory designing, cooperative planning as well as mobility aware transmissions. A network-connected autonomous UAV with feedback and sensing capabilities can be classified as an IoT device but UAVs cannot be treated as a general network component (with a difference of physical configurations and dynamics) and evaluations

are not feasible if performed similarly to static sensor nodes in the network. Zhang et al. [135] described UAVs as powerful IoT components capable of sensing and facilitating communication, exploiting their mobility and flexible deployment. Terrestrial cellular networks are considered to be the enablers of UAV sensing applications, and the concept of non-cooperative cellular-Internet of UAVs is introduced, where intercepted data is periodically transmitted to the base for timely processing. The variations in operational properties, the inclusion of mobility laws and an altogether difference in the dynamics, separate UAVs from regular network nodes.

Table 2.3: Physical Layer Security Models Based on UAV Trajectory, Transmit Power, User Scheduling and Jamming.

Approach	**Author**	**Parameters of Interest**	**Security**	**Threat**	**Key Component**	**Aerial Network Type**
Securing UAV communications.	Zhang et al [93].	UAV trajectory. UAV power control.	Physical layer security.	Eavesdropper.	Block coordinate descent. Successive convex optimization.	Multi-UAV broadcast.
Secure UAV networks.	Li et al [92].	Flight trajectory. Transmission power. Ground node association.	Physical layer security.	Eavesdropper.	Alternating method. Successive convex optimization.	Multi-UAV broadcast.
Secure UAV communications.	Zhong et al [99].	Flight trajectory. Cooperative jamming.	Physical layer security.	Eavesdropper. Confidentiality.	Alternating optimization. Successive convex optimization.	Dual-UAV broadcast.
UAV-Enabled Secure Communications.	Zhou et al [101].	UAV trajectory. Jamming. UAV power.	Physical layer security.	Multiple eavesdroppers.	Alternating iterative algorithm. Successive convex optimization.	Multi-UAV broadcast.
Dual-UAV Secure Communications.	Cai et al [**?**].	UAV trajectory. User scheduling. Jamming.	Physical layer security.	Multiple eavesdroppers. Confidential communication.	Joint optimization algorithm.	Multi-UAV broadcast.
Secrecy of UAV Systems.	Pan et al [117].	UAV trajectory. Signal to noise ratio (SINR).	Physical layer security.	Multiple eavesdroppers. Man in the middle (MITM).	Monte-Carlo simulations.	Multi-UAV broadcast.
Secure data dissemination.	Qureshi et al [136].	Mobility.	Physical layer security.	Multiple eavesdroppers.	Dragonfly optimization. Moth flame optimization. Ant colony optimization.	Multi-Vehicular.
Secure Multi-UAV Communication Systems.	Li et al [137].	UAV trajectory. Jamming. Resource allocation.	Physical layer security.	Multiple eavesdroppers.	Alternating iterative algorithm.	Multi-UAV broadcast.

Continued on next page

Table 2.3 – continued from previous page

Approach	Author	Parameters of Interest	Security	Threat	Key Components	Aerial Network Type
Secure UAV Communications.	Cui et al [87].	Robust UAV trajectory. Transmit power.	Physical layer security.	Multiple eavesdroppers.	Block coordinate descent. Successive convex optimization.	Multi-UAV broadcast.
UAV-aided secure communications.	Lee et al [138].	UAV trajectory. Transmit power. User scheduling. Jamming.	Physical layer security.	Multiple eavesdroppers. Confidentiality	Successive upper bound minimization .	Multi-UAV broadcast.
UAV Assisted Secure Transmission.	Zhao et al [139].	Caching. Jamming.	Physical layer security.	Multiple eavesdroppers.	Interface alignment.	Multi-UAv to small cell base station.
Secure UAV-to-UAV.	Ye et al [140].	Robust UAV trajectory. Transmit power.	Physical layer security.	Multiple eavesdroppers. Secrecy.	Monte-Carlo simulations.	Multi-UAV broadcast.
Cooperative Secure Transmission.	Hua et al [141].	Interference signals. Secrecy rate.	Physical layer security.	Multiple eavesdroppers. Secrecy.	Block coordinate descent. Dinkelbach method. Successive convex approximation.	Multi-UAV broadcast.
Secure Communication Under UAV.	Li et al [142].	Channel estimation. Secrecy capacity.	UAV smart attacks.	Multiple eavesdroppers. Secrecy.	Non cooperative game theory. Nash equilibrium. Q-learning.	Multi-UAV broadcast.
Secure probabilistic caching.	Shi et al [143].	Transmission scheduling.	Physical layer security.	Multiple eavesdroppers.	Secure probabilistic caching.	Multi-UAV relay.
Cooperative Jamming.	Li et al [144].	UAV trajectory. transmit power. Jamming. Partial eavesdropper information.	Physical layer security.	Multiple eavesdroppers.	Block coordinate descent.	Multi-UAV air to air broadcast.
Multi-UAV clustering strategy.	Wu et al [145].	Communication range.	Physical layer security.	Cooperative control. Secure communication.	Hierarchical virtual communication ring (HVCR).	Multi-UAV communications.
Secure task allocation.	Fu et al [146].	Energy consumption. Artificial potential field. Path planning.	Collision.	Network attack. Collision-resistant.	Intrusion detection system.	Multi-UAV communications.
Secure UAV edge computing systems.	Bai et al [147].	UAV energy.	Physical layer security.	Eavesdroppers.	Computation offloading.	UAV-mobile-edge computing (MEC).
UAV-Enabled Secure Communications.	Zhang et al [148].	UAV trajectory. Transmit power. Jamming.	Physical layer security.	Eavesdroppers.	Deep reinforcement learning.	Multi-UAV assisted ground.).

Continued on next page

Table 2.3 – continued from previous page

Approach	Author	Parameters of Interest	Security	Threat	Key Components	Aerial Network Type
UAV-Enabled Secure Communications with no fly constraints.	Gao et al [149].	UAV trajectory. Transmit power. UAV speed. UAV position.	Physical layer security.	Eavesdroppers.	Alternating optimization. Successive convex approximation. Alternating directional method of multipliers (ADMM).	Multi-UAV assisted ground.).
Optimal positioning and secure communication.	Wang et al [150].	UAV trajectory. Transmit power. Jamming.	Physical layer security.	Eavesdroppers.	Multi-dimensional search.	Multi-UAV assisted ground.).

Generally, the efforts towards the safety of UAS are reactive and directed towards channel monitoring and antenna transmission, instead of safeguarding the UAV and overall networked system. Much of the literature is concentrated around resource allocation, signal strength and antenna optimization challenges. As evident from Table 2.3 much of the literature is focused around secure trajectory design and physical layer security when it comes to multi-UAV assisted environments.

UAVs are equipped and made up of independent sophisticated technological components, it is possible to attack an individual component and then launch an attack on the overall aerial network [151]. UAVs collect and collaborate massive amounts of information through its sensors, GPS, camera and neighboring nodes. A hijacked drone can result in a nightmare of amplified magnitudes. Once compromised, a UAV can be used to direct terror attacks, acts of mischief and crimes like the white hat and black marketing. Delivery drones can result in loss of cargo or the expensive hardware itself [53]. An autonomous book delivery drone once hijacked can be used to deliver arms and narcotics. The weak signal strength can be exploited by jamming GPS satellite signals forcing a UAV to lose its sense of location [152, 153, 154, 155].

Attacks can be launched by taking advantage of the leak in the use of encrypted GPS signals. Launching such attacks pose substantial difficulty because authentication mechanisms are implemented to safeguard the GPS navigation system. It is hard for the attacker to generate valid GPS signals, but the capture and relay of existing ones can be exploited. The attacker does not need to know the spreading codes and data content of the signal to launch a selective-delay attack. The hackers can operate on a delay time of signals, and amplify or attenuate them [156].

The attacker can use a compromised UAV to take over the adjoining network by disrupting the Wi-Fi links and the operational command. UAVs possess security flaws that combine

both cyber and physical security concerns. By observing the (unsecured) communication protocols and applying brute-force techniques, an attacker can discover the secret key shared between the node and the operational command. The compromised key can be used to impersonate the operational command and launch an identity cloning attack. An attacker can employ timing attacks to transmit orders to the aerial node just before the real operator does. The node will accept the attackers' command and discard the actual commands from the operator [157, 158]. The attacker can command the camera to turn in the wrong direction restricting the desired information, compromise the data, steal the drone and equipment attached to it.

Intercepting data links and feed capture are also easy to do if the feeds are not encrypted. A man-in-the-middle attack can be mounted on an unprotected drone, sending commands to reroute/reprogram the aerial node. Malware infections can also result from internal adversaries and unskilled drone operators. Internal attackers possess a significant threat towards the overall safe operations as secret operational characteristics can be released unintentionally or on purpose. Alongside this, a static safety mechanism makes it almost impossible to counter internal organizational-based attacks. A supply chain attack seeks to damage the overall aerial network by targeting vulnerable elements in its global supply network. Malware, spyware or viruses are introduced during the manufacture or are a part of an update. The malware can be hidden in the libraries, middleware, OS, firmware and micro-controller chips [159, 160, 161, 162].

The challenges against safe UAS are not completely addressable by using safeguarded transmissions and secure channels. Majority intrusion to the overall networked environment originates from hijacked/identity cloned devices and internal adversaries. The introduction of advanced technology drives attackers towards more sophisticated attacks on safe network deployment. A framework capable of dealing with attackers dynamically, as well as isolating the rogue and compromised nodes, is capable of boosting the overall network safety and mission directives. A layered model implementing transport security and traffic scrutiny (mission data monitoring, path, trajectory and speed characteristics, position tracking, authentication failures, channel use, and request characteristic) and implementing access control and application security as the higher layer is required.

As UAVs are deployed to assist network similar to general terminals, the safety aspects of the regular network hold valid in their case. Institute of Electrical and Electronics Engineers (IEEE) also dictates minimum safety requirements for the proposed wireless standards that are competitive in deployment and are selected based on the configurations and types of nodes. Table 2.4 provides a detailed classification of the IEEE family of wireless standards for supporting secure transmissions. Sub-standards are grouped into

the initiating families for standards [163, 164, 165, 166, 167, 168, 169, 170, 171, 172, 173].

Table 2.4: IEEE Wireless Standards with Security Considerations.

Family	Standards/ Modulation	Classification	Security	Threats
IEEE 802.11 100-250 m	802.11 a/b/g/n ac/ad/af/ah/ai aj/aq/ax/ay/y DSS, FHSS, OFDM,OOK, MIMO-OFDM	WLAN, Wi-Fi	WPA2-AES Pre-Shared Key, WPA2-Radius Authentication Server EAP-TLS	Unauthorized Access, Rogue Access Point, DoD, DDoS, Replay, Man in the Middle, Session Hijacking
IEEE 802.15 10-300 m 2-3 Kms (VLC)	802.15.1/15.2/ 15.3a/15.3b/15.3c/ 15.4a/15.4b/15.4c/ 15.4d/15.4e/15.4f/ 15.4g/15.6/15.7/ 15.8/15.9/15.10 DSSS, Q-PSK, BPSK, OOPASK	WPAN, Coexistence, High Rate WPAN, Low Rate WPAN, BAN,VLC, PAC, KMP, L2 Routing	128 bit AES CBC, 128 bit AES CTR	Unauthenticated Encryption, No Integrity on ACK Packet, Man in the Middle, Unauthorized Access, Rogue Access Point, DoD, DDoS, Replay, Session Hijacking
IEEE 802.16 9.7-16 Kms Max. 30 Kms	802.16.1/16.2 OFDM, SOFDMA, QPSK, BPSK, 16-QAM	WiMAX	PKM-128 bit RSA, DES-CBC, TEK	No Mutual Authentication, Interleaving Attack, Man in the Middle, Unauthorized Access, Rogue Access Point, DoD, DDoS, Replay, Session Hijacking
IEEE 1609 1Km	1609.2, 1609.3, 1609.4, 1609.12 BPSK, QPSK, 16-QAM, 64-QAM	DSRC, WAVE, VANET	Signed PDU (Hash Function), Certificate Authority, Symmetric Key Encryption	Misconfigure Attacks, Man in the Middle, Unauthorized Access, Rogue Access Point, DoD, DDoS, Replay, Session Hijacking

The promising future of UAS is accompanied by the openness of the aerial communication. Both air to air, and air to ground communication and the equipment itself are susceptible to information theft and jamming. SkyGrabber was used by insurgents to hack into United States Military drone in 2009. The software turns satellite signals into live TV feeds which can be easily intercepted by focusing a satellite dish. The insurgents downloaded an un-encrypted US military communication between satellite and drone [156, 174]. In 2011, another computer virus was found in Predator and Reaper Drone operational ground control, for UAV communication networks [159].

Homeland security conducted a drone test at White Sands Missile Range, and rogue GPS signals were broadcasted to the drone from a distance of 1 km. The signal deceived the aerial node navigation control into believing that it was rising straight up. The spoofing attack exploited a known vulnerability in GPS for UAV jacking [175]. Icarus is a radio transmitter that can take charge of in flight drones and grants the attacker full control of the device. The toolkit works against any aerial node that uses DSMx remote control protocol [152]. A UAV node belonging to UAS can impersonate identity employing MAC spoofing and further modification of IP address. The malicious aerial node can also fire

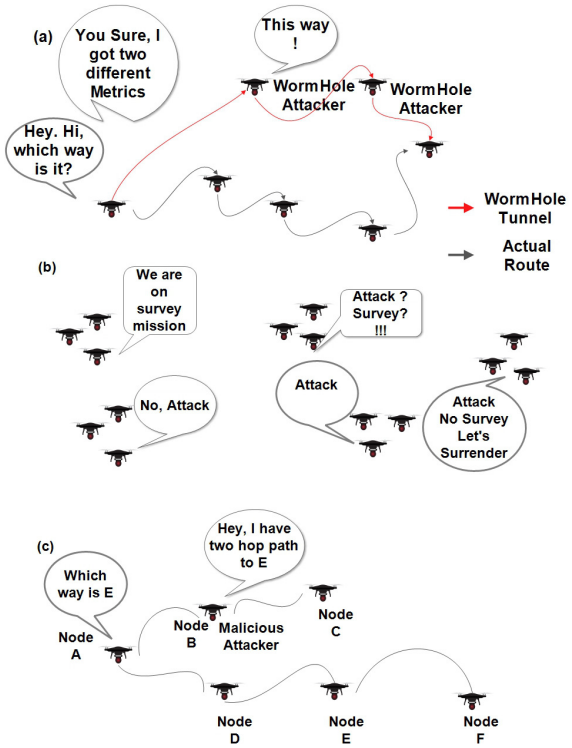


Figure 2.3: UAS Attacks: (a) WormHole Attack; (b) Byzantine Attack; (c) BlackHole Attack.

DoS attacks by generating high power transmissions. An authentication policy cannot safeguard against the attack as a hacked node can be a warhead for such an attack.

Encrypted frequencies of GPS of RQ-170's Achilles were jammed thus disrupting the communication links and forcing it to switch to autopilot. It also interrupted the secure data flow from the GPS satellites. The UAV under attack searched for unencrypted frequencies normally used by commercial airliners. Then spoofing was employed to send wrong GPS coordinates, tricking it into landing at a site which local navigational control thought to be the pre-programmed base, and thus landing directly into the hands of attackers [157]. Hacking is a powerful tool to break into complex connected networks. Maldrone [160], specifically built to target aerial vehicles proves that drones can be commandeered for more nefarious purposes. UAVs come with onboard geofencing software that restricts them from flying close to restricted or sensitive areas. Rogue operators, with the amount of technology available, can always build attack specific devices without any geofencing hardware and software or they could turn to basic hacks.

Once inside the system, an attacker can take advantage of compromised security or jacked nodes to launch a full-scale cyber/ network attack on the overall aerial system. A wormhole attack on UAS is possible when two or more compromised aerial nodes collaborate to

form a tunnel. Blackhole attack is directed using a hacked or malicious UAV by exploiting the properties of wireless routing protocols (Figure 2.3). The grey-hole attack, where a node selectively forwards the packets, is much harder to mitigate in aerial scenarios. Collaborative attacks such as Byzantine are hard to mitigate as a node or group selectively forwards and discards the information creating routing loops. Replay attacks and attacks by fabricated statistical messages can be mounted on aerial nodes as the rapidly changing position proves advantageous to the attacker in impersonating another node's identity. Aerial nodes are also susceptible to rushing attacks which decreases the overall routing potential of multi-hop routing protocols. Colluding mis-relay is another form of Byzantine attack where targeted packet generally carry routing information, resulting in zero or minimalist throughput levels. The complete taxonomy of cyber attacks attacks on UAS is illustrated in Figure 2.4.

Telecommunication operators facilitate managed connections, controlling the end-to-end delivery to maintain the minimum quality of service requirement. Managed connection providers come with extensive experience towards addressing cyber threats directed towards Public Switched Telephone Network and IP networks. Operators manage a layered approach, relying on primary protection methods, for safeguarding the IP network and communication channels, which enables them to achieve minimum safety specifications and high levels of security.

The currently deployed generation of wireless communication, 4G LTE, is characterised by increased security and reliability. The third-generation partnership project (3GPP) demands the embedding of safety capabilities into the network architecture itself. The technological flexibility, safety and security, better radio coverage and speed gains of LTE have paved for recent developments in the field of UAV networks [176, 177, 178].

LTE nodes use Authentication and Key Agreement (AKA) for identifying themselves to the network as well as for mutual authentication. The implemented authentication protocol itself can be different but they all use the same AKA algorithm. The base station (eNodeB) and the nodes communicate through air interface via radio frequency (RF) and at both ends, IP packets are modulated into RF signals and vice versa. The communication between base and node is not necessarily secure but 3GPP dictates that both non-access stratum and radio resource control plane messages feature integrity and reply protection. 3GPP mandates that the user plane signals are not necessarily integrity protected but confidentiality protection is the responsibility of the PDCP and is left to the organisational implementations [179, 180, 181, 182].

The air interface protection provides assurance that the messages are not intercepted and deciphered by malicious attackers. EPS sencryption algorithms and EPS integrity

algorithms are used for confidentiality and integrity. All the encryption algorithms use 256 bit keys where the least significant 128 bits are used [183, 184, 185].

There is a weakness in AKA authentication but LTE itself is susceptible to attacks. As the eNodeB is hosted on sophisticated hardware platforms, it is susceptible to cyber threats. The end nodes are still vulnerable to defection or hostile behaviours under malicious attackers. The rogue base station is a new possible threat to LTE infrastructure, as the eNodeBs are hosted on servers and hardware machines. Rogue base stations are unlicensed entities that are not operated by the organisation [186, 187, 188].

Identity theft attacks are possible using a rogue base station. Rogue base stations can cause jamming and DoS attacks using high-frequency signals. Forged authentication request messages from a rogue base station can affect aerial networks, with an inability to distinguish between authentic and unauthentic eNodeB. An unenclosed air interface can lead to the possibility of eavesdropping. The LTE backhaul interface is also susceptible to eavesdropping and loss of confidentiality [189, 190, 191, 192, 193, 194, 195, 196].

5G communication networks are not only an evolution from the current networks but also add new capabilities to the existing 4G/LTE networks. 5G exploits existing setups where the infrastructure is based on software defined networking and network function virtualization. The standardization of 5G is still in process but 5G networks make use of low, medium and high bands of communication and are termed as new radio air interface. Although still in the inception phase, 5G networks require strong inter-working with 4G networks to establish a smooth transition. The Next Generation Mobile Networks Alliance has introduced basic security requirements for 5G networks which includes radio requirements such as threats against jamming attacks and improved safety of small cell eNodeB's. 5G includes all the safety paradigms of LTE networks with the inclusion of civilian safety and safeguard the communication in mission-critical situations. The standards also need to comply with the restriction of minimum latency guarantee [197, 198, 199, 200].

5G networks feature both message and entity authentication, which ensures that the transmission and the transmitter are part of the network. 5G technology exerts that all the communicating parties, direct or indirect, must be authenticated. Legacy networks require the authentication between nodes and the network, whereas 5G networks impose a demand for authenticating nodes, networks and services. Hybrid authentication also supports multi-tier identity structure. This includes device identity and identity provided by the service [201, 202, 203, 204, 205, 206, 207].

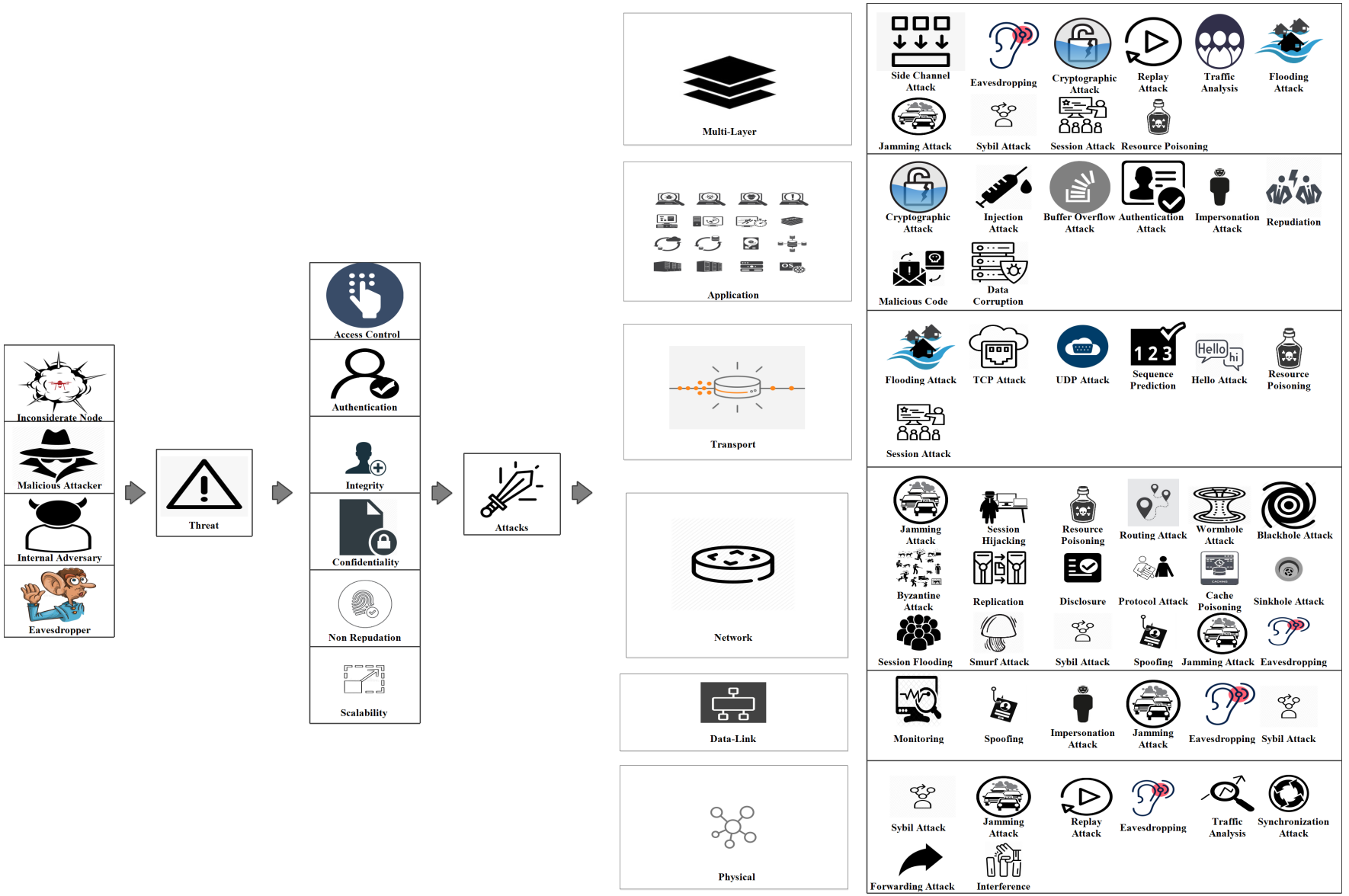


Figure 2.4: Taxonomy of Threats Associated with UAS.

The heterogeneous access privileges where different access technologies and multiple network environments can be deployed, increase the burden of design and motivate malicious intruders to take advantage of junction vulnerabilities. Additionally, the choice of the device, whichever way it accesses the network makes it even harder for the safety designers. The gradual advent of technology also forces the attacks to take more sophisticated forms. 5G networks are susceptible to eavesdropping and man in the middle attacks. Jamming, DoS and DDoS attacks are also passed on to the 5G networks from its predecessors [208, 209, 210, 211, 212].

The future of wireless communication technology, 6^{th} Generation Networks are dedicated towards bringing an open paradigm shift by making wireless networks programmable. 6G is expected to incorporate Artificial Intellgence (AI) with distributed training of base stations and equipments. The individual and organizational goals can be realised through the mutual coexistance of distributed leaning agents in form of collective AI. In order to accomodate the drastic changes, the technology and applications both need to adapt at hardware and software levels [213]. The real time intelligence promised by the 6G Networks can help exploit the full potential of aerial systems as it facilitates both low latency and collective AI. The 6G technology along side IoT is capable of guiding UAS towards information value loops. Where information passes through a network so that it can be communicated, and standards, like technical, legal, regulatory, allow that information to be aggregated across time and space. Augmented behaviour and prediction is then employed for taking action or shape human decisions in a manner leading to improved performance and accuracy.

UAV networks can take advantage of on demand intelligent edge facilitated by the 6G networks and can respond proportionately through unfamiliar or hostile environments [214]. The powerful 6G is expected to provide reliability, low latency, and secure transmission services but the dramatic improvements in technology (AI [215, 216, 217], Molecular Communication [218, 219, 220], Quantum Communication [217, 221], Blockchain [222, 223, 224], Visible Light Communication [225, 226]) will also navigate through security and privacy concerns.

2.1.4 Software Defined Networks for UAVs

Software Defined Networks (SDN) is another development that has revolutionized the communication technology. SDN can be thought of an evolution over traditional networks instead of a new technological development. Till recently, networking, compute and data servers were kept functionally and spatially separate and their management is also separated from each other. Different elements came together only after the realiza-

tion of cheap and abundant data, compute and networking power in the data centers. Virtualization added to the environment, the easy migration of servers as virtual machines. During all this evolution, network always remained the neglected member of the computing family [227, 228]. The major force that hampered the development and led to the slow innovation of network has always been the vertically integrated closed proprietary industry. This tiered structure of specialized applications over specialized control programs over the specialized hardware leads to absolutely no or very little configuration and customization options. It is approximately impossible to develop and test new protocols and prototypes because of this extremely rigid environment [229].

The growing need of flexible and directly programmable agile networks which emerged as a challenge after the introduction of cloud computing, distributed database and other resource intensive applications demands an abstraction for the TCP/IP in order to make the network centrally managed and to appreciate the global application development initiative of the networking research groups [230, 231].

The fundamental or the radical approach that defines SDN is the control and data logic which are physically separate. Time to time there have been efforts to reduce this network complexity and make networks programmable. Open Networking Foundation (ONF) defines the SDN controller as a logical entity which serves as the brain or network intelligence. Controller alongside network hypervisor is responsible for generating an abstract global view of the network. This programmable controller is responsible for the conceptualization of vender independence and freedom from the bottleneck of vertically inclined network industry [232].

The decoupling of decision logic from the data plane, to realize an abstraction that will make the network flexible, scalable, and programmable, is the key component behind the innovation of SDN. The decision logic, commonly known as the control plane (or controller), is the brain of the network, and the data plane is the networking element that sits as a forwarding element (FE). The abstract global view of the network helps custom programming the network without worrying about the underlying vendor-specific hardware. The choice of using a centralized, logical centralized, or distributed controller is still an open area of research. Centralized controllers being easiest to deploy are the heart of experimental SDN and have a single point of failure but come with an advantage of the ease of configuration. Logically centralized controllers are easy to scale as compared with centralized controllers but are susceptible to failures and produce synchronization problems [230, 231, 227, 232]. Fully distributed models are still under experimentation and testing phase. Table 2.5 details landmark SDN controllers and operating systems.

The inception of SDN began as a race towards more programmable networks. Open

Signalling (OPENSIG) and Developed Control of ATM Networks (DCAN) are the initial efforts to make ATM scalable and programmable [233, 234]. The 4D advocated an approach that detaches the routing control from the protocols governing interaction among networking devices [235]. NETCONF [236] came up as a major break which laid the foundation of many SDN controllers today. Project Ethane was the first major effort in development of the architecture which solidified the grounds for SDN [237].

OpenFlow project started as a challenge to the slow and costly innovation in the field of Networking. The slow innovation is underlined by the rigidity of the current network architecture which is dedicated to the vertically scaling industry and makes it impossible to experiment and innovate. OpenFlow is an effort to make network programmable and more and more flexible. A flow table or more generally a routing table, a secure communication channel between controller and switch, and a south-bound protocol namely the OpenFlow Protocol are the basis of the OpenFlow architecture. The interaction between the hardware and the OpenFlow controller is facilitated by the South-Bound protocols via a south bound interface. The controller is the brain of the network which takes care of all the logical processing. The set of application programs interact with the controller with the help of North-Bound protocols (Restful, JAVA RPC etc.) via a north bound interface. There is also a East/West interface which facilitates the interaction between multiple controllers. The flow table is similar to a normal routing table but contains more fields for detailed specification and a match/action rule which defines the destiny of the incoming packet [230, 227, 232].

ForCES is the least talked about SDN archietecture. The ForCES protocol can be used by Control Elements (CE) to manage and configure a standalone or multiple Forwarding Element (FE). A given functionality is realized by numerous logically independent Network Elements (NE) which mostly appear as a standalone piece of network entity. CE implements the ForCES protocol and provides FEs with instructions. Generally CE manager is responsible for all the management tasks. FE also implements the ForCES protocol and use the switch hardware for packet processing as directed by one or more CEs with the help of the ForCES protocol. A FE manager is responsible for generic FE management tasks. ForCES Protocol Transport Mapping Layer uses the functionality of the underlying transport layer protocol [238, 239]. The fundamental difference is that in ForCES the FE and the CE act as a single entity, and the OpenFlow focuses on the decoupling of control and forwarding plane.

Jain, et al. presented the Google's B4 Software Defined WAN. The B4 architecture is three tiered comprising of switch hardware, a site controller and a gateway. The switch hardware with almost no intelligence only forwards traffic according to the flow table

entries. Network Control Server (NSA), Network Control Applications (NCA), Open Flow Controller (OFC) forms the site controller. The purpose of the SDN Gateway is to abstract the implementation details from the network Traffic Engineering (TE) server. The switch events and the information gathered from NCA is used by the OFC to establish a Network State. An Open Flow Agent (OFA) runs on the Linux processor switch which forward packets to the Open Flow Controller which then forwards packets to the protocol stack (Here the BGP stack in particular). The current state of the network is maintained by the Network Information Base (NIB) and the Routing Application Proxy (RAP) is responsible for the linking of Quagga and OF switches. The routing updates are managed by the Quagga. RAPd component takes updates and proxies from Quagga's RIB and delivers it to RAP. RAP converts from RIB entries which form a global network view to low level hardware view of switches [240].

Shin, et al. gave architecture for the application programming interfaces in SDN. Service oriented/aware networking and the network complexity are the driving forces behind the migration from traditional networls to SDN. New set of interfaces were introduced with the programmability of the control logic. The interface managed by the southbound protocols between the control and data plane is known as South-Bound interface. The interface between network infrastructure and control plane is the North-Bound interface whereas the interface between various controllers is called the East/West interface [241]. Heller, et al. [242] discussed the required number of controllers and their arrangement with focus on average and worst case latency as placement metric. Placement varies topology to topology and random placements tend to degrade the network performance exponentially. Finally a K-centre algorithm is proposed to find the placements so as to reduce the average propagation latency.

Tootoonchian, et al. [243] tested their controller i.e. NOX-MT on various performance metrics such as maximum throughput, relationship with switches, relationship with load level and write-intensive loads. Controller response time was justified with the help of minimum and maximum response time, relationship with the load level and number of active switches. Authors showed the improved performance to set up micro benchmark but at the same time suggested more than one controller is required for larger and random networks and placement is of prime importance.

Yao, et al. [244] demonstrated the cascading controller failures and suggested that the major problems arise due to the deployment of lesser number of controller's or a few controllers have a lot more load than others. Authors propose load balancing and load redistribution can help elevate the problem.

Table 2.5: Open Source SDN Controllers and Operating Systems.

	NOX	**POX**	**RYU**	**TREMA**	**FLOODLIGHT**	**OPENDAYLIGHT**	**BEACON**
License	GPL	Apache	Apache 2.0	GPLv2	Apache	EPL 1.0	BSD
Contributors	NICIRA. Stanford University. ON Labs. UC Berkley. ICSI.	NICIRA. Stanford University. ON Labs. UC Berkley. ICSI.	NTT Labs.	NEC. GPLv2 Scheme.	Big switch networks. Based on Beacon.	Open Daylight community. Linux foundations collaborative projects.	Stanford university.
Language support	C++.	Python.	Python.	C/Ruby.	Java. Rest API.	Java.	Java.
Operating system	Windows. Mac. linux.	Windows. Mac. Linux.	Linux.	Linux.	Windows. Mac. Linux.	Platform independent JVM.	Windows. Mac. Linux.
OpenFlow version	1.0	1.0	1.0, 1.2, 1.3, 1.4, 1.5, 1.6. NICIRA extensions.	1.0. 1.3.x via TremaEdge.	1.2, 1.2, 1.3 1.4.	1.1, 1.3, 1.5 1.6.	1.0.
Openstack	No quantum plugin.	No quantum plugin.	Yes.	Yes.	Yes.	Yes.	Yes.
UI	GUI.	Web based.	GUI.	No.	Web based.	GUI.	Web based.
Emulation	Mininet OpenVswitch.	Mininet. OpenVSwitch.	Mininet. OpenVSwitch.	On board.	Mininet. OpenVSwitch.	Mininet. OpenVSwitch.	Mininet. OpenVSwitch.
Threading	Multi.	Single.	Single.	Single.	Multi.	Multi.	Multi.
Interface	OpenFlow southbound.	OpenFlow southbound.	OpenFlow southbound. OVSDB. JSON. REST Api northbound.	OpenFlow southbound.	OpenFlow southbound. JAVA, REST northbound.	OpenFlow southbound. JAVA RPC, REST northbound.	OpenFlow southbound.

Sallahi and St-Hilaire [245, 246] proposed an optimal model for controller placement which takes into account no of packets, available ports, bandwidth switch and hardware cost etc. The model is optimally able to solve the problem of controller placement as well as the no of controller required. The model is also capable of backward compatibility.

Bari, et al. [247] proposed a heuristic approach for dynamic controller provisioning in SDN. Authors talk about partitioning of network into multiple domains in which each domain is controlled by a specific controller. Dynamic Controller provisioning is a NP Hard problem so the authors suggest a heuristic approach that takes into account network topology, traffic matrix, previous switch–to–controller assignment, and set of switches S, possible controller locations, controller capacity vector, and delay constraint. Greedy Knapsack and simulated annealing based approach is adopted by the authors to propose an approximate solution.

Tootoonchian and Ganjali proposed HyperFlow in which NOX controller runs an instance of hyperflow. Hyperflow localizes the decision making, in spite of the fact, that it keeps network logic centralized. It is tested to perform well in mission critical situations. Hyperflow is robust in case of infrastructure failure and has an additional advantage of very less inter area control traffic when it comes to highly partitioned networks [248].

Dixit, et al. [249] proposed ElastiCon, an elastic distribution of SDN controller. The authors propose a distributed controller, a switch migration protocol and a load adapting mechanism. The authors consider liveliness which means at least one controller is active per switch and safety which considers the duplicate entries and flow table consistency as the base of switch migration protocol. Load adaptation is composed of load estimation, adaptation decision making and load adaptation rules.

Schmid and Suomela talked about the locality in distribution of SDN control. The authors presented a view of the distributed SDN control plane with the help of local algorithm i.e. with slight modification these algorithms allow coordination among the controllers that they take care of their own neighborhood alongside cooperating with each other. Authors also propose a local distributed model for it [250].

Yao, et al. [251] gave the capacitated controller problem in which the authors suggest that the server capacity limitation, the latency of message processing and the failure rate of the heavily loaded servers is of utmost concern. The strategy presented reduces the actual instances of the controller and also proves beneficial in load balancing of the overloaded units.

Muñoz, et al. [252] presented Virtual Tenant Networks (VTN) which is generally the virtualization of the SDN Control, making it dynamically scalable and provides flexible

control and configuration. De Oliveira et al [253] proposed SDN based wireless sensor network where nodes were subdivided into switch nodes and controller nodes, making the architecture flexible and scalable. Another important development is the heuristic based SDN controller placement in large scale WAN networks. The authors aim at achieving controller placement according to Pareto-Based optimality principle and provides the optimal placements considering various metrics [254]. SDN/OpenFlow based controller options were also considered in 5G networks. Two layered architecture with a global and several local layers were discussed in order to facilitate movements and migrations [255]. The control plane issues for WiFi SDNs are discussed in [256]. Partitioning of SDN into distributed control instances is presented in [257].

2.2 Conclusion

The chapter presented an aggressive and in-depth analysis of the problem at hand with the help of published research, projects and standards. Both transmission scheduling and mobility based data dissemination frameworks are covered in literature. Alongside the frameworks, middleware and architectures are also surveyed. Apart from research articles and projects, communication standards, industry whitepapers and technological articles are also thoroughly analyzed. Past, present and future of wireless communication technology is accessed on the merits of data dissemination, mobility and trajectory, safety and QoS. The analysis of the published work helped, develop a thorough understanding of the problem at hand and also aided in curating a narrative towards possible solutions. The review of published works also helped in navigating through the research gaps and challenges, borrowing already existing solutions and selecting possible candidates for evaluating the proposed solutions. Published literature also guided us towards developing agile, flexible and multi-dimensionally scalable solutions.

Chapter 3

Transmission Scheduling Based Data Dissemination [1]

The cooperation between WSNs and UAV networks can achieve many goals related to weather forecasting and remote sensing, military operations and surveillance, monitoring of inhabited areas, cooperative systems, information relaying, agricultural support, disaster relief, archaeology, pollution control, etc [23]. The data rate, signal fading, interference, spectral efficiency, and link reliability are major problems in wireless communication. Multiple-Input Multiple-Output (MIMO) is a recent advancement in technology that exploits antenna diversity and spatial multiplexing to increase capacity and enhances the link reliability. The MIMO technology enables many signal paths by employing multiple transmitter and receiver antennas. Effectively, MIMO is a spatial diversity that helps to improve the signal to noise ratio and spatial multiplexing by increasing the capacity of the channel. Multiuser-MIMO (MU-MIMO) is an enhancement over the preexisting MIMO systems in which the station can communicate with multiple users simultaneously while improving capacity and multiplexing gains [258, 259].

Another interesting development in the field of networking is the inception of SDN. The communication networks follow a vertically integrated proprietary and vendor-specific trend. This proprietary network industry along with the hardware and protocols makes it impossible to experiment with the organizational network. Application Specific Integrated Circuits (ASICs)) today come with logic hard coded and leave the organization with very less or no choice of custom tailoring their requirements. The decoupling of decision logic from the data plane, to realize an abstraction that will make the network flexible, scalable, and programmable, is the key component behind the innovation of SDN. The decision logic, commonly known as the control plane, is the brain of the network, and the data plane is the networking element that sits as a forwarding element (FE). The abstract global view of the network helps custom programming without worrying about the underlying vendor-specific hardware [229, 260].

[1] Mohd. Abuzar Sayeed, Rajesh Kumar, Vishal Sharma, *"Efficient data management and control over WSNs using SDN-enabled aerial networks"*, International Journal of Communication Systems (IF 1.319), Wiley, August (2019). [Published]

UAVs are multi-component systems comprising both hardware and software units alongside navigation and control. The basic requirement for UAV guided ad hoc networks is an efficient mobility model, communication system, and situational awareness. The UAV movement is also characterized into two categories, ie, gliding and hovering. Gliding capabilities of UAVs result in longer flight and better coverage but require more space and operational skills, whereas hovering capabilities result in better acquisition but extremely low battery life. Tactical movement, navigation, ground-to-air network formation, efficient relays, and reception of data have always been an issue with WSNs and UAVs. The depleting energy in WSN results in frequent disconnections. The aforementioned issues present an opportunity for exploiting the fast and energy efficient MIMO transmissions and using SDN to achieve flexible deployment of UAVs. This allows constant reconfiguration of the underlying fast changing topology for achieving high gains over the current systems.With the application of SDN, there is an important issue to address, ie, placement of the SDN controller. Also, it requires a decision on keeping the controller centralized, distributed, or logically distributed.

3.1 Efficient Data Management and Control over WSNs using SDN-Enabled Aerial Networks

The proposed system model incorporates efficient and simple movements of UAVs for increasing the flight time and better data transmission/reception. A dynamic, flexible, easy to implement mechanism is presented for topology formation. It is energy efficient and avoids disconnections and dead transmissions. The system model exploits the hovering capabilities of aerial nodes and builds upon them a framework for data distribution from ground nodes to base station via UAVs. The proposed SDN controller defines and guides the overall topology whereas the proposed energy model is consumed by the SDN controller as input. The topology is frequently reconfigured and updated whenever there is a change in state of WSN nodes. The state change of nodes itself is evaluated by the base station/SDN controller. The flow entries of the aerial nodes which decide upon the transmission scheduling are updated on temporal basis by the ground controller. The framework also incorporates sleep state management for WSNs,which relies on UAV maneuvers for energy efficiency and back-off counter, which provide non-conflicting random back-off intervals without increasing the waiting time. The major advantage of the proposed approach is its simplicity as it does not require any special configurations. It employs the existing hardware, software, and available specifications in a more effective and energy efficient way.

3.2 UAVs Coordinated WSNS

The proposed approach focuses on energy-efficient data dissemination in multi-UAVs-enabled WSNs. The network comprises UAVs, sensor nodes, base/ground station, and an SDN controller on the local base station. The sensor nodes are placed into cells that are designed to be octagonal instead of the regular hexagonal layout. The octagonal shape is chosen as the square area bounded by four octagons is used for the placement of base stations. This is inspired by Sharma and Kumar [5]. The center of the cell, which is traditionally occupied by the base station now, has a resident SDN controller. The controller is responsible for logical topology formation and updating of Forwarding Information Base (FIB). The octagonal cells are themselves divided into eight sectors. The sensor nodes occupy the region inside each cell. Figure 3.1 gives a global view of the overall system model.

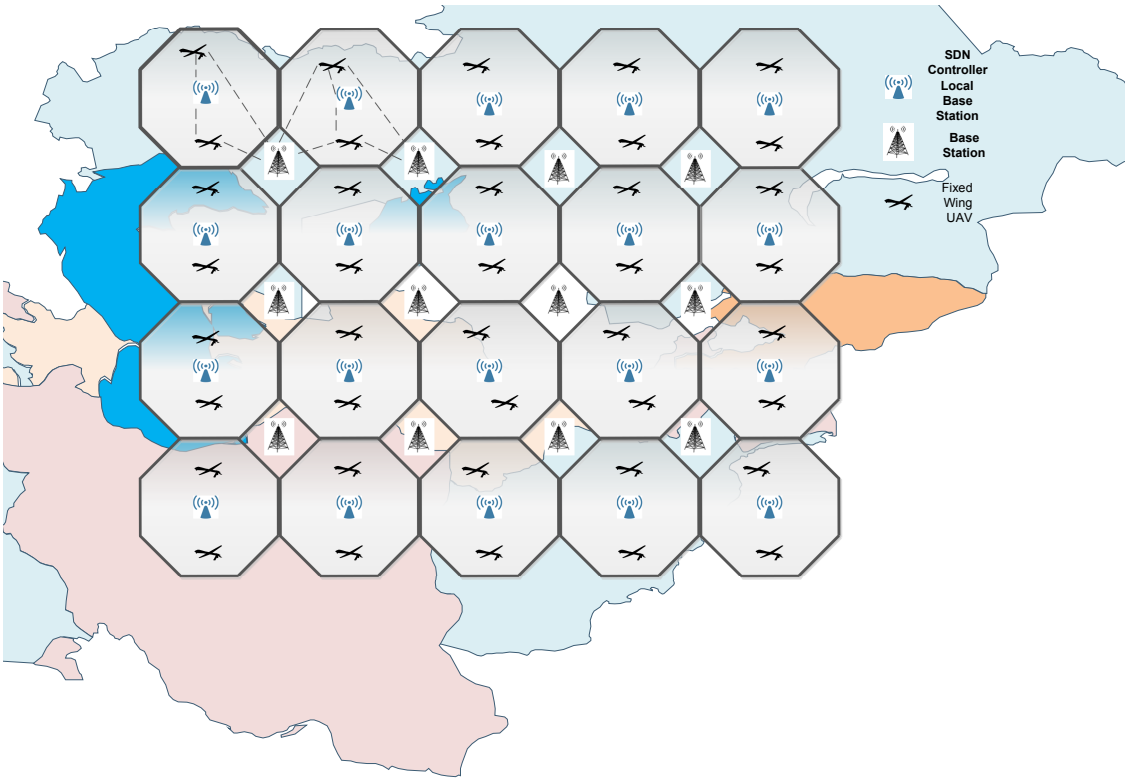


Figure 3.1: An Illustration of the Overall System Layout.

Since WSN nodes are mapped to individual sectors of a cell, it is important to map ground nodes as well as UAVs to particular sectors within the cells. To perform this mapping, the Barycentric coordinate system is applied [261]. Intuitively, the idea of sectors comes from the UAV maneuver angels. Points $(x_i,\ y_i)$, $(x_j,\ y_j)$ define two consecutive UAV turning points. Both the points, together with the center $(x_c,\ y_c)$ of the cell, essentially

form a sector.

The mapping of a point (communication node) (x_n, y_n) to a particular sector is done according to Equation 3.1 to Equation 3.8:

$$x_n = a_i \times x_c + a_j \times x_i + a_k \times x_j, \tag{3.1}$$

$$y_n = a_i \times y_c + a_j \times y_i + a_k \times y_j, \tag{3.2}$$

$$a_i + a_j + a_k = 1, \tag{3.3}$$

$$a_i = \frac{((y_i - y_j) \times (x_n - x_j) + (x_j - x_i) \times (y_n - y_j))}{((y_i - yj) \times (x_c - x_j) + (x_j - xi) \times (y_c - yj))}, \tag{3.4}$$

$$a_j = \frac{((y_j - y_c) \times (x_n - x_j) + (x_c - x_j) \times (y_n - y_j))}{((y_i - y_j) \times (x_c - x_j) + (x_j - x_i) \times (y_c - yj))}, \tag{3.5}$$

$$a_k = 1 - a_i - a_j, \tag{3.6}$$

where, a_i, a_j, a_k are scalers, and,

$$0 \leq a \leq 1, 0 \leq b \leq 1, 0 \leq c \leq 1, \tag{3.7}$$

$$a + b + c = 1. \tag{3.8}$$

Each cell uses two UAVs for relays and transmissions. The UAVs fly autonomously in the same direction clockwise or anticlockwise. The position and velocity of the aerial nodes are controlled by the SDN controller. This is done in such away that at any given time, both the UAVs are along the diagonal of the cell, ie, the UAVs are always in opposite sectors. The topology is formed in such a way that the aerial nodes are always in contact with one of the base stations surrounding the cell. The SDN controller contacts the aerial nodes whenever there is an update in the overall system layout or operation. Figure 3.2 gives a detailed view of a single cell and the sectors occupied by the sensor nodes.

