Detection of Sybil Attack using Centrality and ACO in Opportunistic Networks

Thesis submitted in partial fulfilment of the requirements for the award of degree

Of

Master of Engineering

in

Information Security

Submitted By

Gurleen Kaur

(Roll No. 801433011)

Under the supervision of:

Ms. Tarunpreet Bhatia

Lecturer

COMPUTER SCIENCE AND ENGINEERING DEPARTMENT

THAPAR UNIVERSITY

PATIALA – 147004

July 2016

CERTIFICATE

I hereby certify that the work which is being presented in the thesis entitled, "*Detection of Sybil Attack using Centrality and ACO in Opportunistic Networks*", in partial fulfilment of the requirements for the award of degree of Master of Engineering in *Information Security* submitted in Computer Science and Engineering Department of Thapar University, Patiala, is an authentic record of my own work carried out under the supervision of *Ms.Tarunpreet Bhatia* and refers other researcher's work which is duly listed in the reference section.

The matter presented in the thesis has not been submitted for award of any other degree of this or any other University.

Signature:
Gurleen Kaur

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

Ms. Tarunpreet Bhatia
Lecturer, CSED

Countersigned by

Dr. Maninder Singh
Head
Computer Science and Engineering Department
Thapar University
Patiala

Dr. S.S Bhatia
Dean (Academic Affairs)
Thapar University
Patiala

CERTIFICATE

I hereby certify that the work which is being presented in the thesis entitled, **"***Detection of Sybil Attack using Centrality and ACO in Opportunistic Networks***"**, in partial fulfilment of the requirements for the award of degree of Master of Engineering in *Information Security* submitted in Computer Science and Engineering Department of Thapar University, Patiala, is an authentic record of my own work carried out under the supervision of *Ms.Tarunpreet Bhatia* and refers other researcher's work which is duly listed in the reference section.

The matter presented in the thesis has not been submitted for award of any other degree of this or any other University.

Signature:
Gurleen Kaur

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

Ms. Tarunpreet Bhatia
Lecturer, CSED

Countersigned by

Dr. Maninder Singh
Head
Computer Science and Engineering Department
Thapar University
Patiala

Dr. S.S Bhatia
Dean (Academic Affairs)
Thapar University
Patiala

ACKNOWLEDGEMENT

It is a matter of pride and privilege to express my deep gratitude and a sincere thanks to **Ms. Tarunpreet Bhatia, Lecturer, CSED, Thapar University, Patiala** for her guidance and support throughout the report. I feel very fortunate for her valuable suggestions, guidance encouragement on every step to accomplishment and prepare this highly constructive report.

A special thanks to our **Head of the Department, Dr. Maninder Singh** as well as **PG co-ordinator**, **Dr. Jhilik Bhattacharya, Associate Professor, CSED, Thapar University, Patiala**. The completion of any project is the endeavour of all individuals that supports, include & foster the much needed enthusiasm and confidence to the doer of the project work within the whole task prove to be impossible mission.

I am pleased to write these lines for over whelming support of staff members of CSED, Thapar University for their invaluable contribution to my work. Their suggestions added more charm and information in preparing this report.

My greatest thanks to all who wished me success especially my parents, family and friends, who encouraged and supported me at every point of time.

All I thank the almighty – the supreme the terminal and only supernatural power for imparting me courage, and confidence to attain a full stop for this project.

Gurleen Kaur

(801433011)

ABSTRACT

The evolution of opportunistic networks is on rise due to advancement in the technology of the handheld devices. In opportunistic networks, the routes are built dynamically, so there is no fixed network topology. Also these networks are delay tolerant and therefore tend to suffer from long delays as well as the network partitions; in the meantime they are very much at the risk of security threats. However, mitigating the effects of Sybil attack has been always a demanding and ongoing research topic in network security. Sybil attack is one of the most harmful attacks in networks. In this attack, the malicious node fabricates multiple identities to infect the network. Here, the combination of betweenness centrality and ACO has been used for optimal and secure routing against the Sybil attack. ONE simulator has been used for simulation of the entire scheme, where the simulation scenario consists of three different node groups' *viz.* pedestrians, cars and trams in which the users are free to interact with one another. The effectiveness of the proposed technique has been determined by comparing parameters like packet drop, delivery probability, overhead ratio and throughput of ideal, vulnerable and detection modes. The integration of centrality and ACO has proved to be a very constructive scheme in mitigating the effects of Sybil attack in the opportunistic networks optimally without compromising the important parameters of a reliable and efficient network.

Keywords: ACO, Centrality, HiBOp Routing, Opportunistic Network, OppNet, Sybil Attack

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

ACO Ant Colony Optimization

CIA Confidentiality, Integrity and Availability

DTN Delay Tolerant Network

GUI Graphical User Interface

HiBOp History Based Routing Protocol in Opportunistic Networks

IDE Integrated Development Environment

MANET Mobile Ad-Hoc Network

ONE Opportunistic Network Environment

OppNet Opportunistic Network

PDA Personal Digital Assistant

PRoPHET Probabilistic Routing using History of Encounters and Transitivity

PSO Particle Swarm Optimization

RAPID Resource Allocation Protocol for International Delay Tolerant Network

CHAPTER 1
INTRODUCTION

1.1 Introduction

The evolution of the communication networks has emphasized the use of the wireless communication devices such as mobile phones, smart phones etc. The communication network can be subdivided under the network categories such as the wireless communication networks and the wired communication networks. These networks consist of mainly two types of network nodes, namely, static node and mobile node. Both the static and the mobile network node is either continuously connected or intermittently connected. The intermittently connected static nodes constitute the wireless sensor networks while the mobile mostly connected nodes constitute the mobile ad hoc networks. But the combination of the mobile and static nodes constitutes the opportunistic networks.

Infrastructure based networks were pre-requisites of any communication system. These networks had a particular network topology. The source knew the proper routing path to send and receive messages to and from the destination. But in the scenario of wireless ad-hoc networks where there is only infrastructure less connectivity, certain challenges are encountered. Today even more new technology which is more general than mobile ad-hoc networks (MANETs) and also not essentially restricted to Internet-like architecture with gateways, as often supposed by DTN, hence called as Opportunistic Networks (OppNets).

The widespread use of wireless communication devices such as Smartphone, mobile phones etc, in our day to day life has occupied our lives so much that such devices have become the basic necessity of our life. The presence of fixed infrastructure such as Wi-Fi access points or the mobile phone networks makes the communication possible among these devices. But also these devices tend to communicate in the infrastructure-less scenario too. They generally communicate in an ad-hoc manner in which the two devices may directly exchange messages when in vicinity of each other. For example, Wi-Fi Direct or Bluetooth are the wireless protocols which do not require any fixed infrastructure. Thus, a decentralized opportunistic network is created when various such devices act as a network node in order to transfer each other's

messages in an obliged manner. Hence, it results into a disconnected store carry and forward model.