The UAVs are assumed to fly autonomously with the angle of the bank equaling 45^o

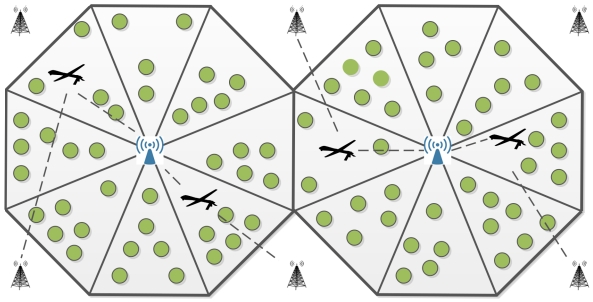


Figure 3.2: System Model with Zoom-in View of a Single Cell.

in eight directions. This 45^o banking angle gives the topology an octagonal shape with base station around the junction of octagons. The maneuvering angles represent the way-points that coordinate the UAV movements. Moreover banking angle greater than 45^o, say 60^o or 75^o, increases the stall speed by 40% and 100%, respectively, thus wasting too much energy. The stall is a point where aircraft starts to descend because it is no longer able to support its own weight. In order to counter this situation, it is intended to increase the speed and adjust the wings of the aircraft. This increase in speed is termed as stall speed. The load factor is a factor that defines the increase in force given a particular angle, which in turn, affects the stall speed and aerodynamic adjustments. Figure 3.3 gives the relation between the load factor, the angle of bank, and the stall speed.

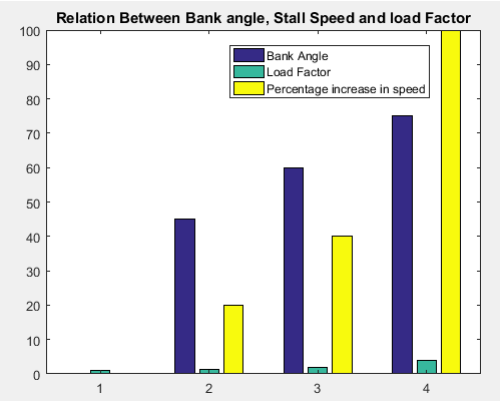


Figure 3.3: Relation between Angle of Bank, Stall Speed and Load Factor.

The base stations, as well as UAVs, are equipped with MIMO antennas. The base station features a 4-input and 4-output (4×4) MIMO antenna. 4×4 MIMO antenna is used as the system layout automatically constraints maximum of four connections (four UAVs surrounding a base station) at any given time. The UAVs are equipped with 2×2 MIMO antennas for transmitting and receiving data. An omni-directional antenna is used for control messages like connection establishment, request-to-send (RTS), clear-to-send (CTS), and busy-to-send (BTS) messages. Sensor nodes are in a sleep state as long as UAV does not enter their particular sector in the cell. Although the sleep and listening

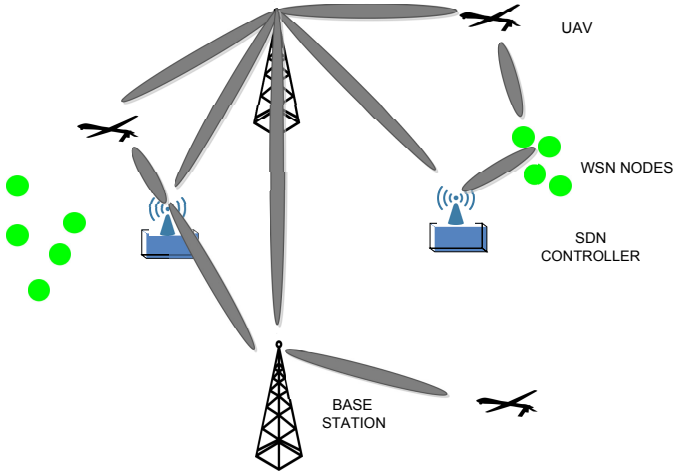


Figure 3.4: Communication Channel Layout (MIMO).

states are also discussed previously in literature [262], in the proposed approach, WSN states or duty cycles are managed by the SDN controller that is responsible for all the dynamic behaviors of the network. Figure 3.4 gives an insight into the reference antenna model of the system.

In every sector of each cell, there is a set F of sensor nodes given by Equation 3.9, such that

$$F = \{x : x \; is \; an \; integer; and \; 0 \leq x \leq n\}, \tag{3.9}$$

where x is the number of sensor nodes in a sector and n is the total number of nodes in a cell. Any number of nodes trying to initiate transmission at any time is given by Equation 3.10 [263]:

$$P((A) = y) = \binom{\lambda v(O)}{y} \cdot \left(\frac{1}{\lambda v(O)}\right)^{y} \cdot \left(1 - \frac{1}{\lambda v(O)}\right)^{\lambda(v(O)-y)}, \tag{3.10}$$

where λ determines the number of nodes per unit area, and is given by Equation 3.11:

$$\lambda = \frac{n}{v(W)}, \tag{3.11}$$

where $v(W)$ is the total area of an octagon. Thus the average distribution of nodes is calculated according to Equation 3.12:

$$Nodes/Sector = n \times \frac{v(O)}{v(W)}, \tag{3.12}$$

where $v(O)$ is the area of a particular sector.

The proposed framework adopts a contention-based scheme for data transmission between WSNs and UAV. As suggested by the equation and the proposed system model, any number of nodes can take part in contention for the UAV channel by means of sending an RTS message. The UAV checks the request against its own flow table. If a UAV is ready to accept the transmission, it sends back the CTS message to the designated node and enables an omni-directional BTS beacon. The beacon serves as a warning signal for other nodes so as to tell them not to initiate a transmission as it may cause a collision. After sensing the BTS signal, a node chooses its random back-off value and reinstates the transmission only when the counter expires. The nodes with long messages do not take part in contention to send the complete message. The whole message is sent burst mode.

3.2.1 Energy Model

At any given time t, the quantity of charge left in a sensor node is given by Equation 3.13 [264, 265]:

$$C(t) = C_0 e^{-(d_{WSN})t}, \tag{3.13}$$

where $C(t)$ is the charge left at time t. C_0 is the initial charge. d_{WSN} is the rate at which charge decays when a node is continuously in operation (sensing or transmitting).

The decay rate d_{WSN} can be derived from Equation 3.14:

$$d_{WSN} = \frac{\ln \frac{C_0}{C(t)}}{t}. \tag{3.14}$$

The d_{WSN} considers the energy consumed during contention, transmission, duty cycling and the energy required for normal operation.

The interval for which a sensor node remains active (not completely discharged), or the mean lifetime of a WSN node, is given by M_{WNode} which can be defined in terms of charge decay rate d_{WSN}, and is given by Equation 3.15:

$$M_{WNode} = \frac{1}{d_{WSN}}. \tag{3.15}$$

Now, the amount of charge left in a sensor node can be defined in terms of mean lifetime

[264], and is given by Equation 3.16:

$$C(t) = C_0 e^{\frac{-t}{M_{WNode}}}. \tag{3.16}$$

At a given time T_x, a wireless node is allowed to transmit or receive only if Inequality 3.17 is satisfied

$$C(T_x) \geq Z_{WSN}, \tag{3.17}$$

here, Z_{WSN} is the minimum charge required for stable operation of the node and $C(T_x)$ is the charge left at time T_x [264, 266], and is calculated according to Equation 3.18.

$$C(T_x) = C_0 e^{\frac{-T_x}{M_{WNode}}}. \tag{3.18}$$

The mean life time of a sector is given by Equation 3.19:

$$M_{WSNS} = \frac{\sum_{n=1}^{s} C(t)_s}{n_s}, \tag{3.19}$$

where, $C(t)_s$ is the charge of nodes constituting a sector.

The mean lifetime of a cluster is defined according to Equation 3.20:

$$M_{WSNC} = \frac{\sum_{n=1}^{c} C(t)_c}{n_c}, \tag{3.20}$$

where, $C(t)_c$ is the charge of nodes constituting a cluster.

The active duration of a cluster is managed by Inequality 3.21:

$$Z_c \leq \sqrt{\frac{1}{c-1}\sum_{i=1}^{c}(C(t)_c - M_{WSNC})^2}, \tag{3.21}$$

where Z_c is calculated according to Equation 3.22,

$$Z_c = |M_{WSNC} - Z_{WSN}|. \tag{3.22}$$

Whenever Inequality 3.21 is satisfied a topology change is initiated by the SDN controller,

and the UAV flow table is updated accordingly.

The active duration of a sector is defined by the inequality 3.23:

$$Z_s \leq \sqrt{\frac{1}{s-1}\sum_{i=1}^{s}(C(t)_s - M_{WSNS})^2}, \tag{3.23}$$

where Z_s is derived from the Equation 3.24,

$$Z_s = |M_{WSNS} - Z_{WSN}|. \tag{3.24}$$

Whenever the inequality is satisfied, the SDN controller either declares it as a dead sector or performs an evaluation based on Equation 3.17.

The overall system power is not only dependent on the charge decay of sensor node but also limited by the battery power of the UAVs. Let d_{UAV} denote the rate at which UAV battery discharges. The charge left in UAV after time T_x is given by Equation 3.25 [264]:

$$U(T_x) = C_0 e^{-(d_{UAV})T_x}, \tag{3.25}$$

Where, $U(T_x)$ is the battery left in UAV at time T_x.

Inequality 3.26 defines the necessary condition For a UAV system, to keep on operating.

$$U(T_x) \geq Z_{UAV}, \tag{3.26}$$

where, Z_{UAV} is the minimum operational power of the UAV. The total power loss rate of the system can be defined according to Equation 3.27:

$$(d_{WSN} + d_{UAV})N, \tag{3.27}$$

where N is the total system power. The mean lifetime of the system can be defined by Equation 3.28 [267]:

$$M_{Sys} = \frac{(\lambda \times v(W) \times M_{WNode}) + (UAV_i \times M_{UNode})}{(\lambda \times v(W)) + N_j}, \tag{3.28}$$

where, M_{UNode} is the mean lifetime of the UAV and UAV_i is the total number of UAVs in the system and is given by Equation 3.29:

$$M_{UNode} = \frac{1}{d_{UAV}}. \tag{3.29}$$

Further, the complete system needs a re-initialization when Inequality 3.30 is satisfied [267]:

$$Z_{com.} \leq \sqrt{\frac{\mathfrak{X}_1 + \mathfrak{X}_2 + \mathfrak{X}_3 + \mathfrak{X}_4}{((\lambda \times v(W)) + UAV_i) - 1}}, \tag{3.30}$$

$$\mathfrak{X}_1 = ((\lambda \times v(W)) - 1){s_1}^2, \tag{3.31}$$

$$\mathfrak{X}_2 = (UAV_i - 1){s_2}^2, \tag{3.32}$$

$$\mathfrak{X}_3 = (\lambda \times v(W))(M_{WNode} - M_{Sys})^2, \tag{3.33}$$

$$\mathfrak{X}_4 = UAV_i(M_{UNode} - M_{Sys})^2, \tag{3.34}$$

where,

$$Z_{com.} = |M_{Sys} - Z_{Sys}|, \tag{3.35}$$

and Z_{Sys} is the minimal operational charge required to keep the overall system up and running.

3.2.2 Back-Off Counter

Back-off timers are used to decrease/limit the rate of data transmission or stop the transmission in order to ensure an acceptable level of QoS, minimize collisions, and achieve better throughput. The back-off mechanisms in WSNs have received a lot of interest previously [268, 269, 270, 271]. Here, the back-off mechanism replicates the defined energy model. The important catch to the WSN back-off interval is the limited battery available. So, for improving the overall average of successfully transmitted messages and also ensuring at the same time that the different back-off intervals chosen by the nodes

are not the same, a function for the remaining battery, $C(T_{hf})$ (charge after half life [266]) is used to calculate the back-off interval and is calculated according to Equation 3.36:

$$C(T_{hf}) = C_0 \left(\frac{1}{2}\right)^{\frac{t}{t_{\frac{1}{2}}}}. \tag{3.36}$$

Initially, a random number G_{nhf} is chosen, according to Equation 3.37:

$$\left(\frac{1}{2}\right)^{G_{nhf}} \times C_0 \geq Z_{WSN}, \tag{3.37}$$

and, limiting value of back-off counter B_{max} is calculated according to Equation 3.38:

$$B_{max} = n_{avg.hf} \times G_{nhf}, \tag{3.38}$$

where, $n_{avg.hf}$ is average number of transmission slots per half life.

Thus, the value of counter N_{ct} ranges between the following as stated by Equation 3.39:

$$0 \leq N_{ct} \leq B_{max}. \tag{3.39}$$

In first iteration, the value of the interval is set to any random value $0 \leq N_{ct_1} \leq B_{max}$ In successive iterations, BTS signal is encountered again. The value of the counter is incremented based on following rule (Equation 3.40):

$$N_{ct_\alpha} = (N_{ct_1})^\alpha, N_{ct_\alpha} \leq B_{max}, \tag{3.40}$$

where α is the iteration number. After certain number of unsuccessful attempts a transmission timeout is reached (Equation 3.41) i.e.

$$N_{ct_\alpha} \geq B_{max}. \tag{3.41}$$

The counter provides non-conflicting random back-off values as it depends on the presently available charge on the node. Separate counter values for every node ready to transmit

(avoiding starvation) are ensured by three factors.

i The probability of two contending nodes having the same charge is very rare.

ii Each node independently chooses its back-off interval from the pool which is derived from its own charge value.

iii Anytime a node reaches its transmission timeout, in the next cycle, the value of its counter is lesser as it a function of its own charge.

3.2.3 SDN Controller

The SDN controller [260] is the brain of the network. The main responsibility of the controller is to manage the dynamic nature of the network. The controller offers services and at times acts as the feedback node. It is also responsible for orchestrating, delegating, resource sharing, managing, and coordinating the network resources, in the proposed case, sensor nodes, and UAVs. The proposed SDN controller is responsible for logical topology formation and maintenance as it also keeps track of the topological updates. It coordinates the sensor to UAV transmission via updating the UAV flow table. Flow table [272] is a structure that contains a set of match and action rules. These rules, in turn, dictate the network behavior. Whenever an SDN switch receives a packet, it validates it against its flow table. The transmission is then duly accepted or terminated as governed by the pre-inserted rule or dynamic decision making is performed as dictated by the controller. The controller is also responsible for WSN sleep timers as it contains the database of the current topology as well as possible updates. Figure 3.5 gives the component level block diagram of the controller.

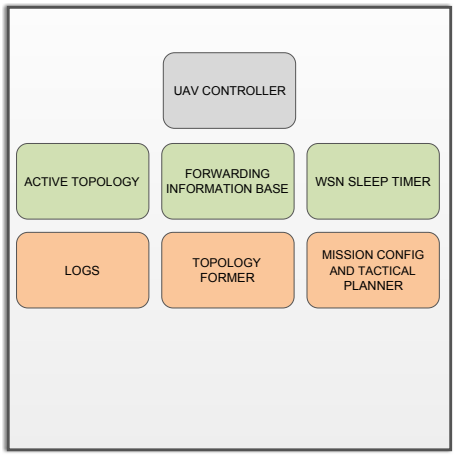


Figure 3.5: Block Diagram of the Software Defined Network (SDN) Controller used in the Proposed Approach.

• *Mission Configuration and Tactical Planner* keeps track of the overall mission statistics

and conceptual layout of the system. The information includes cell structure, information about the nodes, and charge statistics. The main function is to provide preliminary information to the topology former.

• *Topology Former* runs Algorithm 3.1 and builds a conceptual topology by partitioning the cell into sectors based on the UAV movements. The algorithm takes O(n) time for cluster assignment. Cluster Head selection and Topology Formation takes $O(n^2)$ time. Sector re-initialization takes $O(n^2)$ time. Where, n is the number of active ground nodes. The WSN nodes are mapped to a given sector by means of the barycentric coordinate system as outlined by Equations (3.1) to (3.8). Further, the mapped WSN nodes are subdivided into logical clusters on the merit of the mean available charge. The clustering is then used for logical topology formation. Clusters are updated whenever they fall below the desired level of performance. Topology former also takes care of overall system performance and performs mandatory actions as required.

Algorithm 3.1 Topology Formation and Maintenance Algorithm

Input: Set of WSN Nodes W_i
Initialize Network
Mark sectors w.r.t. (x_i, y_i), (x_j, y_j), (x_c, y_c)
Assign nodes to sector using Eqs.(3.1)-(3.8)
Select m nodes randomly (Centroids/Cluster Heads)
for `For each WSN node i` **do**
    Find a m_j
    If (min Charge Difference (m_j, i))
        Assign i to cluster j
    Else
        Proceed to next cluster
    End If
End for
for `For each cluster 1...k....j` **do**
    $M_{WSNC_j} = \frac{\sum_{n=1}^{c} C(t)_c}{n_c}, i.e.\ average$
End for
Replace M_{WSNC_j} as new centroid
Repeat steps 6-13
Halt when no cluster Assignment Changes and repeat step 14
If $(Z_c \leq \sqrt{\frac{1}{c-1}\sum_{i=1}^{c}(C(t)_c - M_{WSNS})^2})$ && $(M_{WSNC_k} < Z_{WSN}))$
    Assign node i to cluster m_j such that $C_{m_j} > Z_{WSN}$
    Alter UAV Flow Table to skip m_k such that $W_i = (W_i - m_k) + i$
Else
    Proceed Normal Operation
End If
If $(Z_s \leq \sqrt{\frac{1}{s-1}\sum_{i=1}^{s}(C(t)_s - M_{WSNC})^2})$
    Re-initialize Algorithm 1
Else If $(C(T_x)W_s \leq Z_{WSN})$
    Dead sector; Sector Initialization Required
Else
    Proceed Normal Operation
End If
If $(Z_{com.} \leq \sqrt{\frac{\chi_1+\chi_2+\chi_3+\chi_4}{((\lambda \times v(W))+UAV_i)-1}})$
    Complete System Initialization
Else
    Proceed Normal Operation
End If
Exit

• *Active Topology* stores the current underlying topology as defined by the topology former and keeps the FIB updated.

• *FIB* stores information about the currently active sensors, charge component, and cluster id's that are used for updating UAV flow table.

• *WSN Sleep Timer* is another integral component of the system, which is made easy by the underlying topology. Usually, sleep timers or methods are hard to apply because of the inconsistent topological conditions and the fact that every node is trying to communicate with every other node. Much of the battery is wasted in constantly listening and sleep switching. With UAVs as sinks and a clearly defined topology with frequent reconfiguration mechanism, it becomes easy to design an efficient sleep timer as follows:

D_{tot} defines the total distance covered by the UAV and is given by Equation 3.42.

$$D_{tot} = 8 \times d((x_i, y_i), (x_j, y_j)), \tag{3.42}$$

where, $d((x_i, y_i), (x_j, y_j))$ refers to the distance between two consecutive banks.

S_{tclk} is the total sleeping duration of a WSN node (during one complete UAV cycle around the cell) and is determined by Equation 3.43:

$$S_{tclk} = \frac{(D_{tot} - (2 \times d((x_i, y_i), (x_j, y_j))))}{U_s}. \tag{3.43}$$

The value of S_{clk} i.e. the sleep timer for WSN nodes is given by Equation 3.44:

$$S_{clk} = \frac{(3 \times d((x_i, y_i), (x_j, y_j)))}{U_s}. \tag{3.44}$$

• *UAV Controller* is responsible for feeding the Flow Table of the UAV with necessary information extracted from the FIB.

Energy model and SDN controller act as preliminaries to the data dissemination model and help simplify the dissemination process to the finest of granularity. Algorithm 3.2 underlines the data dissemination process. The algorithm takes $O(n^2)$ time, where n is the number of clusters. Figure 3.6 presents a brief overview of the overall data dissemination process.

3.3 Performance Evaluation

The proposed framework relies heavily on the efficient placement and application of existing solutions to achieve significant improvements and hence, establishing the backward compatibility and scalability of the developed approach. The evaluation and testing of

Algorithm 3.2 Data Dissemination Algorithm

Input: $|W|$
Initialize Network
while (Signal == BTS) **do**
    If i = 0
    Initialize Back Off Counter, N_{ct}
    Else
    $N_{ct_i} = N^i_{ct_1}$
    End If
End while
while (Signal != BTS) **do**
    If (RTS)
        Identify the Cluster generating data requests
        load sensor set W_c in memory
        Identify the sensors generating requests
        Compare $(W_{c_i}, FlowEntry)$
        If (True)
            Acknowledge Request, CTS
            Allocate UAV to W_{c_i}
            Enable Omni-directional BTS
        Else
            Flag node W_{c_i}
            Proceed to Next Request
        End If
    End If
End while
Start Transmission

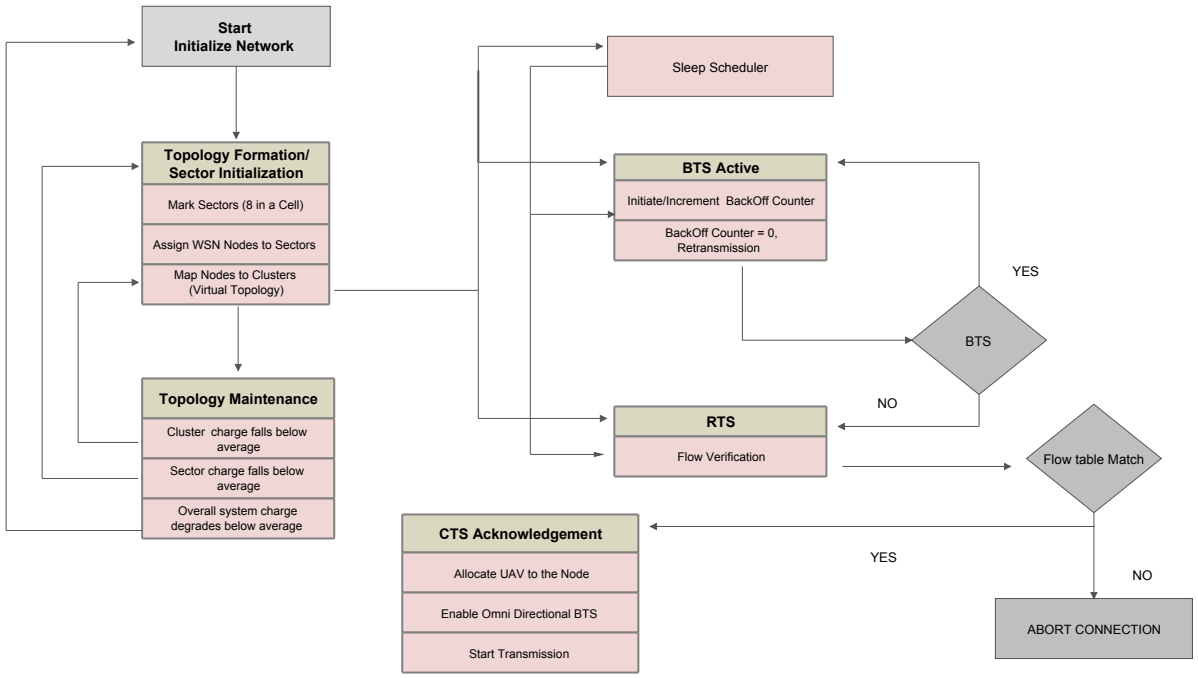


Figure 3.6: An Illustration of the Complete Framework used in the Proposed Approach. Abbreviations: BTS, Busy to Send; CTS, Clear to Send; RTS, Request to Send; UAV, Unmanned Aerial Vehicle.

the proposed framework are done on a model consisting of the SDN controller, base stations, WSN motes, and UAVs by using NS-3 and $Matlab^{TM}$. NS-3 is used to simulate the scenario, algorithms along with the support for SDN modules and recording the data into trace files. The obtained files are then analyzed with $Matlab^{TM}$ by generating the graphs and understanding the traces.

Out of the entire area, the testing is performed on a region of interest with dimensions $50m \times 50m$ and the maximum power of WSN motes being 100 J. For simplicity of the simulations, the initial energy of the UAVs is 2000 J. The total number of UAVs is varied between 2 and 8 (always an even number) in order to perform the scalability test for the proposed model. The radio range of the sensors is within 10 m, and that of the UAV is 500 m in radius. The sensor-to-sensor operations are carried using IEEE 802.11 with 170-m outdoor range. For UAVs, low-power wide-area network (LPWAN) is used with a coverage of 2-km set through a standard communication module with Friis-free space propagation model in NS-3. Table 3.1 lists the values of parameters used for evaluation of the proposed model.

Table 3.1: Parameter Configurations. Abbreviations: RTV, Run Time Value; UAV, Unmanned Aerial Vehicle.

Symbol	Description	Value
d_{WSN}	Charge decay rate	0.0104
C_0	Initial Charge	100
$C(t)$	Charge at time t	RTV
M_{WNode}	Node mean life time	96.15
Z_{WSN}	Minimum charge requirement	5
M_{WSNS}	Mean lifetime of a sector	RTV
M_{WSNC}	Mean lifetime of a cluster	RTV
Z_c	Operable charge range of cluster	RTV
Z_s	Operable charge range of sector	RTV
d_{UAV}	UAV charge decay rate	0.00104
$U(t)$	UAV charge at time t	RTV
Z_{UAV}	UAV minimum charge requirement	50
M_{UNode}	Mean lifetime of UAV	961.54
M_{sys}	Mean lifetime of the system	RTV
Z_{com}	Operable charge range of system	RTV
$C(T_{hf})$	Charge Half life	66.72
G_{nhf}	Random number	$0-4$
B_{max}	Maximum back off counter value	RTV
$n_{avg.hf}$	Average transmission slots	$3000 \times HalfLife$
N_{ct}	Back off counter value	$0 - B_{max}$
D_{tot}	UAV maneuvering distance	Cell Perimeter
S_{tclk}	Total sleep time	RTV
S_{clk}	Sleep timer	RTV
U_s	UAV speed	RTV

The following parameters are used for testing of the model:

i *Throughput:* Throughput is defined as the rate of successful packet delivery over the

channel or data delivered per time slot. In the proposed model, average throughput is measured, and the aim is fixed at achieving a constant and consistent average throughput across the network.

ii *Energy and Lifetime:* Energy depletes constantly with the activity of the system. The model aims at energy conservation by means of applying an easy to operate sleep timer and restricting the number of hops by limiting the transmission between WSN nodes and UAV only. The lifetime of a network is the time through which a network is able to perform the required tasks within specified performance credentials. The proposed model lifetime is evaluated with the constraint of maintaining a constant average throughput above the designated threshold.

iii *Delay:* By definition, it is congestion or link unavailability and is generally considered a measure of the amount of time a signal takes from source to destination. The model aims at limiting the delay to a constant factor by facilitating direct communication between UAV and WSN nodes.

iv *Jitter:* The non-deterministic behavior of the network is outlined by jitter. Delay sensitive models are also sensitive to jitters and can be described as the variation in delay.

v *Latency:* Latency is described in terms of propagation delay and serialization delay, where propagation delay is a function of the distance between the nodes and speed of the carrier, and serialization delay is a function of packet size and transmission rate. The amount of data flowing through a network or a network bottleneck can be visualized as the function of latency and directly affects the throughput of the system irrespective of the technology used.

vi *Packet Delivery Ratio (PDR):* PDR is defined as the ratio of the number of packets successfully delivered to the total packets sent over the network. Throughput serves as an effective measure of performance of a node or a section, but PDR addresses the quality of network design that can lead to poor overall throughput.

The proposed approach is evaluated against the above-defined metrics in comparison with the clustered hierarchical WSNs (CSW) layout [273] and traditional hexagonal cell (TXC)-based WSNs layout [274] approaches. Energy analysis, scalability analysis and performance gains achieved by the SDN controller are also discussed in this section.

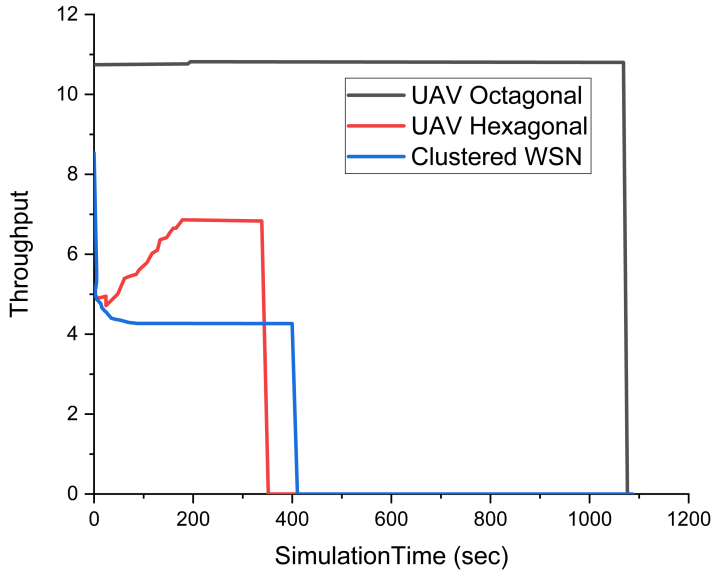
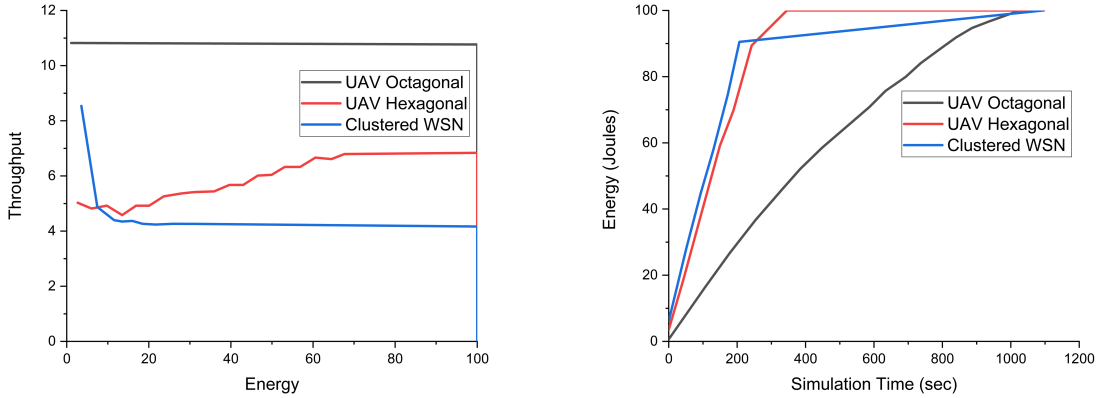


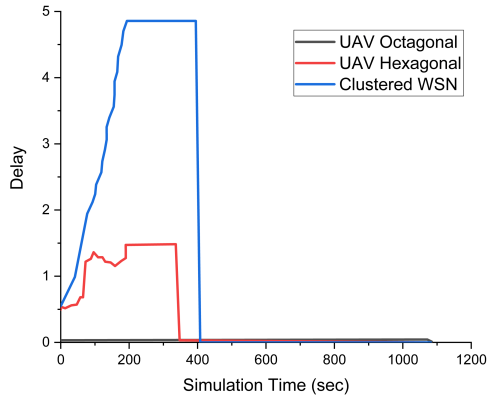
Figure 3.7: Throughput vs Time (Constant Bit Rate). Abbreviations: UAV, Unmanned Aerial Vehicle; WSN, Wireless Sensor Network.



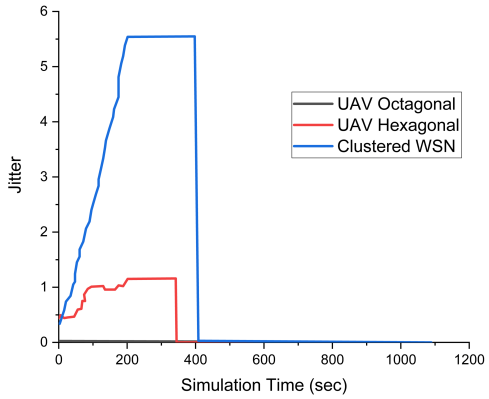
(a) Throughput vs Energy

(b) Energy vs Time

Figure 3.8: Simulation Results (Constant Bit Rate). (a) Throughput vs Energy (b) Energy vs Time. Abbreviations: UAV, Unmanned Aerial Vehicle; WSN, Wireless Sensor Network.

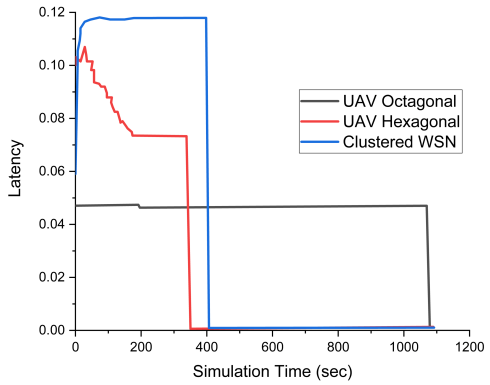


(a) Delay vs Time

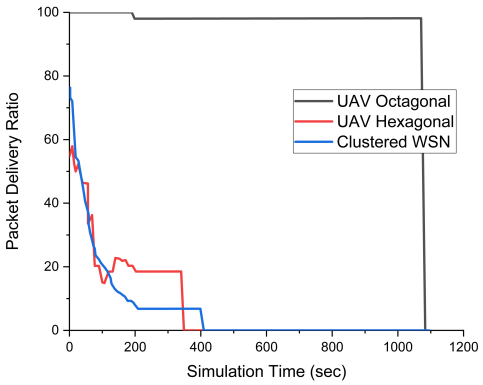


(b) Jitter vs Time

Figure 3.9: Simulation Results (Constant Bit Rate). (a) Delay vs Time (b) Jitter vs Time. Abbreviations: UAV, Unmanned Aerial Vehicle; WSN, Wireless Sensor Network.



(a) Latency Vs Time



(b) PDR vs Time

Figure 3.10: Simulation Results (Constant Bit Rate). (a) Latency vs Time (b) PDR vs Time. Abbreviations: UAV, Unmanned Aerial Vehicle; WSN, Wireless Sensor Network.

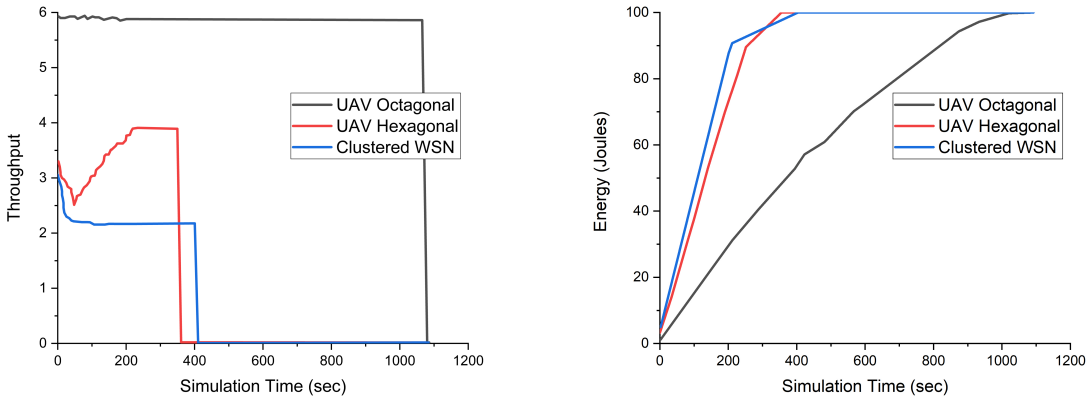
3.3.1 Constant Bit Rate

Simulation results show that the proposed model performs better as it achieves 55% and 36.6% better throughput than CSW and TXC, respectively, as shown in Figures 3.7 and 3.8(a) . The increase in throughput results from the fact that the model restricts sensor nodes from flooding the network with data. Sensor nodes are allowed to send only when the UAV is in range, and there is always one to one communication between the nodes and the UAV instead of multi-hoping resulting in high rates of successful packet delivery.

Sensor nodes are put into sleep mode whenever the sync (UAV) is not in range, unlike CSW and TXC that constantly send packets into the network. As an average measure, a particular sensor node is in the range of UAV only during 25% of the UAV cycle around the cell. A detailed analysis of the proposed approach over the energy model suggests that the proposed approach provides 46.4% and 6.4% better life than the CSW and TXC, respectively, as shown in Figure 3.8(b).

An efficient approach must possess the mandatory characteristic of minimizing the delay. With less number of hops (as sensor nodes communicate directly with the UAV nodes without the involvement of manager nodes) and the nodes trying to send in their specific slots, the proposed approach provides 94% and 28% less delay than the CSW and TXC, respectively, as shown in Figure 3.9(a). The increased number of hops produces uneven delays and the avoidance of uneven delays also affects the overall performance that is a measure of deviation from the true periodic pattern, i.e., jitter. Jitter is reduced by 90% and 16.73% compared with CSW and TXC, respectively, as shown in Figure 3.9(b).

The overall latency of the system, which is effectively a measure of signal travel time from source to destination, plays an important role in the applicability of a model. The system throughput drastically declines with the increase in latency. The system performance degrades as with increasing latency, the packet drop also increases. The efficient sleep timer reduces the packet queue drastically, thus limiting the queuing delays and packet drop count, which in turn, increases the PDR. The back-off counter reduces the contention ratio among the sensor nodes. The distance from the sync is also reduced as the UAV constantly hovers over the sensor nodes. Employing two UAVs in a particular cell also reduces the load on the sync nodes. The proposed model achieves 50% and 16.7% decline in latency with respect to CSW and TXC, respectively, as shown in Figure 3.10(a). The PDR is also improved by 86% and 76% compared with CSW and TXC, respectively, as shown in Figure 3.10(b).



(a) Throughput vs Time

(b) Energy vs Time

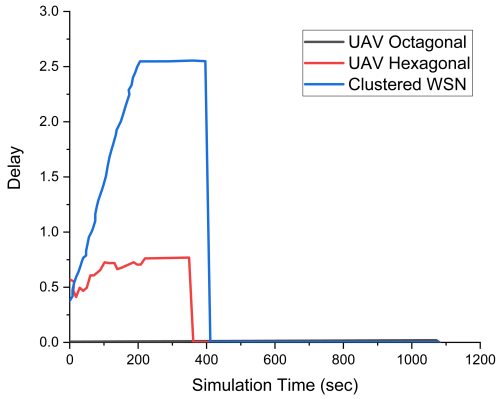
Figure 3.11: Simulation Results (Variable Bit Rate). (a) Throughput vs Time (b) Energy vs Time Abbreviations: UAV, Unmanned Aerial Vehicle; WSN, Wireless Sensor Network.

Table 3.2: Average Percentage Improvement by the Proposed Approach in Comparison with CSW and TXC.

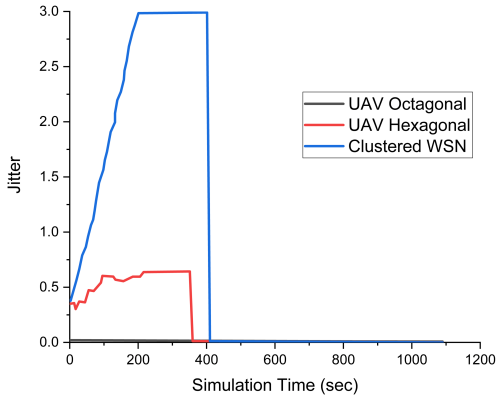
Metrics	Constant Bit rate		Variable Bit Rate	
	CSW	TXC	CSW	TXC
Throughput	55%	36.6%	59.7%	31.4%
Energy	46.4%	6.4%	58.33%	8.33%
Delay	94%	28%	79.97%	16.67%
Jitter	90%	16.73%	93.3%	16.67%
Latency	50%	16.7%	60%	7%
PDR	86%	76%	80%	65%

3.3.2 Variable Bit Rate

The proposed approach is also tested with a variable bit rate (VBR). The VBR is achieved by means of permutation, the bit rate is maneuvered dynamically during the simulation process. The proposed model achieves throughput better than CSW and TXC with an improvement of 59.7% and 31.4%, respectively, as shown in Figure 3.11(a). At the same time, improved energy efficiency, ie, 58.33% and 8.33% better than CSW and TXC, respectively, as shown in Figure 3.11(b). Delay, jitter, and latency are improved by 79.97% and 16.67%, 93.3% and 16.67%, and 60% and 7%, respectively, as shown in Figure 3.12(a),(b) and 3.13(a). PDR is improved by 80% and 65% in comparison with CSW and TXC, respectively, as in Figure 3.13(b). Table 3.2 presents the detailed percentage improvement by the proposed approach in comparison with CSW and TXC, for both constant bit rate (CBR) and VBR.

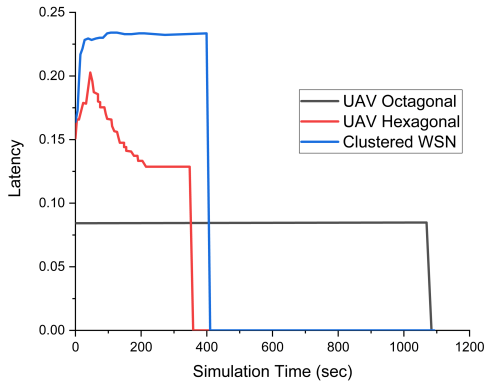


(a) Delay vs Time

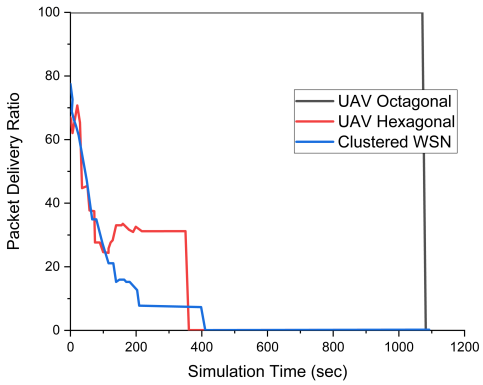


(b) Jitter vs Time

Figure 3.12: Simulation Results (Variable Bit Rate). (a) Delay vs Time (b) Jitter vs Time. Abbreviations: UAV, Unmanned Aerial Vehicle; WSN, Wireless Sensor Network.



(a) Latency vs Time



(b) PDR vs Time

Figure 3.13: Simulation Results (Variable Bit Rate). (a) Latency vs Time (b) PDR vs Time. Abbreviations: UAV, Unmanned Aerial Vehicle; WSN, Wireless Sensor Network.

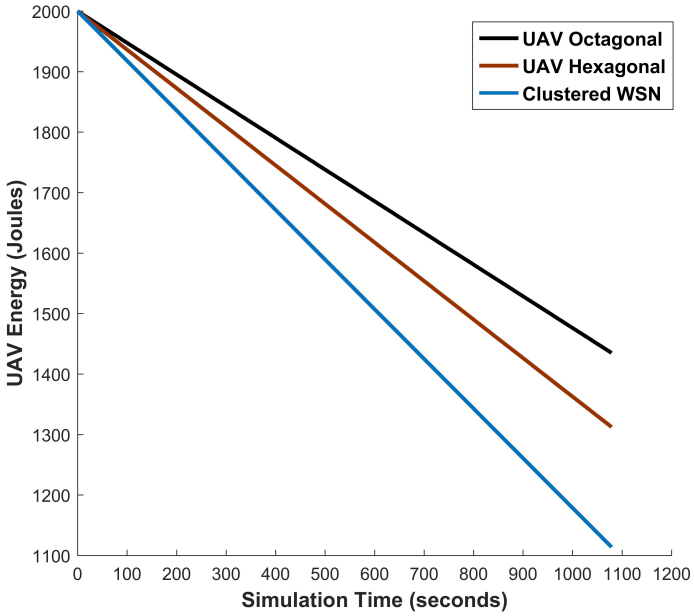


Figure 3.14: Available Energy vs Time. Abbreviations: UAV, Unmanned Aerial Vehicle; WSN, Wireless Sensor Network.

3.3.3 Energy Consumption

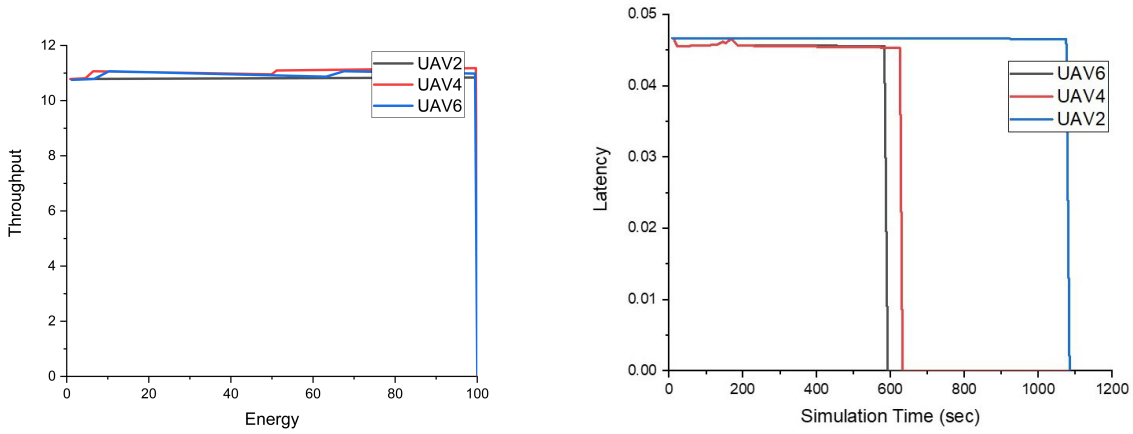
The WSN nodes are battery-powered low computational devices whose frequent replacement and recharging are not always possible, and WSNs have the tendency of frequently running out of power. The approach includes an SDN controller, efficient maneuvering, data collection, and transmission scheme that facilitates higher battery life of WSN nodes and fewer transmission overheads. The back-off counter and sleep timer also add to the overall network lifetime and performance. Whereas UAVs can be frequently replaced and charged as they can always return to the base station. The approach follows a constantly monitored mechanism to facilitate the underlying battery powered WSN nodes with UAVs as relays. The UAVs are also used for relaying in hexagonal and clustered approaches. The relays (UAVs) are mainly responsible for transmitting/receiving data and control packets. Thus, all three approaches follow a smooth gradient decline of the available energy, as shown in Figure 3.14. These results suggest that the proposed approach saves 71.74% of the average battery life in comparison with CSW and TXC that show a decline of 22.37% and 8.54% in the available energy, respectively.

An SDN controller, which resides at the base station, is responsible for installing the flow entries on the designated UAV. One relay entry requires only one control packet, whereas the other approaches are required to find the best path themselves by means of multi-hopping. The easy installation of relays helps conserve the UAV energy in the proposed

approach. The proposed approach boasts the highest PDR that translates directly to a smaller number of retransmissions, which are required if every WSN node can transmit without a good back-off counter. The proposed approach is able to save UAV energy by constraining frequent retransmissions.

3.3.4 Scalability Analysis

The scalability and resilience of the proposed approach are tested by varying the number of UAVs between 2 and 6 in the system and testing it with different bit rates, ie, 10, 20, 30, and 40 kbps. At 10 kbps, all the systems perform within close proximity of each other with a marginal difference in throughput and latency, with 6 UAVs system depleting its energy first followed by four-UAV system and two-UAV system. The order of energy depletion comes from the fact that more UAVs in the system cause more sensor sectors to be active at the same time. Thus, after a certain operational time, the system requires a re-initialization, thus consuming more energy. Further, the 6 UAVs system offers more delays than 4 UAVs and 2 UAVs systems. The ascending order of delays comes from the fact that more UAVs in the system force more active sensors; thus, more packets in the system, which in turn, causes an increased length of queues that elongates the waiting time and dropped packets, causing delays, jitters, and decrease in PDR as shown in Figures 3.15, 3.16 and 3.17.