An obliged and cooperative nature of such decentralized networks, could however lead to the breaching of the security in a network. There could be a continuous threat to the privacy of the network which could end up resulting in discouraged participation in the network.

1.2 Evolution of Opportunistic Networks

The wireless technology provides services like long range communications including Wi-Fi, broadcast and cellular data service etc, which are not viable to implement with the use of cables or wires. Wireless communications have reduced the complex process of installing the cables as a connection among the various equipment locations. The physical layer of the OSI model is used to implement the wireless telecommunication network. Radio communication is generally administered and implemented into these networks. Earlier the mobile devices used to communicate only using the fixed infrastructure but these days the communication is also possible without actually having any infrastructure. The devices within the physical proximity of each other can communicate well without any infrastructure. This can also be considered as the peer-to-peer communication.

In the present day scenario, where the different operating systems run over the different devices, we see the rapid improvement in the efficiency of the wireless communication through the heterogeneous networks. Today, almost each and every person carries the wireless devices such as mobile phones, laptops, PDAs etc. With the fastest generation ever, the technology is swooping on a high rate of knots. Earlier it was only possible to talk to a person sitting far away but today one can even see the other person sitting live in front of him and along with the long talks and chats, people can also share a lot of stuff with each other. These hi-tech gadgets have occupied our lives so much that it has become a need of each and every person on the earth to have at least one of the gadgets in its pocket. The prevalent use of the smart phones due to their ease of use, relatively less expensive and their escalating sensing capabilities such as capturing of the location (GPS, triangulation), the activity (accelometer, gyroscope), the audio signals (microphone), the light and vicinity (i.e. using light sensors) and the images/videos has increased the use of multiple sensing devices as a single device.

The tremendous development of numerous inexpensive, little and self-contained battery powered computers, known as the sensor nodes has contributed to the growth of wireless sensor networks along with multiple other applications such as mobile-ad-hoc networks, delay tolerant networks and the very new concept that is the opportunistic networks. These sensor nodes have the ability to accept the input from the nearby sensor and then process this input in order to wirelessly transfer the results to the transit network. However with very prominent use of these sensors, it is striking that the wireless sensor networks possess the security threats too.

Wireless sensor networks [6,7] consist of the sensor nodes mainly, along with the combination of the radio communications and the system. Some heterogeneous networks that operate in mobile or extreme terrestrial environments lack persistent network connectivity. Below is the brief summary of the networks which have advanced from the wireless networking technology. These networks particularly focus on the top of the physical layer protocols such as Wi-Fi Direct, Bluetooth etc.

1.2.1 Mobile ad-hoc Networks (MANETs)

Mobile ad hoc network (MANET) [2,4] is an infrastructure less, self configuring wireless network. Multiple mobile nodes are present in this network. Due to dynamic topology, the nodes freely move around the network, by dynamically establishing the route among them, establishing their own network. MANETs often focus on the synchronous communication among the two or more nodes in a network [4]. The MANETs are more generalised wireless mesh networks, in the sense, the nodes themselves acts as both router as well as the hosts.

In order to send messages from the source to destination, it is important that a single end-to-end path must exist between them. If no such route exists, then it becomes impossible for the two end points to communicate and hence the network is partitioned. Due to this a different networking approach is required which is known as the Delay Tolerant Networks.

1.2.2 Delay Tolerant Networks

Delay Tolerant Networks (DTNs) [5], or disruption tolerant networks were initially designed to address the technical issues associated with the interplanetary or space communications where the communication is over the extreme distances and thus suffers the long delays. The long delays could be measured sometimes even in hours or in days. The delay is inevitable. However, when there is extreme interference or the

network resources are sternly overburdened, the similar problems may arise even in the more modest distances.

Delay Tolerant Networking is an approach that seeks to address the issues that makes the communication difficult in heterogeneous networks. The communication among different devices with different operating systems is generally completed by the conversational communication possible due to the mobile ad-hoc networks (MANETs) that are constructed as a part of the wireless sensor networks. Further, to conquer a mere incapability of this technology to deliver the data in the absence of the wireless connection such as Wi-Fi etc, a new technology termed as opportunistic network is coined to ensure delivery of the data without actually having a predefined connection among the nodes. The data could be sent to any other node that comes in its vicinity. The average range to forward the data is 300 meters. These networks basically follow the store-carry-forward paradigm in which they just store the data to themselves until they encounter any other node in their vicinity. Thus, the opportunistic networks tend to forward the data opportunistically to a node which is encountered first i.e. the nodes tend to forward the data whenever an opportunistic encounter happens between the two nodes.

1.2.3 Opportunistic Networks

Close proximity of mobile, personal devices etc facilitates efficient application of opportunistic networks [3]. The routes being built dynamically in opportunistic networks, the necessity for awareness of network topology is not imperative. Opportunistic networks transfer the packets opportunistically from source to destination i.e. the data is transferred when the two nodes opportunistically encounter each other. Despite numerous algorithms for data forwarding having been proposed till date so as to pass on the messages, but finding routes towards the required destination in such disconnected environment is a compelling issue of this network because even after choosing a suitable routing methodology, it is still not easy to find if a desired node would behave properly or maliciously in the system [26].

The OppNets enable an integration of the resources that surround us more and more, such as the diverse communication, computation, sensing and storage. Moreover, the OppNet follow one-hop communication among the mobile devices carried by the mobile users. Hence, we can say there is a participatory interaction of the nodes with their surroundings without relying on the wireless infrastructure. These networks

possess open and distributed nature. Thus, the user interactions are secured by relying on the trust rather than the hard cryptography. Establishing trust in such distributed networks is trickier as there is no centralized mechanism for its working. Along with the ease of fast and easy communication there are some privacy, security and trust issues in this scenario. Hence, establishing a connected path from source to destination is not feasible, as the local view of a network is the only basis of forwarding decisions.

Opportunistic Networking is the most recent networking concept which can be easily incorporated by extending the existing wireless technologies such as 3G or Wi-Fi. The mobile devices in an OppNet can communicate opportunistically with each other by transferring the data within their mutual transmission range. It is interesting that the OppNets follow the human mobility pattern to identify the nearby nodes and broadcast the data in a peer to peer fashion.

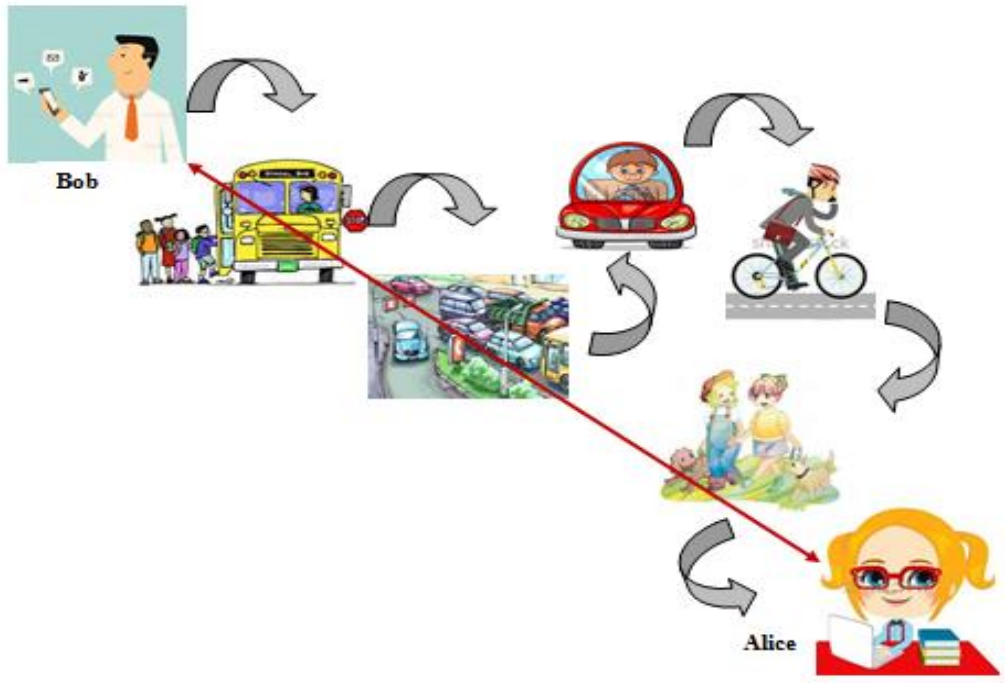

Fig 1.1: The Real Life Scenario of Opportunistic Networking

Fig 1.1 represents the real life scenario of opportunistic networking. We have assumed the conversation scenario between Bob and Alice. Bob transfers message opportunistically for Alice using his smart phone via Wi-Fi to a bus in the nearby area, in the hope that the bus will carry message closer to Alice. While moving through the traffic, this bus forwards message via its Bluetooth to one of its passenger who gets off at a stop in the city of Alice. After getting off the bus, he drives his car in

the city of Alice where he encounters a cyclist who carries the message to a park in the locality of Alice. Further two girls in the park carry that message with them as they are neighbours of Alice. Finally the message is delivered to Alice.

As compared to DTN, where a message is transmitted opportunistically only if an already existing end to end route is not found, OppNets are based on entirely on opportunistic routing algorithm. However in opportunistic networks an existing end to end path is not a requirement. While the connectivity in the MANETs is such that an end to end path might never exist between the two end points. However in opportunistic networks the mobility is turned into an opportunity as the nodes are allowed to hold the messages with them while they move and pass it further to any other node only when a next node is opportunistically encountered.

Table 1.1: Comparison of Generalized Network and Opportunistic Network

Generalized Network	Opportunistic Network
• Nodes are usually static • Communication takes place only if there exists end to end route between the nodes • Static or Dynamic Routing is done depending on the type of network	• Nodes may be static or mobile • Communication is possible even if pre-existing route does not exist between the nodes • Routes are dynamically built even if the communication path is not predestined

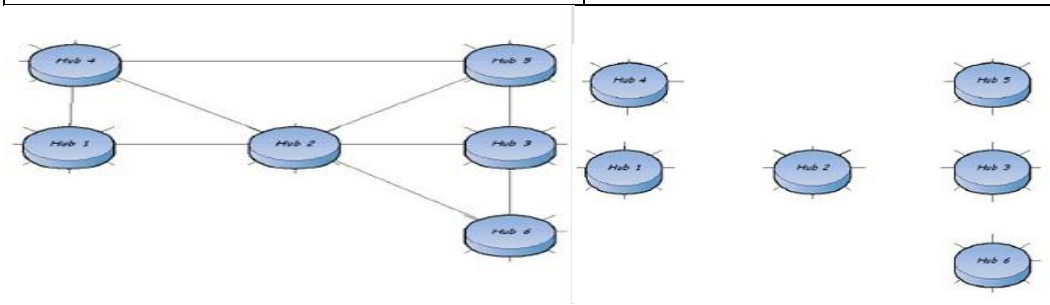

Fig 1.2(a): Generalized Network (b): Opportunistic Network

1.3 Characteristics of Opportunistic Networks

It becomes easy to identify some network when their characteristics are known. Although the opportunistic networks are the extension of mobile ad-hoc networks, their characteristics make them identifiable

- **Store-carry-forward concept:** The fundamental concept of the opportunistic networks is that the nodes would carry the message with them until they do

not encounter any other node to forward the message to. These are particularly infrastructure-less ad-hoc networks. This may cause delay in data transmission among the networks.

- **Node Discovery:** The nodes present in the opportunistic network can be either static or mobile or both. The network nodes within the network range of a particular node are able to find each node to pass on the data to.
- **Temporary Existence:** These networks exists for a particular amount of time which is essential to run particular applications (requested in specific time on a specific location). There can be applications related to the social networking or it could be an application to support the enterprise for creating and delivering products or digital services in a particular area and the time interval. Therefore, the existence of OppNets is just temporary as they exist only for particular applications.
- **One hop Message Exchange:** Unlike any other network where message is communicated using multiple hops, the opportunistic networks nodes go for just one hop message exchange. They forward the message to whatever node they encounter in direct communication range.
- **Dynamic Network Topology:** The network topology of opportunistic networks changes frequently. As the nodes are mobile and so they activate and deactivate according to the requirement.

1.4 Challenges in Opportunistic Networks

Being wireless ad hoc network, the challenges faced by opportunistic networks are quite possible. Many researchers have tried to overcome the challenges but in such a distributed scenario it has not yet come up with the most perfect solution

- **Privacy & Security:** Ensuring privacy and security is a main concern of this network. However fully secure network cannot be formed in such distributed environment but still many methods have come up to accomplish this challenge till date.
- **Trust:** It is important to build up trust among the nodes in terms of confidentiality and integrity. Confidentiality in order to ensure that information is concealed from unauthorized third parties. Integrity meant to ensure that information is not altered while propagating.