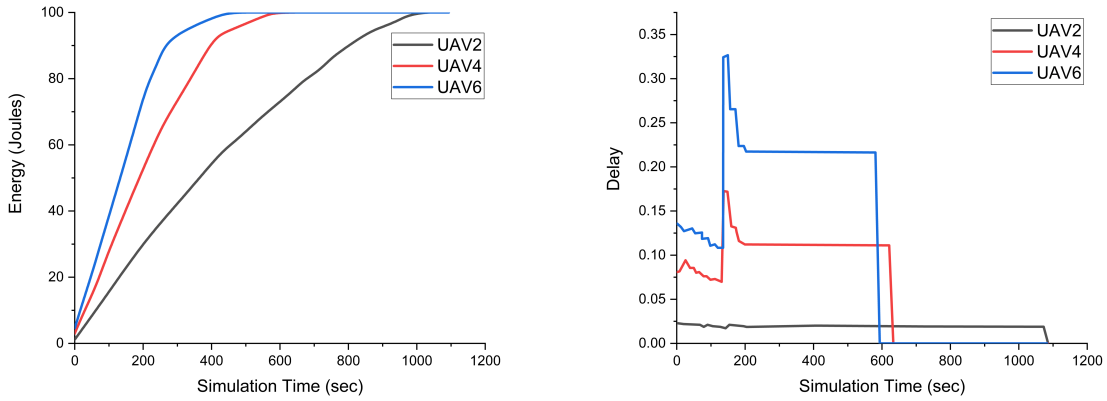


(a) Throughput vs Energy

(b) Latency vs Time

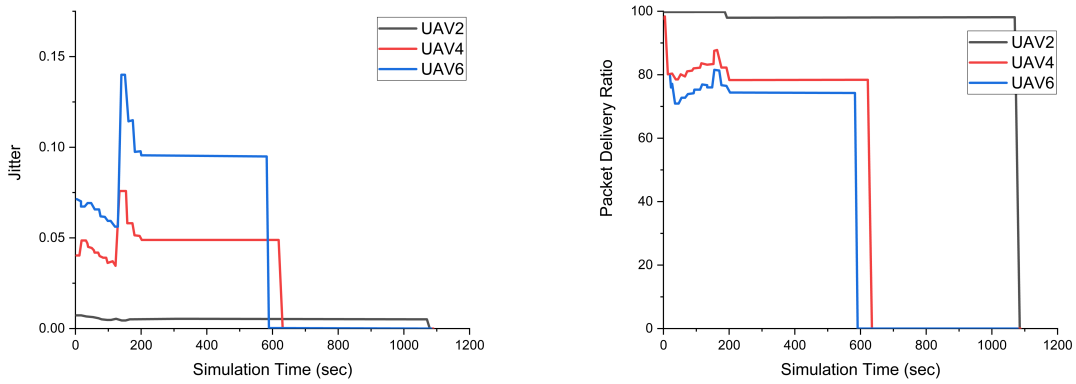
Figure 3.15: Performance Evaluation at 10 kbps by Varying the Number of Unmanned Aerial Vehicles (UAVs). (a) Throughput vs Energy (b) Latency vs Time.

The increase in bit rate ($2x$, $3x$, or $4x$) only has a minimum noticeable impact on delay and jitter. Delay and jitter are affected jointly by the increase in bandwidth as well as with an increase in the number of available transmission slots, as more nodes try to initiate



(a) Energy vs Time (b) Delay vs Time

Figure 3.16: Performance Evaluation at 10 kbps by Varying the Number of Unmanned Aerial Vehicles (UAVs). (a) Energy vs Time (b) Delay vs Time.

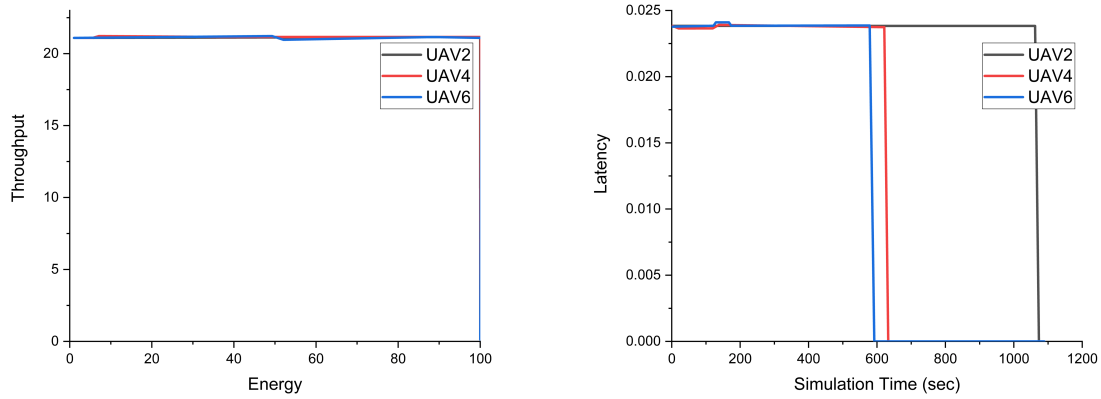


(a) Jitter vs Time (b) PDR vs Time

Figure 3.17: Performance Evaluation at 10 kbps by Varying the Number of Unmanned Aerial Vehicles (UAVs). (a) Jitter vs Time (b) PDR vs Time.

transmission that effects waiting time. Figures 3.18 to 3.26 present the performance evaluation results with CBR 20, 30, and 40 kbps, respectively. The results prove that the system is free from congestive collapse and the performance of the system stays consistent and delivers high average throughput and average latency rates.

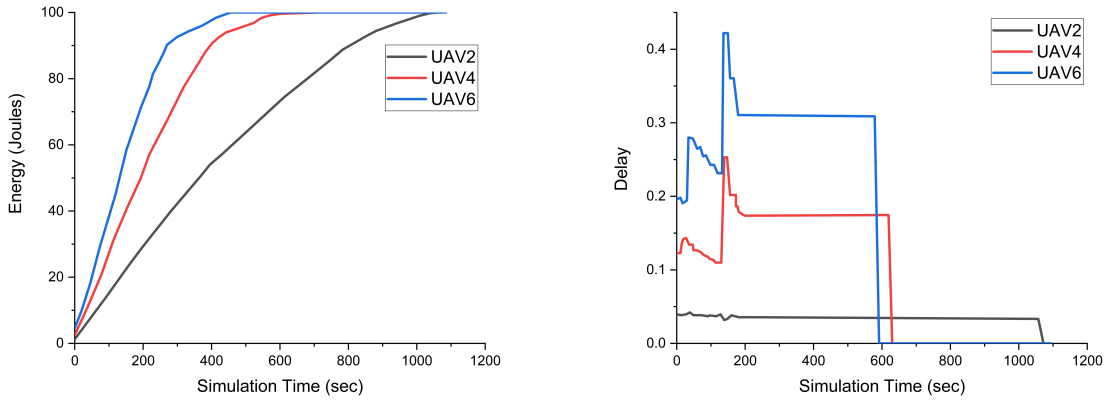
An efficient algorithm is required to manage the system as only increasing the system resources leads to a sudden decline in the overall performance of the system. The SDN controller that monitors the system dynamically adapts to the condition and manages the sleep timer and back-off counter, which effectively makes the overall system scalable and resilient to failures in case of over-stressed conditions. The controller also updates



(a) Throughput vs Energy

(b) Latency vs Time

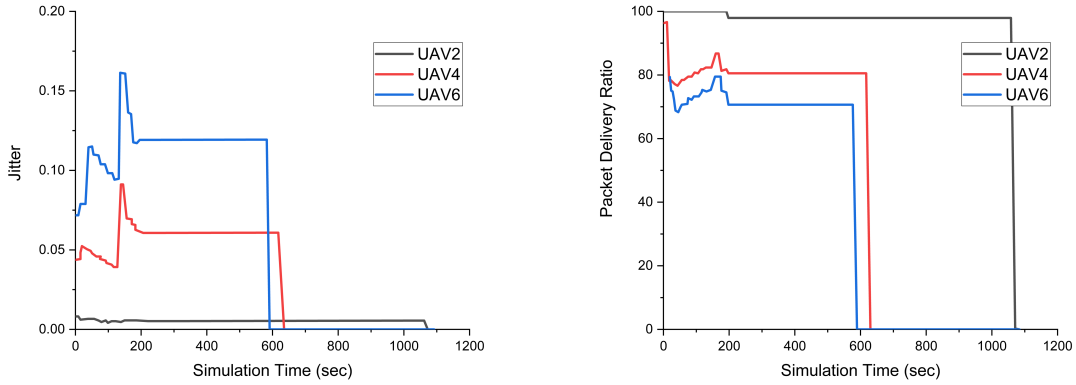
Figure 3.18: Performance Evaluation at 20 kbps by Varying the Number of Unmanned Aerial Vehicles (UAVs). (a) Throughput vs Energy (b) Latency vs Time.



(a) Energy vs Time

(b) Delay vs Time

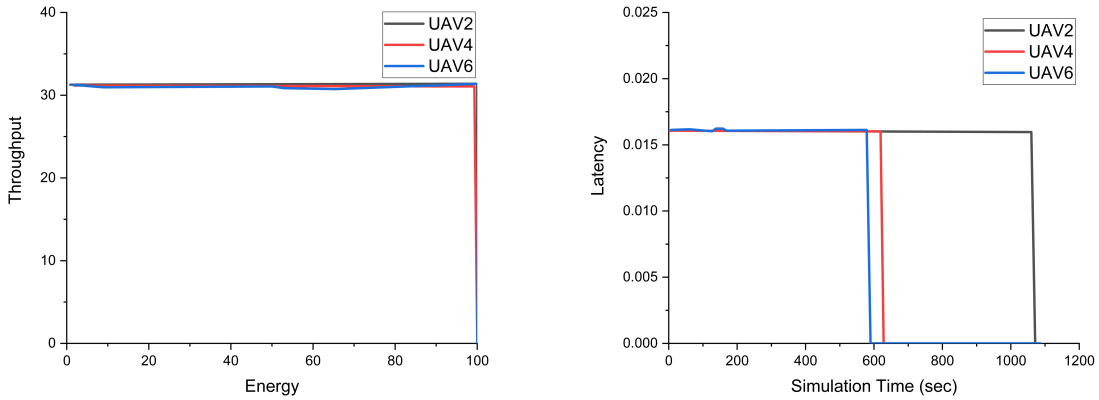
Figure 3.19: Performance Evaluation at 20 kbps by Varying the Number of Unmanned Aerial Vehicles (UAVs). (a) Energy vs Time (b) Delay vs Time.



(a) Jitter vs Time

(b) PDR vs Time

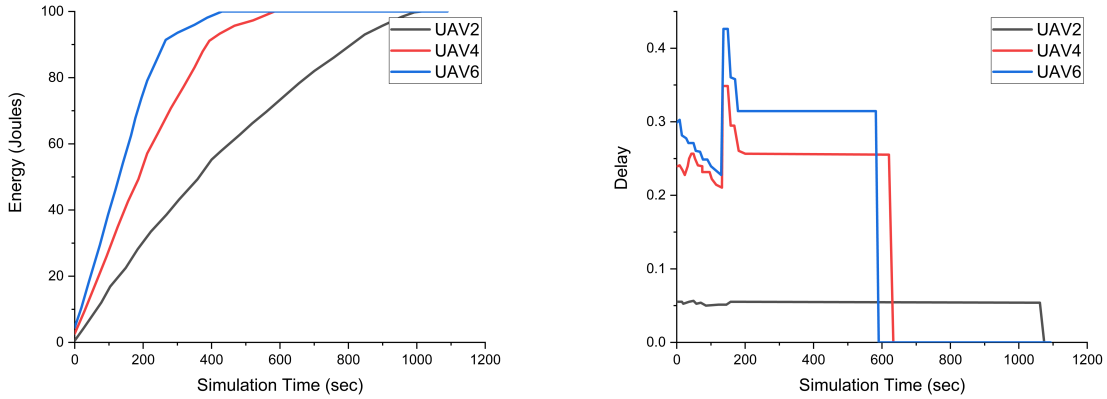
Figure 3.20: Performance Evaluation at 20 kbps by Varying the Number of Unmanned Aerial Vehicles (UAVs). (a) Jitter vs Time (b) PDR vs Time.



(a) Throughput vs Energy

(b) Latency vs Time

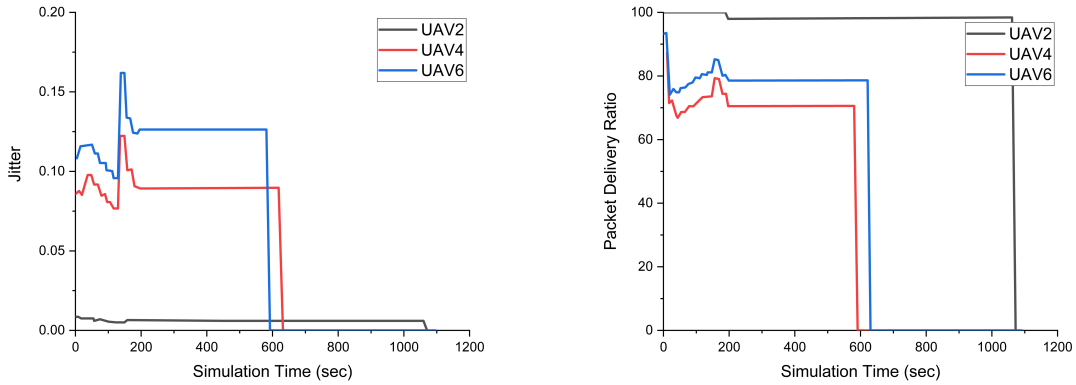
Figure 3.21: Performance Evaluation at 30 kbps by Varying the Number of Unmanned Aerial Vehicles (UAVs). (a) Throughput vs Energy (b) Latency vs Time.



(a) Energy vs Time

(b) Delay vs Time

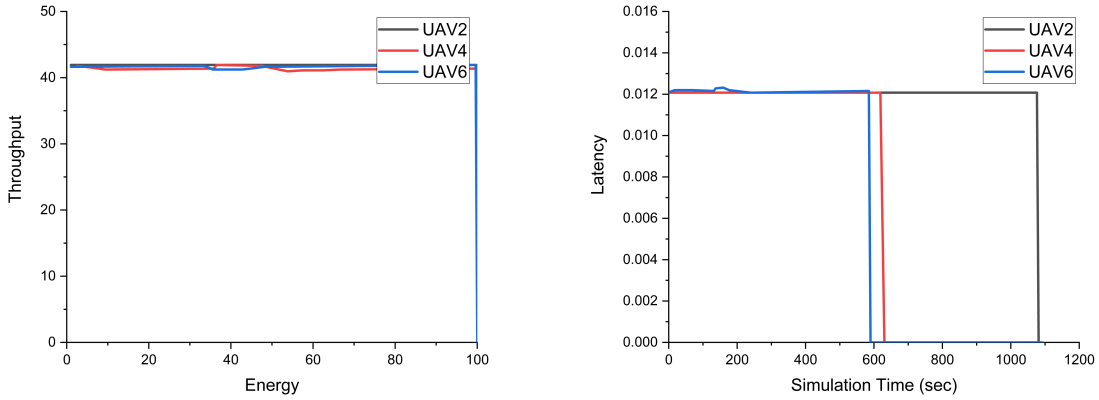
Figure 3.22: Performance Evaluation at 30 kbps by Varying the Number of Unmanned Aerial Vehicles (UAVs). (a) Energy vs Time (b) Delay vs Time.



(a) Jitter vs Time

(b) PDR vs Time

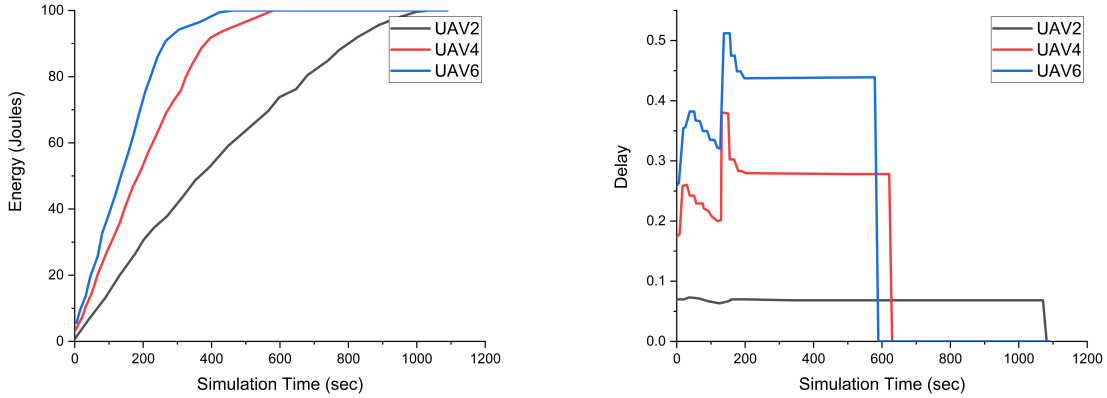
Figure 3.23: Performance Evaluation at 30 kbps by Varying the Number of Unmanned Aerial Vehicles (UAVs). (a) Jitter vs Time (b) PDR vs Time.



(a) Throughput vs Energy

(b) Latency vs Time

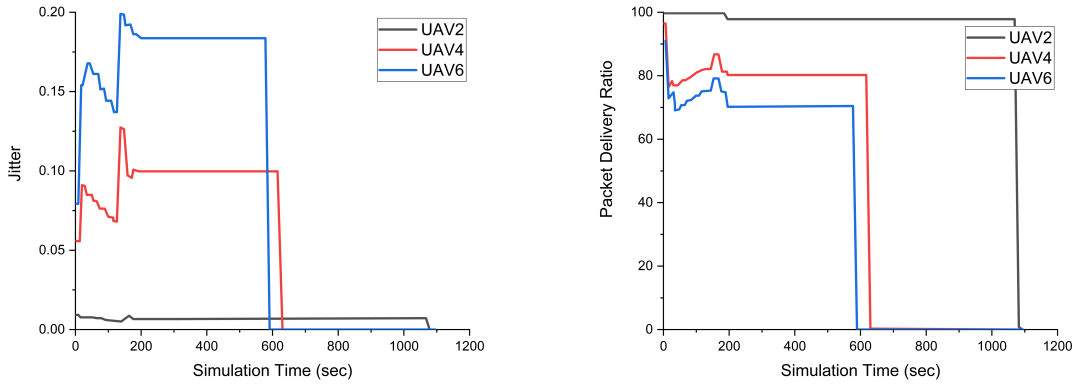
Figure 3.24: Performance Evaluation at 40 kbps by Varying the Number of Unmanned Aerial Vehicles (UAVs). (a) Throughput vs Energy (b) Latency vs Time.



(a) Energy vs Time

(b) Delay vs Time

Figure 3.25: Performance Evaluation at 40 kbps by Varying the Number of Unmanned Aerial Vehicles (UAVs). (a) Energy vs Time (b) Delay vs Time.



(a) Jitter vs Time

(b) PDR vs Time

Figure 3.26: Performance Evaluation at 40 kbps by Varying the Number of Unmanned Aerial Vehicles (UAVs). (a) Jitter vs Time (b) PDR vs Time.

Table 3.3: Variations in Results of the Proposed Approach with and without the use of SDN Controller. Abbreviation: SDN, Software Defined Network.

Scenarios	**Latency**	**Jitter**	**Delay**	**Throughput**
Maximum Scale	0.12 s	6 s	5 s	12kbps(sensors)
Without SDN	0.067 s Latency percentage: 55.83%	1.1 s Jitter percentage: 18.30%	1.4 s Delay percentage: 28.00%	6.4 kbps(sensors) Throughput percentage: 53.30%
With SDN	0.049 s Latency percentage: 40.83%	0.1 s Jitter percentage: 1.60%	0.1 s Delay percentage: 2.00%	10.4 kbps(sensors) Throughput percentage: 86.60%

about nodes and clusters that are allowed to send, thus avoiding waiting time, dead transmissions, and long buffer queues. The overall system evaluation states a considerable performance improvement over CSW and TXC architectures.

The details on the variations in outcomes from using SDN in the proposed approach are compared with a scenario without the use of SDN, as shown in Table 3.3.

3.4 Conclusion

Data dissemination in collaborative networks requires careful planning and execution. The constantly changing topology, uneven delays, in-coordinated sleeping, and relaying wastes power and network resources. A novel data dissemination approach for UAV coordinated WSNs is proposed in this chapter. The UAVs act as relays between the sensor nodes and the base station. The SDN controller manages and configures the

topology and takes care of sleep timers and counters. The proposed approach is tested against CSW layout and TXC layout over various metrics. Analyses prove that the proposed approach is capable of providing better throughput and an enhanced lifetime. The approach also minimizes delays and jitters and improves the PDR.

Chapter 4

Mobility and Trajectory Aware Data Dissemination [2]

Mobility model defines a movement scheme which mimics the real world movements, traffic and response scenarios. One key characteristic of a good mobility model is its ability to adapt to the dynamically changing network behavior [275]. In order to test protocols, real-time scenarios, reconnaissance and surveillance paradigms or disaster management practices, simulations serve as a major test bed. To adapt to the real-time traffic and realistic environment conditions, the mobility model must be able to represent a realistic scenario. The major vehicular mobility models are classified as synthetic, survey-based, trace-based and traffic simulation-based models. Synthetic models include the mathematical representation of the realistic scenarios, whereas survey based models are derived from the movement surveys conducted by authoritative organizations.

Trace-based models are built over real-time mobility traces. Trace based models are preferred over both survey and synthetic models as it is not always possible to devise a mathematical representation of the mobility or conduct a survey in order to gather information. Simulation-based models are characterized by the near realistic simulated behavior [275]. The coordination between aerial and ground nodes is characterized by the erratic and dynamic behavior of the networks. Vehicular models like synthetic, survey and simulation-based approaches do not suffice as the inherent inconsistencies of the erratic network behavior hinder the overall mathematical formulation of the scenario as well as the survey and simulation of every single scenario is not feasible. Trace-based models do not suffice under disaster conditions, military applications, and unforeseen events. In order to entertain the collaborative network formation, a mobility model is required that understands the overall dynamic nature of the network and can react to ever-changing topological conditions.

This chapter presents a novel mobility based data dissemination framework for multi-UAV ad hoc networks. The proposed framework takes into account the average transmission density for setting up the way-points for UAV movements. The way-points are configured

[2] Mohd. Abuzar Sayeed, Rajesh Kumar, *"An Efficient Mobility Model for Improving Transmissions in Multi-UAVs Enabled WSNs"*, Drones, MDPI, August (2018). [Published]

in order to increase the coverage by efficient deployment of aerial nodes and reduced multi-hopping transmissions. Further, the framework is extended to incorporate a Software Defined Network (SDN) controller for secure communications between Multi-UAV and WSNs.

4.1 Mobility Model for Improving Transmissions with Multiple UAVs

Multi-UAV enabled WSNs prove to be of considerable advantage, but, at the same time, require careful selection of the metrics. A random choice of way-points or a scheme that restricts UAV to a fixed particular topology leads to poor coverage and node starvation. Clustering techniques are helpful to prevent long-range broadcasting, collisions, and multi-hopping, but a large number of clusters in a geographical region prevent every node from getting an equal opportunity as well as increasing the waiting time. Strategically important locations can range from dense to scarce based on the number of active nodes. Developing attraction metrics from node density and message relay timings can help in topographic UAV movements and prevent loss of important information.

The proposed system model incorporates an efficient UAV movement technique that increases the coverage as well as provides reliable data dissemination. A scheme for clustering and head selection that provides every node with an opportunity to transmit as well as prevent the overhead communication between the cluster head and the node whenever UAV is in the range, is also presented. The stand-alone regions which are not in range of UAV, are also provided with a mechanism to transmit whenever they have data to send.

The framework starts off by disintegrating entire communication topology into dense and scarce sections. The disintegration is achieved on the basis of average transmission density of the topology under consideration. For the purpose of data aggregation an implicit self clustering technique is adopted. The densely and scarcely populated regions alongside self clustering serves the basis of UAV way-point selection. Modified Dijkstra's Single Source Shortest Path algorithm, where edge weights are calculated on the basis of average transmission density (attraction factor), providing preference to the strategically important locations, is adopted for path generation of the aerial nodes. The major advantage of the proposed approach is in its simplicity as it does not require any special configurations. It employs the existing hardware, software and available specifications in a more effective and efficient manner.

4.1.1 Proposed Approach

4.1.1.1 System Model

The proposed approach aims at improving the coverage and reliability of multi-UAV enabled WSN. The technique provides a novel self-clustering technique and a novel technique for setting way-points for UAV movements. The network is comprised of UAV, WSN nodes and a base station. The UAVs act as a relay between sensor nodes and the base station. The topology is classified as dense, scarce, and scarce but in proximity of the base station. The division is strictly based on network characteristics according to the frequency of transmissions recorded in a particular region. The scarce regions are effectively those regions which are not strategically important. Also decaying charge of sensor nodes lead to the formation of scarce regions. The overall geography can be visualized as a matrix with row-column coordinates serving as the way-points for successive UAV banks. Figure 4.1 presents a detailed view of the system model.

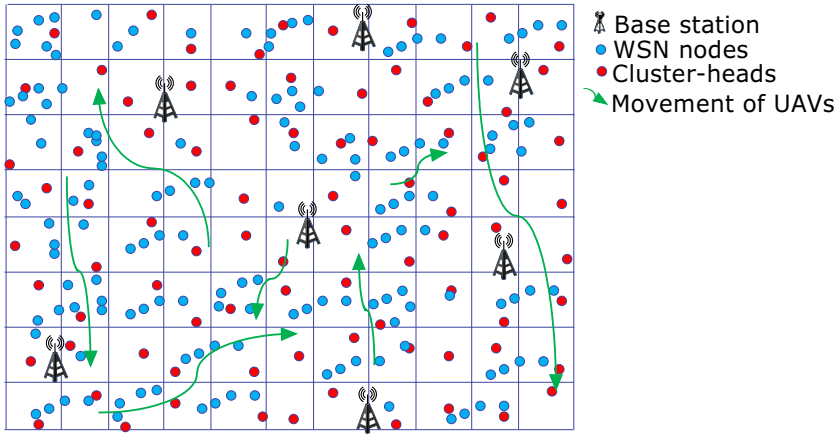


Figure 4.1: System Model: Mobility Model for Improving Transmissions in Multi-UAVs Enabled WSNs. Abbreviations: UAV, Unmanned Aerial Vehicle; WSN, Wireless Sensor Network.

The static WSN nodes are randomly deployed over a certain geography of area $|D|$, which is a subset of the Euclidean space R^d, according to the Poisson distribution, where a node k can transmit anytime. k belongs to the Set (WSN) of the wireless sensor nodes. Each node k can transmit messages x according to Equation 4.1:

$$P(x) = \frac{e^{-\lambda|D|}\lambda|D|^x}{x!}. \tag{4.1}$$

Here, λ is defined as the likelihood parameter that estimates the average expected transmissions by a set of WSN nodes and is given by Equation 4.2:

$$\lambda = \frac{1}{n} \sum_{i=1}^{n} k_i, \tag{4.2}$$

where, n is the number of WSN nodes, $k_i = 0, 1, 2, 3.....i$ and $i = 0, 1, 2, 3.....n$ are the observed occurrences of a transmission.

The overall area is marked in the form of successive checks with the base station placed in any of the square or at the edge of the geography. The base station is capable of accepting direct communication from the WSN nodes as well as the transmissions occurring from the UAVs, acting as a relay between base station and the ground nodes.

The aerial vehicles that are effectively serving as relays move from one dense region to another accepting the transmissions from the nodes lying in these regions as well as the regions falling in the path between two successive banks of the UAV. The UAV is equipped with two antennas. One omni-directional antenna is responsible for sensing the underlying topology for incoming transmissions and broadcasting the messages regarding the availability of the UAV in a specific region. The other bi-directional antenna provides the channel for incoming and outgoing transmissions. During transmission phase, the omni-directional antenna is used for broadcasting a blocking message for other WSN nodes. The scarce regions that do not directly fall under the UAV antennas facilitate transmission by multi-hopping towards the base station or the cluster head of adjacent dense region. Table 4.1 provides a description to the symbols used for explaining the system model. The next subsection describes the proposed approach in detail.

4.1.1.2 Mobility Model

The proposed approach initiates by grouping together the ground nodes into clusters and then segregating them on the basis of dense and scarce. The density of a particular cluster is associated with the number of transmissions originating from the cluster in a given time interval. As the UAV banking is based on the coordinates of the particular row-column of the subdivided area matrix, the square space as a whole is considered to be one cluster. The WSN nodes falling into a particular sector (block of the matrix) are considered by default into the same cluster. Equation 4.3 outlines the cluster head selection process, where H^d is the average one hop distance. Equation 4.4 gives the metric calculation for a single node:

$$Min(H_d), \tag{4.3}$$

$$H_{d_i} = \frac{\sum_{i=1}^{C_n} D_{hop}}{C_n}, \tag{4.4}$$

Table 4.1: Symbol Table.

Symbol	**Description**
H_d	Average One Hop Distance
R_T	Number of Transmission per Unit Time
S_i	Number of Nodes Transmitting per Unit Time
C_n	Number of Nodes in a Sector/Square/Region
S_a	Sector Area
R_{T_sys}	Number of Transmissions per Unit Time in the System
S_{i_sys}	Number of Nodes Transmitting per Unit Time in the System
C_{n_sys}	Number of Nodes in the System
S_{a_sys}	Overall System Area
$\mathcal{T}_{A,area}$	Average number of Transmissions in a Self Cluster
$\mathcal{T}_{A,system}$	Average number of Transmissions in Overall System
F_A	Attraction Function of a Sector/Square/Region
F_{A_sys}	Attraction Function for the Overall System
$\mathcal{W}_e$	Edge Weight
$\mathcal{W}_{e+}$	Normalized Edge Weight
D_b	Average Hops Towards Base Station
D_d	Average Hops Towards Neighbouring Dense Sector/Square/Region

where H_{d_i} is the node under consideration, D_{hop} are one hop distance from the node under consideration, given that the node coordinates lie within (c, x_i, y_i), (c, x_j, y_j), (c, x_k, y_k),(c, x_l, y_l) i.e. within the same sector, where c_i is the base station, and C_n is the number of nodes in the self-cluster.

The transfer between UAV and sensor nodes always happens through the cluster-head, with the condition of Head Swap. The nodes with data, forward this data towards their cluster head where data is accumulated. When UAV is in range of the cluster head, the Head Swap occurs. UAV becomes the cluster head of the sector to facilitate transfer not only from the designated cluster head, but also allows the cluster members to send data directed towards the UAV.

The UAV way-points are set in a way that it moves from one dense cluster head towards another dense cluster head. UAV way-points are decided on the basis of transmission

density and distance. Equation 4.5 defines the calculation of attraction function F_A by means of transmission density:

$$F_A = \sqrt{\left(\frac{R_T}{S_i}\right) \times \left(\frac{C_n}{S_a}\right)}, \tag{4.5}$$

where, R_T is the number of transmissions per unit time in a sector, S_i is the number of nodes transmitting per unit time in a given sector, C_n is the number of nodes in a sector and S_a is the sector area.

Similarly, the $F_{A_{sys}}$ for the whole system is calculated according to Equation (4.6):

$$F_{A_{sys}} = \sqrt{\left(\frac{R_{T_{sys}}}{S_{i_{sys}}}\right) \times \left(\frac{C_{n_{sys}}}{S_{a_{sys}}}\right)}, \tag{4.6}$$

where, $R_{T_{sys}}$ is the number of transmissions per unit time in the whole system, $S_{i_{sys}}$ is the number of nodes transmitting per unit time, in the system, $C_{n_{sys}}$ is the number of nodes in the system and $S_{a_{sys}}$ is the overall area.

The average number of transmissions in a given area or square which is effectively a self-cluster and the overall average transmissions in the system are given by Equations (4.7) and (4.8):

$$\mathfrak{T}_{A,area} = \frac{\sum_i^{C_n} \left(\frac{R_T}{C_n}\right)}{C_n}, \tag{4.7}$$

$$\mathfrak{T}_{A,system} = \frac{\sum_i^{C_{n_{sys}}} \left(\frac{R_{T_{sys}}}{C_{n_{sys}}}\right)}{C_{n_{sys}}}, \tag{4.8}$$

where $\mathfrak{T}_{A,area}$ and $\mathfrak{T}_{A,system}$ are the average number of transmissions in a self-cluster and overall system, respectively.

The inequality in Equation 4.9 identifies the dense clusters from the scares ones. The clusters lying on the left side of the inequality are considered to be dense clusters, whereas the clusters lying on the right side of the inequality are considered to be scarce clusters. Algorithm 4.1 details the complete topology formation mechanism. The algorithm follows

an implicit cluster selection and marking procedure. Cluster selection and marking takes O(n) time. Attraction factor and transmission density calculation costs $O(n^2)$ time. Dense-scarce identification and link cost estimation takes $O(n^2)$ time. Where n is the number of active ground nodes.

$$\Im_{A,area} \leq F_A < \Im_{A,system}. \tag{4.9}$$

The model uses a modified version of Dijkstra's Single Source Shortest Path algorithm where edge weights are given by Equations (4.10) and (4.11):

Algorithm 4.1 Topology Formation

1: Start
2: **Input**: Set of WSN Nodes W_i
3: **Initialize Network**
4: **Mark sensor nodes to a sector w.r.t** (c, x_i, y_i), (c, x_j, y_j), (c, x_k, y_k),(c, x_l, y_l)
5: **Cluster Head selection of a square** $\longrightarrow Min(H_d)$
6: $H_{d_i} = \frac{\sum_{i=1}^{C_n} D_{hop}}{C_n}$
7: **Calculate Attraction Factor**
8: $F_A = \sqrt{\left(\frac{R_T}{S_i}\right) \times \left(\frac{C_n}{S_a}\right)}$
9: $F_{A_{sys}} = \sqrt{\left(\frac{R_{T_{sys}}}{S_{i_{sys}}}\right) \times \left(\frac{C_{n_{sys}}}{S_{a_{sys}}}\right)}$
10: **Calculate average transmissions**
11: $\Im_{A,area} = \frac{\sum_i^{C_n} \left(\frac{R_T}{C_n}\right)}{C_n}$
12: $\Im_{A,system} = \frac{\sum_i^{C_{n_{sys}}} \left(\frac{R_{T_{sys}}}{C_{n_{sys}}}\right)}{C_{n_{sys}}}$
13: **Identify dense and scarce clusters**
14: Dense $\longrightarrow \Im_{A,system} \leq F_A$
15: Scarce $\longrightarrow F_A < \Im_{A,system}$
16: Calculate link costs $\longrightarrow \mathcal{W}_e = \sqrt{\left(\frac{\sum_i^{C_n} \left(\frac{R_T}{C_n}\right)}{C_n} - \frac{\sum_i^{C_{n_{sys}}} \left(\frac{R_{T_{sys}}}{C_{n_{sys}}}\right)}{C_{n_{sys}}}\right)^2}$
17: **Normalize Link Cost**
18: $\mathcal{W}_{e+} = \frac{1}{F_{A_{sys}} - \mathcal{W}_e}$
19: Exit
20: End

$$\mathcal{W}_e = \sqrt{\left(\frac{\sum_i^{C_n} \left(\frac{R_T}{C_n}\right)}{C_n} - \frac{\sum_i^{C_{nsys}} \left(\frac{R_{T_{sys}}}{C_{n_{sys}}}\right)}{C_{n_{sys}}}\right)^2}, \tag{4.10}$$

$$\mathcal{W}_{e+} = \frac{1}{F_{A_{sys}} - \mathcal{W}_e}, \tag{4.11}$$

where, $\mathcal{W}_e$ is the edge weight and $\mathcal{W}_{e+}$ are the normalized edge weights used by the $SSSP$ algorithm. Algorithm 4.2 details the complete UAV path generation mechanism. UAV path generation costs $O(n^2)$ time, where n is the number of sector marked dense by Algorithm 4.1.

Algorithm 4.2 UAV Path Generation

```
Initialize D_bs = 0 , Path = []
while w_q do                    w_q ⟶ queueofclusterheads
    Select cluster head C_i with min W_{e+_i}
    D_bs = W_{e+_i}
    for Every_Neighbor C_j of C_i do
        Calculate D_j
                D_j = W_{e+_i} + W_{e+_{i→j}}
        if D_j < W_{e+_j} then
            D_bs = D_j
        End If
    End For
    Path = C_i → C_j
    Return Path, D_bs
End while
Exit
End
```

The densely populated sectors are serviced by UAV maneuvers directly along with the sectors which fall in line with two consecutive UAV banks. The scarce sectors that don't fall in the path of UAV are the designated Lone sectors. Lone sectors send hello packets towards nearby dense regions and the base station when the network is initialized. The purpose of the hello packets is to determine the number of active nodes in the region and number of hops required to reach dense sector and base station, respectively. Cluster heads belonging to the lone sectors forward packets towards the base station when the inequality in Equation 4.12 is satisfied; otherwise, packets are forwarded towards dense regions of the geographical area:

$$\mathcal{D}_b \leq \mathcal{D}_d, \tag{4.12}$$

where $\mathcal{D}_b$ and $\mathcal{D}_d$ are the average number of hop counts from the base station and nearest dense cluster, respectively. Algorithm 4.3 is responsible for the control and coordination of data transmission originating from lone sectors. Hop sorting takes $O(n^2)$ time, where n is the is the number of active nodes from scarce sectors. Transmission costs $O(n^2)$ time.

The complete Mobility Model alongside cluster and way-point selection is underlined in Algorithm 4.4. Algorithm 4.4 on initiation calls Algorithm 4.1, which deals with cluster head selection and overall topology formation. The algorithm further identifies the regions as dense and scarce. The link costs that are further used for deciding the UAV traversal routine are also determined by the Algorithm 4.2. The UAV path is generated by the

Algorithm 4.3 Data Transmission: Lone Sectors

```
Node from Lone sector
Identify Neighboring dense sectors.
Broadcast "Hello" ← Estimate Hop Count
Sort clusters, base station in Order of Hop Count.
while Node with data do
    Select Optimal Cluster or Base Station
    if Node With Data then
        transmit
    else
        Select next optimal Cluster or Node
     End If
     Iterate till Node with data = FALSE
End While
Exit
End
```

Algorithm 4.4 Proposed Approach

```
Initialize Algorithm
Topology Formation ();
UAV Path Generation ();
Data Transmission ();
Data Transmission Lone Regions ();
Exit
End
```

Algorithm 4.3.

4.1.2 Performance Evaluation

The proposed technique relies heavily on, as well as exploits, the movement characteristics of UAV in order to achieve significant gains over the already existing models. The evaluation and testing of the approach are done on a model consisting of the base station, WSN motes and the UAVs serving as relays by using NS-3 (version $ns - 3.28$, NSNAM, Washington, DC, USA) and $Matlab^{TM}$ (version $R2018a$ Online Licence, MathWorks, Natick, MA, USA). The testing is performed on a 1200×1200 m^2 area. Table 4.2 lists the detailed simulation settings for the proposed model.

Table 4.2: Simulation Settings.

Simulation Settings	**Values**
Ground Nodes	100
UAV	1
Ground Node Type	Static WSN
Area	1200×1200 m^2
WSN-WSN Communication	IEEE 802.11, Direct Sequence Spread Spectrum (DSSS) Rate 1 Mbps
WSN UAV Communication	Low Power Wide Area Network (LPWAN), 2 km Line of Sight Transmission
Propagation Loss Model	Fiss Propagation Loss Model
Packet Size	512 bytes
Data Rate	5120 bytes/s
Data Burst	10 s
Bit Rate	Constant
Protocol	User Datagram Protocol (UDP)
Simulation	NS3
Analysis	Matlab

The following parameters are considered for the testing of the model:

i *Coverage*: Network Coverage is defined as the geographical area covered by the network. In the proposed approach, Coverage is defined as the number of nodes served along the path of the UAV given a certain time interval.

ii *Throughput*: Throughput is defined as the number of successful transmissions over the network. In the proposed approach, average throughput is measured across the network. A throughput variation chart is also presented in order to demonstrate consistency and QoS levels of the proposed approach.

iii *Latency*: Latency is described in terms of propagation delay and serialization delay, where propagation delay is a function of the distance between the nodes and speed of the carrier, and serialization delay is a function of packet size and transmission rate. The amount of data flowing through a network or a network bottleneck can be visualized as the function of latency and directly affects the throughput of the system irrespective of the technology used.

iv *Delay*: Delay is defined as congestion or link unavailability and is generally considered a measure of the amount of time a signal takes from source to destination. The model aims at limiting the delay to a constant factor by facilitating direct communication between UAV and WSN nodes.

v *Jitter*: The non-deterministic behavior of the network is outlined by jitter. Delay sensitive models are also sensitive to jitters and can be described as the variation in delay.

vi *Packet Delivery Ratio (PDR)*: PDR is defined as the ratio of packets sent to the number of packets successfully delivered. Throughput serves as an effective measure of performance of a node or a section, but PDR addresses the quality of network design that can lead to poor overall throughput.

vii *Data Transferred*: Data transferred is the overall data transferred from source to destination nodes throughout the network. It serves as the metric that estimates data over a given connection during the given time interval.

viii *End To End Delivery (EED)*: End To End Delivery is a parameter that estimates per packet delivery from source to destination. Unlike throughput, which treats the whole model as an entity and calculates the average, the EED is a per packet successful evaluation from source to destination.

ix *Packet Drop*: Packet drop is the measure of the number of unsuccessful transmissions across the network. The packet drop is measured with respect to the number

of packets lost in contrast with the number of packets sent. Packet drop can be caused by UAV, not in range or congestion in the network. The frequent broadcasts from the WSN nodes can also result in packet drop. The topological awareness and route calculation of the UAV aims at limiting the packet drop to minimum levels.

The proposed approach is evaluated against the above-defined metrics in comparison with the 3D Random Way Point, 3D Random Walk, Gauss–Markov Mobility Model and Fixed UAV maneuvers.

The most critical point over which a mobility model can be evaluated is the coverage. Coverage in terms of collaborative networks is defined as the number of ground nodes served or guided over the course of time. The proposed approach provides a steep coverage of 98%.

The random way-point and random walk models are characterized by following the same direction for longer tenures. Both the models provide excellent coverage if the ground nodes are laid across their movement diagonal, which is not always, the case, in real-time scenarios. The random way-point and random walk models provide 91% and 90% coverage, respectively. In the Gauss–Markov model, the next way-point relies heavily on the previous speed and direction. It possesses the tendency to skip densely populated regions as the next way-point is not selected on the basis of density and transmission characteristics of the nodes. The model provides 55% coverage.

The fixed maneuver for a proactive model performs well over its fixed coordinates, but the overall geography demands constant survey and analysis to manually fix new coordinates over time. The 10% coverage provided by the model comes from the path fixed previously without considering the ever-changing patterns of the erratic dynamic network. Figure 4.2 presents the overall coverage comparisons.

Throughput is directly proportional to the coverage. The greater the coverage, the more ground nodes gets serviced or receive a chance to forward data. Throughput is also affected by the density of the areas served. The close-packed areas tend to have more ground nodes thus increasing the chance of data transmission. The approach works better as it focuses on identifying the denser areas from the scarce ones and then selecting way-points accordingly, instead of random movement or movements dictated by speed and direction. The fixed maneuvers do not suffice as both life and transmission density of the WSN nodes is dynamic, and the technique cannot adapt to the changes. The proposed technique provides throughput levels of 82%.

The random-way-point and random walk models achieve 74% and 72% throughput, respectively. The Gauss–Markov model achieves a throughput of 55.7% while the fixed

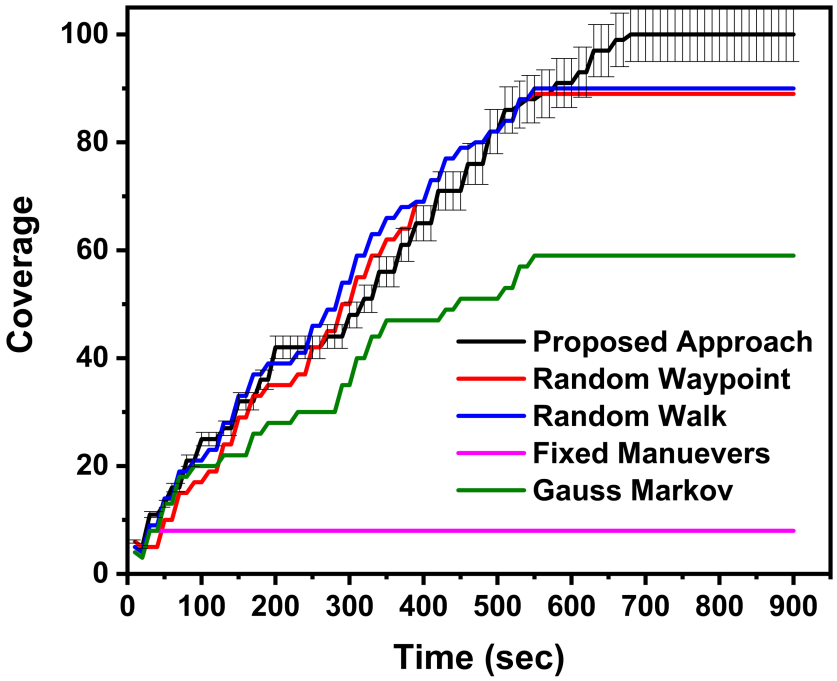


Figure 4.2: Geographical Coverage Comparison among the Proposed Approach, Random Waypoint, Random Walk, Fixed Maneuvers and Gauss Markov.

maneuver technique significantly under performs with throughput levels of 7.5%. Figure 4.3 presents the throughput evaluation of approaches in confederation. To test the Quality of Service provided by the proposed approach, the increases and decreases in throughput levels over the course of simulation are presented in the bar graph. The test results demonstrate consistent throughput levels for the proposed approach. Figure 4.4 presents the QoS comparison based on the throughput levels for the stated approaches. Although random way-point and random walk are evenly matched, they under perform significantly.

The latency of the system, which is a measure of a signal's travel time from source to destination, plays an important role in the applicability of a model. The system throughput drastically declines with the increase in latency. The system performance degrades, as with increasing latency, the packet drop also increases. The proposed model features an overall latency of 9%. The random way-point, random walk, Gauss–Markov and fixed maneuver models have 12.5%, 12.5%, 15% and 85% latency, respectively. The latency comparisons are presented in Figure 4.5.

The minimum average delay is a necessary condition for an efficient model. Facilitation of direct communication between UAV and sensor nodes as well as a reduction in the

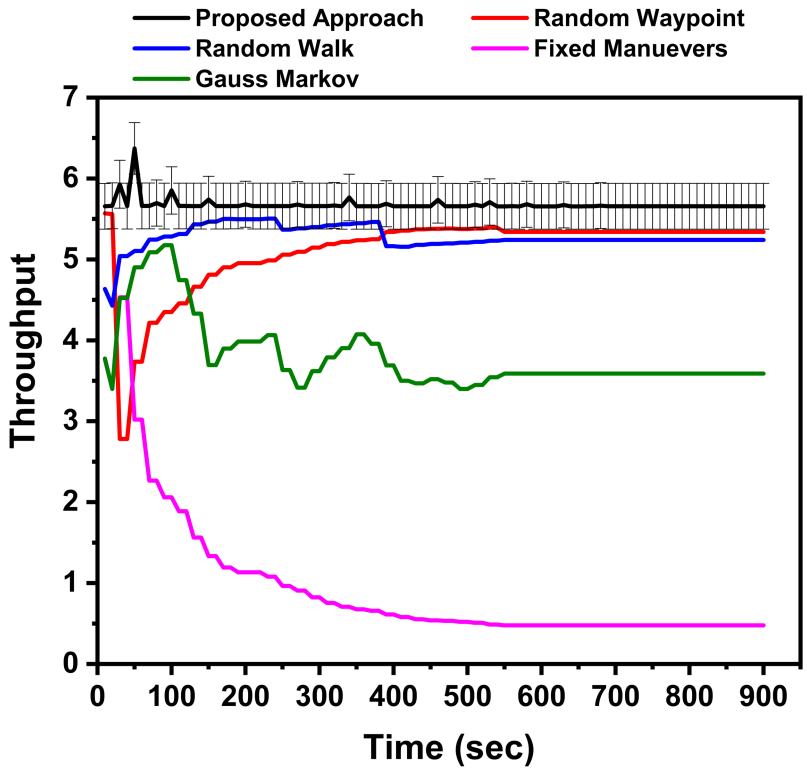


Figure 4.3: Throughput Comparison among the Proposed Approach, Random Waypoint, Random Walk, Fixed Maneuvers and Gauss Markov..

multi-hopping nature of data transmission effectively brings down the overall delay. The statistically important areas are served directly by the UAV and very few of the remaining scarce areas resort to multi-hopping. The average delay of the proposed model is restricted to 0.625%.

The random way-point and random walk models have 11.25% and 35.63% delays, respectively. The Gauss–Markov model with its variable velocity property restricts the average delay to 5%. The fixed maneuver models have an important characteristic of following their well-defined path and always staying in connection to the base station, thus effectively matching the proposed model with 0.625% average delays. However, this delay is with respect to their coverage and throughput values.

Figure 4.6 gives the average delays for the different approaches. Jitter, which is the measure of the variations in delay, is presented in Figure 4.7. With the minimized delay, the proposed approach features the jitter value around 2% and the fixed maneuver model matches the jitter values of the proposed approach. The random way-point, random walk, and Gauss–Markov models have 9%, 6%, and 5% jitter, respectively.

PDR, which measures the number of packets delivered successfully across the network

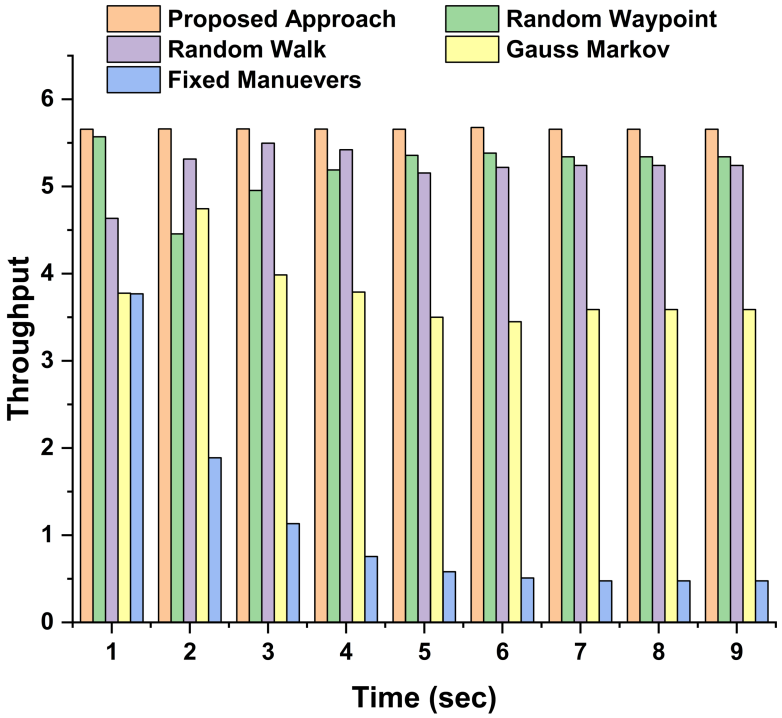


Figure 4.4: QoS Comparison among the Proposed Approach, Random Waypoint, Random Walk, Fixed Maneuvers and Gauss Markov based on Temporal Throughput Levels.

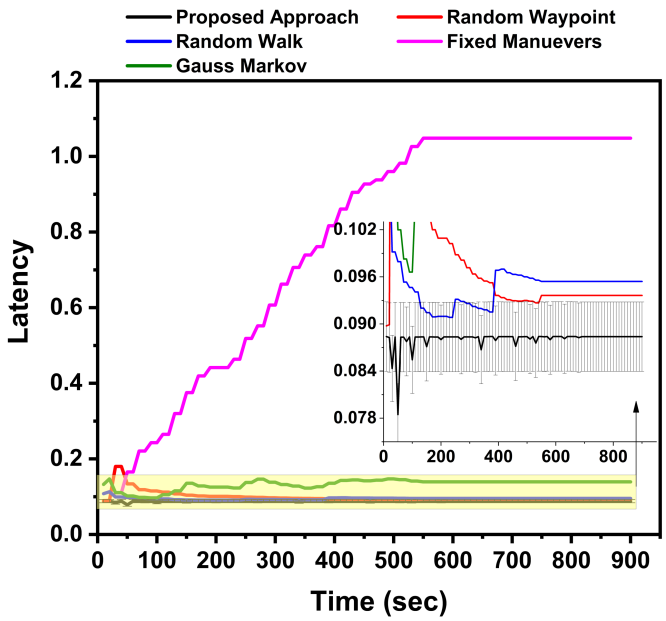


Figure 4.5: Latency Comparison among the Proposed Approach, Random Waypoint, Random Walk, Fixed Maneuvers and Gauss Markov.

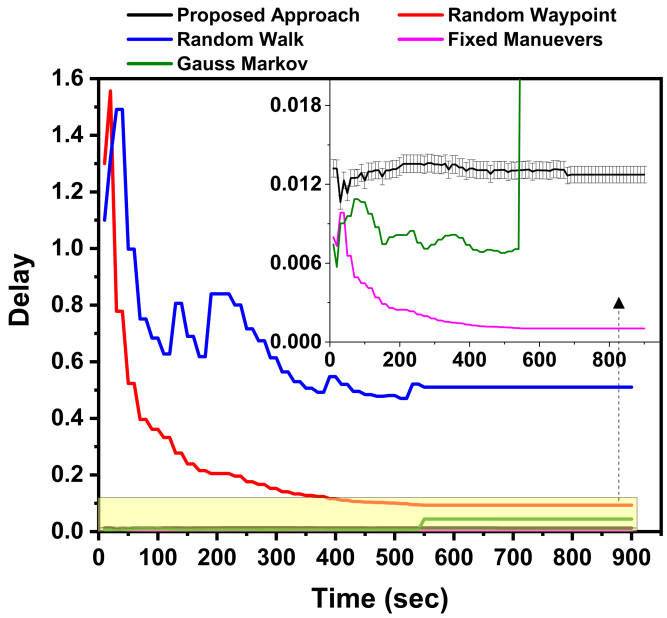


Figure 4.6: Delay Comparison among the Proposed Approach, Random Waypoint, Random Walk, Fixed Maneuvers and Gauss Markov.

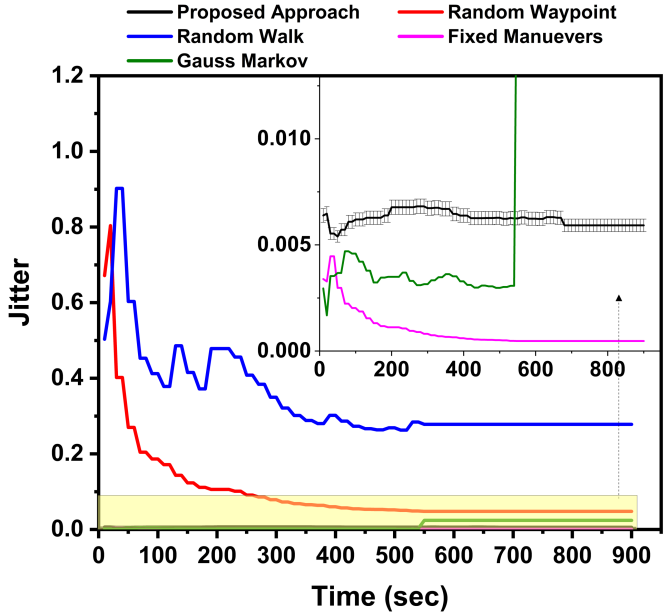


Figure 4.7: Jitter Comparison among the Proposed Approach, Random Waypoint, Random Walk, Fixed Maneuvers and Gauss Markov.

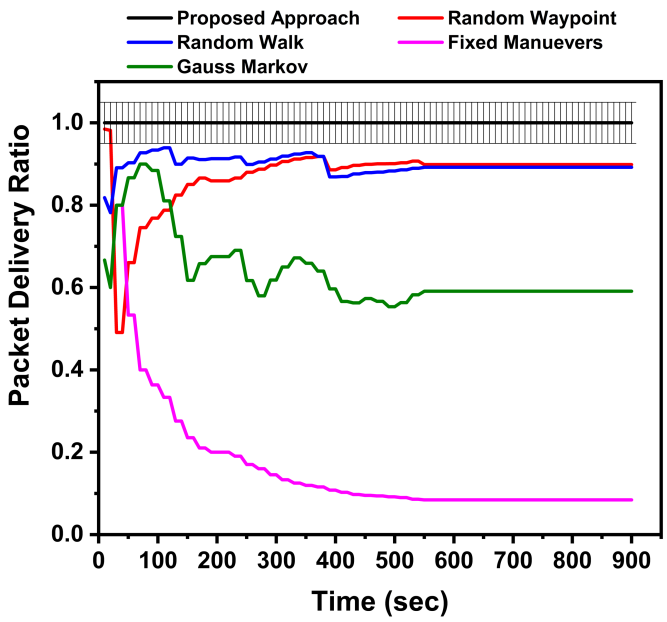


Figure 4.8: Packet Delivery Ratio Comparison among the Proposed Approach, Random Waypoint, Random Walk, Fixed Maneuvers and Gauss Markov.

over the course of time, is an important metric for the mobility model evaluation. The proposed approach that features movement from one dense to another dense region and also collecting data from scarce regions by means of multi-hopping or direct transmission towards base station has a high PDR value of 99%. The random way-point and random walk models that boast of their capabilities of traversing the whole geographical area slowly also possess high PDR of 91% and 90%, respectively, which is slightly less than the proposed approach. The Gauss–Markov model has a PDR of 62%, while the fixed maneuver model due to lack of its coverage has a resultant PDR of 12%. Figure 4.8 presents the PDR comparisons.

The overall data transferred and the end-to-end delivery comparisons are presented in Figures 4.9 and 4.10. The proposed approach features 91% average data transferred statistics. The random way-point and random walk models are at 74% and 72%, respectively. Gauss–Markov and fixed models deliver data transfer average of 49% and 7%, respectively.

The proposed approach features a constant EED delivery timing statistics, which is 0.8%. The random way-point and random walk models result in 12.5% and 24.1%, respectively. Gauss–Markov had an EDD of 3.3% and the fixed model matches the proposed approach as it is following its fixed trajectory and consistent connection with the base station. However, this improved characteristic of the fixed model is compromised by their lesser throughput and coverage values.

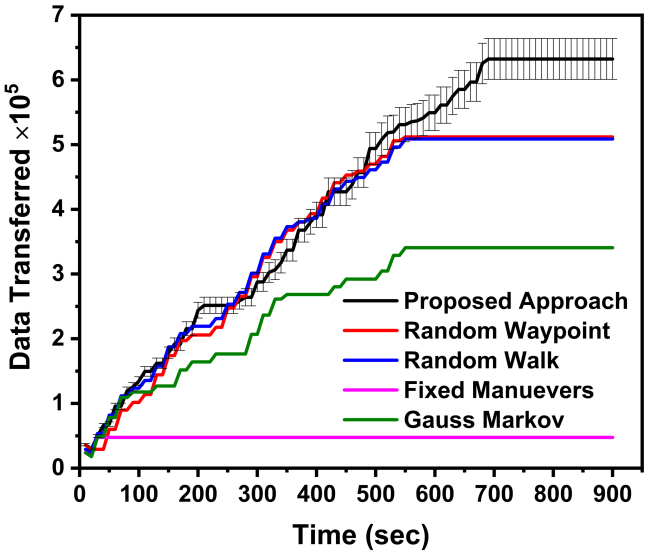


Figure 4.9: Amount of Data Transferred Comparison among the Proposed Approach, Random Waypoint, Random Walk, Fixed Maneuvers and Gauss Markov.

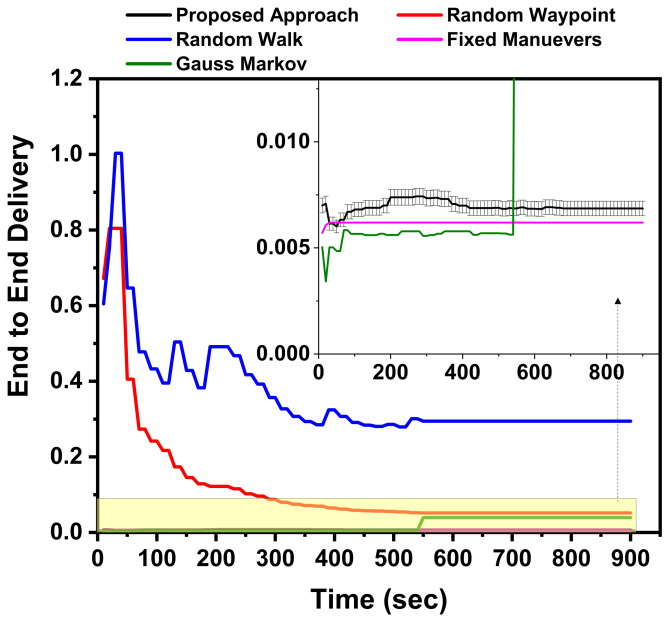


Figure 4.10: End-to-End Delivery Comparison among the Proposed Approach, Random Waypoint, Random Walk, Fixed Maneuvers and Gauss Markov.

Table 4.3: Comparative Analysis of the Proposed Approach against the Featured Techniques.

Metrics	Proposed Approach	Random Way-Point	Random Walk	Gauss Markov	Fixed Maneuvers
Coverage	98%	91%	90%	55%	10%
Throughput	82%	74%	72%	55.7%	7.1%
Latency	8.3%	12.5%	12.5%	16%	86%
Delay	0.625%	11.25%	35.625%	5%	0.625%
Jitter	2%	9%	6%	5%	2%
PDR	99%	91%	90%	60%	12%
Data Transferred	91%	74%	72%	49%	7%
EED	0.8%	12.5%	24.1%	3.3%	0.8%
Packet Drop	0.8%	4.1%	4.1%	35%	83%

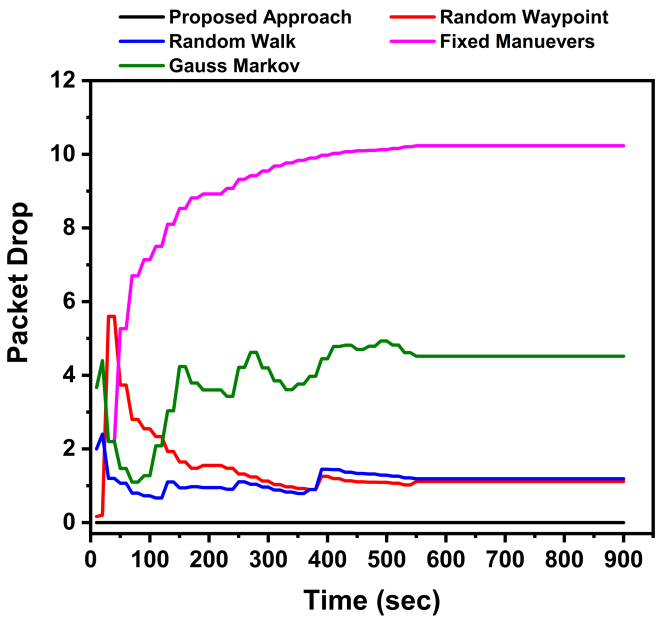


Figure 4.11: Packet Drop Comparison among the Proposed Approach, Random Waypoint, Random Walk, Fixed Maneuvers and Gauss Markov.

Table 4.4: Statistical Variation among Proposed and Compared Approaches.

Coverage						
	Mean	**Std. Dev.**	**Std. Error of Mean**	**Variance**	**Mode**	**Median**
Proposed Approach	67.37	30.81	3.25	949.56	100.00	73.50
Random Waypoint	63.90	28.88	3.04	833.89	89.00	79.00
Random Walk	65.88	27.70	2.92	767.32	90.00	79.00
Fixed Maneuvers	7.90	0.67	0.07	0.45	8.00	8.00
Gauss–Markov	43.99	16.91	1.78	285.90	59.00	51.00
Data Transferred						
Proposed Approach	411306	195463.98988	20603.71362	3.82062E10	632340	432540
Random Waypoint	369756	164153.46941	17303.29497	2.69464E10	511920	453060
Random Walk	371694	155860.53646	16429.14309	2.42925E10	508680	443340
Fixed Maneuvers	46932	3952.15976	416.59422	1.56196E7	47520	47520
Gauss–Markov	254610	96515.75736	10173.65411	9.31529E9	340740	292140
Delay						
Proposed Approach	0.01298	4.3795E-4	4.61639E-5	1.918E-7	0.01274	0.01306
Random Waypoint	0.19316	0.22999	0.02424	0.05289	0.09323	0.10398
Random Walk	0.61413	0.20325	0.02142	0.04131	0.51045	0.51045
Fixed Maneuvers	0.00208	0.0019	1.998E-4	3.59281E-6	0.00104	0.00117
Gauss–Markov	0.02259	0.01801	0.0019	3.2448E-4	0.0445	0.00903
End to End Delivery						
Proposed Approach	0.00694	2.72533E-4	2.87275E-5	7.42745E-8	0.00686	0.00688
Random Waypoint	0.12133	0.15818	0.01667	0.02502	0.05169	0.05744
Random Walk	0.36507	0.13633	0.01437	0.01859	0.29429	0.29429
Fixed Maneuvers	0.00619	5.29694E-5	5.58346E-6	2.80575E-9	0.00619	0.00619
Gauss–Markov	0.01914	0.0167	0.00176	2.78986E-4	0.03948	0.00578
Jitter						
Proposed Approach	0.00624	3.28373E-4	3.46136E-5	1.07829E-7	0.00592	0.00626
Random Waypoint	0.09954	0.11881	0.01252	0.01412	0.04785	0.05345
Random Walk	0.34526	0.12074	0.01273	0.01458	0.27826	0.27826
Fixed Maneuvers	9.41456E-4	8.51129E-4	8.97169E-5	7.2442E-7	4.69991E-4	5.31537E-4
Gauss–Markov	0.01171	0.01022	0.00108	1.04357E-4	0.02414	0.0037
Latency						
Proposed Approach	0.0881	0.00118	1.24404E-4	1.39287E-6	0.08839	0.08838
Random Waypoint	0.09936	0.01469	0.00155	2.15671E-4	0.09363	0.09363
Random Walk	0.09495	0.00311	3.27508E-4	9.65355E-6	0.09542	0.09542
Fixed Maneuvers	0.76525	0.32149	0.03389	0.10336	1.04832	0.92693
Gauss–Markov	0.13303	0.01287	0.00136	1.65581E-4	0.13934	0.13934
Packet Drop						
Proposed Approach	0.000	0.000	0.000	0.000	0.000	0.000
Random Waypoint	1.409	0.850	0.090	0.722	1.116	1.116
Random Walk	1.135	0.244	0.026	0.060	1.189	1.189
Fixed Maneuvers	9.280	1.733	0.183	3.002	10.232	10.095
Gauss–Markov	4.028	0.959	0.101	0.920	4.516	4.516
Packet Delivery Ratio						
Proposed Approach	1.00000	0.00000	0.00000	0.00000	1.00000	1.00000
Random Waypoint	0.87195	0.07724	0.00814	0.00597	0.89856	0.89856
Random Walk	0.89678	0.02206	0.00233	0.00049	0.89198	0.89198
Fixed Maneuvers	0.16948	0.15489	0.01633	0.02399	0.08421	0.09524
Gauss–Markov	0.63499	0.08680	0.00915	0.00753	0.59107	0.59107
Throughput						
Proposed Approach	5.67642	0.08361	0.00881	0.00699	5.65683	5.65727
Random Waypoint	5.10392	0.50364	0.05309	0.25365	5.34029	5.34029
Random Walk	5.27120	0.16014	0.01688	0.02564	5.24021	5.24021
Fixed Maneuvers	0.95980	0.87702	0.09245	0.76916	0.47696	0.53941
Gauss–Markov	3.80016	0.43892	0.04627	0.19265	3.58843	3.58843

Packet drop specifies the ability of the model to avoid creating congestion or not allowing nodes to generate unnecessary traffic. Unnecessary traffic mostly comes from request-reply or data broadcast messages. Figure 4.11 presents the comparison of packet drop in the specified approaches. The fixed maneuver models have the highest packet drop

of 83%. This high packet drop is due to the fact most of the nodes are resorting to multi-hopping resulting in frequent contest among the nodes. The Gauss–Markov model has a packet drop of 35%. The random way-point and random walk models have slow convergence, but coverage is high. They have a drop rate of 4.1%. The proposed approach has a high coverage, less end-to-end delivery times and delay. The packet drop ratio of the proposed approach is 0.8%.

The overall comparative analysis of the proposed approach against the standard discussed approaches is presented in Table 4.3. The statistical variations among the proposed and compared approaches are presented in Table 4.4.

4.2 SDN-Based Secure Mobility Model [3]

Multi-UAV collaborative networks provide with the opportunity to exploit civil, chemical, biological, radiological, nuclear and geographical reconnaissance, survey, management, and control. For the collaborative network formation, coverage is of prime paramountcy. Alongside coverage, possession of information and communication security is withal a major challenge. The coverage quandary can be resolved by a perspicacious selection of UAV way-points. But the security paradigm which can be an effect of faulty node, intrusion or even choice of erroneous communication channels needs to be taken care of through efficacious strategies. Consequently, both a specialized UAV mobility model and a security mechanism are required in order to establish prosperous collaborative networks. In this section, an SDN-based secure mobility model is proposed which takes into account the topological density and restricts the UAV and ground node (Wireless Sensor Networks (WSNs)) transmissions to authenticity.

SDN is effectively a new paradigm in the field of computer networks which separates data forwarding from the control logic thus facilitating better flexibility, scalability, and dynamic adaptability. Mobility model for multi-UAV WSN networks takes into account the attraction factor for setting up the waypoints for UAV movements. The authentication is performed on the basis of pre-installed flows. The pre installed flow table of the UAV is constantly updated with the changing topology. The controller-generated dynamic waypoints prevent UAV from erratic movements as well as any unidentified transmission is discarded based on the flow action rules. The proposed approach is compared against the traditional Clustered Hierarchical WSN layout [276] with UAVs as sinks and against a technique where UAV maneuvers are statically fixed before the flight.

[3] Rajesh Kumar, Mohd. Abuzar Sayeed, Vishal Sharma, Ilsun You, *"An SDN-Based Secure Mobility Model for UAV-Ground Communications"*, Mobile Internet Security: MobiSec, Springer, December (2018). [Published]

4.2.1 Proposed Secure Mobility Model

SDN-based mobility model for Multi-UAV coordinated WSN networks dissects the complete geography into a matrix, as shown in Figure 4.1. The approach inherets the same system model as section 4.1.1.1. The WSN nodes falling into a particular sector (block of the matrix) are default considered into the same cluster and the cluster head and controller selection is done according to Equation 4.13:

$$\min(D_m)\, and\, max(\mathcal{L}), \forall(\mathcal{N}), \tag{4.13}$$

such that:

$$\mathcal{L}_A > 0, \tag{4.14}$$

$$\mathcal{T}_s \geq Mean\, \mathcal{T}_{\mathcal{L}}. \tag{4.15}$$

where, $\mathcal{L}$ refers to the set containing the total connections for nodes, $\mathcal{L}_A$ is the number of connections active on a node, $\mathcal{T}_s$ is the mean life time of the selected node, and $\mathcal{T}_{\mathcal{L}}$ refers to the mean life time of $|N|$ nodes, D_m is the average one hop distance for nodes represented with a set N, which is given as the distance metric, as according to Equation 4.16:

$$D_{m_i} = \frac{\sum_{i=1}^{\mathcal{S}_n} \mathcal{H}}{\mathcal{S}_n}, \mathcal{S}_n \leq |\mathcal{N}|. \tag{4.16}$$

Here, D_{m_i} is the node under consideration, $\mathcal{H}$ is one hop distances from the node under consideration with $\mathcal{S}_n$ being the active nodes, given that the node coordinates lie within the same sector as that of the base station. Inequality 4.17 states the condition for the model to proceed further.

$$0 \leq D_{m_i} \leq \frac{\mathcal{S}_n(\mathcal{S}_n - 1)}{2\mathcal{N}}, \tag{4.17}$$

where, the extreme values are expressed according to Equation 4.18:

$$D_{m_i} = \begin{cases} 0, D^{(selected)}{}_m = \infty, \mathcal{L} = min, \mathcal{T}_s = max, Isolated = True. \\ \dfrac{\mathcal{S}_n(\mathcal{S}_n - 1)}{2\mathcal{N}}, D^{(selected)}{}_m = max\, \mathcal{L} = min, \mathcal{T}_s = max, Isolated = True. \\ Otherwise\text{Select}. \end{cases} \tag{4.18}$$

The controller suggested in the paper has six major components namely; Mission Control, UAV Topology Map, Active Topology, Density Function for Route Establishment (DFRE), Flow Table, and Logs.

Mission control component of the UAV Controller keeps track of the overall mission statistics and the conceptual layout of the system. The information includes cell structure and information about the geography. The main function is to provide preliminary information to the UAV topology map. Active topology component stores the current UAV movement statistics and functions which dictate the overall movement criterion, and geometric characteristics of the flight path. Active topology also forwards the overall sensed statistics of the geographical area to the UAV topology map. The UAV topology map component serves as data storage for mission control and active topology components.

DFRE works on the stored statistics to find an efficient and viable route for the UAVs. Once the complete area is surveyed, the component starts with calculating the density component of respective areas. Figure 4.12 presents the block diagram of the SDN controller used by the proposed model for coordinating UAVs with WSNs over a defined geographical area.

The transfer between UAV and sensor nodes always happens through the cluster-head. When UAV is in range of the cluster head, the Head Swap is performed for inter-changing the cluster heads. UAV becomes the cluster head of the sector to facilitate transfer not only from the designated cluster head but also allows the cluster members to send data directly towards the UAV.

The UAV way-points are set in a way that it moves from head of one densely populated cluster towards the head of another densely populated cluster. UAV way-points are decided on the basis of topological density and distance. The transmissions are facilitated by coordination function, which is calculated by means of topological density as as given by 4.19:

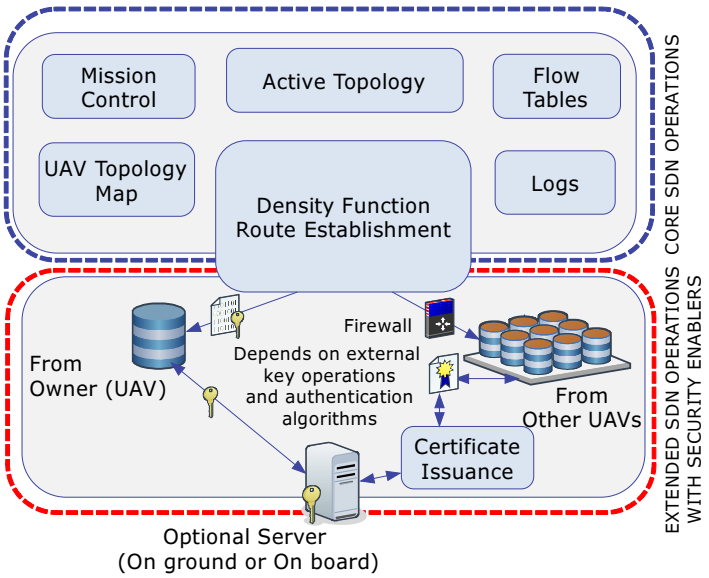


Figure 4.12: A Component Diagram of the Considered SDN Controller for UAV-WSN Coordinations.

$$A_f = \frac{\mathcal{S}_a}{\mathcal{A}} \times \frac{\mathcal{S}_n}{\mathcal{N}} \left(\sqrt{\frac{1}{|\mathcal{N}|} \left(T_{psys} - \overline{T_{psys}} \right)^2} - \sqrt{\frac{1}{\mathcal{S}_n} \left(T_p - \overline{T_p} \right)^2} \right), \tag{4.19}$$

where, T_p is the number of transmissions per unit time in a sector, $\mathcal{S}_a$ denotes the sector area, and T_{psys} is the number of transmissions per unit time in the entire system.

Similarly, the model can be extended to calculate the coordination of each sector as well as the entire zone while fixating the number of transmissions permissible to each node, each sector and each area under the control of a single base station.

After estimating the coordination function of each region, the DFRE further prioritizes the areas of interest as dense and scarce. The inequality in (4.20) identifies the densely populated clusters from the scares ones based on the average hop distances of the area, such that:

$$1 \leq \mathcal{A}_{range} \leq \frac{\mathcal{N}(\mathcal{N}-1)}{2}, \tag{4.20}$$

Area can be evaluated according to 4.21:

$$Area = \begin{cases} Dense, if, \left(\dfrac{min(\mathcal{S}_n) - mean\mathcal{S}_n}{2} \right) < \mathcal{A}_{range} \leq \dfrac{\mathcal{N}(\mathcal{N}-1)}{2}. \\ Sparse, if, 1 \leq \mathcal{A}_{range} \leq \left(\dfrac{min(\mathcal{S}_n) - mean\mathcal{S}_n}{2} \right). \end{cases} \tag{4.21}$$

With all the areas mapped, the DFRE component now performs the weight assignment in order to proceed with the shortest route selection procedure. The model uses a network graph for coordination in which the edge weights E_w, between the nodes are given by Equation 4.22:

$$E_w = \frac{T_{psys}\eta_1 + |\mathcal{N}|\eta_2}{\eta_1 \times \eta_2} - \frac{T_p\eta_3 + \mathcal{S}_n\eta_4}{\eta_3 \times \eta_4}, \tag{4.22}$$

such that:

$$\eta_1 + \eta_2 = 1, \tag{4.23}$$

and,

$$\eta_3 + \eta_4 = 1, \tag{4.24}$$

while,

$$\eta_1, \eta_2, \eta_3, \eta_4 \neq 0, \tag{4.25}$$

where, η_1, η_2, η_3 and η_4 are the balancing constants for T_{psys}, $\mathcal{N}$, T_p, and $\mathcal{S}_n$, respectively.

The densely populated sectors are serviced by UAV maneuvers directly along with the sectors which fall in line with two consecutive UAV banks. The scarce sectors which do not fall in the path of UAV are the designated as isolated zones. These isolated zones fixate on sensors, which send hello packets towards nearby dense regions and the base station when the network is initialized. The purpose of the hello packets is to determine the number of active nodes in the region and number of hops required to reach the dense sector and the base station.

The proposed model considers that the Flow table component of the controller is pre-installed with the specific information of the available sensor nodes. The data transmission is controlled by the flow table match action rules. The DFRE component keeps tracks of the overall topology and updates the flow tables accordingly. In addition, it interacts with the security module to authenticate the way-points and maintain the legitimacy of incoming connections. Further, to verify the connectivity between the UAVs and the WSNs, DFRE checks for previously calculated way-points and matches with the next possible way-points. In such a way, the movement of UAVs is authenticated and verified before transmissions. The details of security considerations and requirements are provided below:

i The system maintains the check on the certificates generated by the controller for other UAVs in the form of a centralized corpus on the controller. It also maintains the details of keys to be used for securing the communications.

ii The channel security is based on the network architecture and depends on the initial phases of mutual authentication, which are not covered at the moment and is marked as an assumption.

iii The keys for securing the location as well as the system conditions are generated by the owner UAV, which can relay with an optional server to check for freshness and prevent any replay attacks.

iv Once the keys are initiated, the DFRE module improvises the availability of way-points and allocate it to the topology generator, which helps to fixate the points for maneuverability. Any violation in the way-points is tracked through crypto-mechanisms based on keys generated in the initial phase.

v The certificate issuance helps to re-verify the UAVs and the way-points and avoids overheads associated with re-verification. However, the requirement of verification of way-points depends on the type of network layout and the environment in which the UAVs are deployed.

At the moment, the major security requisites are discussed as an abstracted aspect by following the layout in Figure 4.12. However, the future works will present the detailed working as well as detailed security analysis of the proposed system.

4.2.2 Performance Evaluation

The proposed technique relies on exploits the movement characteristics of UAV in order to achieve significant gains over the already existing models. The evaluation and testing of the approach are done on a model consisting of the base station, WSN motes and the UAVs serving as relays by using $NS3$ and $Matlab^{TM}$. The testing is performed on a $1200 \times 1200\ m^2$ area. The number of UAVs is varied between 1 and 10 with WSN nodes equaling 100.

The average packet size is varied between 512 bytes to 1024 bytes and the value of balancing constants η are kept fixed at 0.5. The connections are generated through the modeling without overlapping and the proposed approach is compared with hierarchical WSN layout and Statically Maneuvered UAV approaches. The approaches are compared on the basis of throughput, coverage, and latency. At the moment only performance-based evaluations are presented and the security evaluations will be covered in upcoming

works.

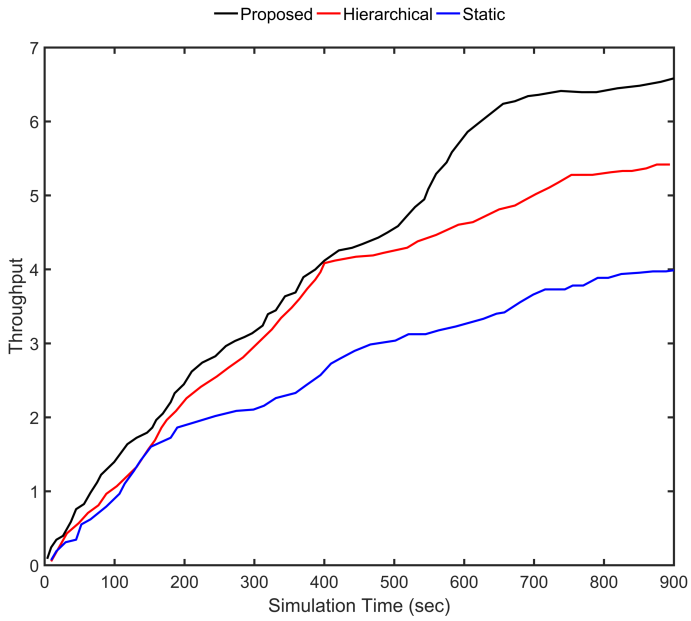


Figure 4.13: Throughput Comparison among the Proposed Approach, Hierarchical WSN Layout and Statically Maneuvered UAV. Abbreviations: WSN, Wireless Sensor Networks.

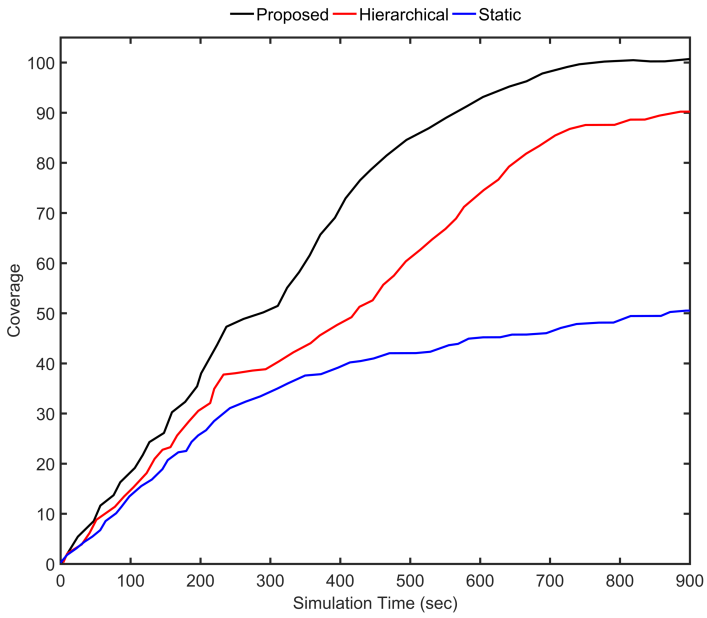


Figure 4.14: Coverage Comparison among the Proposed Approach, Hierarchical WSN Layout and Statically Maneuvered UAV. Abbreviations: WSN, Wireless Sensor Networks.

The proposed approach performs at the maximum throughput level of 95.7% as compared to 77.1% and 57.1% throughput levels of hierarchical WSN approach and static deployment of UAVs respectively. Figure 4.13 gives the throughput comparison of the considered approaches against the proposed approach. Initially, three approaches have comparable throughput but with time the static approach starts degrading. The traditional hierarchical approach initially performs in close proximity to the proposed approach but cannot match the steep ascent as the proposed approach performs uniformly throughout the simulation tests.

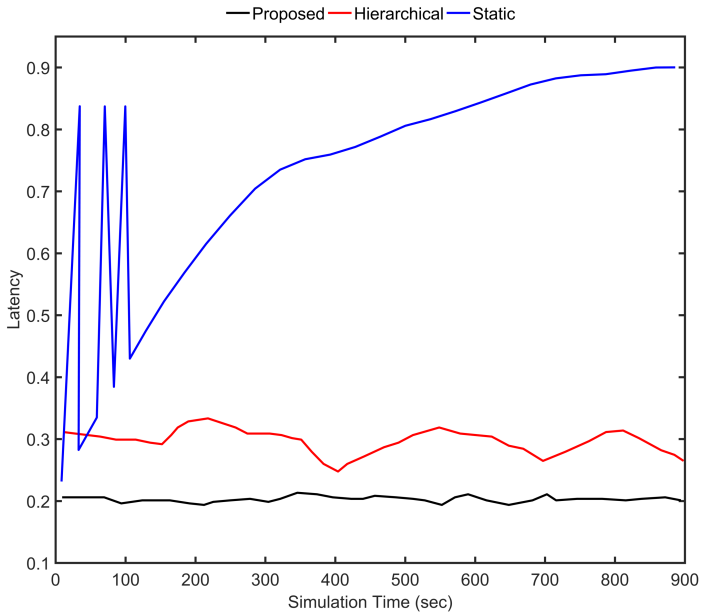


Figure 4.15: Latency Comparison among the Proposed Approach, Hierarchical WSN Layout and Statically Maneuvered UAV. Abbreviations: WSN, Wireless Sensor Networks.

The proposed approach provides the maximum coverage of around 99% in comparison to 84% and 49% coverage of hierarchical and static deployment. The approach also provides a faster and efficient coverage against the other two solutions. Figure 4.14 gives the coverage relationship between the existing and the proposed approaches. The latency of the proposed approach is approximately constant at 20% gains. The hierarchical approach works with a varying latency between 19% and 34%. The latency levels always stay in close proximity to the proposed approach but with consistent fluctuation. The static UAV approach possesses inconsistent latency measures with a maximum of 84% and average latency of around 65%, as shown in Figure 4.15.

4.3 Conclusion

Efficient topological formations and coordinated movements help to achieve effective and sustainable UAV-coordinated WSNs. In this chapter, two complementary mobility based data dissemination schemes for multi-UAV ad hoc networks are presented. First, a novel mobility scheme based on the transmission density of the WSN nodes is proposed for moving UAVs in a coordinated manner for improved coverage and better performance. The proposed approach is evaluated against Random way-point, Random Walk, Gauss–Markov and Fixed Maneuver UAV movements. The random models produce close but considerably fewer performance levels as long as the WSN nodes lie in their movement corridor. The Gaussian model gives results on average performance when applied to the UAV movements. The fixed maneuvering scheme produces less delay but with a huge compromise on throughput, coverage, and latency. The proposed approach shows significant gains in coverage, throughput, jitter, and data transfer ratios. The packet drop rate is decreased exponentially and massive gains are observed for packet delivery ratio.

Second, a novel mobility scheme based on the transmission density of the WSN nodes is proposed which is capable of including way-point-security of UAVs. The UAVs perform successive shifts towards dense regions thus resulting in high coverage and throughput. The proposed approach incorporates a simple flow based technique through SDN controller for authentication and coordination of WSN as well as aerial nodes. Significant gains are observed for metrics like throughput, coverage, and latency. The details on authentication procedures and verification mechanisms will be presented in our future works.

Chapter 5

Throughput Maximization for Multi-UAV Networks [4]

Dynamic control and state estimation of the aerial network are driving forces behind the optimized UAV trajectory. The proposed approach models throughput maximization and capacity enhancement of the multi-UAV assisted ground networks as a trajectory optimization paradigm and considers UAV state as the criteria for UAV re-purposing. UAV re-purposing is effectively a technique where available less congested UAVs are directed towards geographical sectors with high latency and packet loss rates. The state of the aerial nodes is determined iteratively using graph neural networks (GNN). GNN architectures use iterative message passing to produce a cumulative state information vector employing aggregation schemes at each level [277, 278, 279, 280]. The proposed GNN's node embedding incorporates UAV's position concerning sector anchor in a 3D area and node features, including throughput, latency, and packet loss. Incorporating UAV positioning is important for feature state calculation as two aerial nodes with the same characteristics are indistinguishable without geo-positioning.

5.1 Efficient Deployment with Throughput Maximization

The majority of approaches following multi-UAV-assisted throughput maximization have studied trajectory optimization as a function of underlying ground nodes and application scenarios. The proposed approach performs iterative learning at both local and global topological levels and considers application scenario independent ground nodes, which makes it more reactive and adaptable to sudden changes in geography, node failures, and bottlenecks as compared to the mathematical optimization techniques proposed in the literature. Trajectory and throughput optimization require tracking multiple aerial and ground nodes. The techniques proposed in the literature have traditionally investigated linear tracking in a plane. The simplification reduces the throughput maximization into

[4] Mohd. Abuzar Sayeed, Rajesh Kumar, Vishal Sharma, Mohd Asim Sayeed *"Efficient Deployment with Throughput Maximization for UAVs Communication Networks"*, Sensors (IF 3.275), MDPI (2020). [Published]

an optimization problem but does not address the aerial node tracking when targets move in a 3D plane. While multi-UAV trajectory optimization generally focuses on aerial nodes moving in the 2D front parallel plane, this is an atypically simple, special case. The proposed approach considers aerial nodes moving continuously in all three dimensions. Moreover, 2D tracking suffers a steep performance decline when speed and distances increase, as overall mapping accuracy is always higher in 3D than in 2D. The proposed approach employs separation and dimensionality to provide more than additive improvements as the aerial nodes packed closely together in a 2D front parallel perspective can be far apart if altitude is considered, and can be mapped accurately in a 3D geography. Moreover, the mapping accuracy improves when aerial nodes are separated by different altitude planes.

The proposed approach presents a multi-UAV assisted ground network, where UAVs are deployed as transceivers as well as base stations in a given 3D area. A dynamically re-configurable topology is presented where state information of aerial nodes is generated and updated periodically to keep track of congestion and declining throughput. The proposed approach aims at pushing data rates close to the throughput upper bound of UAV-assisted ground networks through aerial node re-purposing, reinforcing burdened nodes, and links. The approach models aerial nodes and associated links for traffic characterizations, delay, loss, and throughput to estimate the topological re-configurations and capacity predictions. For performance analysis, the proposed approach is compared against software-defined UAVs (U-S) and UAVs as base stations (U-B) inspired by the configurations in [281] and [282], respectively.

5.1.1 Network Model

UAV networks are complex design paradigms banking on effective trajectory selections, situation awareness, and communication in conjunction with dynamic network reassessment and load characterization. Without featuring a dynamic trajectory modification in accordance with the iterative situational-updates, the overall system performance declines, given sufficient ground and aerial resources. The proposed approach focuses on throughput maximization in multi-UAV assisted ground networks. The technique employs UAV mapping and trajectory optimization using UAV re-purposing to minimize delays and packet loss and maximize throughput. The network comprises aerial and ground nodes. The UAVs act as both transceiver and base for the underlying ground network. Aerial nodes initially follow a predetermined path through the sectors. A sector is a 3D volumetrically equal division of the geographical topology. Sector anchor is a set of random points in a divided 3D plane such that each division has at least one

anchor. A single UAV topology can be classified into two categories within the same temporal instance. Local topology defines a node's attributes concerning its immediate neighbors. The global topology defines the UAV positioning concerning the overall geographical deployment. Figure 5.1 details the complete network layout. The topological characterization reveals the relationship dynamics of the UAV-assisted ground network deployment. To perform trajectory optimization and UAV re-purposing, it is important to map aerial and ground nodes to particular sectors. Unless intervened, UAVs fly autonomously over a predetermined trajectory with constant velocity.

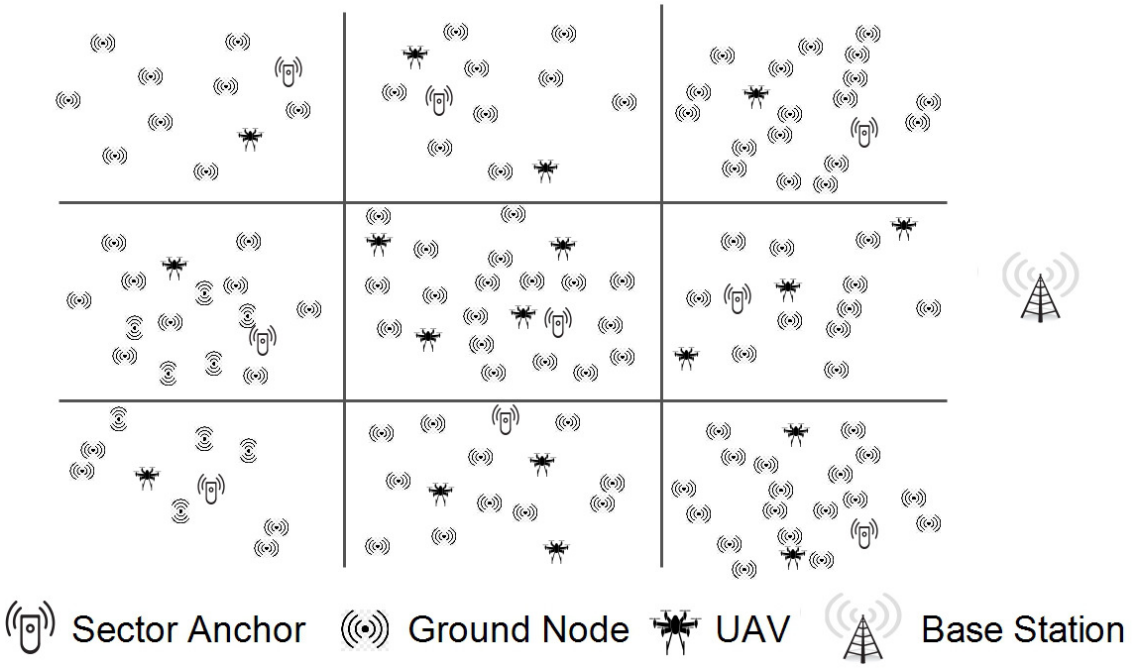


Figure 5.1: Proposed Approach: Network Model.

Each aerial and ground node is mapped to its corresponding sector in accordance with the local network layout. The corresponding sector anchors for each sub-area are marked. The sector anchor can be adjusted to the center of the node cluster within its specific sub-area. The connected mesh of aerial nodes serves as the initial network map or graph. As the network progresses, with continued iterative transmissions, each node calculates its own set of features and link characteristics of the adjoining nodes. Every time the network gets up and running, graph dependent shortest path algorithms are used to initialize the network. The issue with the shortest path or multipath approaches is that they do not take into account the distance and latency of the links while updating paths during their initialization phase. The problems associated with the absence of steady and dynamic learning of network patterns cause complete re-initializations of the paths around the node where the link is broken or congested.

Collaborative networks rely on traditional multi-hopping techniques for data dissemination. The data path from source to destination is calculated employing graph algorithms (example: Dijkstra's shortest path algorithm or Bellman–Ford algorithm). The network itself forms a dynamic graph with temporary connections. The shortest and most efficient link from i to j can be a single shortest path; however, it suffers from delay and packet loss due to congestion. The tremendous decline in overall network performance and inefficient data transmissions result from slow reaction and path reconstruction, link failures originating from the dynamic topological arrangements, flooding, network clogging, and higher latency towards alternate route calculation. Moreover, the traffic originating from one subsection of the network will start sharing the paths when destined to another subsection, further increasing the latency and impacting overall throughput.

The solution can be found in multi-path techniques for providing alternate paths and reduced latency, but it further increases the complexity and generates overheads for calculating and maintaining multiple paths from source to destination. Maintaining all the multiple paths is generally not required for multi hopping transmissions and can be avoided by employing efficient trajectory optimization, thus boosting overall network performance. The article presents a solution that provides a multipath arrangement for congested links and burdened nodes through UAV re-purposing. It starts by calculating node and their link states, including the state of its neighbors, and updates the node parameters. If an additional path is required by the network in an area, the UAV positioning is adjusted and new paths are dynamically arranged. The UAV is re-positioned according to the criteria which maintains old links alongside the new.