- **Selfishness:** The nodes are independent to forward the packets to other nodes individually. But this rule is sometimes violated by selfish or some malicious nodes by refusing to serve as bundle relays. This creates a challenging scenario especially in distributed networks such as social networks.
- **Lack of Central Authority:** Because the opportunistic networks do not possess any fixed topology and they have lack of knowledge as to through which path to send data, thus it can be said that these networks lack in central authority too. No particular hub is available to control the nodes.
- **Routing and Forwarding:** The opportunistic networks are extremely dynamic in nature. This enables a great speed and mobility environment for information to travel but with a restriction of available opportunities and a risk of transferring data to insecure nodes.
- **Connectivity:** Lack of prior information such as knowledge, location, time and bandwidth of any contact can lead to intermittent connectivity.
- **Delay Tolerance:** It is one of key focus in opportunistic networks. As opportunistic networks are subsets of DTNs, it is obvious the delay will be encountered frequently in this network too.
- **Heterogeneity:** Multiple devices with different operating systems need to interact with each other. However, devices being accessed by different methods at different radio frequencies and inter-operability will result in exploitation of opportunistic networking applications.

1.5 Thesis Layout

The rest of the thesis is organised in the following manner:

- Chapter 2 reflects the security and the routing issues in opportunistic networks
- Chapter 3 summarises the detailed research work related to the opportunistic networks and its security
- Chapter 4 demonstrates the problem statement and motivation of this thesis
- Chapter 5 describes the simulator used
- Chapter 6 defines the proposed algorithm to defend Sybil attack
- Chapter 7 analyzes the results obtained by the proposed algorithm
- Chapter 8 concludes the thesis work and discusses the possible future scope

CHAPTER 2

SECURITY & ROUTING ISSUES IN OPPNETS

2.1 Routing Protocols in Opportunistic Networks

Due to the decentralised nature of the opportunistic networks, the major challenges are faced in the routing as well. The opportunistic network posses the dynamic routing which is why the network node pass on the message to the other node only when they come in physical proximity of each other. The network node willing to pass the message to other node keeps the message to itself until the other node is encountered. Because the path is not fixed in this scenario the network nodes tend to forward the data to any node that happens to be opportunistically encountered. In order to make the routing decisions each node has to rely on the local knowledge of the network. If the encountered nodes are useful in forwarding then the efficiency and the network performance are positively affected. The routing protocols described below make use of features like mobility in opportunistic networks.

i. **Epidemic [9]:** This protocol follows the concept of flooding the network with messages. It is a multipath routing protocol. It aims at maximizing the delivery rate. Therefore, multiple messages are forwarded along each and every path, due to which the destination possibly ends up receiving redundant copies of the message. Although, this approach performs well under the ideal conditions, for example, unlimited bandwidth, buffer and energy. However, too much redundancy in a network results into the draining of battery and wastage of buffer space and hence the network performance is degraded. This protocol is quite easy to implement. It results in the increasing delivery ratio and decreasing delivery delay will at the same time results in higher overhead.

ii. **Direct Delivery [2]:** As the name suggests this routing protocol delivers the data to whichever node comes in its direct communication range where the maximum hop count for forwarding paths is one. The message probably arrives directly at the destination node from the source node. While in other routing protocols such as epidemic routing, in order to reduce the delivery cost, the protocols set the maximum hop count more than one. But in this case, no intermediate forwarding nodes are used as the maximum hop count is one. This protocol does not create multiple copies of the messages. So the

redundancy is not there, due to which the delivery cost is optimal but the delivery ratio and delivery delay would not be as efficient as other routing protocols.

iii. **PRoPHET [11]:** The Probabilistic Routing Protocol using History of Encounters and Transitivity (PRoPHET) uses the past encounters to predict the future in a best way. Its main goal is to reduce the delivery cost, by preventing the unnecessary message replicates to occur. This goal is acquired by assuming that he previous node encounters would indicate the probability inclination of the future encounters among the same nodes. Thus the encounters occur systematically. Delivery probability for every destination is maintained by each node. The estimated delivery probability increases during each encounter with the destination but also decreases with time. Whenever the delivery probability is higher for the destination only then the message copies are forwarded between the newly encountered nodes rather than the nodes currently carrying the message. In short, we can say that message copies are forwarded to the newly encountered nodes when they are more liable to deliver the messages to the intended destination.

iv. **Spray and Wait [12]:** This protocol works in two phases; spray phase and wait phase. In spray phase, the source node will generate and "spray" the message copies by distributing the message to only the few relay nodes encountered first. After receiving the copies the relays are in wait phase, where each relay "waits" to meet the destination and then delivers the message directly to the destination. Epidemic routing with maximum hop count two would be similar to this protocol. For example, the source node might forward the message to the newly encountered node and that node would forward the message to the next four nodes it would encounter. If the nodes receiving the copy of the bundle never cross the path of destination, the system will completely fail. Only a restricted number of message copies are infused into the network.

v. **MaxProp [13]:** This protocol is basically meant for the routing in vehicle based disruption tolerant networks. It aims at increasing the delivery rate and decreasing the latency. It schedules the packets for transmission to its peers by prioritising the messages based on heuristics, say; low hop count messages are prioritized. Also, if the buffer space is full it would manage to delete the

unwanted messages accordingly. It would cope-up better during the non-ideal situations where the network buffers or the transfer duration may be limited.

vi. **RAPID [2]:** It is the Resource Allocation Protocol for International DTN. This protocol also copes better in the non-ideal situations where bandwidth is limited and all the messages may not be exchanged during encounters. It aims at optimising routing performance by explicitly selecting any one performance metric such as delivery probability or delivery delay. The messages to be forwarded are prioritised using the explicit utility function, meant to estimate the performance measured by the selected performance metric.

vii. **HiBOp [14]:** HiBOp is a History Based Opportunistic routing protocol. This protocol aims at reducing network clogging by drastically limiting the number of copies spread into the network, due to which it performs better than the epidemic and PRoPHET routing protocols and gives better throughput. This protocol utilizes the context information of the node in order to decrease the overhead of flooding [14]. Context refers to the personal information about the users such as their name, their work, their address, their hobbies etc which helps this protocol to forward the message to all the users that share the similar context properties. This context information is also used by the PRoPHET routing, in a way that it exploits the user's mobility patterns, their frequency of contact and their place of visit, information in order to forward the data in the opportunistic networks. In short, the context is a form of local environment of the user which is stored in the form of identity tables in HiBOp routing Protocol. Every node also stores the history of each node encountered by using the identity value in the history table. This history table is maintained by each node. There are 3 phases of this protocol:

- **Emission Phase:** The message is injected into the network by flooding replicas of the messages among the appropriate number of nodes. The number of neighbours to which the message is to be sent by the sender is calculated by using the formula that takes into the account the probability to deliver the message to the destination. Following is the formula in which two components are weighted with a factor α ($0 \leq \alpha \leq 1$). The first component $P_{H,}$ maintains the legacy of past history of a node. While the second component is meant for describing the current status of the node's environment.

$$P = \alpha . P_H + (1 - \alpha), max\{\eta . P_{cc}, P_{IT}\}$$

where, $$P_H = min\{1, P'_H + [1 - e^{-(h-1)}]\}$$

$$P_H = \frac{\sum_{j\epsilon\{match\}} P_{op}^{(j)} . W_j}{\sum_{j\epsilon\{dst\_info\}} W_j}$$

$$P_{IT} = \frac{\sum_{j\epsilon\{match\}} W_j}{\sum_{j\epsilon\{dst\_info\}} W_j}$$

$$P_{cc} = max_{j\epsilon cc} P_{IT}^{(j)}$$

The α factor gives more weight to the past history or to the current environment of a node which is described in combination by P_{IT} and $P_{CC.}$

The component P_{CC} is related to a neighbour while the component P_{IT} is related to the local node due to which the η factor (η<1) scales down P_{CC} with respect to $P_{IT.}$

- **Forwarding Phase:** The node's mobility and its contacts are used by HiBOp to take the messages closer to the destination. This occurs in two manners: the message is to be forwarded to which node in the network is determined by matching the information of the sender with the context information of other nodes. Also before forwarding the message the delivery probability is also calculated using the node's Identity Table, Context Information and its history table.
- **Delivery Phase:** Once the destination node is found by the intermediate node, the message is delivered and the process stops

Moreover this protocol reduces the network congestion by significantly limiting the multiple copies from spreading into the network. Due this merit the overhead in HiBOp is comparatively less than the epidemic and the prophet routing protocol. HiBOp emits the message in a network by spreading the message to some specific nodes. Therefore in this manner HiBOp manages to transmit message with less overhead. This protocol is suitable for human mobility models and so the opportunistic networks are the good example for that because a general pattern is followed in these networks for which this protocol is mainly designed.

2.2 Security Issues in Opportunistic Networks

Every network has some security issues. The security issues in opportunistic networks have been defined using the CIA triad of the Network Security:

- **Confidentiality:** The message content may be disclosed to the malicious or third party nodes. Once they have the access the confidentiality of the message is breached.
- **Integrity:** Any misbehaving intermediate node can maliciously cause threat to the integrity of the data by obfuscating the malicious packets into the original ones.
- **Availability:** Redundancy of the data packets might cause disruption of the system. Limited bandwidth can also cause delays in communication.

2.3 Attacks in Opportunistic Networks

The network availability or the network performance may significantly get reduced when some attack occurs within the opportunistic network itself. The attacks occurring in opportunistic networks are not so different from MANETs, since the misbehaving node is the only reason for a network to act inefficiently. The attacks can be easily differentiated on the basis of their properties. The attacks are classified in two manners:

- Data Traffic Attack
- Control Traffic Attack

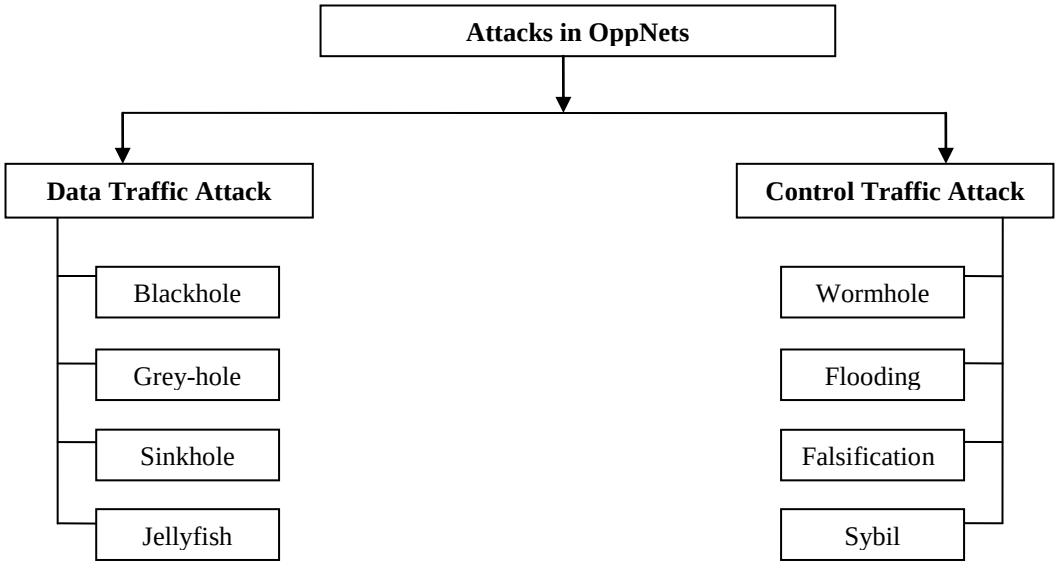

Fig 2.1: Classification of Attacks in Opportunistic Networks

2.3.1 Data Traffic Attacks

These are the attacks that deal with the dropping of the packets or delay forwarding of the packets by the malicious nodes. Some attacks choose to drop only the victim packets and some drops all the packets that pass through them. This ultimately causes the adverse effect on the network performance and also causes the considerable loss of significant data. Following are the categories of the data traffic attacks:

- **Blackhole Attack:** In this attack, a node maliciously discards a message after accepting it from a particular node or selfishly resists the forwarding of the message according to the routing protocol. In case a replica-based routing protocol is used in an OppNet, the impact of this attack will be less as compared to any other network. Since, in the replica-based routing protocol, multiple message replicas are created, however even if a malicious node discards one of the replica the impact won't be much. This implies the OppNets are naturally resilient to this attack.
- **Grey-hole Attack:** This attack drops the packets but behaves differently according to the situation. It mainly focuses on dropping only the targeted packets. It targets a particular network's packets and consistently drops them while it behaves normally with the other network nodes. The grey-hole attack also drops the packets during a particular time interval whereas it behaves normally during other instances.
- **Sinkhole Attack:** In this attack, an opponent node aims to attract nearly all the traffic from particular network nodes through a compromised node, creating a figurative sinkhole with the opponent node in the middle. Unlike blackhole attack in OppNets, it is very much possible attack and hence can cause a significant data loss as all the data including the replicates will also get attracted towards the sinkhole node.
- **Jellyfish Attack:** It is a type of selective Blackhole attack. The malicious node delays or drops the packets for a certain amount of time after acquiring the data packets from the authorized nodes. This attack is most prominent in the wireless ad-hoc networks. And so it is also very possible in opportunistic networks too.