GNN has a specific ability to acknowledge the natural order of nodes in a graph, i.e., no particular order but traversing the nodes in all possible orders. Traditional neural models process the patterns in a stacked specific order which makes them less suited towards the dynamic nature of topology and fast movement of the aerial nodes. In a network graph, a connection means the state of the node which itself is dependent on the state of neighboring nodes and links. Traditional neural models account for this interconnected dependency, as a feature of the node itself, whereas GNN performs propagation guided by the graph structure instead of using it as part of features. GNN can retain states up to arbitrary lengths, thereby better capturing the graph dependence of states via transmission and movement characteristics. The GNN operations, in the proposed approach, can be summarized as: calculate node state, propagate node state along the edges of the graph and re-calculate node states according to the received updates. The functionality of GNN in coordination with the proposed approach is detailed in Section 4. Equation 5.14 and Figure 5.2 elaborates on the operational GNN feed-forward network

and state output calculation. Figure 5.3 shows how UAVs propagate the feature vector to the neighboring UAVs. The recipient aerial nodes append their feature vectors according to the received updated vector from the neighbors.

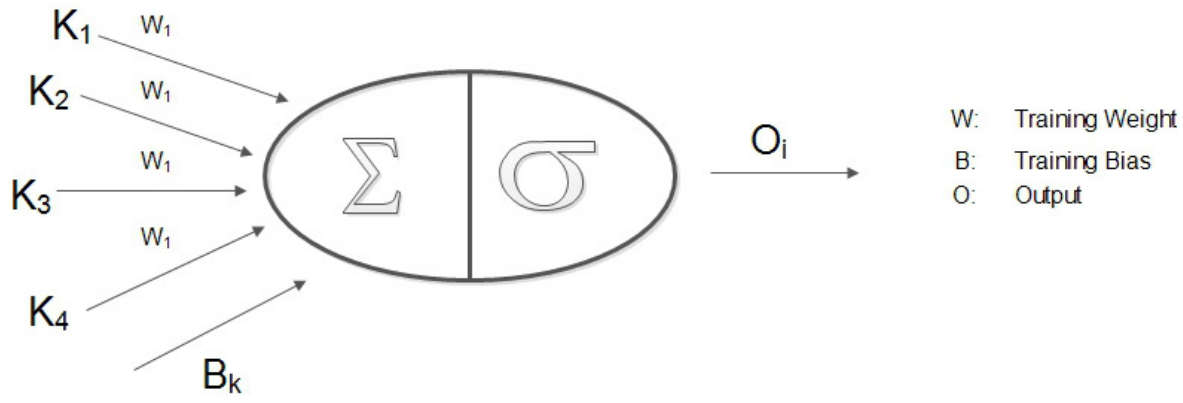


Figure 5.2: Graph Neural Network: Output Generation.

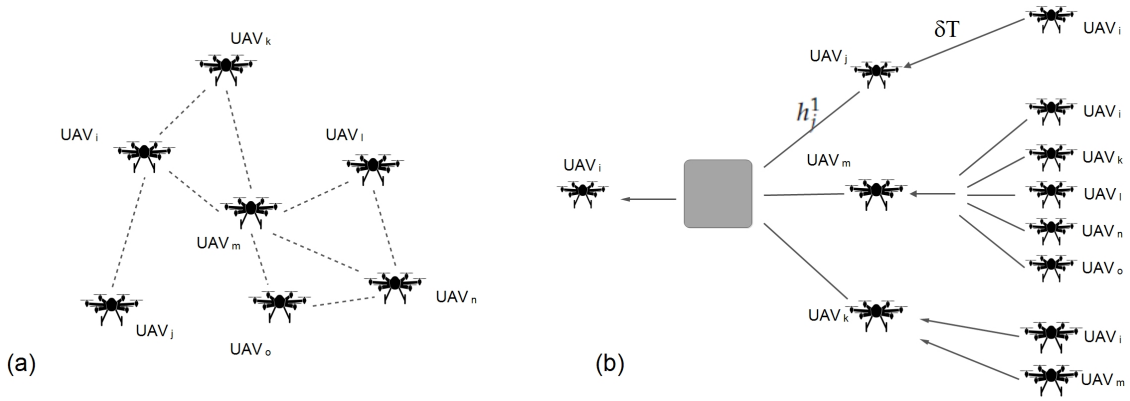


Figure 5.3: (**a**) Topological Relationship of i^{th} UAV. (**b**) Aggregate State Definition of i^{th} UAV.

Example The UAV re-positioning can facilitate alternative paths where a node/link is broken/congested. The node state is used to decide upon moving in another UAV with desirable current state characteristics. The path in a given set of UAV links is denoted by $ABCD$ (Figure 5.4). $ABCD$ are weights whose values depend upon the feature vector. The GNN can learn this graph alongside node features and link states. During steady network operation, suppose link B becomes congested, a graph neural network will present this abrupt change in behavior in O_i is gieven by Equation 5.11. The proposed approach now estimates an aerial node close to UAV_1 or UAV_2 and re-purposes it to send packets from UAV_1 to UAV_5 using link E. The complete state estimation and UAV re-purposing techniques are presented in Subsection 5.1.2.

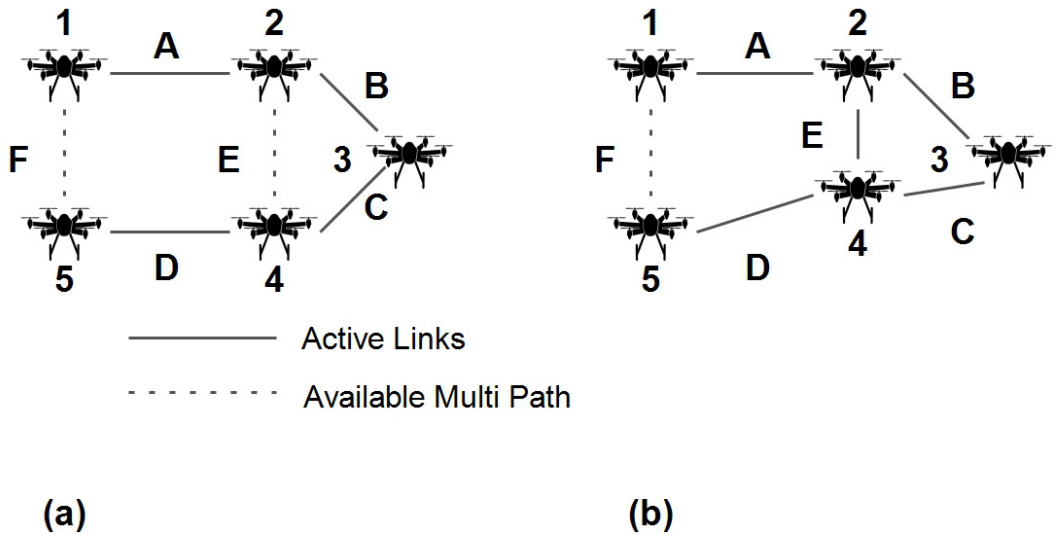


Figure 5.4: Proposed Approach: (**a**) Network Graph with Congested Link B (**b**) UAV Re-purposed to Activate Link E Alongside B.

5.1.2 Proposed Approach

The proposed approach aims at pushing the maximum data rate of UAV-assisted ground networks towards the throughput upper bound of-UAV assisted ground network deployment. Maximum data rates are achieved by minimizing the overall latency and packet loss. UAV re-purposing achieves minimal packet loss and delays by allowing dynamic topological changes considering the state of the UAV, state of the neighboring nodes, and the overall state of the sector. Individual UAV feature vectors are used to collaboratively determine the state of an aerial node concerning its neighbors and load characteristics. The initial feature vector is defined over the node's latency, loss, observed throughput, and distance from the sector anchor. GNN aggregation is used iteratively to determine each UAV state with respect to its one-hop neighbors and so on. The dynamic and continuous node assessment keeps track of each aerial node and its network statistics. The overall sector state is assessed against the UAV states, and congested nodes (high latency and packet drop) are served using re-purposed UAVs.

Network latency is a numerical measure of delay and is described as the time it takes for a signal to propagate across the network connection, towards its destination. The latency of a UAV-assisted ground network is defined as Equation 5.1:

$$L_w = l_r + l_q + (l_t \times h_c) + l_p + l_c, \tag{5.1}$$

where, L_w is the latency of a wireless link, l_r is the router traversal latency, l_q is queuing delay and is defined as the amount of time that data packet spends in the queue before

transmission, l_t is transmission delay and is a measure of time, it takes to place an entire packet on the transmission channel. Transmission delay is the ratio between packet size and transmission rate. h_c is hop count, l_p is the propagation delay, or the signal propagation time across the transmission channel. Propagation delay is the ratio between the node displacement and speed of the communication channel. Connection delay (l_c) is the time it takes to establish the connection between aerial and ground nodes.

Packet loss rate or packet loss probability of a UAV-assisted ground network is defined as Equation 5.2:

$$L_p = \frac{Tx_p - Rx_p}{Tx_p}, \tag{5.2}$$

where, L_p is the packet loss ratio, Tx_p is the actual number of packets transmitted and Rx_p defines the packets received.

Network throughput is the rate of packet delivery along with a communication network. Mathis et al. [283] proposed the upper bound on the data transfer rate over a communication channel. The throughput upper bound Th_{max} for a UAV-assisted ground network is defined as Equation 5.3:

$$Th_{max} \leq MSS \times \frac{1}{I_{let}} \times \frac{1}{I_{del}}, \tag{5.3}$$

where MSS is the maximum packet size.

$$I_{let} = \frac{1}{n}\sum_{i=1}^{n} L_{w_i} = \frac{1}{n}\sum_{i=1}^{n} l_{r_i} + l_{q_i} + (l_{t_i} \times h_{c_i}) + l_{p_i} + l_{c_i}, \tag{5.4}$$

$$I_{del} = \frac{1}{n}\sum_{i=1}^{n} L_{p_i} = \frac{1}{n}\sum_{i=1}^{n} \frac{Tx_{p_i} - Rx_{p_i}}{Tx_{p_i}}, \tag{5.5}$$

and

$$I_{del} = \begin{cases} 1 & \text{if } Tx_{p_i} = Rx_{p_i}. \\ \dfrac{1}{\frac{1}{n}\sum_{i=1}^{n} L_{p_i}} & \text{otherwise.} \end{cases} \tag{5.6}$$

In order to achieve the maximum data rates in UAV-assisted ground networks (Th_{maxw}), the proposed approach minimizes the I_{let} according to Equation 5.4 and I_{del} according to Equation (5.5), which in turn can be minimized by minimizing the L_w Equation 5.1 and L_p as given by Equation 5.2. The goal of the proposed approach is to achieve Th_{maxw}

values close to and approaching Th_{max} as dictated by Equation 5.7.

$$Th_{maxw \rightarrow max} \propto min(L_w, L_p). \tag{5.7}$$

An instance of a multi-UAV-assisted ground network constitutes n number of UAV nodes in a 3D plane participating in a collaborative network formation. The dynamic movement of nodes in (x,y,z) plane imposes significant difficulty in network reconfiguration for optimal channel utilization and data rate maximization. A feature vector is designed to represent the link wise network state which incorporates latency and congestion over each link. The feature vector δT at the i^{th} node is defined as Equation 5.8:

$$\delta T \longleftarrow \{L_{w_i}, L_{p_i}, Th_{0_i}, d_i\}, \tag{5.8}$$

where, Th_{0_i} is the observed data rate at i^{th} node and d is node's displacement from the sector anchor. The d_i is the Mahalanobis distance [284] calculated between node positions and sector anchor. d_i is defined as Equation 5.9:

$$d_i = \sqrt{(y-\mu)C^{-1}(y-\mu)'}, \tag{5.9}$$

where, y is the set of anchor points, μ is the mean of UAV coordinates and C is the covariance matrix.

UAVs hover with random way-point selection or any other predefined mobility, but are ready to change course and follow a newly set path as dictated by the proposed trajectory optimization technique. The multi-hop UAVs will change their adjacency relationships more frequently than the single hop nodes. The local and global arrangements can be represented as graph $G(U_{(x,y,z)}, A)$ and adjacent matrix $A_{(i,j)}$ as is stated by Equation 5.10.

$$A(i,j) = \begin{cases} 1 & \text{if } uav_i \quad \& \quad uav_j \text{ are single hop nodes} \\ 0 & \text{if } uav_i \quad \& \quad uav_j \text{ are multi hop nodes} \end{cases} \tag{5.10}$$

At any reference interval, the exact state of the aerial network must be accounted for facilitating efficient positioning of the relay nodes. The state of the aerial network can be heuristically defined using graph neural network [285]. The expected behavior of the node is required to adjust the positioning of the nodes in advance to push the overall network capacity towards Th_{maxw}. With the graph neural network, the i^{th} UAV's state O_i is given by Equation 5.11. This state is defined over the current state of the UAV

node and its neighboring UAVs, presenting the neural network output considering the UAV's feature vector and input vectors received from the neighboring UAVs. The number of layers considered in the proposed model is equal to the graph levels formed by UAV nodes in a sector. The arrangement of layers according to UAV topology is described by Figure 5.3. The UAV node's state vector h_i concerning neighboring UAVs is described by Equations 5.11 and 5.12:

$$O_i = \rho_w(h_i, \delta T_i), \tag{5.11}$$

$$h_i = \Upsilon_w(\delta T_i, A_{[i]}, h_{ne[i]}, \delta T_{ne[i]}), \tag{5.12}$$

where, δT_i is the feature vector, $A_{[i]}$ is the adjacency matrix for i^{th} node. $h_{ne[i]}$ defines state of i^{th} UAV's neighbours. $\delta T_{ne[i]}$ define features of the neighbouring UAVs.

The state h of an aerial node at the 0^{th} layer is given by Equation 5.13. The 0^{th} layer UAV treats its feature vector as its state. The 0^{th} layer is the initial layer from the disjoint graph considered for UAV state calculation.

$$h_i^0 = \delta T_i. \tag{5.13}$$

At k^{th} layer, the state of i^{th} node can be defined as Equation 5.14:

$$h_i^k = \sigma\left(W_k Ag, B_k h_i^{k-1}\right), \tag{5.14}$$

where, W_k and B_k are weight and bias respectively, used for training the neural network at k^{th} layer and Ag is the aggregate function as detailed in Equation 5.15 with parameters α, β, γ and δ as according to Equation 5.16. Algorithm 5.1 presents the UAV state calculation process. The cost of UAV state identification is $O(n^3)$, where n is the number of currently deployed aerial nodes.

$$Ag = \sum_{i=0}^{n} \left(\alpha L_{w_i} + \beta L_{p_i} + \gamma Th_{0_i} + \delta d_i\right), \tag{5.15}$$

$$\alpha + \beta + \gamma + \delta = 1. \tag{5.16}$$

where, n is the number of nodes in a divided sector.

The proposed approach considers a maximum of three hop neighbors' states. The actual UAV topology over geography and the definition of UAV states derived from the geographical layout are presented in Figure 5.3.

UAV_i will have a state corresponding to its latency, packet drop, instantaneous throughput, and distance from sector anchor, given by Equation 5.11. UAV re-purposing is required to ensure consistent and improved data rates if the throughput of a sector Z_{rate} as given by Equations 5.17 and 5.18 falls below the expected throughput. The expected rate Z_{exp} is proportional to the channel capacity C_s of the sector, such that:

$$Z_{rate} \propto \frac{1}{\sum_i^n O_i}, \tag{5.17}$$

$$Z_{rate} < Z_{exp} | Z_{exp} = \frac{C_s}{2}. \tag{5.18}$$

The distance d_{ai} between a sector anchor A_i (A_{ix}, A_{iy}, A_{iz}) and an aerial node UAV_i (U_{ix}, U_{iy}, U_{iz}) in a w-dimensional space is given by Equation 5.21:

Algorithm 5.1 UAV State Identification

Output: O_i
Input: UAV Coordinates,
Feature Vector $\delta T \longleftarrow \{L_{w_i}, L_{p_i}, Th_{0_i}, d_i\}$,
Distance $d_i = \sqrt{(y-\mu)C^{-1}(y-\mu)'}$,
Adjacent Matrix $A_{(x,y,z)}$
Begin
Initialization:
$h_i^0 = \delta T_i$
while i in aerial nodes **do**
    while k in layers **do**
        $h_i^k \leftarrow \sigma\left(W_k Ag, B_k h_i^{k-1}\right)$
        $AGGN \leftarrow \sum_{i=0}^{n} (\alpha L_{w_i} + \beta L_{p_i} + \gamma Th_{0_i} + \delta d_i)$
        $\alpha + \beta + \gamma + \delta = 1$
        $O_i = \rho_w(h_i, \delta T_i)$
End

The candidate solution for UAV re-purposing is assigned according to Equation 5.19. UAV is re-purposed to a designated overburdened high latency node such that its distance from the sector anchor d_{ai} and current state O_i is minimal. Algorithm 5.2 elaborates on the UAV trajectory optimization and UAV re-purposing process. UAV re-purposing costs $O(n^2)$, where n is the number of currently deployed aerial nodes. Figure 5.5 details the UAV re-purposing scenario.

$$min(O_i, d_{ai}). \tag{5.19}$$

Tangent of the i_{th} UAV towards the burdened node is used to set the re-purpose direction and the minimum required movement d_m is assigned according to the prorogation length Sp_i of the UAV signals according to Equation 5.20.

If no UAV nodes are available for re-purposing, a directly connected UAV with minimum current state O_i value is considered.

$$d_m = \frac{Sp_i}{2}. \tag{5.20}$$

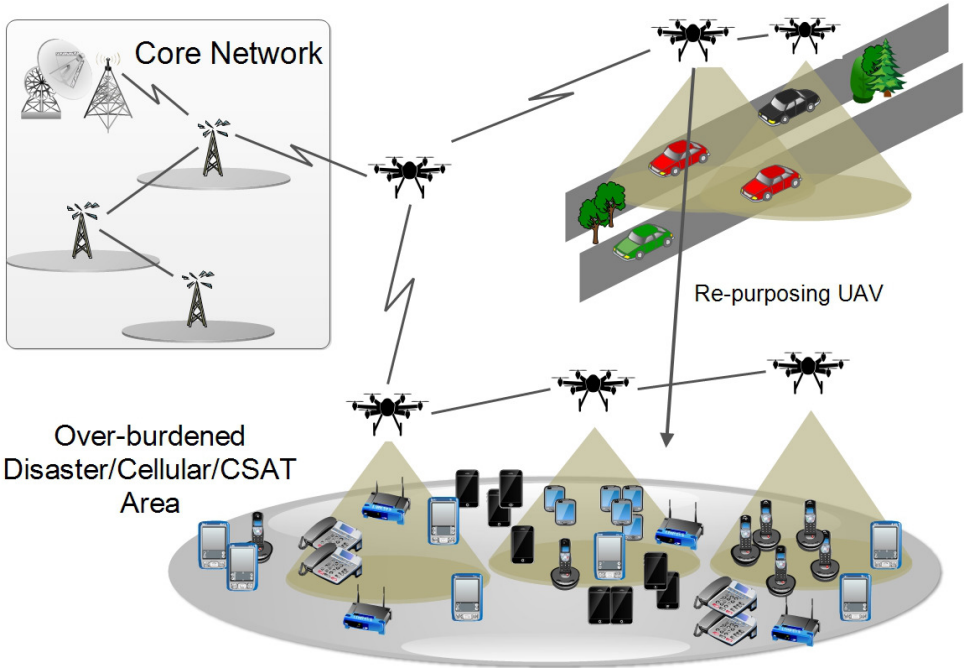


Figure 5.5: An Illustration of State-based UAV Re-purposing.

Algorithm 5.2 UAV Re-purposing

Output: d_m
Input: O_i
Begin
Initialization:
$Z_{rate} \propto \frac{1}{\sum_i^n O_i}$,
$Z_{rate} < Z_{exp} | Z_{exp} = \frac{C_s}{2}$
while i in serial nodes in a sector **do**
    $d_{ai} = \sqrt{(A_{ix} - U_{ix})^2 + (A_{iy} - U_{iy})^2 + (A_{iz} - U_{iz})^2} = \sqrt{\sum_{r=1}^{w} (A_{ir} - U_{ir})^2}$
    $min(O_i, d_{ai})$
Re-purposing Distance:

$d_m = \frac{Sp_i}{2}$

End

$$d_{ai} = \sqrt{(A_{ix} - U_{ix})^2 + (A_{iy} - U_{iy})^2 + (A_{iz} - U_{iz})^2} = \sqrt{\sum_{r=1}^{w} (A_{ir} - U_{ir})^2}. \tag{5.21}$$

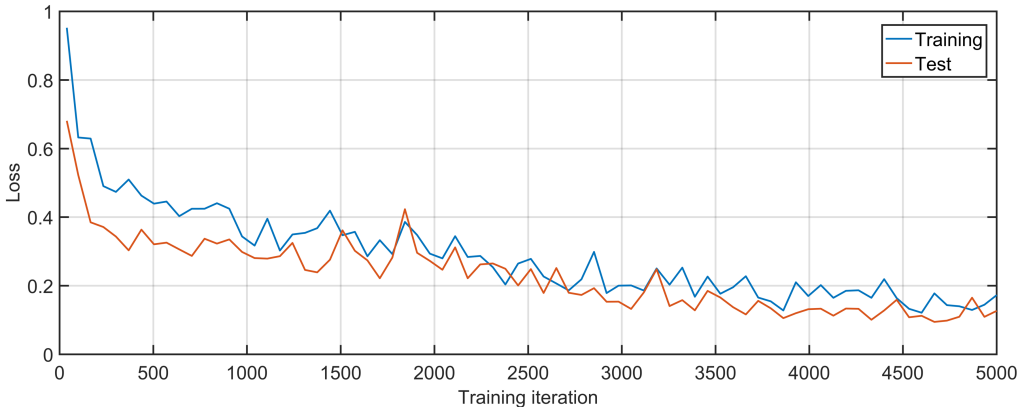


Figure 5.6: Training and Testing Loss for GNN.

To estimate the cost and complexity of the proposed solution, the initial training of the algorithm is performed using 10 formations of UAV networks, and the GNN is trained over 5000 iterations, followed by re-testing using 5 formations of the UAV network. Figure 5.6 gives training and testing losses over each iteration, where 1000 iterations take 4 minutes to complete approximately. The results suggest that the loss is quickly reduced and the GNN is able to correctly predict the node states.

5.1.3 Results and Discussion

To evaluate the proposed approach, simulations are carried using NS-3 (Python bindings) with 50–100 UAVs and an area of 2000×2000 m^2. Comparisons are made on grounds of achieved throughput, delay, packet loss, jitter, and packet delivery ratio. To demonstrate the accuracy and correctness, the proposed approach is validated against OLSR driven UAV assisted ground networks. The proposed approach is compared against software-defined UAVs (U-S) and UAVs as base stations (U-B) inspired by the configurations and settings in [281] and [282] for performance and efficiency analysis. The scalability of the proposed technique is verified by varying aerial node deployment and data rates. The section is further discussed in four parts: Simulation settings, Accuracy and correctness, Performance and efficiency analysis, Scalability test.

5.1.3.1 Simulation Settings

Table 5.1: Simulation Parameters.

Simulation Settings	**Values**
No. of Ground Nodes	200
No. of Aerial Nodes	50–100
Ground Node Classification	Wireless Ground Nodes
Dimension	1200×1200 m^2
Ground Communication	IEEE 802.11, Direct Sequence Spread Spectrum (DSSS) Rate 11 Mbps
Aerial-Ground Communication	Low Power Wide Area Network (LPWAN), 2 km Line of Sight Transmission
Aerial-Aerial Communication	LTE
Loss Model	Fiss Propagation Loss Model
Datagram/Segment Size	1460 bytes
Data Rate	1–4 Mbps
Data Burst	Variable
Bit Rate	Constant
Protocol	Transmission Control Protocol (TCP)/User Datagram Protocol (UDP)
Simulation	NS3 (Python Bindings)
Analysis	Python

Simulation results are dependent on data rates and packet size. The complete simulation settings are provided in Table 5.1. The following parameters are used to test the efficiency of the approach:

i *Throughput*: Throughput is the measure of the amount of data successfully transmitted between source and destination over a transmission media. The comparative analysis is performed by equating maximum data rates in UAV-assisted ground networks Th_{maxw}.

ii *Delay*: Delay is a unit time measurement of end-point to end-point communication considering network bottlenecks and unavailability of transmission media. Latency is the cumulative measurement of propagation and serialization delays. Although there exists a subtle distinction between latency and delay, but in the proposed approach latency and delay are used interchangeably as delay is defined as a cumulative entity comprising of router traversal latency, queuing delay, transmission delay, hop count, propagation delay, and connection delay.

iii *Jitter*: Jitter quantifies delay-sensitive dynamic network behavior. The proposed approach considers jitter as the variation in delay.

iv *Packet Delivery Ratio (PDR)*: Packet delivery ratio is the ratio of packets transmitted by the sender to the actual number of packets received at the destination node.

v *Packet Loss*: Packet loss accounts for the number of packets lost in transmission. The proposed approach ascertains it as a proportion between unsuccessful transmis-

sions and the actual number of transmission over the transmission media. Packet loss can occur with UAV being out of range, congestion, frequent broadcasts from ground nodes, dense ground sections, or the overall amount of data being transmitted.

5.1.3.2 Accuracy and Correctness

Multi-UAV-assisted ground networks are multi-hop network configurations where aerial nodes act as transceivers or base stations. The correctness of the proposed approach is demonstrated by running the multi-UAV-assisted ground network configuration in conjunction with the proposed approach. The underlying ground configuration uses OLSR for multi-hop data routing. The largest contributor to network latency in a multi-hop network is the number of hops between the communicating nodes and the actual geographical distance between the nodes. Bottleneck congestions occurring as a result of unequal data transmission capacity of links and devices also contribute substantially to the overall network delays. Multi-hop networks also suffer from suboptimal routing conditions by making suboptimal paths to the destination. Suboptimal path selection increases the overall data arrival intervals. The proposed approach provides solutions to the multi-hop delays and bottleneck congestions by facilitating additional resources in the form of UAV re-purposing. The choice of more than one aerial node reduces the suboptimal routing paths as well. Figure 5.7 reflects the decrease in overall delay as the proposed approach features an average delay of 1.3 s compared to an 8.6 s delay of OLSR configuration.

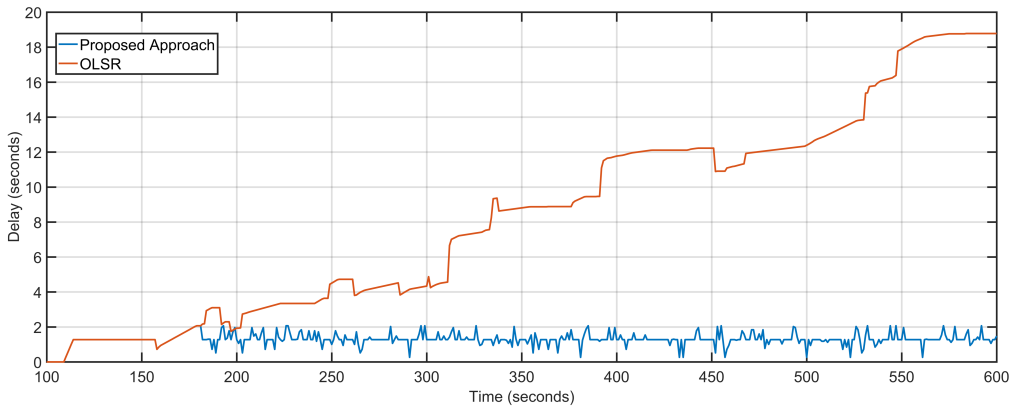


Figure 5.7: Delay Comparison among Proposed Approach and OLSR Configuration. Abbreviations: OLSR, Optimal Link State Routing Protocol.

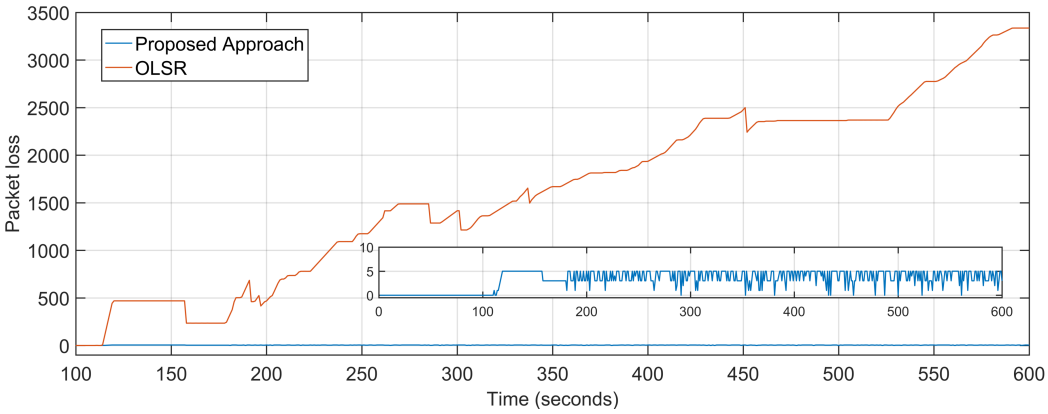


Figure 5.8: Packet Loss Comparison among Proposed Approach and OLSR Configuration. Abbreviations: OLSR, Optimal Link State Routing Protocol.

The average packet loss of the proposed approach is 4 as compared to the staggering 1672 of the OLSR configuration (Figure 5.8). The average jitter, also considered as the variation in delay over time, of the proposed approach is 0.03 and that of the OLSR configuration is 1.4 (Figure 5.9). The proposed approach minimizes the distance as well as the number of hops between the source and destination, resulting in fewer packets lost in transition. Random non-optimized mobility of the aerial nodes adds massively to the packet drop statistics. Packet loss is also directly equated to network congestion and overloaded links and devices. Packets are dropped in volumes if the end device or transmission channel cannot cope with the transmission rates. The unprecedented advantage of the proposed approach towards delay minimization contributes to the advantage when it comes to packet loss rates.

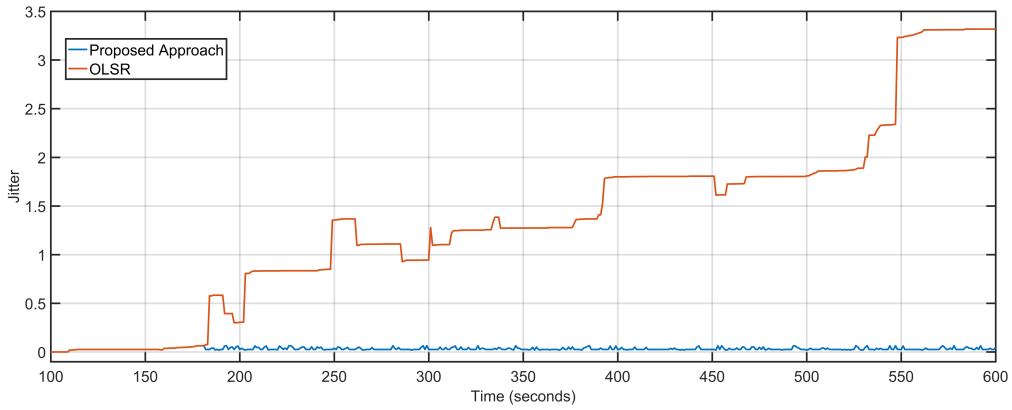


Figure 5.9: Jitter Comparison among Proposed Approach and OLSR Configuration. Abbreviations: OLSR, Optimal Link State Routing Protocol.

The proposed approach is directed towards throughput maximization by minimizing the

overall network delays and packet loss. The minimal packet loss rate converts to a high packet delivery ratio. The PDR of the proposed approach is 0.99 as compared to the OLSR configuration's 0.55 (Figure 5.10). Minimized delay of 1.30 s, less average packet loss of 4, and high PDR of 0.99 result in maximized throughput values. The throughput of the proposed approach is 1021.25 Kbps, as compared to 480.42 Kbps of OLSR network configuration (Figure 5.11). Table 5.2 details the comparative analysis between the proposed approach and OLSR ground network configuration.

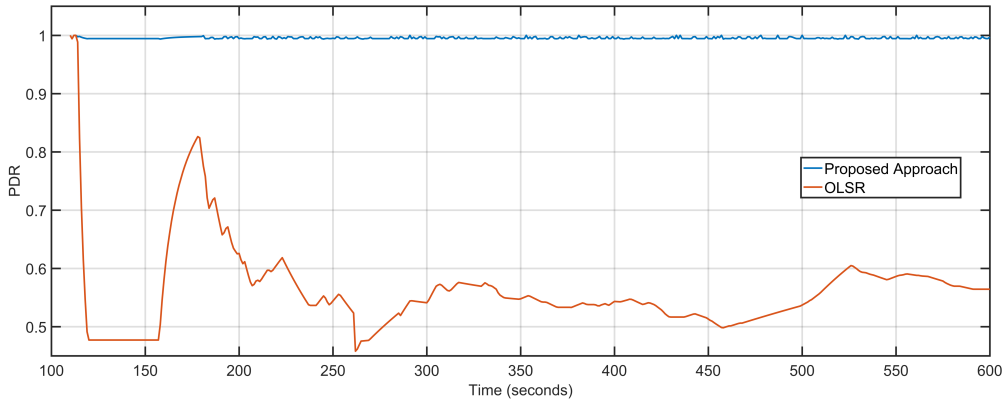


Figure 5.10: Packet Delivery Ratio Comparison among Proposed Approach and OLSR Configuration. Abbreviations: OLSR, Optimal Link State Routing Protocol.

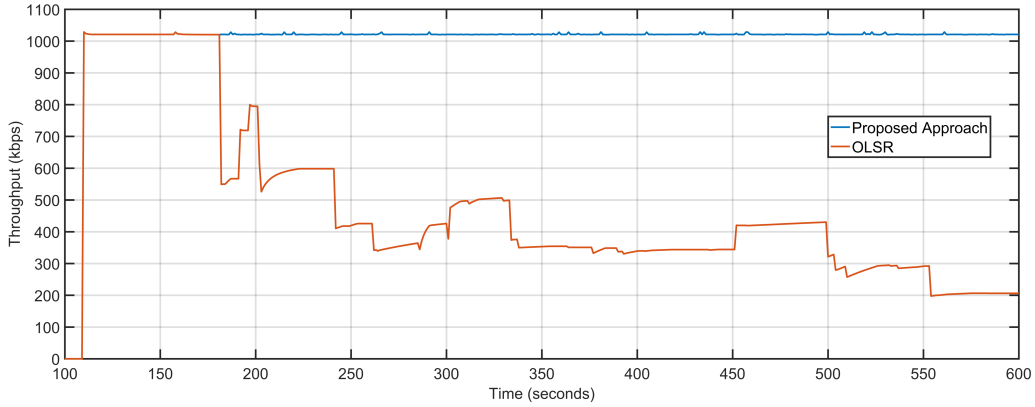


Figure 5.11: Throughput Comparison among Proposed Approach and OLSR Configuration. Abbreviations: OLSR, Optimal Link State Routing Protocol.

Table 5.2: Comparative Analysis Proposed Approach and OLSR Configuration.

Approach	**Delay**	**Packet Loss**	**Jitter**	**PDR**	**Throughput**
Proposed Approach	1.30	4	0.03	0.99	1021.25 Kbps
OLSR	8.55	1672	1.4	0.55	480.42 Kbps

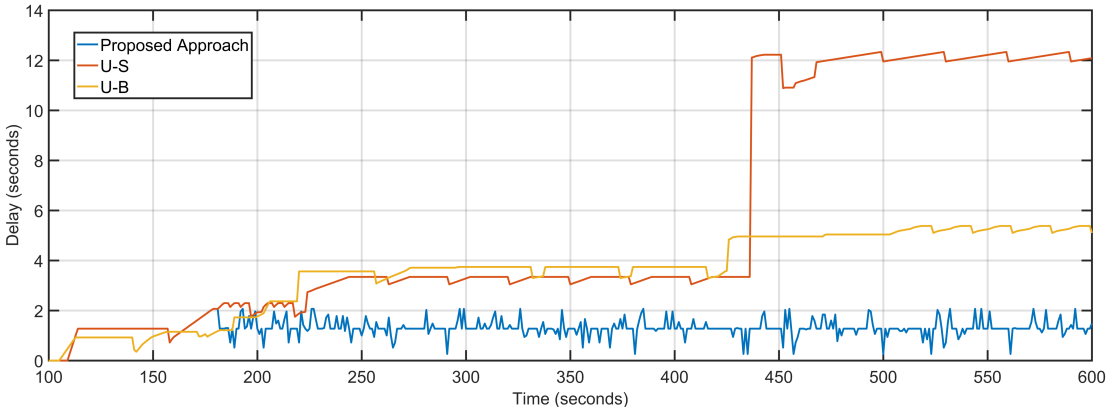


Figure 5.12: Delay Comparison among Proposed Approach, U-S and U-B. Abbreviations: U-S, Software Defined UAV; U-B, UAV as Base Station.

5.1.3.3 Performance and Efficiency Analysis

The performance and efficiency of the proposed approach are evaluated against software-defined UAVs (U-S) and UAVs as base stations (U-B). The three approaches are tested on the same testbed with 50 UAVs. The packet size is 1460 bytes. The data rate is 1 Mbps with a constant bit rate and variable bursts.

The proposed approach features an average delay of 1.30 s as compared to 5.8 s and 3.67 s of U-S and U-B respectively (Figure 5.12). The proposed approach dynamically tracks the aerial topology for bottleneck congestion by keeping track of individual delays and packet loss of the aerial nodes, as well as the sector, where nodes are deployed. Both U-S and U-B feature geographical positioning of nodes with respect to the load characteristics of the underlying geography. U-B has a slight edge over U-S because after fixing the UAV positions, U-B keeps them static. Thus, featuring fewer average delays in the regions where UAVs are deployed which brings down the overall average delay.

The average delay and packet loss of the system depends massively on the distance and number of hops over which data is transferred. The proposed approach not only re-purposes the UAV towards over-burdened nodes but also takes distance and hop count into account by measuring the 3D distance in terms of signal propagation. U-S and U-B have average packet loss of 13 and 16 respectively as compared to four of the proposed approaches (Figure 5.13). The low average packet drop is derived from the predictive dynamic tracking of the proposed approach. The packet loss of U-B is higher than U-S despite boasting lesser delays, this is because after keeping UAV positioning static, the remaining sectors experience a steep decline in packet delivery. The proposed approach, U-S, and U-B feature average jitter of 0.03, 0.99, and 1.04, respectively (Figure 5.14).

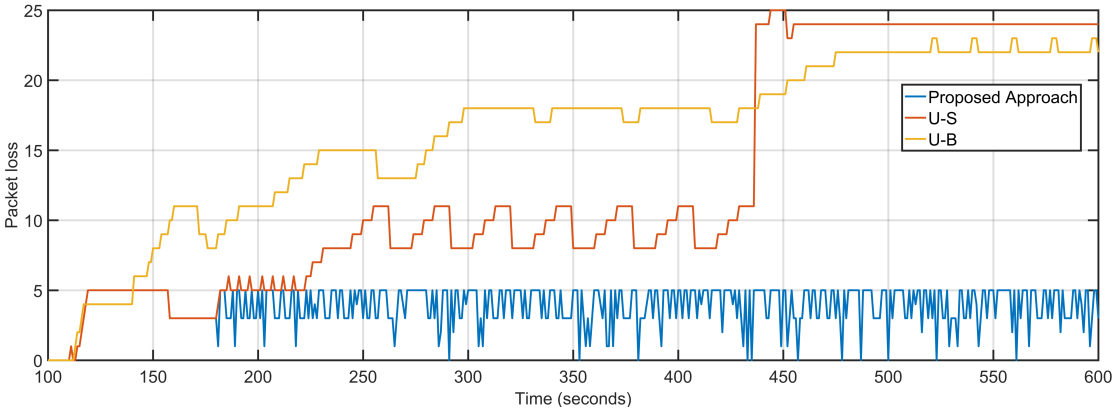


Figure 5.13: Packet Loss Comparison among Proposed Approach, U-S and U-B. Abbreviations: U-S, Software Defined UAV; U-B, UAV as Base Station.

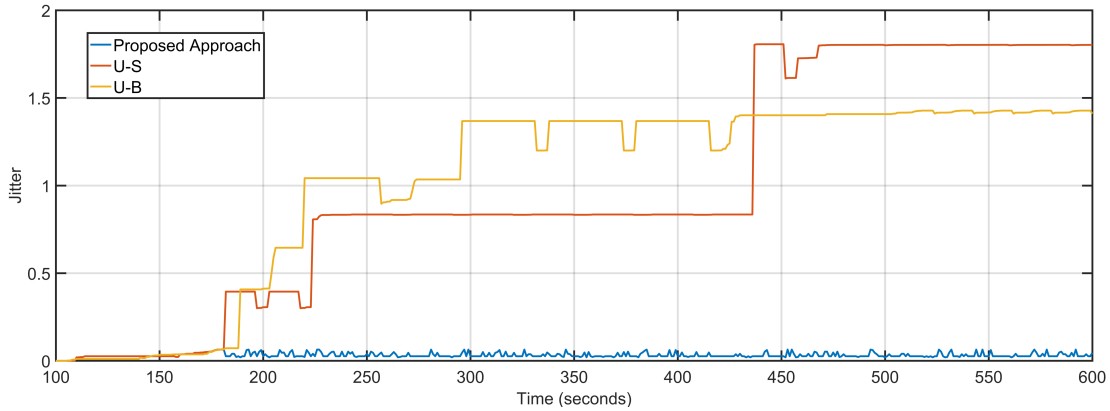


Figure 5.14: Jitter Comparison among Proposed Approach, U-S and U-B. Abbreviations: U-S, Software Defined UAV; U-B, UAV as Base Station.

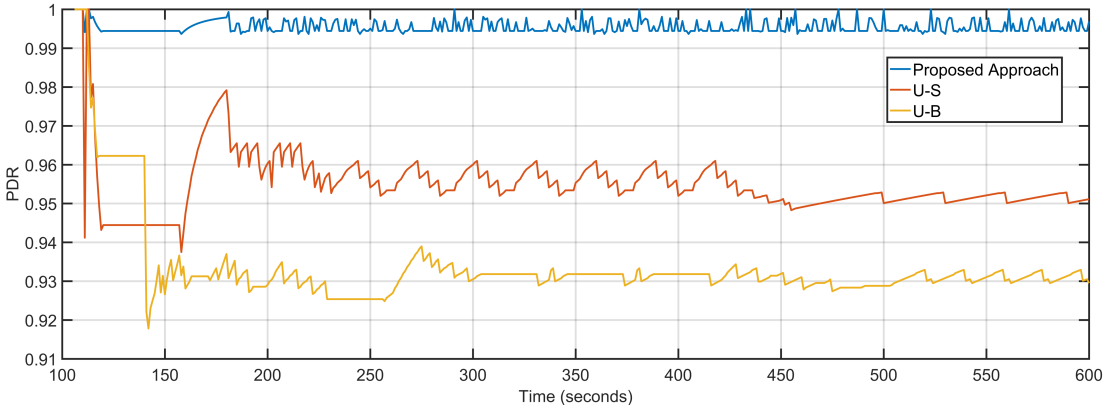


Figure 5.15: Packet Delivery Ratio Comparison among Proposed Approach, U-S and U-B. Abbreviations: U-S, Software Defined UAV; U-B, UAV as Base Station.

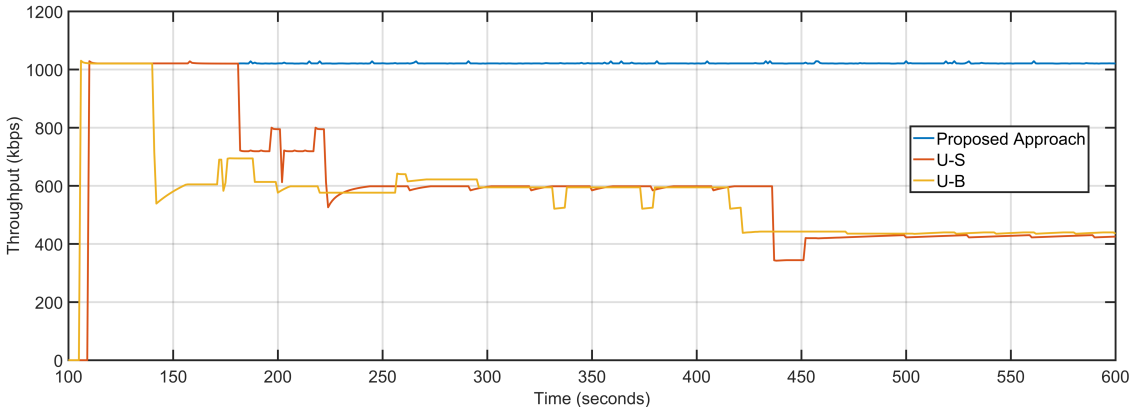


Figure 5.16: Throughput Comparison among Proposed Approach, U-S and U-B. Abbreviations: U-S, Software Defined UAV; U-B, UAV as Base Station.

Table 5.3: Comparative Analysis of the Proposed Approach against U-S and U-B.

Approach	**Delay**	**Packet Loss**	**Jitter**	**PDR**	**Throughput**
Proposed Approach	1.30	4	0.03	0.99	1021.25 Kbps
U-S	5.80	13	0.99	0.95	609.81 Kbps
U-B	3.67	16	1.04	0.93	569.94 Kbps

Less delay and near-optimal packet loss result in maximized PDR and throughput of the proposed approach as compared to its counterparts. The PDR values of the proposed approach, U-S and U-B are 0.99, 0.95 and 0.93 respectively (Figure 5.15). The efficient re-purposing and dynamic tracking of nodes and overall topology result in maximum throughput gains. The average throughputs of the proposed approach, U-S and U-B are 1021.25 Kbps, 609.81 Kbps, and 569.94 Kbps, respectively (Figure 5.16). Table 5.3 details the comparative analysis between the three approaches.

5.1.3.4 Scalability Test

The scalability of the proposed approach is tested by varying the number of aerial nodes and data rates. Simulations are performed by varying the data rate 1–4 Mbps. Another test was performed by keeping the data rate constant to 1 Mbps and varying the deployed UAVs between 50–100. The packet size is 1460 bytes with a constant bit rate and variable bursts.

Delay and packet loss increase slightly when data rates are gradually incremented. Increasing data rate but keeping the number of UAVs constant reverses the gains of higher data rates when it comes to delay and packet loss. The transmission capacity of the ground and aerial devices increases but the number of UAVs available for reception and re-purposing remains the same. The higher data generation with lesser available sinks

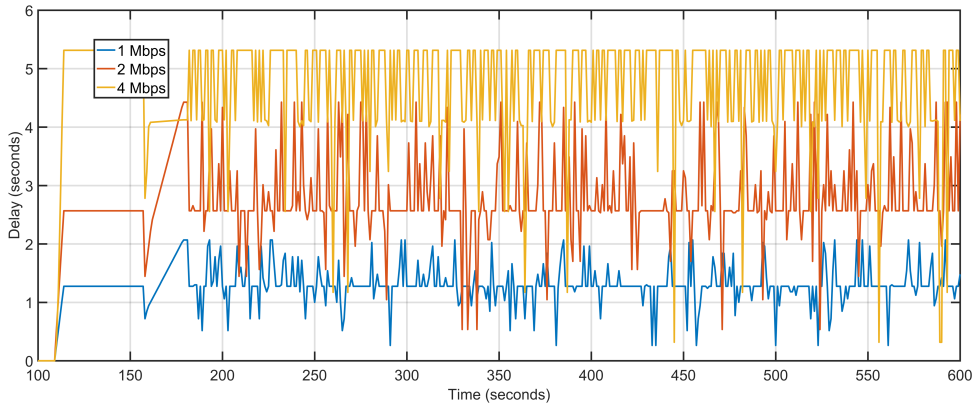


Figure 5.17: Delay Analysis of the Proposed Approach by Varying the Data Rate between 1 Mbps, 2 Mbps and 4 Mbps. Abbreviations: Mbps, Megabits per Second.