2.3.2 Control Traffic Attacks

These attacks tend to control the traffic of a network such as routing and localization.

- **Wormhole Attack:** This attack is difficult to prevent from occurring in an opportunistic network. This attack prevents the path establishment by preventing the nodes from finding the genuine routes that are more than two hops away. This is also sometimes known as the Tunnelling Attack.
- **Flooding Attack:** Sometimes a network may be flooded with the messages. But the flooding could also be incapable of being traces, once the nodes' identity is spoofed. Because only the limited resources are available for the participating devices, for example, battery which can be drained by reception and transmission of the messages, therefore this attack can also act as a denial of service (DoS) attack against the participating nodes in a network.
- **Routing information falsification Attack:** Sometimes in opportunistic network, nodes tend to share or exchange their routing information with each other. In this case, it is possible that a malicious node will supply the false information to the newly encountered nodes. This would adversely affect the routing performance of a network by distorting the other node's view. When this attack used in combination with the Sybil attack it can even spoof information regarding the multiple false identities.
- **Sybil Attack:** In this attack, the malevolent node creates illegitimate multiple identities in order to gain the access to the useful information being exchanged among the legitimate nodes. The additional identities are known as Sybil nodes. Due to the lack of central authority to certify identity to the individual nodes in an OppNet, a single malicious node arbitrarily spoofs many identities within a network. Under this attack even if the limited multiple copies of a message are being spread in a network, the malicious node could accept all the copies under different identities and then can either maliciously drop the packets or keep the packets with itself or even could obfuscate the malicious packets into the legitimate packets and forward to other nodes. Sybil Attack is an attack in which multiple Sybil nodes are created to degrade the network performance. The Sybil nodes are the multiple identities of the actual malicious node in the Sybil attack. These multiple Sybil nodes pretend to be the original and unique nodes in order to attract the packets to themselves and then perform some malicious activity on the targeted packets.

Fig 2.2 shows the scenario of Sybil attack in a network. The Sybil node creates multiple fake identities and attracts the useful information from the legitimate or honest node in order to perform attack.

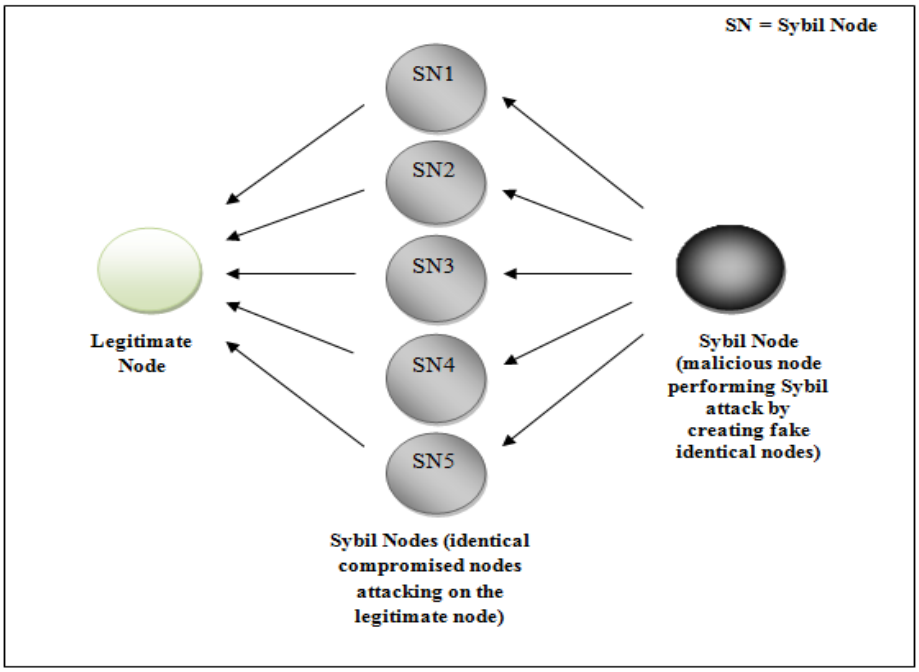

Fig 2.2: The Sybil Attack

There are multiple ways to define the Sybil attack. For example, the Sybil attack has occurred by directly communicating with the node or indirectly communicating with the node. The other way could be that if the malicious node has stolen the identity of any legitimate node or just created a fake identity. Another possible scenario is the way the attacker is going to perform the attack i.e., simultaneously or non- simultaneously. All these implementation phases of Sybil attack are defined below in Fig 2.3.

- **Direct & Indirect Communication:** When Sybil and the legitimate nodes communicate directly with each other, it is considered as direct communication. When the Sybil node communicates with the legitimate node via some fake identity of Sybil node, it is considered as indirect communication.