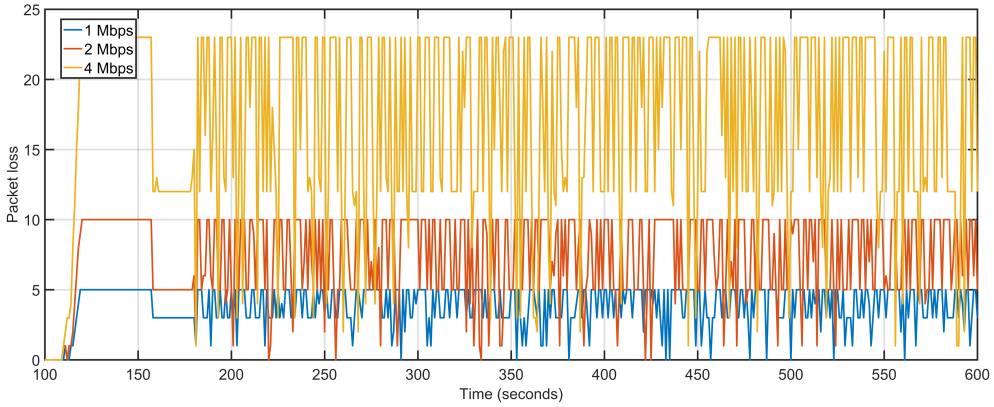


Figure 5.18: Packet Loss Analysis of the Proposed Approach by Varying the Data Rate between 1 Mbps, 2 Mbps and 4 Mbps. Abbreviations: Mbps, Megabits per Second.

pushes back the networks towards multi-hoping and sub-optimal path selections. This abrupt behavior is effectively managed by the proposed approach which sees only a slight variation in delay values. The average delay values at 1 Mbps, 2 Mbps, and 4 Mbps are 1.30 s, 2.78 s, and 4.70 s, respectively (Figure 5.17). With increasing data rates, the packet drop at the interface queue is affected. High data rates cause congestion and overflow in the forwarding node resulting in packet drops. The average packet drop at 1 Mbps, 2 Mbps, and 4 Mbps are 4, 8, and 17, respectively (Figure 5.18). The average jitter at 1 Mbps, 2 Mbps, and 4 Mbps are 0.03, 0.05, and 0.04, respectively (Figure 5.19).

The microscopic variations in delay and packet loss rates keep the average PDR levels constant (Figure 5.20). Throughput is affected marginally with data rate being increased from 1 Mbps to 2 Mbps, with values shifting from 1021.25 Kbps to 2039.26 Kbps. The only noticeable difference in throughput arrives when the data rate is further doubled from 2 Mbps to 4 Mbps and the throughput levels rise from 2039.26 Kbps to 3284.56

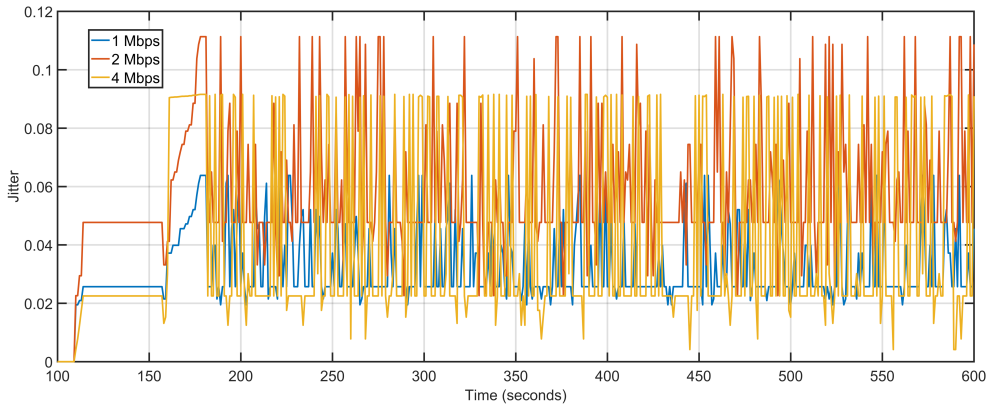


Figure 5.19: Jitter Analysis of the Proposed Approach by Varying the Data Rate between 1 Mbps, 2 Mbps and 4 Mbps. Abbreviations: Mbps, Megabits per Second..

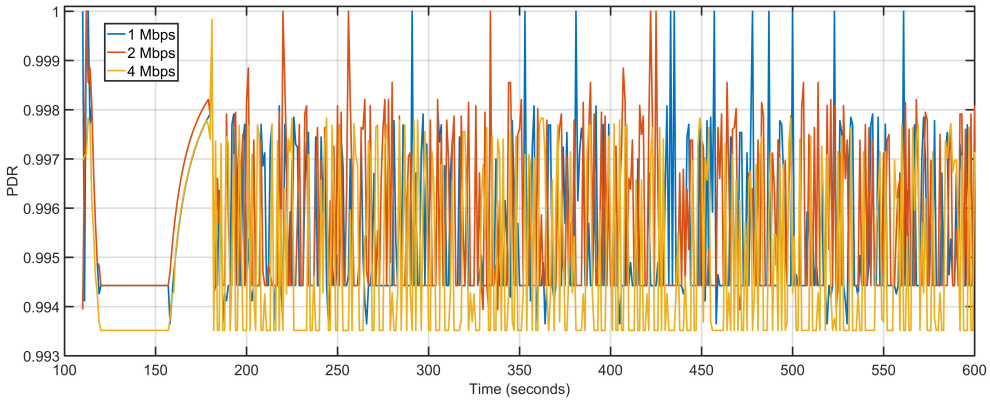


Figure 5.20: Packet Delivery Ratio Analysis of the Proposed Approach by Varying the Data Rate between 1 Mbps, 2 Mbps and 4 Mbps. Abbreviations: Mbps, Megabits per Second.

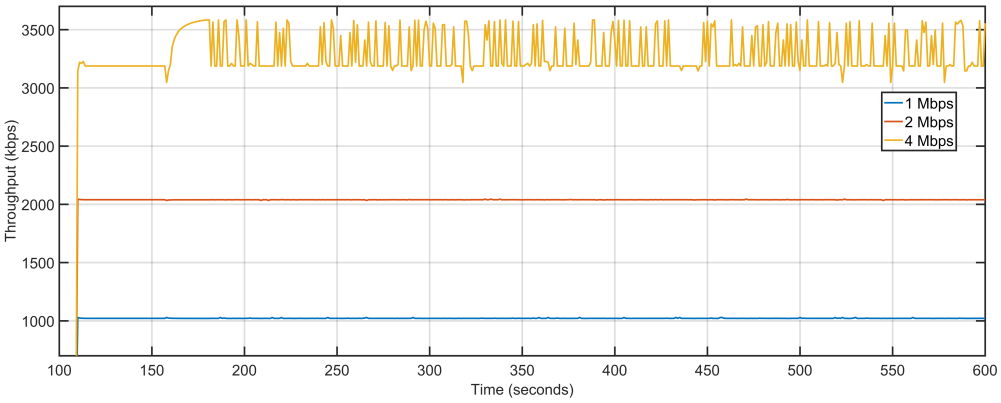


Figure 5.21: Throughput Analysis of the Proposed Approach by Varying the Data Rate between 1 Mbps, 2 Mbps and 4 Mbps. Abbreviations: Mbps, Megabits per Second.

Kbps (Figure 5.21). Table 5.4 details the performance of the proposed approach with varying data rates. Simulation tests over iteratively increasing data rates suggest that an efficient compromise between the available number of nodes and data rate is required to achieve consistent performance levels.

Table 5.4: Scalability Test by Varying the Data Rate between 1 Mbps, 2 Mbps and 4 Mbps.

Data Rate	**Delay**	**Packet Loss**	**Jitter**	**PDR**	**Throughput**
1 Mbps	1.30	4	0.03	0.99	1021.25 Kbps
2 Mbps	2.78	8	0.05	0.99	2039.26 Kbps
4 Mbps	4.70	17	0.04	0.99	3284.56 Kbps

The second scalability run is performed by keeping the data rate constant at 1 Mbps and varying the number of aerial nodes between 50, 75, and 100. Iteratively increasing the number of nodes witnesses a gradual but slow rise in delay and packet loss. The increased delay and packet loss are a result of more devices contending for the same transmission channels resulting in congestion and backoffs. An aerial node anticipates congestion in the network resulting from more and more nodes competing for the same channel. The node initializes its backoff counter and waits for a random amount of time before retransmitting. When the transmission is re-attempted, congestion is detected again, resulting in an incremented backoff value. The congestion persists as a result of increasing the number of aerial nodes but not maintaining sufficient data rates. The average delay values of 50 UAVs, 75 UAVs and 100 UAVs are 1.30, 1.34 and 1.71 respectively (Figure 5.22). The average packet losses after deploying 50 UAVs, 75 UAVs, and 100 UAVs are 4, 7, and 12 respectively (Figure 5.23). The average jitters at 50 UAVs, 75 UAVs and 100 UAVs are 0.03, 0.04 and 0.06 respectively (Figure 5.24).

Once again, the microscopic variations in delay and packet loss rates have less impact on average PDR (Figure 5.25). The throughput on the other hand witnessed a steep decline as the number of aerial nodes increase. One of the factors behind the decline is that more and more nodes contest for channel access causing congestion and nodes to back off, the other reason being the congestion and backoffs activate the proposed approach towards re-purposing UAVs. The high re-purposing results in high mobility of the aerial nodes, which in turn affects the overall throughput. The average throughputs at 50 UAVs, 75 UAVs, and 100 UAVs are 1021.25 Kbps, 728.57 Kbps, and 696.34 Kbps, respectively (Figure 5.26). Table 5.5 details the contrast in the execution of the proposed technique when the numbers of aerial nodes are varied.

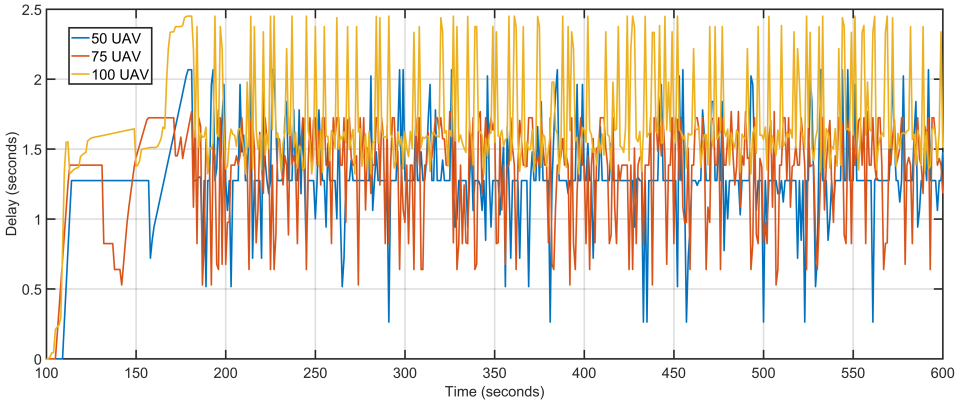


Figure 5.22: Delay Analysis of the Proposed Approach by Varying the UAVs between 50, 75 and 100. Abbreviations: UAV, Unmanned Aerial Vehicle.

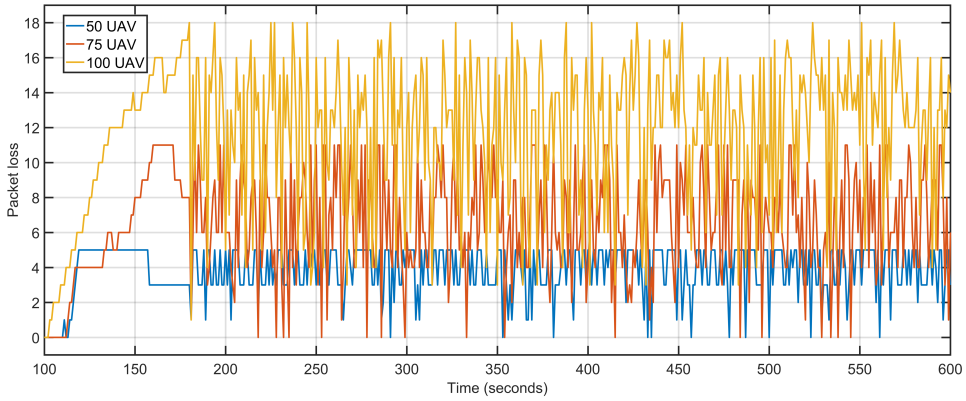


Figure 5.23: Packet Loss Analysis of the Proposed Approach by Varying the UAVs between 50, 75 and 100. Abbreviations: UAV, Unmanned Aerial Vehicle.

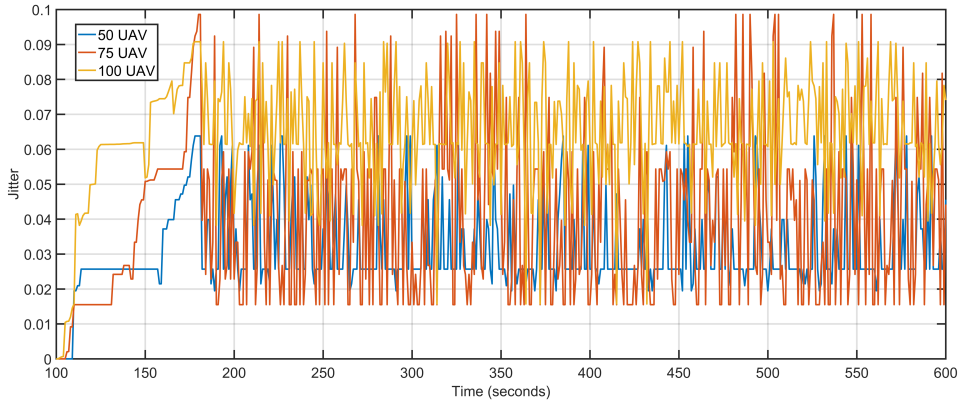


Figure 5.24: Jitter Analysis of the Proposed Approach by Varying the UAVs between 50, 75 and 100. Abbreviations: UAV, Unmanned Aerial Vehicle.

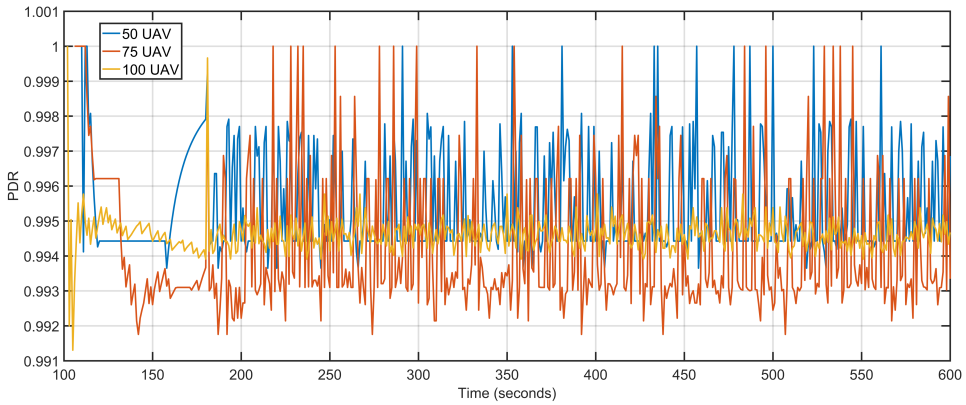


Figure 5.25: Packet Delivery Ratio Analysis of the Proposed Approach by Varying the UAVs between 50, 75 and 100. Abbreviations: UAV, Unmanned Aerial Vehicle.

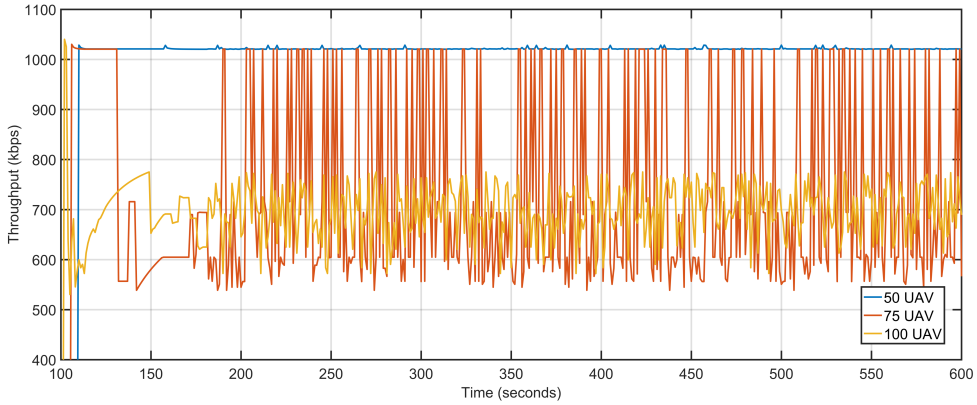


Figure 5.26: Throughput Analysis of the Proposed Approach by Varying the UAVs between 50, 75 and 100. Abbreviations: UAV, Unmanned Aerial Vehicle.

Table 5.5: Scalability Test by Varying the UAVs between 50, 75 and 100.

No. of UAVs	**Delay**	**Packet Loss**	**Jitter**	**PDR**	**Throughput**
50	1.30	4	0.03	0.99	1021.25 Kbps
75	1.34	7	0.04	0.99	728.57 Kbps
100	1.71	12	0.06	0.99	696.34 Kbps

5.2 Conclusions

In this chapter, a UAV re-purposing-based approach for throughput maximization, delay, and packet loss minimization is presented. The proposed approach employs GNN-based dynamic learning and prediction mechanism to re-purpose available UAVs towards the congested and over-burdened sectors of the topology. The state monitoring neural network architecture makes the approach more reactive and aggressive while at the same time channel prorogation based distancing makes the solution more efficient. The proposed approach is compared against the OLSR-driven UAV-assisted ground network model to demonstrate the correctness. The proposed UAV re-purposing technique tremendously outperforms the classical approach with notable gains in throughput and packet delivery ratio while at the same time minimizing the losses. Moreover, a comparative study of the proposed approach is provided by comparing it against U-S and U-B. The approach establishes its supremacy by demonstrating considerable gains over U-S and U-B when compared on the merits of throughput while at the same time achieves lesser delays and packet loss as compared to the two models. The scalability analysis of the proposed approach demonstrates the effectiveness of the approach under adverse scenarios. Scalability test also establishes another important general network characteristic that the data rate and the number of devices must work together under guided compromise to archive significant gains.

The simulation results prove that an efficient compromise between the data rate and the number of nodes is required to maintain consistent system performance levels. Increasing data rates without changing the number of nodes or increasing the number of nodes without improving the data rate leads to a gradual decline in system performance.

Chapter 6

Safety Framework for Multi-UAV Ad hoc Networks [5]

The autonomously connected networks are bringing in unprecedented innovations in military and civilian aviation, but if unaddressed, the conceptualization of attacks on UAV systems is as inherent as the exciting possibilities and future that comes along UAS. As auxiliary efforts are pushed towards collaborative autonomous network formations, and despite serving prodigious applications, more efforts are needed towards secure transmissions by safeguarding the UAV nodes against malicious attacks. This has always lacked the pedestal position among the researchers.

Generally, the efforts towards the safety of UAS are reactive and directed towards channel monitoring and antenna transmission, instead of safeguarding the UAV and overall networked system. Much of the literature is concentrated around resource allocation, signal strength and antenna optimization challenges. The reactive hierarchical network and cyber threats originate from more direct active attacks against UAVs and UAS, targeted towards data, control, and communication. Active attacks make the overall network vulnerable and facilitate control over UAV nodes (or introduce malicious UAVs), hence paving a way towards network intrusions. Active attacks against UAS include UAV-jacking, GPS attacks, UAV identity cloning, rogue UAV operators and outside drones, internal adversary, supply chain attacks and UAV capturing.

UAVs are equipped and made up of independent sophisticated technological equipment, it is possible to attack an individual component and then launch an attack on the overall aerial network. UAVs collect and collaborate massive amounts of information through its sensors, GPS, camera and neighboring nodes. A hijacked drone can result in a nightmare of amplified magnitudes. Once compromised, a UAV can be used to direct terror attacks, acts of mischief and crimes like the white hat and black marketing. Delivery drones can result in loss of cargo or the expensive hardware itself [175].

An autonomous book delivery drone once hijacked can be used to deliver arms and

[5] Mohd. Abuzar Sayeed, Rajesh Kumar, Vishal Sharma *"Safeguarding unmanned aerial systems: an approach for identifying malicious aerial nodes"*, IET Communications (IF 2.100), 2020. [Published]

narcotics. UAVs are coordinated using GPS signals from high altitude satellites. The signals from the long-range orbital satellites are weak and are easily masked by a local transmitter, making them susceptible to spoofing and jamming. UAV-jacking attacks can be mounted by fooling the navigation controls of an in-flight UAV. An intended attacker can manipulate the un-encrypted navigational command sent to the UAV, fooling its navigation system into tracking a falsified/counterfeit GPS signal. The attacker can force a UAV to land, as an off-target location can be projected as a pre-programmed mission directive. The weak signal strength can be exploited by jamming GPS satellite signals forcing a UAV to lose its sense of location [152]. The hackers can operate on a delay time of signals, and amplify or attenuate them [156]. The node will accept the attackers' command and discard the actual commands from the operator [157, 158]. The malware can be hidden in the libraries, middleware, OS, firmware and micro controller chips [159, 160]. The supply chain threat exists because the drones are largely manufactured and assembled from components manufactured by different vendors.

With the number of possible permutations for compromising operational safety of an aerial network, once, inside the network, the attacker can unleash malicious nodes, with a threat to UAV systems ranging anywhere from confidentiality, integrity, authentication, non-repudiation to scalability. Attacks on UAV systems are possible at any layer of communication: Application (malicious code, repudiation, data corruption, impersonation, authentication), Transport (TCP attacks, flooding, session attacks), Network (DoS, routing attacks, flooding, resource poisoning, wormhole, Byzantine, information disclosure, packet replication, cache poisoning), Data Link (MAC attack, DoS, traffic monitoring) and Physical (jamming and DoS).

The rudimentary step towards an end-to-end secure UAS is not only safeguarding communication paths but also securing the overall environment which makes up the platform. Communication paths, end devices, base station, packet core, backbone network and underlying IP networks together constitute the UAS operational environment. The drone should be able to verify the source of transmissions (command/control) it is receiving, and reject those coming from malicious transmitters. Drone operational environment should be built in a way that it is automatically able to detect common attacks such as replay, which use the same principles as a DDoS attack to bombard the target device with commands to disrupt or gain entry.

A layered model can facilitate a centralized framework that elevates the challenges towards the placement of safety paradigms. Functions can be implemented in aerial nodes or central command directive depending on the stated mission requirements and classified threats. Furthermore, bringing the functions towards the network edge, or the

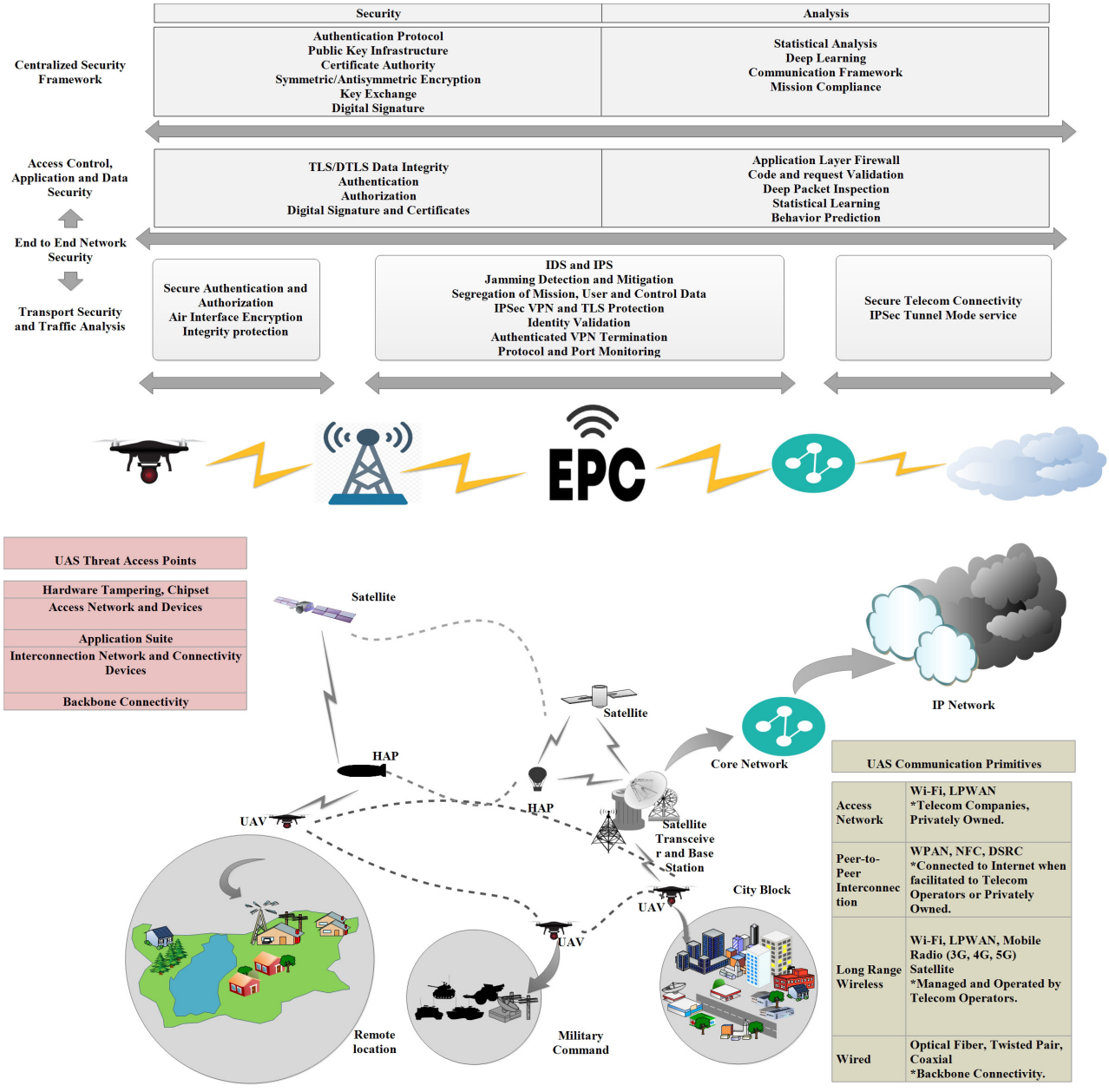


Figure 6.1: Unmanned Aerial System (UAS), UAS Communication Primitives, Threats, Layers of Security and Secure Framework Requirements.

end nodes, increases the effectiveness of the overall solution. Figure 6.1 provides depth and details of the UAS structure, security and functional requirements towards a layered framework.

6.1 Identifying Malicious Aerial Nodes

Malicious attackers can gain entry into the UAS by utilizing UAV jacking, GPS attacks, UAV identity cloning, rogue/inconsiderate UAVs, outside drones, internal adversaries, unskilled operators, supply chain attacks and UAV capture. Once inside the system, several possible attacks can be mounted, thus, making it obligatory to have a layered centralized framework that safeguards from malicious intruders and incorporates privacy protection mechanisms.

The proposed UAS safety framework addresses the threats originating from rogue and inconsiderate UAVs, from within the organizational structure, eavesdroppers and malicious attackers and incorporates privacy protection mechanisms. At the foreground, the framework enforces a grid-based system layout with a dynamically shuffling grid as the baseline defense mechanism against statistical, information monitoring, hijacking, eavesdropping and mobility pattern threats. Intelligent behavior prediction and statistical analysis runs in the background and keeps track of changes in the overall system behavior and statistics. Statistical and behavioral analysis is important as every time a rogue behavior is detected, the overall system is analyzed and security paradigms are re-initiated to recover the aerial system.

In order to achieve centralized monitoring, tracking and guiding, the proposed framework introduces a conceptual grid based topological layout. The safety primitives are established based on aerial node's position along the grid. The network safety is ascertained by temporally shuffling the grid. Shuffling is orchestrated on the basis of a timeout counter or whenever an unusual behavior is detected or the UAV crosses over to another section of the grid. Communication channels are secured using public key security and privacy mechanisms. The proposed channel security mechanism is low on memory and processing requirements and elevates threats originating from MITM, mobility patterns and statistical analysis. UAV behavior prediction is performed by Long Short Term Memory (LSTM)/Convolutional Neural Network (CNN) and multivariate statistical analysis using principal component analysis (PCA) for threat detection, mitigation and recovery. Behavior prediction is responsible for re-initiating the conceptual system layout and security paradigms. The proposed framework is evaluated with LSTM and CNN. Also, a comparative study of the proposed framework against Behavior Rule Based UAV Intru-

sion Detection System (BRUIDS) [286] and Hierarchical Detection and Response System (HDRS) [287] is presented.

6.1.1 Proposed Framework

A multi-tier framework for UAS safety is proposed in this section. The framework can capitalize and take advantage of 4G, 5G or any available communication channel and is split into three components: the UAS mission planning, the UAS safety component (resides in part at both UAV and base station) and the communication component. The UAS safety component also features the mission-specific routing, MAC, logs and database to facilitate efficient operation and provides input to the prediction algorithms. The communication component employs 4G, 5G, LPWAN or any available communication technology to facilitate seamless communication between UAV and other components of the system, including other UAVs. The proposed framework employs LSTM [288]/CNN [289] for behaviour and time-series predictions. PCA based multivariate statistical outlier detection is used to detect outliers in the group. The framework marks an inception work in the field of UAS and UAV safety. Being one of a kind approaches, the analysis of the proposed framework is performed by running the same testbed against different algorithms (LSTM and CNN). Also, a comparative analysis of the proposed approach with BRUIDS and HRDS is presented.

The UAS safety framework projects the underlying geography into a virtual grid. The base station divides the area into a user defined or dynamic $(L \times B \times H)$ grid. The aerial nodes do not know about this geographical cross-section and the layout information is kept with the base station only to counter the threats from a compromised or rogue UAV. The cross-section is assumed to be a cube or a three-dimensional hexagon, as the omni-directional antenna emissions are spherical or nearly spherical. Each aerial node is equipped with a GPS sensor and periodically updates the base station. The UAVs send two types of packets. The data packet carries user and mission data. The GPS info (path, trajectory and speed characteristics, position tracking), encryption details, security keys, permission details, UAV-UAV communication requests, details about authentication failures, channel use and request characteristic are sent through control messages.

The UAS mission planning component considers mission directives, objectives and statistical primitives through its mission control sub-component. The topology former keeps in the desired topology best suited to the mission and considers the ever-changing network to restructure the topology when required. Active topology contains the current operational network formation and the forwarding information base works on the active topology component to derive current route information.

The UAS safety component consists of security, analysis and mission data sub-components. The security sub-component, in conjunction with analysis sub-component, serves as the primary module and is responsible for maintaining overall communication security and guarding against the threats arising from malicious inconsiderate rogue UAVs and internal adversaries.

The proposed framework runs three phases simultaneously. The communication links are secured using cryptographic algorithms and prevention against malicious intruders or hijacked nodes are facilitated by behavior prediction and outlier detection techniques. The data traffic between UAV-base station and UAV-UAV is encrypted using asymmetric algorithms. Elliptic Curve Cryptography (ECC) which uses public-key encryption based on elliptic curves over finite fields is used for encrypting data traffic between aerial and ground stations. ECC is used instead of Rivest Shamir Adelman (RSA) algorithm because ECC provides the same level of security with a considerably smaller key size than RSA. A $256-bit$ ECC encryption is equivalent to $3072-bit$ RSA encryption. The larger key size of RSA imposes timing constraints and require more processing power on the miniature aerial nodes, increasing the system complexity. Shared key symmetric algorithms like Advanced Encryption Standard (AES) provide the same level of security with even smaller key sizes. A $128-bit$ AES provides cryptographic strength equivalent to $256-bit$ ECC. Symmetric cryptography is a challenge as the key needs to be stored in the UAV all the time and a compromised node can compromise the overall system. However, an asymmetric algorithm can initiate a mid-flight key generation and secure key exchange in a hostile environment.

Elliptic curve Diffie-Hellman is used as the key agreement protocol, as it is not only used for encryption but key generation and key exchange as well. The communicating entities create public ($PU_a = PR_a \times G, PU_b = PR_b \times G$) and private keys ($PR_a, PR_b$) using the same domain parameters (the same base point G which generates the subgroup, elliptic curve and finite field). Man in the middle or a malicious UAV can intercept the transmission and capture the public keys but it is impossible to generate private keys without solving the discrete logarithmic problem. The discrete logarithmic problem belongs to the intersection of non-deterministic polynomial time (NP), $Co-NP$ and bounded-error quantum polynomial-time. Furthermore, the shared symmetric key can be generated using the public and private keys to facilitate encryption using ciphers like AES, DES or 3DES. Elliptic curve digital signature algorithm (ECDSA) is used to verify data integrity. Instead of generating the HASH of the entire message, the ECDSA works on the hash function itself. $160-bit$ ECDSA provides the same integrity level as the $1024-bit$ DSA constraining the same signature size.

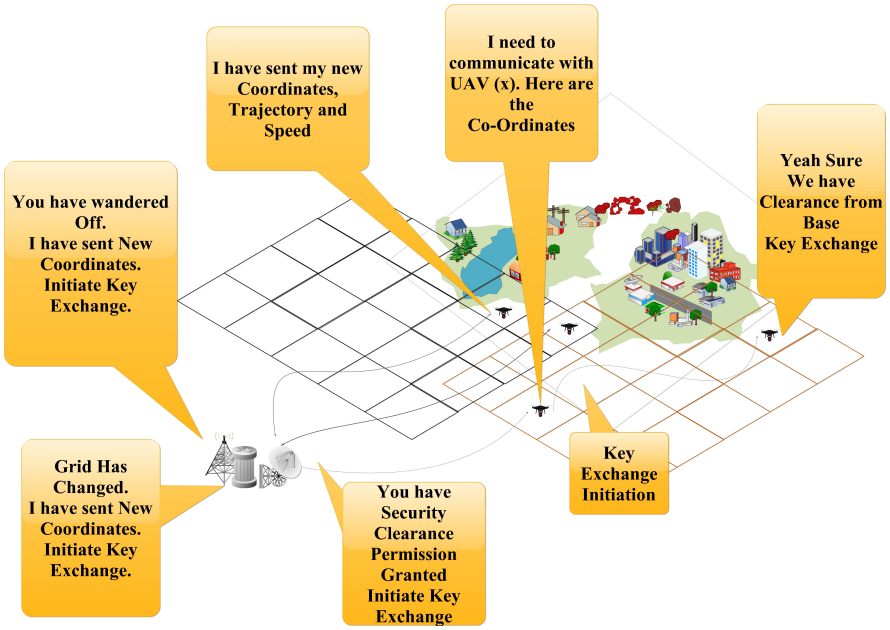


Figure 6.2: Dynamic Grid Layout of the Proposed UAS Safety Framework.

To safeguard against the threats mounted from movement patterns and traffic analysis, the overall area is divided into a grid and every UAV entering the grid or a new location on the grid is required to generate new pair of keys with the base station for that particular section of the grid. The base station divides the area into smaller sectors based on geography/positioning by considering the signal strength of the UAVs. The base station periodically requests UAV's position (UAV periodically sends the same to the intended base station). The base station can randomly (or predetermined, based on prediction algorithm) disqualify the current key and enter into negotiating new pair of keys between itself and the aerial node, whenever UAV has entered a new section on the grid. The base station also keeps track of UAV trajectory and velocity and can initiate new key exchange if the UAV is not on its expected path and behavior, given the acceptable delta of behavioral change (under no circumstances the UAV is informed about the virtual segmentation of the overall geography).

UAVs can communicate with each other if the base station agrees and initiates a key exchange between the communicating parties. Every transmission (data or control) except the key negotiation process is encrypted. The base station also periodically updates and changes the grid positioning accompanied by key negotiation, providing additional security against the threats related to mobility and data monitoring (Figure 6.2).

The behavioral analysis and prediction are important to provide security against hijacked rouge UAVs and inconsiderate nodes, to safeguard the overall performance and integrity of the network. The UAV is required to inform the base station (base station also keeps

track of the GPS data on its own) about any change in path, trajectory, speed, data traffic and authentication failures. The change in parameters is acceptable within a given delta threshold (mission dependent and based on the previous system runs), which are decided based on geography and emission characteristics. The system gathers the data required from UAVs for the initial predefined interval. The collected parameter behavior set is processed with LSTM/CNN for time series prediction. As UAV behavior is established (forecast), the current behavior is matched with the observed behavior. If the current behavior lies within the acceptable deviations from the forecasted behavior, the new values are retained in the system log files. The framework uses the retained files as new data for training the LSTM/CNN. Continuous learning makes the system dynamic and robust. The non-static threshold value, which changes with every learning event the system performs using LSTM/CNN, is used for determining the acceptable deviations from the predicted behavior.

LSTM is a deep learning algorithm that makes use of artificial recurrent neural networks architecture. LSTM networks are best suited to make predictions based on time series data. LSTM removes long-term dependency problem, as look backward capabilities are required for behaviour prediction of UAVs. A sudden influx of messages from a particular aerial node can be because of a grid shift initiated by the base station, a UAV willing to communicate with another UAV or a UAV has crossed the sector boundaries. Without timing information and the capability to look beyond certain intervals or the capability to support non-periodic parameter vectors, the message influx will be marked false positively as a DoS attack.

Sudden changes in speed and trajectory or authentication failures can also be judged false-positive without the presence of non-periodic neural networks. The input vector provided to the LSTM constitutes position, path, trajectory and velocity tracking (hijacking), authentication failures (identity and integrity compromise) and data traffic and channel use requests (DoS attacks). The scalability of the framework is ensured by the fact that the input vector is extendable in all possible scenarios of attacks and threats.

LSTM loops pass information from the current cell/unit of the LSTM to the next, and so on. Every LSTM cell decides which information is to be kept and what part of the information can be discarded/forgotten before passing it to its successor. For the prediction of UAV behavior in terms of velocity and path, given that drones flight plan and maneuvers are recorded, initially, the LSTM is trained with ideal expected behavior and is given by Equation 6.1:

$$h_{(t-1)} \in M_{Z_{(x,y)}}, \tag{6.1}$$

where, M_Z is the direction cosine between successive points in 3D plane at time $t-1$ and t, $Z_{(x,y)}$ is the set of coordinates in UAV's path (expected) at time $t-1$ and $x_t \in Z_{(x,y)}$.

Packet delivery ratio is considered for prediction of traffic patterns and is given by Equation 6.2:

$$h_{(t-1)} \in PDR_{(t-1)}, \tag{6.2}$$

where, PDR_t is packet delivery ratio and $x_t \in PDR_t$.

Packet received information is used for Predicting channel abuse or denial of service attack and can be written as according to Equation 6.3:

$$h_{(t-1)} \in PR_{(t-1)}, \tag{6.3}$$

where, PR_t is packet received from a single drone and $x_t \in PR_t$.

Key exchange count is used for Predicting authentication pattern and identity tracking and is given Equation 6.4:

$$h_{(t-1)} \in KEx_{(t-1)}, \tag{6.4}$$

where, KEx_t is key exchange count for a single drone and $x_t \in KEx_t$.

The process is described for a single cell in LSTM with incoming input from previous cell as $h_{(t-1)}$ and current input as x_t. $x_t \in$ the set of parameters as described in Equations $(1-4)$. Equation 6.5 defines the forget gate layer.

$$f_t = \sigma(W_f.[h_{(t-1)}, x_t] + b_f), \tag{6.5}$$

where, σ is sigmoid function. W_f is the weight. $h_{(t-1)}$ is the information from previous cell. $x_t \in$ parameters at time t and b_f is the bias.

Equations 6.6 and 6.7 define the information at time t that is to be stored. *tanh* function gives values between -1 and 1.

$$i_t = \sigma(W_i.[h_{(t-1)}, x_t] + b_i), \tag{6.6}$$

$$C_t' = tanh(W_C.[h_{(t-1)}, x_t] + b_C). \tag{6.7}$$

The update function responsible for updating the cell value from time $t-1$ to t is defined by Equation 6.8:

$$C_t = f_t * C_{(t-1)} + i_t * C_t'. \tag{6.8}$$

Equations 6.9 and 6.10 define the output from the cell under consideration at time t.

$$o_t = \sigma(W_o.[h_{(t-1)}, x_t] + b_o), \tag{6.9}$$

$$h_t = o_t * tanh(C_t). \tag{6.10}$$

where, h_t is the output to next cell that is time $t+1$. h_t is the predicted outcome for time $t+1$ after the LSTM are trained.

CNN is a multi-layer deep learning algorithm that works sufficiently well on much smaller pre-processing inputs. CNNs have a specific application for recognition and classification. The hidden convolutional layers of CNN receive the same input vector supplied to the LSTM and convolutes or transforms it and passes it to the next layer. The CNN maps the past parameter values to the current observed values. CNN model has convolutional hidden layers that operate over a sequence of input parameters followed by another convolutional layer doing the same and so on. The pooling layer separates the convolutional output into more segregated and applicable patterns. Both layers are followed by a densely connected layer which translates the convolutional feature extraction. The proposed framework consists of a convolutional layer of 64 filters and a kernel size of 3×3. With max-pooling size set to 2, the input vector includes direction cosines of UAV, PDR, received packet and authentication failures. Our input has six columns. Followed by a pooling layer and dense layer to translate features.

Multivariate system analysis works on the same parameters as the event prediction model to find the outliers. PCA is used to identify the dominant pattern in the vector sets. PCA transforms the correlated elements of the vector into uncorrelated orthogonal elements which are termed as principal components (PC). The PCA finds the first PC such that it accounts for the highest variability in the data, and then the second in order, such that both the components are orthogonal and so on. The resulting vectors form an orthog-

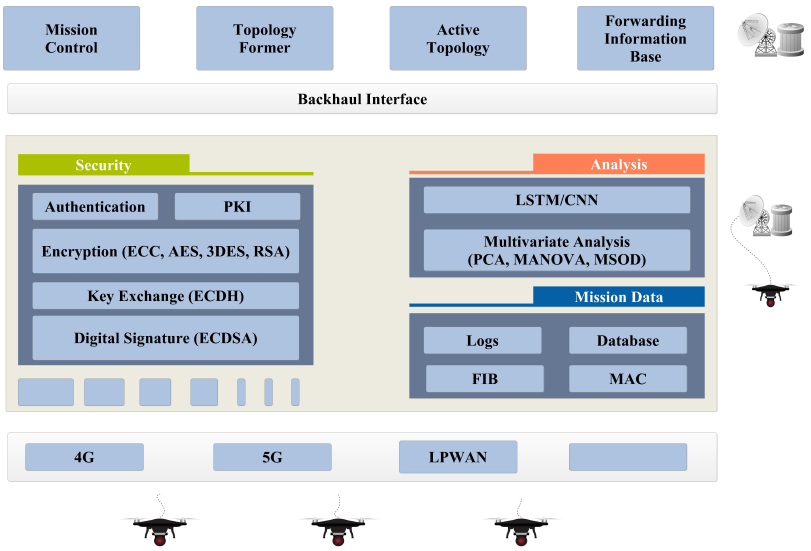


Figure 6.3: An Illustration of the UAS Safety Framework.

onal linearly independent set. The identified PCs (position, path, trajectory, velocity, authentication failures, data traffic and channel request) are subjected to test against the predetermined delta threshold for finding the outlier. The PCA is a dimensionality reduction algorithm. It generates the covariance matrix, computes eigenvectors and values for this covariance matrix and lastly, uses these eigenvectors and values in selecting the most important features in the data set.

The UAS safety framework is described in Figure 6.3 and the complete flow of events is present in Figure 6.4. Algorithm 6.1 presents the channel security and encryption mechanism at the base station. Algorithm 6.2 outlines the analysis and prediction component of the base station. Analysis and prediction costs O(W), where W is the size of the vector fed into the behavioural analysis algorithm. Algorithm 6.3 outlines the UAV operations.

Algorithm 6.1 : Base Station (Encryption)

1: **Input**: Topology in 3 dimensions A
2: Initialize Network and Mark Geographical Area
3: Begin Securing UAV's
4: **if** $OmniDirectionAntenna = True$ **then**
5: Divide the Topology in 3D grids g_i
6: **else**
7: Divide the Topology in 2D grids g_i
8: Initialize Random Number generator for sector time outs RG_t and count down $RG_t - > 0$
9: Reset R=0.
10: Generate new pairs of keys for each sector using ECC, $K1_{sector_i}$ & $K2_{sector_i}$
11: Exchange keys with UAV's in each sector where $K2_{sector_i}$ & $K2_{sector_i}$ is the key pair for i th UAV in Sector $sector$
12: Encrypt all transmission with the exchanged keys.
13: **if** $RG = 0$ **then**
14: goto 3
15: **if** $R = 1$ **then**
16: goto 3

Algorithm 6.2 : Base Station (Analysis)

Ensure Algorithm at base station (Encryption) is initiated
Request UAV logs
Receive UAV's logs
p_i = UAV position
p_k = UAV path
t_i = UAV trajectory
v_i = UAV velocity
ar_i = Authentication request
af_i = Authentication failure
c_i = Channel requests
dt_i = Traffic rate
Apply LSTM/CNN 4-11
P_i = Predicted behavior of UAV_i
if P_i = acceptable Threshold **then**
    continue
else
    re-initiate key Exchange for UAV_i
Outlier = PCA/Multivariate statistical Outlier detection(MSOD).
if *Outlier* = matches mission parameter **then**
    continue
else
    Re-initiate Algorithm at Base station (Encryption)

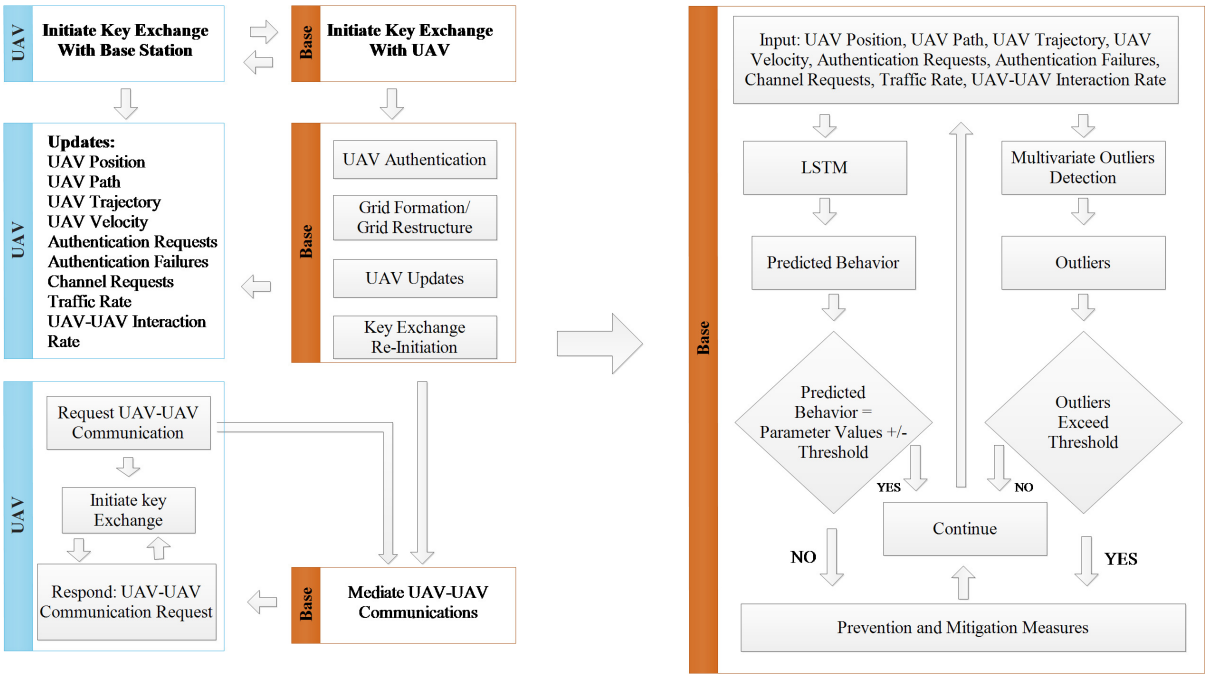


Figure 6.4: Flow Diagram: Proposed UAS Safety Framework.