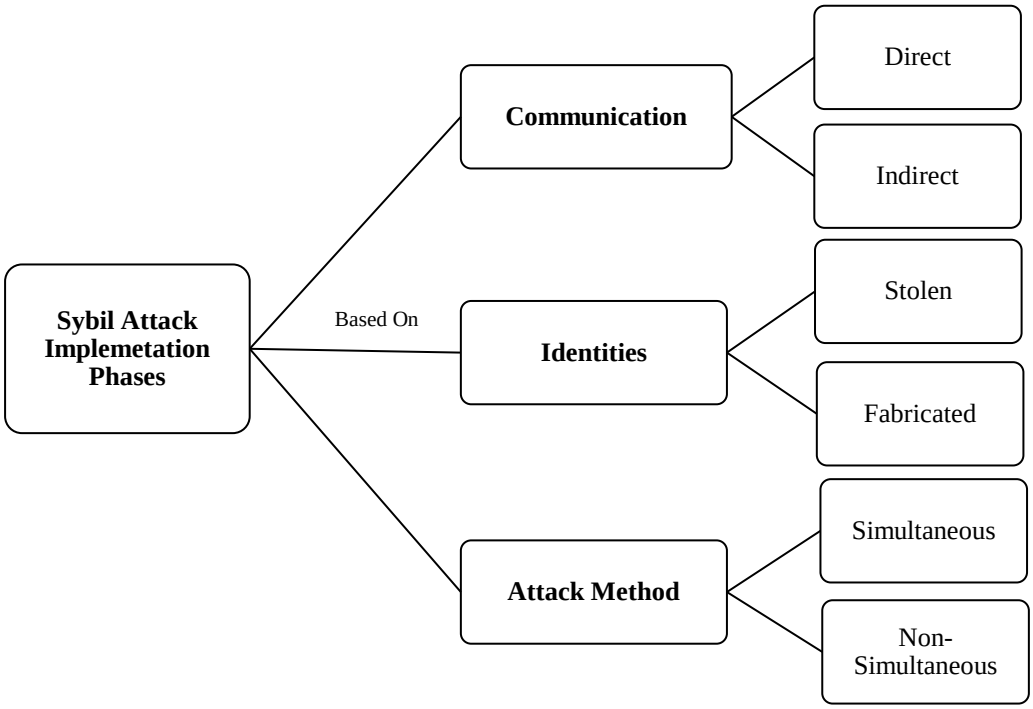

Fig 2.3: Classifying ways to implement Sybil attack

- **Stolen & Fabricated Identities:** There are two ways in which a Sybil node can get an identity i.e. it can either steal an identity of a legitimate node or it can fabricate a new identity. Identities of a legitimate node stolen by the Sybil node can just go undetected if the attacker destroys or disable the other self-replicated nodes completely. While the original identities of legitimate nodes, are fabricated by the Sybil nodes. These fabricated identities are used by the Sybil nodes multiple times in the same network.
- **Simultaneous & Non-Simultaneous Attack:** In the simultaneous attack, the fake identities of the Sybil nodes may perform the attack simultaneously. Though they have single identity, therefore the identities are circulated among all the Sybil nodes. This way they perform the simultaneous attack. The other way is that the identities could interchange among the Sybil nodes. For example, number of identities used is equal to the number of physical devices. Another way is that a particular node might leave or join the network multiple times using the single identity. This is the non- simultaneous Sybil attack.

CHAPTER 3

LITERATURE REVIEW

3.1 Literature Review

The opportunistic networks have occupied a wide space in pervasive networking these days. The prevalent use of mobile hand held devices has made these networks a crucial part for their existence. In these networks, the message is forwarded by utilizing the communication opportunities that arise from the movement of a node. This is done by achieving the store-carry-forward approach [1,2,3]. This means that the nodes would store and carry the message with them until they do not come across any other node in their direct communication. Thus the communication unlike multi-hop in mobile ad hoc networks (MANETs); it is one-hop in opportunistic networks. The nodes would opportunistically forward the message to the intended destination directly [3,4,5]. However, the consistency of the message transmission is not certain in opportunistic networks and is dependent on the intermediate nodes. The routes are also dynamic, so the local knowledge of the topology is not required. Moreover, the forwarding of any message in opportunistic network is totally based on the movement of intermediate nodes. Despite many researchers have proposed the measures for secure routing but still there is no effective way to provide security to the data packets in the opportunistic networks.

Boldrini et al. [14] compared the HiBOp routing protocol with the context aware routing protocols such as Epidemic and PRoPHET routing protocol. The author considered both uni-cast as well as group communication scenarios. The author successfully has shown the drastic reduction in resource utilization in terms of network traffic and buffer space occupied by the node. The less resource consumption feature of HiBOp routing makes the opportunistic networks naturally resilient to the congestion.

Querica et al. [15] presented a new scheme called MobID wherein portable devices are subjected to decentralised defence. It is based on two types of networks *viz.* Network of friends and network of foes. The former consists of honest nodes and the latter contains the suspicious ones. Further, the author calculated betweenness metric of centrality to determine the likelihood of a node to be a Sybil one. This enables the device to verify if the unknown individual is responsible for Sybil attack. Moreover,

the author claims to analyse the real mobile and the social network data to ensure that the proposed scheme successfully suppress the interactions of the honest nodes with the Sybil nodes in the mobile environment.

Xu et al. [16] studied the centrality metrics that could forward the message effectively in the opportunistic networks even during the limited bandwidth. The proposed an algorithm for unaware destination forwarding that aims to popularise a node and its contact durations among other nodes. The author evaluated the results using trace driven simulation. The proposed algorithm when compared to other destination unaware algorithms turned out to be more effective as it achieved comparatively higher system throughput and the lower forwarding cost.

Zeng et al. [17] proposed a novel protocol SybilACO that confines the influence of Sybil attack. It is achieved using the ant colony optimization technique in which the nodes work randomly and leave the trails on path. The trail left by each node on the path becomes diluted while at the end the trails just decay slowly from the path. The author ensures that his defending scheme efficiently reduces the number of attack edges due to which only the honest nodes accept and are accepted by the other honest nodes in the scheme with higher probability and rejection the Sybil attack with greater probability.

Barbian et al. [18] proposed a complementary metric for online social networks termed as trust centrality. Unlike in other networks the centrality metric in this paper is based on trust rather than the connectedness. The author evaluates the trust centrality using a case study. The author claims trust centrality to be a helpful metric when the influence from non-hierarchical information is considered.

Ahmad et al. [19] proposed a hybrid method for identification of attacks or spam's utilising Sybil accounts on social networks, with a special focus on Facebook. Also a new online data collection approach is implemented. The pages retrieved from face book are categorised into six different groups depending upon the behaviour of users' preferences. A profile graph is created for each group wherein similarity in behaviours of different groups is measured as a function of common things between pages. The feature set thus obtained is utilised to identify malicious and benign communities. It is observed that higher closeness similarity and behaviour similarity represents malicious nodes.

Michalak et al. [20] presented the efficient computational aspect of shapely values for network centralities. The author emphasized over weighted as well as non-weighted

networks to develop the analytical formulae as well as efficient algorithms for shapely value based centrality. By empirically evaluating the proposed algorithms, the author ensures that the significant speedups are delivered by them when compared to the traditional Monte Carlo approach. The results show that in case of the non-weighted networks, even after the allowance of margin of 10% error, the proposed algorithms were able to arrive at the solution 1600 times earlier as when compared to the Monte Carlo estimation.

Zang et al. [21] presented an algorithm, named as, two-class undirected mixed membership stochastic block models, to discover Sybil nodes in the network. The author assumes the network to be a graph in which there exists an edge between the two nodes. The main purpose of this algorithm is to calculate the probability of the nodes to be Sybil and also to calculate the probability of an honest node having the links with the Sybil nodes. The author ensures the effectiveness of the proposed algorithm by validating the experiments on both synthetic and real world social networks.

Yu et al. [22] proposed a scheme to curb Sybil attacks without any extra support from an explicit positioning hardware. In other words, to verify the positions of Sybil nodes the author proposed a robust cooperative method by utilizing Random Sample Consensus Algorithm. The author also designed a system to verify the source of a vehicle and coined it a term known as Presence Evidence System (PES). The proposed system enhanced the accuracy of detection by using statistical analysis. The author provides simulations to prove the results.