Algorithm 6.3 : UAV (Operations)

Send Logs to base station periodically and when requested.
p_i = UAV position
p_k = UAV path
t_i = UAV trajectory
v_i = UAV velocity
ar_i = Authentication request
af_i = Authentication failure
c_i = Channel requests
dt_i = Traffic rate
Exchange Key's With the Base Station.
Perform course correction if requested by Base station.

The data set under consideration includes time, position, trajectory, velocity, authentication failures, data traffic and channel request. However, since authentication failures are not frequently dominant features and channel request is directly proportional to data traffic, these are not considered in this step of the framework. For position and trajectory, direction cosines are used. The data set thus essentially becomes (direction cosines of UAV, velocity, PDR, throughput, jitter). The data set is normalised and each feature is weighted equally as according to Equation 6.11 and 6.12.

$$cov_{x,y} = \frac{\sum_{i=1}^{N}(x_i - \bar{x})(y_i - \bar{y})}{N-1}, \tag{6.11}$$

$$\det(\lambda I - \mathcal{A}) = 0. \tag{6.12}$$

where, λ is the eigen value and $\mathcal{A}$ is a matrix $cov_{x,y}$. For each eigen value corresponding, an eigen vector is given by Equation 6.13:

$$(\lambda I - \mathcal{A})v = 0, \tag{6.13}$$

where, v is the eigen vector.

Only the most significant eigenvectors are taken from the feature set: $eigen_1, eigen_2, \ldots, eigen_n$. These feature signatures help identify the UAV situation report (at a given time, the UAV trajectory is unique). For future caparisons and dimensionality reduction, the final set is calculated as according to Equation 6.14:

$$f_s = r_s \times d_s, \tag{6.14}$$

where, f_s is the final vector set, r_s is the row vector of feature set and d_s is the column vector of transformed data.

6.1.2 Performance Evaluation

To evaluate the proposed approach, simulations are performed on $NS3$ with 100 UAVs and 1 base station on an area of 2000 $\times$ 2000 m^2. With each iteration, 10% of the UAVs go rogue, and the final iteration is run with 100 rogue UAVs. Details of the simulation are presented in Table 6.1. The threat signatures introduced in the system are impersonation attacks and privacy violations, hijacking, spoofing, masquerading, flooding

(DDoS), jamming, routing attacks and application-layer attacks. A total of 550 attacks are injected into the system. Analysis of the proposed approach is presented on the merits of several attacks detected, detection rate, number of undetected attacks, false-positive rate, accuracy and the percentage of UAVs recovered from malicious attacks.

The following parameters are used for testing the proposed model:

i *Detection Rate:* Detection rate is defined as the fraction of all faulty nodes which are detected faulty by the proposed approach.

ii *False Positive Rate:* False-positive is the error in reporting a particular event, which is not present. False-positive is considerably different from over testing an event.

iii *Recovery Rate:* Recovery is defined as the percentage of UAVs mitigated from under the malicious attacks.

iv *Accuracy:* Accuracy is defined as the degree to which the result of a measurement conforms to the correct value or a standard.

Table 6.1: Simulation Details.

Experimental Configuration	
Area	2000 × 2000 meters
UAV-UAV Communication	IEEE 802.11 Direct Sequence Spread Spectrum (DSSS) Orthogonal Frequency Division Multiplexing (OFDM)
UAV-Base Communication	Low Power Wide Area Network (LPWAN) Long Term Evolution (LTE)
Protocol	User Datagram Protocol (UDP) Transmission Control Protocol (TCP)
Data Rate	10 Mbps
Packet Size	1024 bytes
Rogue UAV Rate	10 %

The proposed approach is implemented with LSTM/CNN and compared with BRUIDS and HDRS. The proposed approach detects 96% attacks with LSTM and 96.90% attacks with CNN. The attack detection rate of BRUIDS is 8.53% and that of HDRS is 92.72% (Figure 6.5). The simulation results suggest that all methods have good attack detection strength when the number of attacks is low. When the number of attacks grow, the proposed method still performs amicably. The performance gains and robustness of the proposed approach under ever variable and growing threat scenarios can be attributed to the time and space independent safety mechanisms. Also instead of using a static training mechanism, the training process keeps evolving alonside the growing network.

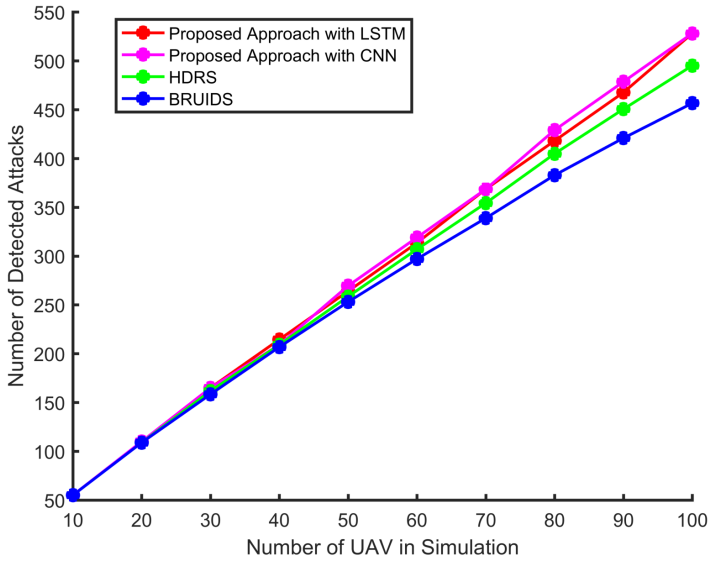


Figure 6.5: Detected Attacks Comparison among Proposed Approach (LSTM), Proposed Approach (CNN), BRUIDS, HRDS. Abbreviations: LSTM, Long Short Term Memory; CNN, Convolutional Neural Network: BRUIDS, Behavior Rule Based UAV Intrusion Detection System; HRDS, Hierarchical Detection and Response System.

With a high detection rate, the number of undetected attacks fall to a low of 3.034 with LSTM and 2.45 with CNN. The number of undetected attacks with BRUIDS and HDRS is 6.31 and 4.01, respectively (Figure 6.6).

The proposed approach has a false positive rate of 0.9 with LSTM and 0.6 with CNN. The areas which are prone to very high data rate are profiled with LSTM and CNN based time series forecasting such that it is not treated as an attack and thereby raising a false positive. An event may arise where authentication, frequently changing environment, grid re-allocation or any other influx in transmission is classified as a threat but temporal predictions and behavioural analysis alongside frequently evolving training mechanism meticulously prevents that. The false-positive rates of BRUIDS and HDRS are 2.6 and 1.8, respectively (Figure 6.7).

The greatest drawback both the approaches suffer from is the profiling of the nodes as well as the geography, not every situation is an attack scenario and vice versa. Random attack pattern can go missing or undetected in BRUIDS and HDRS, but proposed approach takes into consideration every individual node, and the system as a whole, to detect and block the attacks.

Detection rate is the overall percentage of threats identified by a technique whereas the accuracy is defined as the average accuracy calculated iteratively throughout the

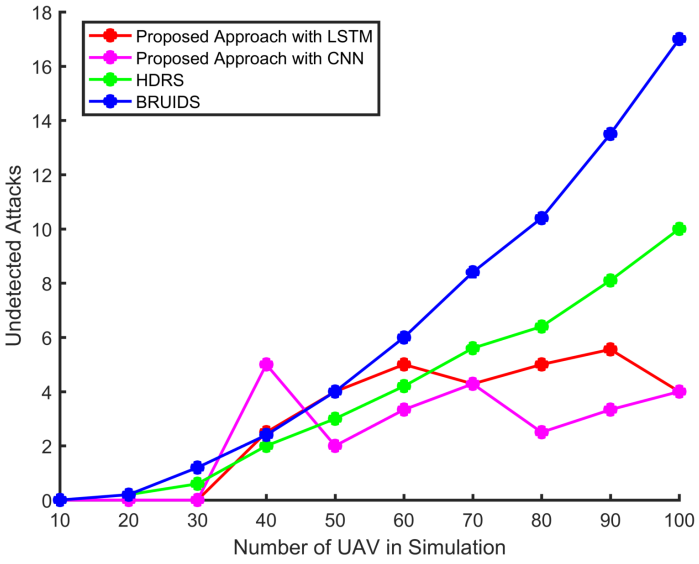


Figure 6.6: Undetected Attacks Comparison among Proposed Approach (LSTM), Proposed Approach (CNN), BRUIDS, HRDS. Abbreviations: LSTM, Long Short Term Memory; CNN, Convolutional Neural Network: BRUIDS, Behavior Rule Based UAV Intrusion Detection System; HRDS, Hierarchical Detection and Response System.

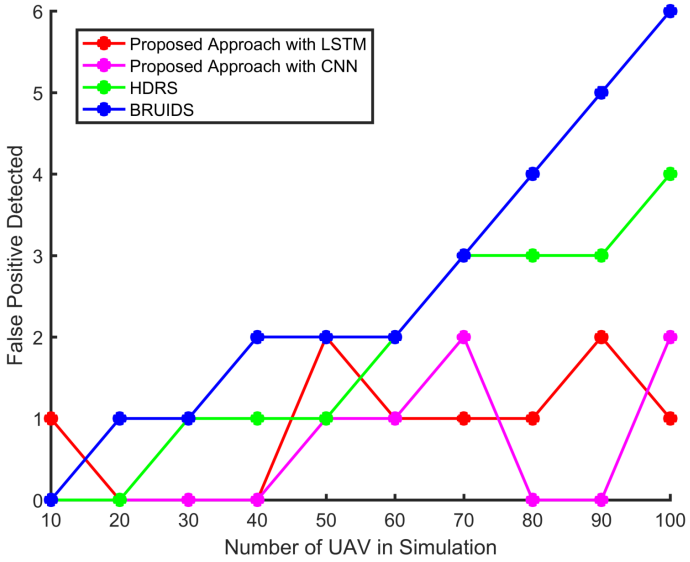


Figure 6.7: False Positive Rate Comparison among Proposed Approach (LSTM), Proposed Approach (CNN), BRUIDS, HRDS. Abbreviations: LSTM, Long Short Term Memory; CNN, Convolutional Neural Network: BRUIDS, Behavior Rule Based UAV Intrusion Detection System; HRDS, Hierarchical Detection and Response System.

repeated simulation. The detection rate of the proposed approach is 96.96% with LSTM and 97.55% with CNN. While the detection rate of BRUIDS is 91.4% and that of HRDS is 94.4% (Figure 6.8). The accuracy of the proposed approach is 94.80% with LSTM

and 96.70% with CNN. BRUIDS and HRDS have an accuracy of 87.24% and 91.74%, respectively (Figure 6.9).

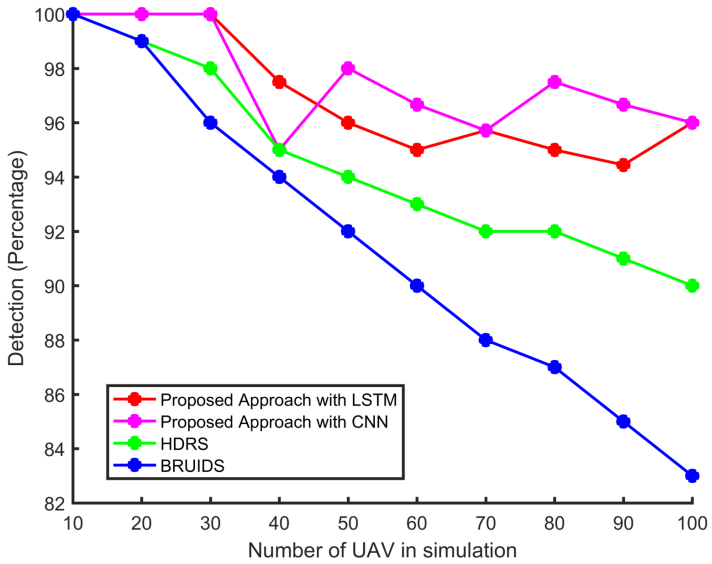


Figure 6.8: Detection Rate Comparison among Proposed Approach (LSTM), Proposed Approach (CNN), BRUIDS, HRDS. Abbreviations: LSTM, Long Short Term Memory; CNN, Convolutional Neural Network: BRUIDS, Behavior Rule Based UAV Intrusion Detection System; HRDS, Hierarchical Detection and Response System.

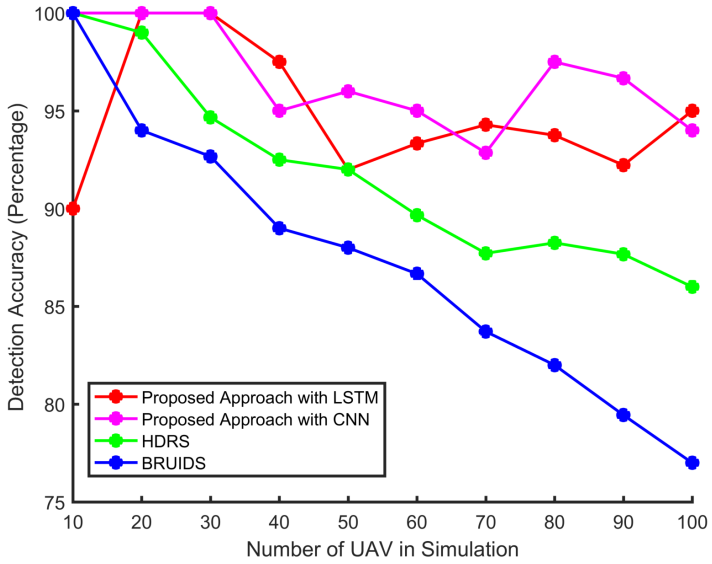


Figure 6.9: Accuracy Comparison among Proposed Approach (LSTM), Proposed Approach (CNN), BRUIDS, HRDS. Abbreviations: LSTM, Long Short Term Memory; CNN, Convolutional Neural Network: BRUIDS, Behavior Rule Based UAV Intrusion Detection System; HRDS, Hierarchical Detection and Response System.

In the simulation, the framework achieves 86.79% recovery rate with LSTM and 86.25%

recovery rate with CNN (Figure 6.10). The key exchange and UAV authentication mechanism ensure that a trusted UAV is only allowed in the system. On the first sign of trouble, the system re-initiates key exchange so that UAV gets a chance to get reintegrated into the system. However, if the UAV has indeed turned rogue the system makes sure that its keys are invalid, and its transmissions are overlooked and dropped by the rest of the UAV in the system. Both BRUIDS and HDRS systems have no provision of recovery.

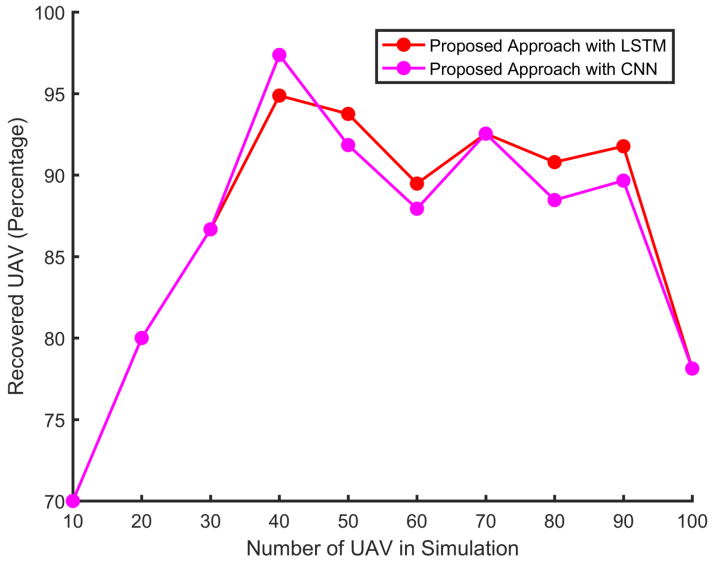


Figure 6.10: Malicious UAV Recovery Rate Comparison among Proposed Approach (LSTM), Proposed Approach (CNN), BRUIDS, HRDS. Abbreviations: LSTM, Long Short Term Memory; CNN, Convolutional Neural Network: BRUIDS, Behavior Rule Based UAV Intrusion Detection System; HRDS, Hierarchical Detection and Response System.

The event prediction using time series forecasting plays an important role in profiling a UAV in the system. Not just the UAV but also specific areas in the grid are profiled based on the data traffic received when the UAV was present at that coordinates. Vulnerable spots of the topology can be profiled, and the flight path of the UAV can be set accordingly. The UAV profiling and outlier detection monitor the system for nodes that go rogue over time. While this may not constitute an attack but a UAV that strays from mission objective becomes vulnerable and liable to be attacked, the proposed security system can identify vulnerable UAVs and try to get them back on mission directive. Comparative statistical analysis of the proposed framework with BRUIDS and HDRS is presented in Table 6.2.

The dynamically changing grid, of which the nodes are uninformed, forces the aerial nodes

towards short-lived authentications and on-demand key exchanges; hence, making it difficult for the rogue UAVs and malicious attackers to engage against the network.

The dynamic grid shuffle, renewal of authentication credential whenever a UAV has crossed into a different section of the grid, On-demand authentications, key exchange whenever the proposed framework suggests deflection from the normal UAV behaviour and the UAV's unawareness of the grid itself elevates the timing constraints as well as safeguards the overall system from the threats originating from the study of mobility and topology. The key exchange and authentication are always between base station-UAV and UAV-UAV and the parameters fed into the learning, prediction and analysis algorithms are independent of network size. Thus, making the network scalable with the capability to accommodate any number of nodes.

Table 6.2: Comparative statistical analysis of the proposed framework with BRUIDS and HDRS.

Technique	Attacker Type	Threat Classification	Criterion	Application Character	Detection Rate	Accuracy	False Positive Rate
BRUIDS	Malicious Nodes	UAV Hijacking Data Corruption Data Disclosure UAV Capture Energy Statistics	Integrity Confidentiality Availability	Probabilistic Specification Based Rules Table driven	91.4 percent	87.24 percent	2.6
HDRS	Malicious Nodes	False Information Data disclosure GPS Spoofing Jamming Black Hole Attacks Grey Hole Attacks	Integrity Denial of Service	Behaviour Categorization Hierarchical Intrusion Detection Deterministic Mobility Model	94.4 percent	91.74 percent	1.8
Proposed Approach	Inconsiderate Nodes Eavesdroppers Internal Adversary Malicious Attacker	Impersonation attacks, Privacy and Policy Violation UAV-Jacking/Capture Spoofing Masquerading Flooding (DDoS) Routing and TCP Attacks Jamming Application Attacks	Authentication Integrity Confidentiality Non-repudiation Availability Access Control Scalability	Cryptographic Privacy Protection Multivariate Statistical Analysis (Continuous In Flight) Deep Learning (CNN/LSTM) Predictions (Continuous In Flight)	96.96, 97.55 percent	High (94.80 to 96.70 percent)	0.6 to 0.9

6.2 Conclusion

This chapter presents an insight into the relatively untouched field of UAS safety and threats directed from inconsiderate nodes, eavesdroppers, internal adversaries and malicious attackers. A scalable framework is proposed as a solution. The proposed framework identifies safety vulnerabilities by monitoring UAV behaviour and statistics. Any deviation is inspected and analysed as a possible threat. The proposed approach guarantees minimal false positive rates. The performance and effectiveness of the complete framework are evaluated side by side using LSTM and CNN and compared with intrusion detection techniques proposed in the literature. Simulation results and analysis prove a significant improvement in threat detection and accuracy with minimal false positive rates.

Chapter 7

Conclusions and Future Works

This chapter concludes the thesis and also provides an insight into the conducted research work, as to how the proposed techniques can be further extended and enhanced. Section 7.1 provides the final concluding summary of the research accomplished. Section 7.2 provides a future directions to the proposed frameworks.

7.1 Conclusion

The thesis presents data dissemination frameworks for multi-UAV ad hoc networks. Alongside the data dissemination framework UAS safety and QoS enhancement approach is also presented. The main contribution of this thesis are done in several phases and they are as follows:

i. Transmission scheduling based data dissemination framework for UAV coordinated WSNs is proposed in Chapter 3, where UAV nodes adapt to data relaying roles between the ground sensor nodes and the base station. The SDN controller manages, configures, maintains and resets the topology and takes care of sleep timers and back-off counters. The proposed framework enhances both throughput and overall network lifetime. Delays and jitters are also minimized alongside enhanced packed delivery ratio.

ii. The proposed framework allows sensor nodes to communicate only when aerial nodes are in range, assuring a one to one communication scenario alongside restricting the ground nodes from flooding the network. Time bound communication paradigm and reduced multi-hopping transmissions result in higher rates of successful packet delivery and increased throughput.

iii. Sensor nodes are put to sleep whenever the sync (UAV) is not in range, unlike traditional approaches where ground nodes constantly flood data packets into the network. As an average measure, a particular sensor node is in the range of UAV only during 25 percent of the UAV cycle time. The proposed SDN controller facilitates efficient maneuvering, data collection, and transmission scheme, resulting in high battery performance with fewer overheads. The back-off counter also add

to the overall network lifetime and performance. Whereas UAVs can be frequently replaced and charged as they can always return to the base station.

iv. The deployment flexibility achieved through the application of SDN controller instead of hardwired transmission control can be visualized through the multi-dimensional scalability of the proposed approach. Comparable performance levels are achieved through both CBR and VBR simulations. The real time applicability of the proposed approach is further strengthened by the separate tests performed on the merits of shifting bit rates and varying aerial nodes. Furthermore Table 3.3 consolidates the application of SDN controller.

v. Mobility and Trajectory based framework for UAV coordinated WSNs is proposed in Chapter 4, where aerial way-points are decided on the basis of attraction factor. The attraction factor in turn is decided on the merits of transmission density of the underlying ground topology. The proposed approach shows significant gains in coverage, throughput, jitter, and data transfer ratios. The packet drop rate is reduced exponentially and massive gains are observed for packet delivery ratio.

vi. The transmission density based UAV's movement, keep the coverage high in terms of the number of ground nodes served. The high service ratio is directly proportional to the achieved maximum throughput levels.With direct aerial-ground communications and reduced multi-hopping, the proposed model is able to restrain delays. Aerial nodes move fromone dense region to another dense region while at the same time collect data from scarce regions by means of multi-hopping or direct transmission towards base station, resulting in high PDR and data transfer.

vii. The attraction factor based data dissemination scheme is further enhanced by the addition of an SDN controller. The proposed SDN controller is used for authentication and coordination of aerial and ground nodes. Alongside providing dimensionality to the scalability of the proposed approach, the SDN controller boosts it's applicability, given any collaborative aerial ground network formations.

viii. A QoS enhancement mechanism for aerial-ground ad hoc networks is proposed in Chapter 5. GNN-based dynamic learning and prediction mechanism is used for guiding UAVs towards overburdened network locations. The proposed UAV repurposing technique tremendously outperforms the classical approach with notable gains in throughput and packet delivery ratio while at the same minimizing the losses.

ix. The applicability, accuracy and correctness of the proposed approach is established by evaluating it against classical OLSR. Alongside performance analysis against the

techniques proposed in literature, the approach proves consistent and scalable when tested with varying bandwidth levels and number of nodes.

x. A framework for UAS safety is proposed for aerial-ground networks. The proposed framework identifies network vulnerabilities by monitoring UAV behaviour and UAS statistics. The proposed approach guarantees minimal false positive rates. The performance and effectiveness of the complete framework is evaluated side by side using LSTM and CNN. Both LSTMand CNN produce comparable results when compared with classical approaches on the merits of detection rate, false positive rate, recovery rate and accuracy.

xi. An important feature of the proposed frameworks is the SDN controller. The proposed solutions are implemented as SDN controller components. The component level design technique makes it easy to upgrade, maintain, replace, re-configure and combine the proposed functionalities with minor re-adjustments. The re-adjustments arise and are dictated by the deployment environment under consideration.

7.2 Scope for Future Work

The work presented in the thesis focuses on efficient data dissemination in multi-UAV ad hoc networks. The proposed techniques and frameworks can be expanded in several ways. Some of the suggestions for future work in this direction are:

i. A centralized SDN controller is proposed for transmission scheduling based data dissemination. Much work is required towards making the controller logically distributed. The logically distributed controller can further enhance the dynamic decision making and boost the overall design. The proposed framework can also be pushed towards completely distributed environment but that will require an efficient scheme which manages the UAV both as separate entities and an integral component of the network.

ii. The mobility based data dissemination approach presents a generalized model for UAV traversals according to the transmission statistics of the underlying geography. The model can be extended to include multi-path traversals that will effectively result in better coverage, throughput and data transfer results in less time. The proposed approach can also be incorporated into Software Defined Networks as a controller component and thus increase its applicability towards various system models and approaches.

iii. Efficient data dissemination schemes and effective trajectory design for UAVs can be utilized for mobile edge computing. It is also important to focus on scalable drone-based networks since the number of users and ground nodes are exponentially increasing. Edge computing can also lead to development of integrated optimization approaches that consider the trade-offs between the aforementioned application objectives such as maximum coverage at the cost of power consumption or the number of drones. Also it should be noted that it is a challenging task as equipping UAVs with high computing devices. UAVs onboard data processing will consume excessive energy that can degrade the overall performance of the mission-critical system.

iv. With information so central and integral in modern infrastructure and defense, Multi UAV data dissemination can be coupled with IoT technology for defense specific purposes. The military is naturally moving towards and adopting technology or tools that improve communication, routing, or processing of information. Internet-connected devices provide access to real-time data, which can be used to make smart, data-driven decisions. The defense industry is already utilizing IOT technology towards logistics, smart bases, data warfare and unmanned systems.

v. QoS can be further enhanced by developing a software defined network (SDN) controller for trajectory optimization. Mid-flight routine modification and network independence facilitated by the SDN controller will make the framework more robust and flexible while boosting scalability at the same time. The interface independent transition supported by SDN will make the proposed approach more reactive and fast to abrupt network changes. The framework can be modified to incorporate energy levels of aerial and ground nodes as part of the feature vector to avoid transmission black holes. A separate algorithm can be developed for monitoring parameter changes over time and facilitate more robust parameter predictions.

vi. Future UAS safety frameworks can focus on the development of algorithms that predict the delta-thresholds based on the pre-determined parameters. As of now, much of the work in the field of UAV network safety is restricted around the optimization of trajectory and channel modelling. Instead, more efficient solutions can be found in statistical analysis and artificial intelligence algorithms, which better suit the dynamic range of applications. Machine learning algorithms can also be trained to fit in a wide range of threat signatures to increase the response time of the system. The inclusion of secure and efficient mutual authentication principles can further enhance the safety of UAS.

References

[1] Mohammad Mozaffari, Walid Saad, Mehdi Bennis, Young-Han Nam, and Mérouane Debbah. A tutorial on uavs for wireless networks: Applications, challenges, and open problems. *IEEE Communications Surveys & Tutorials*, 21(3):2334–2360, 2019.

[2] Ian F Akyildiz, Won-Yeol Lee, Mehmet C Vuran, and Shantidev Mohanty. Next generation/dynamic spectrum access/cognitive radio wireless networks: A survey. *Computer networks*, 50(13):2127–2159, 2006.

[3] Ian F Akyildiz and Xudong Wang. A survey on wireless mesh networks. *IEEE Communications magazine*, 43(9):S23–S30, 2005.

[4] Ricardo Silva, Jorge Sá Silva, and Fernando Boavida. Mobility in wireless sensor networks–survey and proposal. *Computer Communications*, 52:1–20, 2014.

[5] Vishal Sharma and Rajesh Kumar. A cooperative network framework for multi-uav guided ground ad hoc networks. *Journal of Intelligent & Robotic Systems*, 77(3-4):629–652, 2015.

[6] Ilker Bekmezci, Ozgur Koray Sahingoz, and Şamil Temel. Flying ad-hoc networks (fanets): A survey. *Ad Hoc Networks*, 11(3):1254–1270, 2013.

[7] Haque Nawaz, Husnain Mansoor Ali, and Asif Ali Laghari. Uav communication networks issues: A review. *Archives of Computational Methods in Engineering*, pages 1–21, 2020.

[8] Hakim Badis and Abderrezak Rachedi. Modeling tools to evaluate the performance of wireless multi-hop networks. In *Modeling and Simulation of Computer Networks and Systems*, pages 653–682. Elsevier, 2015.

[9] Mamata Rath, Bibudhendu Pati, and Binod Kumar Pattanayak. An overview on social networking: design, issues, emerging trends, and security. *Social Network Analytics: Computational Research Methods and Techniques*, 21, 2018.

[10] Jingjing Gu, Tao Su, Qiuhong Wang, Xiaojiang Du, and Mohsen Guizani. Multiple moving targets surveillance based on a cooperative network for multi-uav. *IEEE Communications Magazine*, 56(4):82–89, 2018.

[11] Meng Hua, Yi Wang, Zhengming Zhang, Chunguo Li, Yongming Huang, and Luxi Yang. Power-efficient communication in uav-aided wireless sensor networks. *IEEE Communications Letters*, 22(6):1264–1267, 2018.

[12] Navuday Sharma, Maurizio Magarini, Dushantha Nalin K Jayakody, Vishal Sharma, and Jun Li. On-demand ultra-dense cloud drone networks: Opportunities, challenges and benefits. *IEEE Communications Magazine*, 56(8):85–91, 2018.

[13] Ali Masood, Navuday Sharma, M Mahtab Alam, Yannick Le Moullec, Davide Scazzoli, Luca Reggiani, Maurizio Magarini, and Rizwan Ahmad. Device-to-device discovery and localization assisted by uavs in pervasive public safety networks. In *Proceedings of the ACM MobiHoc workshop on innovative aerial communication solutions for FIrst REsponders network in emergency scenarios*, pages 6–11, 2019.

[14] Vishal Sharma, Rajesh Kumar, and Punjab Patiala. Service-oriented middleware for multi-uav guided ad hoc networks. *IT CoNvergence PRActice (INPRA)*, 2(3):24–33, 2014.

[15] Simon Morgenthaler, Torsten Braun, Zhongliang Zhao, Thomas Staub, and Markus Anwander. Uavnet: A mobile wireless mesh network using unmanned aerial vehicles. In *2012 IEEE Globecom Workshops*, pages 1603–1608. IEEE, 2012.

[16] Navuday Sharma, Maurizio Magarini, Laura Dossi, Luca Reggiani, and Roberto Nebuloni. A study of channel model parameters for aerial base stations at 2.4 ghz in different environments. In *2018 15th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, pages 1–6. IEEE, 2018.

[17] Lu Song and Ting-lei Huang. A summary of key technologies of ad hoc networks with uav node. In *2010 International Conference on Intelligent Computing and Integrated Systems*, pages 944–949. IEEE, 2010.

[18] Nader Mohamed, Jameela Al-Jaroodi, Imad Jawhar, and Sanja Lazarova-Molnar. A service-oriented middleware for building collaborative uavs. *Journal of Intelligent & Robotic Systems*, 74(1-2):309–321, 2014.

[19] Lav Gupta, Raj Jain, and Gabor Vaszkun. Survey of important issues in uav communication networks. *IEEE Communications Surveys & Tutorials*, 18(2):1123–1152, 2015.

[20] Daniele Giovanni Cileo, Navuday Sharma, and Maurizio Magarini. Coverage, capacity and interference analysis for an aerial base station in different environments. In *2017 International Symposium on Wireless Communication Systems (ISWCS)*, pages 281–286. IEEE, 2017.

[21] Kai Daniel and Christian Wietfeld. Using public network infrastructures for uav remote sensing in civilian security operations. Technical report, DTIC Document, 2011.

[22] Kevin S Pratt, Robin Murphy, Sam Stover, and Chandler Griffin. Conops and autonomy recommendations for vtol small unmanned aerial system based on hurricane katrina operations. *Journal of Field Robotics*, 26(8):636–650, 2009.

[23] Pasquale Pace, Gianluca Aloi, Giuseppe Caliciuri, and Giancarlo Fortino. A mission-oriented coordination framework for teams of mobile aerial and terrestrial smart objects. *Mobile Networks and Applications*, 21(4):708–725, 2016.

[24] Seongsoo Cho, Jeong Hyun Yi, Bhanu Shrestha, and Changho Seo. Multipath routing technique for responding to sniffing attacks in wireless multimedia sensor network environment. *International Journal of Sensor Networks*, 24(3):200–207, 2017.

[25] Vishal Sharma, Fei Song, Ilsun You, and Mohammed Atiquzzaman. Energy efficient device discovery for reliable communication in 5g-based iot and bsns using unmanned aerial vehicles. *Journal of Network and Computer Applications*, 97:79–95, 2017.

[26] Yi Zhou, Nan Cheng, Ning Lu, and Xuemin Sherman Shen. Multi-uav-aided networks: Aerial-ground cooperative vehicular networking architecture. *ieee vehicular technology magazine*, 10(4):36–44, 2015.

[27] Ozgur Koray Sahingoz. Networking models in flying ad-hoc networks (fanets): Concepts and challenges. *Journal of Intelligent & Robotic Systems*, 74(1-2):513–527, 2014.

[28] Samuel Henrique Silva, Paul Rad, Nicole Beebe, Kim-Kwang Raymond Choo, and Mahesh Umapathy. Cooperative unmanned aerial vehicles with privacy preserving deep vision for real-time object identification and tracking. *Journal of Parallel and Distributed Computing*, 131:147–160, 2019.

[29] Luca Chiaraviglio, Fabio D andreagiovanni, Raymond Choo, Francesca Cuomo, and Stefania Colonnese. Joint optimization of area throughput and grid-connected microgeneration in uav-based mobile networks. *IEEE Access*, 7:69545–69558, 2019.

[30] Luca Chiaraviglio, Fabio d'Andreagiovanni, William Liu, Jairo Gutierrez, Nicola Blefari-Melazzi, Kim-Kwang Raymond Choo, and Mohamed-Slim Alouini. Multi-area throughput and energy optimization of uav-aided cellular networks powered by solar panels and grid. *IEEE Transactions on Mobile Computing*, 2020.

[31] Keke Gai, Yulu Wu, Liehuang Zhu, Kim-Kwang Raymond Choo, and Bin Xiao. Blockchain-enabled trustworthy group communications in uav networks. *IEEE Transactions on Intelligent Transportation Systems*, 2020.

[32] Joe Nalepka and Jake Hinchman. Automated aerial refueling: extending the effectiveness of uavs. In *AIAA Modeling and Simulation Technologies Conference and Exhibit*, page 6005, 2005.

[33] Azad M Madni, Michael W Sievers, James Humann, Edwin Ordoukhanian, Barry Boehm, and Scott Lucero. Formal methods in resilient systems design: application to multi-uav system-of-systems control. In *Disciplinary Convergence in Systems Engineering Research*, pages 407–418. Springer, 2018.

[34] Boris Galkin, Jacek Kibilda, and Luiz A DaSilva. Uavs as mobile infrastructure: Addressing battery lifetime. *IEEE Communications Magazine*, 57(6):132–137, 2019.

[35] Akram Al-Hourani, Sithamparanathan Kandeepan, and Simon Lardner. Optimal lap altitude for maximum coverage. *IEEE Wireless Communications Letters*, 3(6):569–572, 2014.

[36] Jiangbin Lyu, Yong Zeng, Rui Zhang, and Teng Joon Lim. Placement optimization of uav-mounted mobile base stations. *IEEE Communications Letters*, 21(3):604–607, 2016.

[37] Boris Galkin, Jacek Kibilda, and Luiz A DaSilva. Coverage analysis for low-altitude uav networks in urban environments. In *GLOBECOM 2017-2017 IEEE Global Communications Conference*, pages 1–6. IEEE, 2017.

[38] Ajay Pratap and Rajiv Misra. Firefly inspired improved distributed proximity algorithm for d2d communication. In *2015 IEEE International Parallel and Distributed Processing Symposium Workshop*, pages 323–328. IEEE, 2015.

[39] Vishal Sharma, Mehdi Bennis, and Rajesh Kumar. Uav-assisted heterogeneous networks for capacity enhancement. *IEEE Communications Letters*, 20(6):1207–1210, 2016.

[40] Boris Galkin, Jacek Kibiłda, and Luiz A DaSilva. A stochastic model for uav networks positioned above demand hotspots in urban environments. *IEEE Transactions on Vehicular Technology*, 68(7):6985–6996, 2019.

[41] Boris Galkin, Jacek Kibilda, and Luiz A DaSilva. Deployment of uav-mounted access points according to spatial user locations in two-tier cellular networks. In *2016 Wireless Days (WD)*, pages 1–6. IEEE, 2016.

[42] Debasis Das, Rajiv Misra, and Anurag Raj. Approximating geographic routing using coverage tree heuristics for wireless network. *wireless networks*, 21(4):1109–1118, 2015.

[43] Debasis Das and Rajiv Misra. Improvised dynamic network connectivity model for vehicular ad-hoc networks (vanets). *Journal of Network and Computer Applications*, 122:107–114, 2018.

[44] Vishal Sharma, Kathiravan Srinivasan, Han-Chieh Chao, Kai-Lung Hua, and Wen-Huang Cheng. Intelligent deployment of uavs in 5g heterogeneous communication environment for improved coverage. *Journal of Network and Computer Applications*, 85:94–105, 2017.

[45] Vishal Sharma, Dushantha Nalin K Jayakody, and Kathiravan Srinivasan. On the positioning likelihood of uavs in 5g networks. *Physical Communication*, 31:1–9, 2018.

[46] Jingjing Wang, Chunxiao Jiang, Zhongxiang Wei, Cunhua Pan, Haijun Zhang, and Yong Ren. Joint uav hovering altitude and power control for space-air-ground iot networks. *IEEE Internet of Things Journal*, 6(2):1741–1753, 2018.

[47] Bin Jiang, Jiachen Yang, Huifang Xu, Houbing Song, and Gan Zheng. Multimedia data throughput maximization in internet-of-things system based on optimization of cache-enabled uav. *IEEE Internet of Things Journal*, 6(2):3525–3532, 2018.

[48] Ben Grocholsky, James Keller, Vijay Kumar, and George Pappas. Cooperative air and ground surveillance. *IEEE Robotics & Automation Magazine*, 13(3):16–25, 2006.

[49] Agwad El-Sayed and Mohamed ElHelw. Distributed component-based framework for unmanned air vehicle systems. In *2012 IEEE International Conference on Information and Automation*, pages 45–50. IEEE, 2012.

[50] Lefteris Doitsidis, Kimon P Valavanis, Nikos C Tsourveloudis, and Michael Kontitsis. A framework for fuzzy logic based uav navigation and control. In *IEEE International Conference on Robotics and Automation, 2004. Proceedings. ICRA'04. 2004*, volume 4, pages 4041–4046. IEEE, 2004.

[51] Juan López, Pablo Royo, Enric Pastor, Cristina Barrado, and Eduard Santamaria. A middleware architecture for unmanned aircraft avionics. In *Proceedings of the 2007 ACM/IFIP/USENIX international conference on Middleware companion*, pages 1–6, 2007.

[52] Dac-Tu Ho and Shigeru Shimamoto. Highly reliable communication protocol for wsn-uav system employing tdma and pfs scheme. In *2011 IEEE Globecom Workshops (Gc Wkshps)*, pages 1320–1324. IEEE, 2011.

[53] Sarra Berrahal, Jong-Hoon Kim, Slim Rekhis, Noureddine Boudriga, Deon Wilkins, and Jaime Acevedo. Unmanned aircraft vehicle assisted wsn-based border surveillance. In *2015 23rd International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*, pages 132–137. IEEE, 2015.

[54] Sotheara Say, Hikari Inata, Jiang Liu, and Shigeru Shimamoto. Priority-based data gathering framework in uav-assisted wireless sensor networks. *IEEE Sensors Journal*, 16(14):5785–5794, 2016.

[55] DG Reina, Radu-Ioan Ciobanu, SL Toral, and C Dobre. A multi-objective optimization of data dissemination in delay tolerant networks. *Expert Systems with Applications*, 57:178–191, 2016.

[56] Radu-Ioan Ciobanu, DG Reina, Ciprian Dobre, SL Toral, and P Johnson. Jder: A history-based forwarding scheme for delay tolerant networks using jaccard distance and encountered ration. *Journal of network and computer applications*, 40:279–291, 2014.

[57] Jesús Sánchez-García, José Manuel García-Campos, SL Toral, DG Reina, and Federico Barrero. An intelligent strategy for tactical movements of uavs in disaster scenarios. *International Journal of Distributed Sensor Networks*, 12(3):8132812,

2016.

[58] Abdul Waheed Khan, Abdul Hanan Abdullah, Mohammad Abdur Razzaque, Javed Iqbal Bangash, and Ayman Altameem. Vgdd: a virtual grid based data dissemination scheme for wireless sensor networks with mobile sink. *International Journal of Distributed Sensor Networks*, 11(2):890348, 2015.

[59] Hyondong Oh, Seungkeun Kim, Hyo-Sang Shin, Antonios Tsourdos, and Brian A White. Behaviour recognition of ground vehicle using airborne monitoring of unmanned aerial vehicles. *International Journal of Systems Science*, 45(12):2499–2514, 2014.

[60] Austin Jensen and YangQuan Chen. Tracking tagged fish with swarming unmanned aerial vehicles using fractional order potential fields and kalman filtering. In *2013 International Conference on Unmanned Aircraft Systems (ICUAS)*, pages 1144–1149. IEEE, 2013.

[61] Austin M Jensen, David K Geller, and YangQuan Chen. Monte carlo simulation analysis of tagged fish radio tracking performance by swarming unmanned aerial vehicles in fractional order potential fields. *Journal of Intelligent & Robotic Systems*, 74(1-2):287–307, 2014.

[62] Imad Jawhar, Nader Mohamed, Jameela Al-Jaroodi, and Sheng Zhang. A framework for using unmanned aerial vehicles for data collection in linear wireless sensor networks. *Journal of Intelligent & Robotic Systems*, 74(1-2):437–453, 2014.

[63] Imad Jawhar, Nader Mohamed, Jameela Al-Jaroodi, and Sheng Zhang. Data communication in linear wireless sensor networks using unmanned aerial vehicles. In *2013 International Conference on Unmanned Aircraft Systems (ICUAS)*, pages 492–499. IEEE, 2013.

[64] Iván Maza, Fernando Caballero, Jesús Capitán, José Ramiro Martínez-de Dios, and Aníbal Ollero. Experimental results in multi-uav coordination for disaster management and civil security applications. *Journal of intelligent & robotic systems*, 61(1-4):563–585, 2011.

[65] Vishal Sharma, Ilsun You, and Rajesh Kumar. Energy efficient data dissemination in multi-uav coordinated wireless sensor networks. *Mobile Information Systems*, 2016, 2016.

[66] Zhen Xue, Jinlong Wang, Guoru Ding, Haibo Zhou, and Qihui Wu. Maximization of data dissemination in uav-supported internet of things. *IEEE Wireless Communications Letters*, 8(1):185–188, 2018.

[67] Ayşegül Tüysüz Erman, Arta Dilo, and Paul Havinga. A virtual infrastructure based on honeycomb tessellation for data dissemination in multi-sink mobile wireless sensor networks. *EURASIP Journal on Wireless Communications and Net-*

working, 2012(1):17, 2012.

[68] Vishal Sharma, Hsing-Chung Chen, and Rajesh Kumar. Driver behaviour detection and vehicle rating using multi-uav coordinated vehicular networks. *Journal of Computer and System Sciences*, 86:3–32, 2017.

[69] Cheng Zhan and Yong Zeng. Completion time minimization for multi-uav-enabled data collection. *IEEE Transactions on Wireless Communications*, 18(10):4859–4872, 2019.

[70] Xiying Fan, Chuanhe Huang, Bin Fu, Shaojie Wen, and Xi Chen. Uav-assisted data dissemination in delay-constrained vanets. *Mobile Information Systems*, 2018, 2018.

[71] Ahmed A Al-Habob, Octavia A Dobre, Sami Muhaidat, and H Vincent Poor. Energy-efficient data dissemination using a uav: An ant colony approach. *IEEE Wireless Communications Letters*, 2020.

[72] Fei Xiong, Hao Zheng, Lang Ruan, Hai Wang, Lijuan Tang, Xu Dong, and Aijing Li. Energy-saving data aggregation for multi-uav system. *IEEE Transactions on Vehicular Technology*, 69(8):9002–9016, 2020.

[73] Vishal Sharma, Ilsun You, Rajesh Kumar, and Varun Chauhan. Offrp: optimised fruit fly based routing protocol with congestion control for uavs guided ad hoc networks. *International Journal of Ad Hoc and Ubiquitous Computing*, 27(4):233–255, 2018.

[74] Vishal Sharma, DG Reina, and Rajesh Kumar. Hmadso: a novel hill myna and desert sparrow optimization algorithm for cooperative rendezvous and task allocation in fanets. *Soft Computing*, 22(18):6191–6214, 2018.

[75] Vishal Sharma, Ilsun You, Dushantha Nalin K Jayakody, Daniel Gutierrez Reina, and Kim-Kwang Raymond Choo. Neural-blockchain-based ultrareliable caching for edge-enabled uav networks. *IEEE Transactions on Industrial Informatics*, 15(10):5723–5736, 2019.

[76] Vishal Sharma and Rajesh Kumar. Uavs assisted queue scheduling in ground ad hoc networks. *International Journal of Ad Hoc and Ubiquitous Computing*, 30(1):1–10, 2019.

[77] Qingqing Wu, Yong Zeng, and Rui Zhang. Joint trajectory and communication design for multi-uav enabled wireless networks. *IEEE Transactions on Wireless Communications*, 17(3):2109–2121, 2018.

[78] Fen Cheng, Shun Zhang, Zan Li, Yunfei Chen, Nan Zhao, F Richard Yu, and Victor CM Leung. Uav trajectory optimization for data offloading at the edge of multiple cells. *IEEE Transactions on Vehicular Technology*, 67(7):6732–6736, 2018.

[79] Yong Zeng, Xiaoli Xu, and Rui Zhang. Trajectory design for completion time

minimization in uav-enabled multicasting. *IEEE Transactions on Wireless Communications*, 17(4):2233–2246, 2018.

[80] Yong Zeng and Rui Zhang. Energy-efficient uav communication with trajectory optimization. *IEEE Transactions on Wireless Communications*, 16(6):3747–3760, 2017.

[81] Qingqing Wu, Yong Zeng, and Rui Zhang. Joint trajectory and communication design for uav-enabled multiple access. In *GLOBECOM 2017-2017 IEEE Global Communications Conference*, pages 1–6. IEEE, 2017.

[82] Dingcheng Yang, Qingqing Wu, Yong Zeng, and Rui Zhang. Energy tradeoff in ground-to-uav communication via trajectory design. *IEEE Transactions on Vehicular Technology*, 67(7):6721–6726, 2018.

[83] Jie Xu, Yong Zeng, and Rui Zhang. Uav-enabled wireless power transfer: Trajectory design and energy optimization. *IEEE Transactions on Wireless Communications*, 17(8):5092–5106, 2018.

[84] Zhenyu Na, Jun Wang, Chungang Liu, Mingxiang Guan, and Zihe Gao. Join trajectory optimization and communication design for uav-enabled ofdm networks. *Ad Hoc Networks*, 98:102031, 2020.

[85] Shuhang Zhang, Hongliang Zhang, Qichen He, Kaigui Bian, and Lingyang Song. Joint trajectory and power optimization for uav relay networks. *IEEE Communications Letters*, 22(1):161–164, 2017.

[86] Moataz Samir, Sanaa Sharafeddine, Chadi M Assi, Tri Minh Nguyen, and Ali Ghrayeb. Uav trajectory planning for data collection from time-constrained iot devices. *IEEE Transactions on Wireless Communications*, 19(1):34–46, 2019.

[87] Miao Cui, Guangchi Zhang, Qingqing Wu, and Derrick Wing Kwan Ng. Robust trajectory and transmit power design for secure uav communications. *IEEE Transactions on Vehicular Technology*, 67(9):9042–9046, 2018.

[88] Yulin Hu, Xiaopeng Yuan, Jie Xu, and Anke Schmeink. Optimal 1d trajectory design for uav-enabled multiuser wireless power transfer. *IEEE Transactions on Communications*, 67(8):5674–5688, 2019.

[89] Dinh-Hieu Tran, Thang X Vu, Symeon Chatzinotas, Shahram ShahbazPanahi, and Björn Ottersten. Coarse trajectory design for energy minimization in uav-enabled. *IEEE Transactions on Vehicular Technology*, 69(9):9483–9496, 2020.

[90] Zubair Md Fadlullah, Daisuke Takaishi, Hiroki Nishiyama, Nei Kato, and Ryu Miura. A dynamic trajectory control algorithm for improving the communication throughput and delay in uav-aided networks. *IEEE Network*, 30(1):100–105, 2016.

[91] Hazem Sallouha, Mohammad Mahdi Azari, and Sofie Pollin. Energy-constrained uav trajectory design for ground node localization. In *2018 IEEE Global Commu-*

nications Conference (GLOBECOM), pages 1–7. IEEE, 2018.

[92] Zhiyang Li, Ming Chen, Cunhua Pan, Nuo Huang, Zhaohui Yang, and Arumugam Nallanathan. Joint trajectory and communication design for secure uav networks. *IEEE Communications Letters*, 23(4):636–639, 2019.

[93] Guangchi Zhang, Qingqing Wu, Miao Cui, and Rui Zhang. Securing uav communications via joint trajectory and power control. *IEEE Transactions on Wireless Communications*, 18(2):1376–1389, 2019.

[94] Shuowen Zhang, Yong Zeng, and Rui Zhang. Cellular-enabled uav communication: A connectivity-constrained trajectory optimization perspective. *IEEE Transactions on Communications*, 67(3):2580–2604, 2018.

[95] Jingyu Xiong, Hongzhi Guo, and Jiajia Liu. Task offloading in uav-aided edge computing: Bit allocation and trajectory optimization. *IEEE Communications Letters*, 23(3):538–541, 2019.

[96] Sixian Li, Bin Duo, Xiaojun Yuan, Ying-Chang Liang, and Marco Di Renzo. Reconfigurable intelligent surface assisted uav communication: Joint trajectory design and passive beamforming. *IEEE Wireless Communications Letters*, 9(5):716–720, 2020.

[97] Nan Zhao, Xiaowei Pang, Zan Li, Yunfei Chen, Feng Li, Zhiguo Ding, and Mohamed-Slim Alouini. Joint trajectory and precoding optimization for uav-assisted noma networks. *IEEE Transactions on Communications*, 67(5):3723–3735, 2019.

[98] Gang Tang, Zhipeng Hou, Christophe Claramunt, and Xiong Hu. Uav trajectory planning in a port environment. *Journal of Marine Science and Engineering*, 8(8):592, 2020.

[99] Canhui Zhong, Jianping Yao, and Jie Xu. Secure uav communication with cooperative jamming and trajectory control. *IEEE Communications Letters*, 23(2):286–289, 2018.

[100] Sara Pérez-Carabaza, Jürgen Scherer, Bernhard Rinner, José A López-Orozco, and Eva Besada-Portas. Uav trajectory optimization for minimum time search with communication constraints and collision avoidance. *Engineering Applications of Artificial Intelligence*, 85:357–371, 2019.

[101] Xiaobo Zhou, Qingqing Wu, Shihao Yan, Feng Shu, and Jun Li. Uav-enabled secure communications: Joint trajectory and transmit power optimization. *IEEE Transactions on Vehicular Technology*, 68(4):4069–4073, 2019.

[102] Zhenyu Na, Mengshu Zhang, Jun Wang, and Zihe Gao. Uav-assisted wireless powered internet of things: Joint trajectory optimization and resource allocation. *Ad Hoc Networks*, 98:102052, 2020.

[103] Juan Liu, Xijun Wang, Bo Bai, and Huaiyu Dai. Age-optimal trajectory planning for uav-assisted data collection. In *IEEE INFOCOM 2018-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pages 553–558. IEEE, 2018.

[104] Ruide Li, Zhiqiang Wei, Lei Yang, Derrick Wing Kwan Ng, Nan Yang, Jinhong Yuan, and Jianping An. Joint trajectory and resource allocation design for uav communication systems. In *2018 IEEE Globecom Workshops (GC Wkshps)*, pages 1–6. IEEE, 2018.

[105] Changsheng You and Rui Zhang. 3d trajectory optimization in rician fading for uav-enabled data harvesting. *IEEE Transactions on Wireless Communications*, 18(6):3192–3207, 2019.

[106] Yan Sun, Dongfang Xu, Derrick Wing Kwan Ng, Linglong Dai, and Robert Schober. Optimal 3d-trajectory design and resource allocation for solar-powered uav communication systems. *IEEE Transactions on Communications*, 67(6):4281–4298, 2019.

[107] Jie Xu, Yong Zeng, and Rui Zhang. Uav-enabled wireless power transfer: Trajectory design and energy region characterization. In *2017 IEEE Globecom Workshops (GC Wkshps)*, pages 1–7. IEEE, 2017.

[108] Jingzhi Hu, Hongliang Zhang, and Lingyang Song. Reinforcement learning for decentralized trajectory design in cellular uav networks with sense-and-send protocol. *IEEE Internet of Things Journal*, 6(4):6177–6189, 2018.

[109] Jingwei Zhang, Yong Zeng, and Rui Zhang. Uav-enabled radio access network: Multi-mode communication and trajectory design. *IEEE Transactions on Signal Processing*, 66(20):5269–5284, 2018.

[110] Yunlong Cai, Fangyu Cui, Qingjiang Shi, Minjian Zhao, and Geoffrey Ye Li. Dual-uav-enabled secure communications: Joint trajectory design and user scheduling. *IEEE Journal on Selected Areas in Communications*, 36(9):1972–1985, 2018.

[111] Ying Wang, Zhendong Li, Yuanbin Chen, Man Liu, Xinpeng Lyu, Xiangwang Hou, and Jingjing Wang. Joint resource allocation and uav trajectory optimization for space–air–ground internet of remote things networks. *IEEE Systems Journal*, 2020.

[112] Qiyu Hu, Yunlong Cai, Guanding Yu, Zhijin Qin, Minjian Zhao, and Geoffrey Ye Li. Joint offloading and trajectory design for uav-enabled mobile edge computing systems. *IEEE Internet of Things Journal*, 6(2):1879–1892, 2018.

[113] Guangchi Zhang, Haiqiang Yan, Yong Zeng, Miao Cui, and Yijun Liu. Trajectory optimization and power allocation for multi-hop uav relaying communications. *IEEE Access*, 6:48566–48576, 2018.

[114] Freddy Demiane, Sanaa Sharafeddine, and Omar Farhat. An optimized uav trajectory planning for localization in disaster scenarios. *Computer Networks*, 179:107378,

2020.

[115] Yu Xu, Lin Xiao, Dingcheng Yang, Laurie Cuthbert, and Yapeng Wang. Energy-efficient uav communication with multiple gts based on trajectory optimization. *Mobile Information Systems*, 2018, 2018.

[116] Xiao Liu, Yuanwei Liu, Yue Chen, and Lajos Hanzo. Trajectory design and power control for multi-uav assisted wireless networks: A machine learning approach. *IEEE Transactions on Vehicular Technology*, 68(8):7957–7969, 2019.

[117] Gaofeng Pan, Hongjiang Lei, Jianping An, Shuo Zhang, and Mohamed-Slim Alouini. On the secrecy of uav systems with linear trajectory. *IEEE Transactions on Wireless Communications*, 19(10):6277–6288, 2020.

[118] Yong Zeng, Rui Zhang, and Teng Joon Lim. Throughput maximization for uav-enabled mobile relaying systems. *IEEE Transactions on Communications*, 64(12):4983–4996, 2016.

[119] Shuhang Zhang, Hongliang Zhang, Boya Di, and Lingyang Song. Joint trajectory and power optimization for uav sensing over cellular networks. *IEEE Communications Letters*, 22(11):2382–2385, 2018.

[120] Cheng Zhan, Yong Zeng, and Rui Zhang. Trajectory design for distributed estimation in uav-enabled wireless sensor network. *IEEE Transactions on Vehicular Technology*, 67(10):10155–10159, 2018.

[121] Meng Hua, Yi Wang, Chunguo Li, Yongming Huang, and Luxi Yang. Uav-aided mobile edge computing systems with one by one access scheme. *IEEE Transactions on Green Communications and Networking*, 3(3):664–678, 2019.

[122] Sixing Yin, Shuo Zhao, Yifei Zhao, and F Richard Yu. Intelligent trajectory design in uav-aided communications with reinforcement learning. *IEEE Transactions on Vehicular Technology*, 68(8):8227–8231, 2019.

[123] Youngjun Choi, Mengzhen Chen, Younghoon Choi, Simon Briceno, and Dimitri Mavris. Multi-uav trajectory optimization utilizing a nurbs-based terrain model for an aerial imaging mission. *Journal of Intelligent & Robotic Systems*, 97(1):141–154, 2020.

[124] Vincent Roberge, Mohammed Tarbouchi, and Gilles Labonté. Comparison of parallel genetic algorithm and particle swarm optimization for real-time uav path planning. *IEEE Transactions on industrial informatics*, 9(1):132–141, 2012.

[125] Mushu Li, Nan Cheng, Jie Gao, Yinlu Wang, Lian Zhao, and Xuemin Shen. Energy-efficient uav-assisted mobile edge computing: Resource allocation and trajectory optimization. *IEEE Transactions on Vehicular Technology*, 69(3):3424–3438, 2020.

[126] Fangyu Cui, Yunlong Cai, Zhijin Qin, Minjian Zhao, and Geoffrey Ye Li. Multiple access for mobile-uav enabled networks: Joint trajectory design and resource

allocation. *IEEE Transactions on Communications*, 67(7):4980–4994, 2019.

[127] Peiming Li and Jie Xu. Fundamental rate limits of uav-enabled multiple access channel with trajectory optimization. *IEEE Transactions on Wireless Communications*, 19(1):458–474, 2019.

[128] Xu Jiang, Zhilu Wu, Zhendong Yin, and Zhutian Yang. Power and trajectory optimization for uav-enabled amplify-and-forward relay networks. *IEEE Access*, 6:48688–48696, 2018.

[129] Chao Shen, Tsung-Hui Chang, Jie Gong, Yong Zeng, and Rui Zhang. Multi-uav interference coordination via joint trajectory and power control. *IEEE Transactions on Signal Processing*, 68:843–858, 2020.

[130] Kaiyu Zhu, Xiaodong Xu, and Shujun Han. Energy-efficient uav trajectory planning for data collection and computation in mmtc networks. In *2018 IEEE Globecom Workshops (GC Wkshps)*, pages 1–6. IEEE, 2018.

[131] Jiangchun Gu, Haichao Wang, Guoru Ding, Yitao Xu, Zhen Xue, and Huaji Zhou. Energy constrained completion time minimization in uav-enabled internet of things. *IEEE Internet of Things Journal*, 2020.

[132] Yong Zeng, Rui Zhang, and Teng Joon Lim. Wireless communications with unmanned aerial vehicles: Opportunities and challenges. *IEEE Communications Magazine*, 54(5):36–42, 2016.

[133] Hamid Menouar, Ismail Guvenc, Kemal Akkaya, A Selcuk Uluagac, Abdullah Kadri, and Adem Tuncer. Uav-enabled intelligent transportation systems for the smart city: Applications and challenges. *IEEE Communications Magazine*, 55(3):22–28, 2017.

[134] Lihua Jian, Zhen Li, Xiaomin Yang, Wei Wu, Awais Ahmad, and Gwanggil Jeon. Combining unmanned aerial vehicles with artificial-intelligence technology for traffic-congestion recognition: Electronic eyes in the skies to spot clogged roads. *IEEE Consumer Electronics Magazine*, 8(3):81–86, 2019.

[135] Hongliang Zhang, Lingyang Song, Zhu Han, and H Vincent Poor. Cooperation techniques for a cellular internet of unmanned aerial vehicles. *IEEE Wireless Communications*, 26(5):167–173, 2019.

[136] Kashif Naseer Qureshi, Awais Ahmad, Francesco Piccialli, Giampaolo Casolla, and Gwanggil Jeon. Nature-inspired algorithm-based secure data dissemination framework for smart city networks. *Neural Computing and Applications*, pages 1–20, 2020.

[137] Ruide Li, Zhiqiang Wei, Lei Yang, Derrick Wing Kwan Ng, Jinhong Yuan, and Jianping An. Resource allocation for secure multi-uav communication systems with multi-eavesdropper. *IEEE Transactions on Communications*, 2020.

[138] Hoon Lee, Subin Eom, Junhee Park, and Inkyu Lee. Uav-aided secure communications with cooperative jamming. *IEEE Transactions on Vehicular Technology*, 67(10):9385–9392, 2018.

[139] Nan Zhao, Fen Cheng, F Richard Yu, Jie Tang, Yunfei Chen, Guan Gui, and Hikmet Sari. Caching uav assisted secure transmission in hyper-dense networks based on interference alignment. *IEEE Transactions on Communications*, 66(5):2281–2294, 2018.

[140] Jia Ye, Chao Zhang, Hongjiang Lei, Gaofeng Pan, and Zhiguo Ding. Secure uav-to-uav systems with spatially random uavs. *IEEE Wireless Communications Letters*, 8(2):564–567, 2018.

[141] Meng Hua, Yi Wang, Qingqing Wu, Haibo Dai, Yongming Huang, and Luxi Yang. Energy-efficient cooperative secure transmission in multi-uav-enabled wireless networks. *IEEE Transactions on Vehicular Technology*, 68(8):7761–7775, 2019.

[142] Chao Li, Yan Xu, Junjuan Xia, and Junhui Zhao. Protecting secure communication under uav smart attack with imperfect channel estimation. *IEEE Access*, 6:76395–76401, 2018.

[143] Fang Shi, Junjuan Xia, Zhenyu Na, Xin Liu, Yunfei Ding, and Zhi Wang. Secure probabilistic caching in random multi-user multi-uav relay networks. *Physical Communication*, 32:31–40, 2019.

[144] Yupeng Li, Rongqing Zhang, Jianhua Zhang, Shijian Gao, and Liuqing Yang. Cooperative jamming for secure uav communications with partial eavesdropper information. *IEEE Access*, 7:94593–94603, 2019.

[145] Jiehong Wu, Liangkai Zou, Liang Zhao, Ahmed Al-Dubai, Lewis Mackenzie, and Geyong Min. A multi-uav clustering strategy for reducing insecure communication range. *Computer Networks*, 158:132–142, 2019.

[146] Zhangjie Fu, Yuanhang Mao, Daojing He, Jingnan Yu, and Guowu Xie. Secure multi-uav collaborative task allocation. *IEEE Access*, 7:35579–35587, 2019.

[147] Tong Bai, Jingjing Wang, Yong Ren, and Lajos Hanzo. Energy-efficient computation offloading for secure uav-edge-computing systems. *IEEE Transactions on Vehicular Technology*, 68(6):6074–6087, 2019.

[148] Yu Zhang, Zhiyu Mou, Feifei Gao, Jing Jiang, Ruijin Ding, and Zhu Han. Uav-enabled secure communications by multi-agent deep reinforcement learning. *IEEE Transactions on Vehicular Technology*, 69(10):11599–11611, 2020.

[149] Ying Gao, Hongying Tang, Baoqing Li, and Xiaobing Yuan. Joint trajectory and power design for uav-enabled secure communications with no-fly zone constraints. *IEEE Access*, 7:44459–44470, 2019.

[150] Wei Wang, Xinrui Li, Miao Zhang, Kanapathippillai Cumanan, Derrick Wing Kwan

Ng, Guoan Zhang, Jie Tang, and Octavia A Dobre. Energy-constrained uav-assisted secure communications with position optimization and cooperative jamming. *IEEE Transactions on Communications*, 2020.

[151] Alan Roder and Kim-Kwang Raymond Choo. Unmanned aerial vehicles (uavs) threat analysis and a routine activity theory based mitigation approach. In *National Cyber Summit*, pages 99–115. Springer, 2019.

[152] Dan Goddin. There a new way to take down drones and it doesnot involve shotguns. Security Editorial, October 2016.

[153] Gokul Kannan Sadasivam and Chittaranjan Hota. Scalable honeypot architecture for identifying malicious network activities. In *2015 international conference on emerging information technology and engineering solutions*, pages 27–31. IEEE, 2015.

[154] Pratik Narang, Subhajit Ray, Chittaranjan Hota, and Venkat Venkatakrishnan. Peershark: detecting peer-to-peer botnets by tracking conversations. In *2014 IEEE Security and Privacy Workshops*, pages 108–115. IEEE, 2014.

[155] Bhawna Narwal, Amar Kumar Mohapatra, and Kaleem Ahmed Usmani. Towards a taxonomy of cyber threats against target applications. *Journal of Statistics and Management Systems*, 22(2):301–325, 2019.

[156] Pascal Meunier. Drone flaw known since 1990s was a vulnerability. Blog, December 2009.

[157] Katia Moskvitch. Are drones the next target for hackers? InDeapth Internet Article, February 2014.

[158] Stephen Pritchard. Drones are quickly becoming a cybersecurity nightmare. Technical Article, March 2019.

[159] Associated Press. Computer virus infects drone plane command centre in us. News Article, October 2011.

[160] Christian de Looper. Drones now big hacking target, first drone malware identified. Tech. Article, February 2015.

[161] Manoun Alazab, Robert Layton, Sitalakshmi Venkataraman, and Paul Watters. Malware detection based on structural and behavioural features of api calls. 2010.

[162] Mamoun Alazab, Sitalakshmi Venkatraman, Paul Watters, Moutaz Alazab, and Ammar Alazab. Cybercrime: the case of obfuscated malware. In *Global security, safety and sustainability & e-Democracy*, pages 204–211. Springer, 2011.

[163] Bob O'hara and Al Petrick. *IEEE 802.11 handbook: a designer's companion*. IEEE Standards Association, 2005.

[164] Guido R Hiertz, Dee Denteneer, Lothar Stibor, Yunpeng Zang, Xavier Pérez Costa, and Bernhard Walke. The ieee 802.11 universe. *IEEE Communications Magazine*,

48(1):62–70, 2010.

[165] Brian P Crow, Indra Widjaja, Jeong Geun Kim, and Prescott T Sakai. Ieee 802.11 wireless local area networks. *IEEE Communications magazine*, 35(9):116–126, 1997.

[166] Daniel Jiang and Luca Delgrossi. Ieee 802.11 p: Towards an international standard for wireless access in vehicular environments. In *VTC Spring 2008-IEEE Vehicular Technology Conference*, pages 2036–2040. IEEE, 2008.

[167] Andreas F Molisch, Kannan Balakrishnan, Chia-Chin Chong, Shahriar Emami, Andrew Fort, Johan Karedal, Juergen Kunisch, Hans Schantz, Ulrich Schuster, and Kai Siwiak. Ieee 802.15. 4a channel model-final report. *IEEE P802*, 15(04):0662, 2004.

[168] Eirini Karapistoli, Fotini-Niovi Pavlidou, Ioannis Gragopoulos, and Ioannis Tsetsinas. An overview of the ieee 802.15. 4a standard. *IEEE Communications Magazine*, 48(1):47–53, 2010.

[169] Jianliang Zheng and Myung J Lee. A comprehensive performance study of ieee 802.15. 4. *Sensor network operations*, 4:218–237, 2006.

[170] David Johnston and Jesse Walker. Overview of ieee 802.16 security. *IEEE Security & Privacy*, 2(3):40–48, 2004.

[171] Claudio Cicconetti, Luciano Lenzini, Enzo Mingozzi, and Carl Eklund. Quality of service support in ieee 802.16 networks. *IEEE network*, 20(2):50–55, 2006.

[172] Claudio Cicconetti, Alessandro Erta, Luciano Lenzini, and Enzo Mingozzi. Performance evaluation of the ieee 802.16 mac for qos support. *IEEE Transactions on mobile computing*, 6(1):26–38, 2006.

[173] SM Suhail Hussain, Taha Selim Ustun, Paul Nsonga, and Ikbal Ali. Ieee 1609 wave and iec 61850 standard communication based integrated ev charging management in smart grids. *IEEE Transactions on Vehicular Technology*, 67(8):7690–7697, 2018.

[174] Charles Arthur. Skygrabber: the dollar 26 software used by insurgents to hack into us drones. News Article, December 2009.

[175] Lorenzo Franceschi Bicchierai. Drone hijacking? that's just the start of gps troubles. News Article, July 2012.

[176] Bertold Van der Bergh, Alessandro Chiumento, and Sofie Pollin. Lte in the sky: Trading off propagation benefits with interference costs for aerial nodes. *IEEE Communications Magazine*, 54(5):44–50, 2016.

[177] Rafhael Amorim, Huan Nguyen, Preben Mogensen, István Z Kovács, Jeroen Wigard, and Troels B Sørensen. Radio channel modeling for uav communication over cellular networks. *IEEE Wireless Communications Letters*, 6(4):514–517, 2017.

[178] Azade Fotouhi, Haoran Qiang, Ming Ding, Mahbub Hassan, Lorenzo Galati Giordano, Adrian Garcia-Rodriguez, and Jinhong Yuan. Survey on uav cellular com-

munications: Practical aspects, standardization advancements, regulation, and security challenges. *IEEE Communications Surveys & Tutorials*, 21(4):3417–3442, 2019.

[179] J Schlienz and A Roessler. Device to device communication in lte whitepaper. *ROHDE & SCHWARZ: Munich, Germany*, 2015.

[180] JS Roessler. Lte-advanced (3gpp rel. 12) technology introduction white paper. *Rohde & Shwarz*, 2015.

[181] Telesystem Innovations. Lte in a nutshell. *White paper*, 2010.

[182] Sravanthi Kanchi, Shubhrika Sandilya, Deesha Bhosale, Adwait Pitkar, and Mayur Gondhalekar. Overview of lte-a technology. In *2013 IEEE global high tech congress on electronics*, pages 195–200. IEEE, 2013.

[183] Anastasios N Bikos and Nicolas Sklavos. Lte/sae security issues on 4g wireless networks. *IEEE Security & Privacy*, 11(2):55–62, 2012.

[184] Jeffrey Cichonski, Joshua Franklin, and Michael Bartock. Guide to lte security. Technical report, National Institute of Standards and Technology, 2016.

[185] Jeffrey Cichonski, Joshua Franklin, and Michael Bartock. Lte architecture overview and security analysis. Technical report, National Institute of Standards and Technology, 2016.

[186] Balu L Parne, Shubham Gupta, and Narendra S Chaudhari. Pse-aka: Performance and security enhanced authentication key agreement protocol for iot enabled lte/lte-a networks. *Peer-to-Peer Networking and Applications*, 12(5):1156–1177, 2019.

[187] Xiehua Li and Yongjun Wang. Security enhanced authentication and key agreement protocol for lte/sae network. In *2011 7th International Conference on Wireless Communications, Networking and Mobile Computing*, pages 1–4. IEEE, 2011.

[188] Chengzhe Lai, Hui Li, Rongxing Lu, and Xuemin Sherman Shen. Se-aka: A secure and efficient group authentication and key agreement protocol for lte networks. *Computer Networks*, 57(17):3492–3510, 2013.

[189] Silke Holtmanns, Siddharth Prakash Rao, and Ian Oliver. User location tracking attacks for lte networks using the interworking functionality. In *2016 IFIP Networking conference (IFIP Networking) and workshops*, pages 315–322. IEEE, 2016.

[190] Ramzi Bassil, Imad H Elhajj, Ali Chehab, and Ayman Kayssi. Effects of signaling attacks on lte networks. In *2013 27th International Conference on Advanced Information Networking and Applications Workshops*, pages 499–504. IEEE, 2013.

[191] Md Zakirul Alam Bhuiyan, Guojun Wang, and Kim-Kwang Raymond Choo. Secured data collection for a cloud-enabled structural health monitoring system. In *2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd*

International Conference on Data Science and Systems (HPCC/SmartCity/DSS), pages 1226–1231. IEEE, 2016.

[192] Sulabh Bhattarai, Stephen Rook, Linqiang Ge, Sixiao Wei, Wei Yu, and Xinwen Fu. On simulation studies of cyber attacks against lte networks. In *2014 23rd International Conference on Computer Communication and Networks (ICCCN)*, pages 1–8. IEEE, 2014.

[193] James Henrydoss and Terry Boult. Critical security review and study of ddos attacks on lte mobile network. In *2014 IEEE Asia Pacific Conference on Wireless and Mobile*, pages 194–200. IEEE, 2014.

[194] Altaf Shaik, Ravishankar Borgaonkar, N Asokan, Valtteri Niemi, and Jean-Pierre Seifert. Practical attacks against privacy and availability in 4g/lte mobile communication systems. *arXiv preprint arXiv:1510.07563*, 2015.

[195] Roger Piqueras Jover. Security attacks against the availability of lte mobility networks: Overview and research directions. In *2013 16th international symposium on wireless personal multimedia communications (WPMC)*, pages 1–9. IEEE, 2013.

[196] Teng Fei and Wenye Wang. Lte is vulnerable: implementing identity spoofing and denial-of-service attacks in lte networks. In *2019 IEEE Global Communications Conference (GLOBECOM)*, pages 1–6. IEEE, 2019.

[197] NGMN Alliance. 5g white paper. *Next generation mobile networks, white paper*, 1, 2015.

[198] Mikio Iwamura. Ngmn view on 5g architecture. In *2015 IEEE 81st Vehicular Technology Conference (VTC Spring)*, pages 1–5. IEEE, 2015.

[199] Pekka Pirinen. A brief overview of 5g research activities. In *1st International Conference on 5G for Ubiquitous Connectivity*, pages 17–22. IEEE, 2014.

[200] Ilsun You, Vishal Sharma, Mohammed Atiquzzaman, and Kim-Kwang Raymond Choo. Gdtn: Genome-based delay tolerant network formation in heterogeneous 5g using inter-ua collaboration. *PloS one*, 11(12):e0167913, 2016.

[201] Xinsheng Ji, Kaizhi Huang, Liang Jin, Hongbo Tang, Caixia Liu, Zhou Zhong, Wei You, Xiaoming Xu, Hua Zhao, Jiangxing Wu, et al. Overview of 5g security technology. *Science China Information Sciences*, 61(8):081301, 2018.

[202] Peter Schneider and Günther Horn. Towards 5g security. In *2015 IEEE Trustcom/BigDataSE/ISPA*, volume 1, pages 1165–1170. IEEE, 2015.

[203] Ijaz Ahmad, Tanesh Kumar, Madhusanka Liyanage, Jude Okwuibe, Mika Ylianttila, and Andrei Gurtov. Overview of 5g security challenges and solutions. *IEEE Communications Standards Magazine*, 2(1):36–43, 2018.

[204] Madhusanka Liyanage, Ijaz Ahmad, Ahmed Bux Abro, Andrei Gurtov, and Mika Ylianttila. *Comprehensive Guide to 5G Security*. Wiley Online Library, 2018.

[205] Yulei Wu, Hong-Ning Dai, Hao Wang, and Kim-Kwang Raymond Choo. Blockchain-based privacy preservation for 5g-enabled drone communications. *arXiv preprint arXiv:2009.03164*, 2020.

[206] Abbas Yazdinejad, Reza M Parizi, Ali Dehghantanha, and Kim-Kwang Raymond Choo. Blockchain-enabled authentication handover with efficient privacy protection in sdn-based 5g networks. *IEEE Transactions on Network Science and Engineering*, 2019.

[207] Jose M De Fuentes, Lorena Gonzalez-Manzano, Javier Lopez, Pedro Peris-Lopez, and Kim-Kwang Raymond Choo. Security and privacy in internet of things. *Mobile Networks and Applications*, 24(3):878–880, 2019.

[208] Syed Rafiul Hussain, Mitziu Echeverria, Omar Chowdhury, Ninghui Li, and Elisa Bertino. Privacy attacks to the 4g and 5g cellular paging protocols using side channel information. In *NDSS*, volume 19, pages 24–27, 2019.

[209] Puguang Liu, Bo Liu, Yipin Sun, Baokang Zhao, and Ilsun You. Mitigating dos attacks against pseudonymous authentication through puzzle-based co-authentication in 5g-vanet. *IEEE Access*, 6:20795–20806, 2018.

[210] Ana Serrano Mamolar, Zeeshan Pervez, Jose M Alcaraz Calero, and Asad Masood Khattak. Towards the transversal detection of ddos network attacks in 5g multi-tenant overlay networks. *Computers & Security*, 79:132–147, 2018.

[211] An Braeken, Madhusanka Liyanage, Pardeep Kumar, and John Murphy. Novel 5g authentication protocol to improve the resistance against active attacks and malicious serving networks. *IEEE Access*, 7:64040–64052, 2019.

[212] Ankush Singla, Syed Rafiul Hussain, Omar Chowdhury, Elisa Bertino, and Ninghui Li. Protecting the 4g and 5g cellular paging protocols against security and privacy attacks. *Proceedings on Privacy Enhancing Technologies*, 2020(1):126–142, 2020.

[213] Faisal Tariq, Muhammad RA Khandaker, Kai-Kit Wong, Muhammad A Imran, Mehdi Bennis, and Merouane Debbah. A speculative study on 6g. *IEEE Wireless Communications*, 27(4):118–125, 2020.

[214] Minghao Wang, Tianqing Zhu, Tao Zhang, Jun Zhang, Shui Yu, and Wanlei Zhou. Security and privacy in 6g networks: New areas and new challenges. *Digital Communications and Networks*, 6(3):281–291, 2020.

[215] Lauri Lovén, Teemu Leppänen, Ella Peltonen, Juha Partala, Erkki Harjula, Pawani Porambage, Mika Ylianttila, and Jukka Riekki. Edgeai: A vision for distributed, edgenative artificial intelligence in future 6g networks. *The 1st 6G Wireless Summit*, pages 1–2, 2019.

[216] Shuping Dang, Osama Amin, Basem Shihada, and Mohamed-Slim Alouini. What should 6g be? *Nature Electronics*, 3(1):20–29, 2020.

[217] Syed Junaid Nawaz, Shree Krishna Sharma, Shurjeel Wyne, Mohammad N Patwary, and Md Asaduzzaman. Quantum machine learning for 6g communication networks: State-of-the-art and vision for the future. *IEEE Access*, 7:46317–46350, 2019.

[218] Nariman Farsad, H Birkan Yilmaz, Andrew Eckford, Chan-Byoung Chae, and Weisi Guo. A comprehensive survey of recent advancements in molecular communication. *IEEE Communications Surveys & Tutorials*, 18(3):1887–1919, 2016.

[219] Yi Lu, Matthew D Higgins, and Mark S Leeson. Comparison of channel coding schemes for molecular communications systems. *IEEE Transactions on Communications*, 63(11):3991–4001, 2015.

[220] Valeria Loscri, César Marchal, Nathalie Mitton, Giancarlo Fortino, and Athanasios V Vasilakos. Security and privacy in molecular communication and networking: Opportunities and challenges. *IEEE transactions on nanobioscience*, 13(3):198–207, 2014.

[221] Jian-Yong Hu, Bo Yu, Ming-Yong Jing, Lian-Tuan Xiao, Suo-Tang Jia, Guo-Qing Qin, and Gui-Lu Long. Experimental quantum secure direct communication with single photons. *Light: Science & Applications*, 5(9):e16144–e16144, 2016.

[222] Shinsaku Kiyomoto, Anirban Basu, Mohammad Shahriar Rahman, and Sushmita Ruj. On blockchain-based authorization architecture for beyond-5g mobile services. In *2017 12th International Conference for Internet Technology and Secured Transactions (ICITST)*, pages 136–141. IEEE, 2017.

[223] Khashayar Kotobi and Sven G Bilen. Secure blockchains for dynamic spectrum access: A decentralized database in moving cognitive radio networks enhances security and user access. *ieee vehicular technology magazine*, 13(1):32–39, 2018.

[224] Pietro Ferraro, Christopher King, and Robert Shorten. Distributed ledger technology for smart cities, the sharing economy, and social compliance. *IEEE Access*, 6:62728–62746, 2018.

[225] Seyhan Ucar, Sinem Coleri Ergen, Oznur Ozkasap, Dobroslav Tsonev, and Harald Burchardt. Secvlc: Secure visible light communication for military vehicular networks. In *Proceedings of the 14th ACM International Symposium on Mobility Management and Wireless Access*, pages 123–129, 2016.

[226] Sunghwan Cho, Gaojie Chen, and Justin P Coon. Enhancement of physical layer security with simultaneous beamforming and jamming for visible light communication systems. *IEEE Transactions on Information Forensics and Security*, 14(10):2633–2648, 2019.

[227] Thomas D Nadeau and Ken Gray. *SDN: Software Defined Networks: an authoritative review of network programmability technologies.* " O'Reilly Media, Inc.", 2013.

[228] Khaled Alwasel, Devki Nandan Jha, Eduardo Hernandez, Deepak Puthal, Mutaz Barika, Blesson Varghese, Saurabh Kumar Garg, Philip James, Albert Zomaya, Graham Morgan, et al. Iotsim-sdwan: A simulation framework for interconnecting distributed datacenters over software-defined wide area network (sd-wan). *Journal of Parallel and Distributed Computing*, 143:17–35, 2020.

[229] Hyojoon Kim and Nick Feamster. Improving network management with software defined networking. *IEEE Communications Magazine*, 51(2):114–119, 2013.

[230] Nick McKeown, Tom Anderson, Hari Balakrishnan, Guru Parulkar, Larry Peterson, Jennifer Rexford, Scott Shenker, and Jonathan Turner. Openflow: enabling innovation in campus networks. *ACM SIGCOMM Computer Communication Review*, 38(2):69–74, 2008.

[231] Adrian Lara, Anisha Kolasani, and Byrav Ramamurthy. Network innovation using openflow: A survey. *IEEE communications surveys & tutorials*, 16(1):493–512, 2013.

[232] Open Networking Foundation. Software-defined networking: the new norm for networks. *ONF white paper*, 2012.

[233] Andrew T Campbell, Irene Katzela, Kazuho Miki, and John Vicente. Open signaling for atm, internet and mobile networks (opensig'98). *ACM SIGCOMM Computer Communication Review*, 29(1):97–108, 1999.

[234] Bernardo Bátiz-Lazo. Emergence and evolution of atm networks in the uk, 1967–2000. *Business History*, 51(1):1–27, 2009.

[235] Albert Greenberg, Gisli Hjalmtysson, David A Maltz, Andy Myers, Jennifer Rexford, Geoffrey Xie, Hong Yan, Jibin Zhan, and Hui Zhang. A clean slate 4d approach to network control and management. *ACM SIGCOMM Computer Communication Review*, 35(5):41–54, 2005.

[236] Rob Enns, Martin Bjorklund, and Juergen Schoenwaelder. Netconf configuration protocol. Technical report, RFC 4741, December, 2006.

[237] Martin Casado, Michael J Freedman, Justin Pettit, Jianying Luo, Nick McKeown, and Scott Shenker. Ethane: Taking control of the enterprise. *ACM SIGCOMM computer communication review*, 37(4):1–12, 2007.

[238] Avri Doria, Jamal Hadi Salim, Robert Haas, Hormuzd M Khosravi, Weiming Wang, Ligang Dong, Ram Gopal, and Joel M Halpern. Forwarding and control element separation (forces) protocol specification. *RFC*, 5810:1–124, 2010.

[239] R Haas, H Khosravi, W Wang, L Dong, R Gopal, and J Halpern. Forwarding and control element separation (forces) protocol specification. 2010.

[240] Sushant Jain, Alok Kumar, Subhasree Mandal, Joon Ong, Leon Poutievski, Arjun Singh, Subbaiah Venkata, Jim Wanderer, Junlan Zhou, Min Zhu, et al. B4: Expe-

rience with a globally-deployed software defined wan. *ACM SIGCOMM Computer Communication Review*, 43(4):3–14, 2013.

[241] Myung-Ki Shin, Ki-Hyuk Nam, and Hyoung-Jun Kim. Software-defined networking (sdn): A reference architecture and open apis. In *2012 International Conference on ICT Convergence (ICTC)*, pages 360–361. IEEE, 2012.

[242] Brandon Heller, Rob Sherwood, and Nick McKeown. The controller placement problem. *ACM SIGCOMM Computer Communication Review*, 42(4):473–478, 2012.

[243] Amin Tootoonchian, Sergey Gorbunov, Yashar Ganjali, Martin Casado, and Rob Sherwood. On controller performance in software-defined networks. In *2nd {USENIX} Workshop on Hot Topics in Management of Internet, Cloud, and Enterprise Networks and Services (Hot-ICE 12)*, 2012.

[244] Guang Yao, Jun Bi, and Luyi Guo. On the cascading failures of multi-controllers in software defined networks. In *2013 21st IEEE International Conference on Network Protocols (ICNP)*, pages 1–2. IEEE, 2013.

[245] Afrim Sallahi and Marc St-Hilaire. Optimal model for the controller placement problem in software defined networks. *IEEE communications letters*, 19(1):30–33, 2014.

[246] Afrim Sallahi and Marc St-Hilaire. Expansion model for the controller placement problem in software defined networks. *IEEE Communications Letters*, 21(2):274–277, 2016.

[247] Md Faizul Bari, Arup Raton Roy, Shihabur Rahman Chowdhury, Qi Zhang, Mohamed Faten Zhani, Reaz Ahmed, and Raouf Boutaba. Dynamic controller provisioning in software defined networks. In *Proceedings of the 9th International Conference on Network and Service Management (CNSM 2013)*, pages 18–25. IEEE, 2013.

[248] Amin Tootoonchian and Yashar Ganjali. Hyperflow: A distributed control plane for openflow. In *Proceedings of the 2010 internet network management conference on Research on enterprise networking*, volume 3, 2010.

[249] Advait Dixit, Fang Hao, Sarit Mukherjee, TV Lakshman, and Ramana Rao Kompella. Elasticon; an elastic distributed sdn controller. In *2014 ACM/IEEE Symposium on Architectures for Networking and Communications Systems (ANCS)*, pages 17–27. IEEE, 2014.

[250] Stefan Schmid and Jukka Suomela. Exploiting locality in distributed sdn control. In *Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking*, pages 121–126, 2013.

[251] Guang Yao, Jun Bi, Yuliang Li, and Luyi Guo. On the capacitated controller

placement problem in software defined networks. *IEEE Communications Letters*, 18(8):1339–1342, 2014.

[252] Raul Muñoz, Ricard Vilalta, Ramon Casellas, Ricardo Martinez, Thomas Szyrkowiec, Achim Autenrieth, Víctor López, and Diego López. Integrated sdn/nfv management and orchestration architecture for dynamic deployment of virtual sdn control instances for virtual tenant networks. *Journal of Optical Communications and Networking*, 7(11):B62–B70, 2015.

[253] Bruno Trevizan De Oliveira, Lucas Batista Gabriel, and Cintia Borges Margi. Tinysdn: Enabling multiple controllers for software-defined wireless sensor networks. *IEEE Latin America Transactions*, 13(11):3690–3696, 2015.

[254] Stanislav Lange, Steffen Gebert, Thomas Zinner, Phuoc Tran-Gia, David Hock, Michael Jarschel, and Marco Hoffmann. Heuristic approaches to the controller placement problem in large scale sdn networks. *IEEE Transactions on Network and Service Management*, 12(1):4–17, 2015.

[255] Abdelkader Aissioui, Adlen Ksentini, Abdelhak Mourad Gueroui, and Tarik Taleb. Toward elastic distributed sdn/nfv controller for 5g mobile cloud management systems. *IEEE Access*, 3:2055–2064, 2015.

[256] Julius Schulz-Zander, Nadi Sarrar, and Stefan Schmid. Towards a scalable and near-sighted control plane architecture for wifi sdns. 2014.

[257] Anand Krishnamurthy, Shoban P Chandrabose, and Aaron Gember-Jacobson. Pratyaastha: an efficient elastic distributed sdn control plane. In *Proceedings of the third workshop on Hot topics in software defined networking*, pages 133–138, 2014.

[258] Peter Almers, Ernst Bonek, A Burr, Nicolai Czink, Mérouane Debbah, Vittorio Degli-Esposti, Helmut Hofstetter, Pekka Kyösti, Dave Laurenson, Gerald Matz, et al. Survey of channel and radio propagation models for wireless mimo systems. *EURASIP Journal on Wireless Communications and Networking*, 2007(1):019070, 2007.

[259] Quentin H Spencer, Christian B Peel, A Lee Swindlehurst, and Martin Haardt. An introduction to the multi-user mimo downlink. *IEEE communications Magazine*, 42(10):60–67, 2004.

[260] ONF. Sdn architecture 1.1. *Open Networking Foundation Technical Reference TR-521*, 2016.

[261] Vaclav Skala. Barycentric coordinates computation in homogeneous coordinates. *Computers & Graphics*, 32(1):120–127, 2008.

[262] Junchao Ma, Wei Lou, Yanwei Wu, X-Y Li, and Guihai Chen. Energy efficient tdma sleep scheduling in wireless sensor networks. In *IEEE INFOCOM 2009*, pages 630–

638. IEEE, 2009.

[263] Janine Illian, Antti Penttinen, Helga Stoyan, and Dietrich Stoyan. *Statistical analysis and modelling of spatial point patterns*, volume 70. John Wiley & Sons, 2008.

[264] Hans Petter Langtangen. *Finite Difference Computing with Exponential Decay Models*. Springer Nature, 2016.

[265] Peter Olofsson and Mikael Andersson. *Probability, statistics, and stochastic processes*. Number 04; QA274, O4. Wiley Online Library, 2005.

[266] Gerhart Friedlander, Joseph W Kennedy, Edward S Macias, and Julian M Miller. *Nuclear and radiochemistry*. John Wiley & Sons, 1981.

[267] Graham Upton and Ian Cook. *Understanding statistics*. Oxford University Press, 1996.

[268] Joseph Polastre, Jason Hill, and David Culler. Versatile low power media access for wireless sensor networks. In *Proceedings of the 2nd international conference on Embedded networked sensor systems*, pages 95–107, 2004.

[269] Injong Rhee, Ajit Warrier, Mahesh Aia, Jeongki Min, and Mihail L Sichitiu. Z-mac: a hybrid mac for wireless sensor networks. *IEEE/ACM Transactions On Networking*, 16(3):511–524, 2008.

[270] Wei-Peng Chen, Jennifer C Hou, and Lui Sha. Dynamic clustering for acoustic target tracking in wireless sensor networks. *IEEE transactions on mobile computing*, 3(3):258–271, 2004.

[271] Bilal Muhammad Khan, Falah H Ali, and Elias Stipidis. Improved backoff algorithm for ieee 802.15. 4 wireless sensor networks. In *2010 IFIP Wireless Days*, pages 1–5. IEEE, 2010.

[272] ONF. Software-defined networking: The new norm for networks. *Open Networking Foundation*, 2012.

[273] Dajin Wang, Liwei Lin, and Li Xu. A study of subdividing hexagon-clustered wsn for power saving: Analysis and simulation. *Ad Hoc Networks*, 9(7):1302–1311, 2011.

[274] K Shashi Prabh and Tarek F Abdelzaher. On scheduling and real-time capacity of hexagonal wireless sensor networks. In *19th Euromicro Conference on Real-Time Systems (ECRTS'07)*, pages 136–145. IEEE, 2007.

[275] Jerome Harri, Fethi Filali, and Christian Bonnet. Mobility models for vehicular ad hoc networks: a survey and taxonomy. *IEEE Communications Surveys & Tutorials*, 11(4):19–41, 2009.

[276] Ameer Ahmed Abbasi and Mohamed Younis. A survey on clustering algorithms for wireless sensor networks. *Computer communications*, 30(14-15):2826–2841, 2007.

[277] Michael Schlichtkrull, Thomas N Kipf, Peter Bloem, Rianne Van Den Berg, Ivan Titov, and Max Welling. Modeling relational data with graph convolutional net-

works. In *European Semantic Web Conference*, pages 593–607. Springer, 2018.

[278] Jiaxuan You, Rex Ying, and Jure Leskovec. Position-aware graph neural networks. *arXiv preprint arXiv:1906.04817*, 2019.

[279] Muhan Zhang and Yixin Chen. Link prediction based on graph neural networks. In *Advances in Neural Information Processing Systems*, pages 5165–5175, 2018.

[280] Franco Scarselli. A short description of the graph neural network toolbox. 2011.

[281] Shams ur Rahman, Geon-Hwan Kim, You-Ze Cho, and Ajmal Khan. Positioning of uavs for throughput maximization in software-defined disaster area uav communication networks. *Journal of Communications and Networks*, 20(5):452–463, 2018.

[282] Thushan Sivalingam, KB Shashika Manosha, Nandana Rajatheva, M Latva-aho, and Maheshi B Dissanayake. Positioning of multiple unmanned aerial vehicle base stations in future wireless network. In *2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring)*, pages 1–6. IEEE, 2020.

[283] Matthew Mathis, Jeffrey Semke, Jamshid Mahdavi, and Teunis Ott. The macroscopic behavior of the tcp congestion avoidance algorithm. *ACM SIGCOMM Computer Communication Review*, 27(3):67–82, 1997.

[284] Prasanta Chandra Mahalanobis. On the generalized distance in statistics. National Institute of Science of India, 1936.

[285] Franco Scarselli, Marco Gori, Ah Chung Tsoi, Markus Hagenbuchner, and Gabriele Monfardini. The graph neural network model. *IEEE Transactions on Neural Networks*, 20(1):61–80, 2008.

[286] Robert Mitchell and Ray Chen. Adaptive intrusion detection of malicious unmanned air vehicles using behavior rule specifications. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 44(5):593–604, 2013.

[287] Hichem Sedjelmaci, Sidi Mohammed Senouci, and Nirwan Ansari. A hierarchical detection and response system to enhance security against lethal cyber-attacks in uav networks. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 48(9):1594–1606, 2017.

[288] Sepp Hochreiter and Jürgen Schmidhuber. Long short-term memory. *Neural computation*, 9(8):1735–1780, 1997.

[289] Yann LeCun, Léon Bottou, Yoshua Bengio, and Patrick Haffner. Gradient-based learning applied to document recognition. *Proceedings of the IEEE*, 86(11):2278–2324, 1998.

List of Publications

Science Citation Index Journal

1. Mohd. Abuzar Sayeed, Rajesh Kumar, Vishal Sharma, *"Efficient data management and control over WSNs using SDN-enabled aerial networks"*, Wiley, International Journal of Communication Systems, Vol 33.1, pages e4170, 2020.

2. Mohd. Abuzar Sayeed, Rajesh Kumar, Vishal Sharma, *"Safeguarding unmanned aerial systems: an approach for identifying malicious aerial nodes"*, Institution of Engineering and Technology, IET Communications, Vol 14.17, pages 3000–3012, 2020.

3. Mohd. Abuzar Sayeed, Rajesh Kumar, Vishal Sharma, Mohd. Asim Sayeed *"Efficient Deployment with Throughput Maximization for UAVs Communication Networks"*, Multidisciplinary Digital Publishing Institute, MDPI Sensors, Vol 20.22, pages 6680, 2020.

4. Mohd. Abuzar Sayeed, Rajesh Kumar, *"An efficient mobility model for improving transmissions in multi-UAVs enabled WSNs"*, Multidisciplinary Digital Publishing Institute, MDPI Drones, Vol 2.3, pages 31, 2018.

International Conference

1. Mohd. Abuzar Sayeed, Rajesh Kumar, Vishal Sharma, Ilsun You *"An SDN-Based Secure Mobility Model for UAV-Ground Communications"*, MobiSec: International Symposium on Mobile Internet Security, pages 169–179, 2017.