Abbas et al. [23] designed a lightweight scheme that does not require any centralised trusted third party or any additional hardware in order to detect the Sybil nodes. The author also determines the exit and the entry behaviour of both legitimate and the Sybil nodes. In order to differentiate the legitimate nodes from the Sybil nodes, the author used the received signal strength approach along with the threshold calculated on the basis of nodes' entry and exit behaviour.

Tian et al. [24] demonstrated wide range of Sybil detection methods in wireless sensor networks. In particular, the purposed Sybil attack detection is based on the anchor nodes location. The two principles, localization and the positioning are improved in the proposed detection scheme. The author confirms the effectiveness of detection methods by theoretically analysing the experiments.

Chang et al. [25] projected a scheme to estimate trust level among users based on the local ranking system in order to prevent the Sybil attacks in mobile social networks. The author claims that the proposed scheme acquires three unique features. First, both the trust and distrust relations forms the basis of the system. Second, only a limited amount of information is carried by the users instead of the whole social graph. Third, with the use of high centrality several suspicious edges are removed in order to undermine the impact of attack edges. The author carries out ample experiments to validate the system's effectiveness.

Parris et al. [26] used the social relations of a node to mitigate the flooding attacks. According to the scheme a node forwards the data to only those nodes that are friends to the forwarding nodes. The public private keys are tested on manually created attack model by the author. Once the node is authenticated it is either considered as a trusted node or a selfish node.

Cao et al. [27] utilized the multidimensional scaling to develop an identity authentication scheme. The author emphasized that the certification chain-based cryptography is more suitable for the OppNets rather than identity based or threshold based cryptography. The nodes are classified as clusters and the destination node is communicated in response to an initial query made to other members of group regarding their trust relationship. This is done by using the trust model based on multidimensional scheme that scrutinized similarity of the items present in low dimensional space. A trusted certificate network is established among the nodes which is responsible to implement the identity authentication in a distributed manner. M-CCIA is responsible for issuing the trust certificate. M-trust model evaluates the trust before issuing the certification.

Noh et al. [28] designed a robust recommendation algorithm known as RobuRec to defend the online recommender systems from Sybil attacks. This algorithm exploits a unique feature of admission control which predicts suitable recommendations regardless of the ratings specified by the honest or the Sybil nodes. The author confirms that RobuRec performs significantly better than the existing schemes such as PCA and LTSMF in terms of Prediction Shift (PS) and Hit Ratio (HR).

Trifa et al. [29] followed a new approach to detect the Sybil attacks. The author call the whole process as a Sybil Tracking process which is further completed by Sybil detection, Sybil notification and Sybil node isolation. The Sybil detection process monitors the Sybil nodes in the network. Sybil notification handles the responsibility

to notify the neighbours of node about the attack. Finally, the isolation process keeps the overlay away from the neighbouring nodes. The author proves the scheme to be flourishing by validating the experiments using simulation which showed that the Sybil tracking process was successfully able to acquire approximately 94% of the Sybil nodes.

Lin et al. [30] implemented social similarity based trust routing in the OppNets. The author incorporates routing decision with the social trust. The trust model based on the trustworthiness and previous records of a desired node is established. The behaviour of a node is evaluated on the basis of acknowledgement produced during encounter with each node. Moreover, an opportunity is given to the selfish nodes to change their behaviour from 'selfish' to the 'trusted' so as to forward the packets as an authorised node. The simulations show that TRSS successfully detects selfish or any malicious nodes.

Ciobanu et al. [31] ensured that routing and forwarding can be improved using the social network information of the node as the node is more liable to link the nodes of its own social community rather than the other nodes. Implementing Poisson distribution on a nodes' contact history predicts its future behaviour. In addition, a selfish node detection and prevention mechanism is also employed to avoid congestion and reduce the battery consumption.

Xi et al. [32] presented a novel trust management scheme based on the information of behaviour feedback. The author proposed an OppNet trust model that consists of the two components named as identity trust and behaviour trust which are provided by the Verified Feedback Packets (VFP). This model is managed by the social context based key management and after verifying the nodes' authenticity, the secure forwarding scheme is applied to forward the data. The proposed technique guarantees that the identity of any node which cannot be authenticated by the certificate, that node can create a trust network with other nodes on the basis of their trust behaviour.

Wang et al. [33] presented Sybil Trust scheme to prevent Sybil attacks in peer to peer networks by considering neighbour similarity trust. According to the scheme, the legitimate nodes should not have too much neighbours. But in case there are, then Sybil trust would use only the subset of peer's edges and will ignore others. The author analyses the scheme on the basis of two performance metrics i.e., communication cost and the computation cost. As a result it detected more malicious

peers as compared to already existing schemes such as Eigen trust and Eigen group trust.

Trifunovic et al. [34] demonstrated certain Sybil defence mechanisms while at the same time the author also introduced three defensive measures in opportunistic networks and evaluated their efficiency. The author established the basis of social Sybil defence in opportunistic network by creating a social network graph. The author monitors the way the attacker manipulates this graph and fabricates fake identities into it. However, in short it can be said that the author potentially utilized the social nature of opportunistic networks as a tool to defend the Sybil attacks which came out to be very optimal.

Vendramin et al. [35] recently introduced a hybrid social aware routing protocol known as CGrAnt, for opportunistic network which is based on the concept of centrality and Ant Colony Optimisation Technique. The author used degree centrality to choose the best message forwarders. The performance metrics such as message delivery ratio, message redundancy ratio and average message delivery delay of CGrAnt were compared against that of the Epidemic, PRoPHET and dLife protocol. However, CGrAnt proved more efficient than the existing protocols. The simulations were carried using ONE simulator.

CHAPTER 4

PROBLEM STATEMENT

4.1Problem Statement

Opportunistic networks provide an appealing and challenging environment in the wireless technologies where highly advanced PDAs are embedded with various high-end user applications that require frequent transmission of data. In the flexible environment of opportunistic networks where the message is transferred to randomly emerging nodes, it becomes hard to select the intermediate nodes for the message transfer, especially if they are in close proximity to each other. The sender node may simply pick up malicious node to forward the signal or haphazardly send signals between two nodes without a fixed protocol. Thus, an optimised path to relay the messages will save the transmission from a lot of such troubles.

4.2 Motivation

Every network faces the security and privacy threats. Widespread use and availability of mobile communication devices create a massive contact opportunities among humans. OppNets provide a versatile scenario for wireless communications but with limitations. The security and privacy issues are the challenging part of this network. The opportunistic networks being decentralised in nature tend to possess multiple harmful threats. Hence, here an effort has been made to mitigate these threats using the optimization technique.

4.3 Objectives

- To implement the Sybil Attack in Opportunistic Networks
- To detect the Sybil nodes using the concept of centrality
- To obtain the optimised nodes using ACO to prevent transmission of packets to Sybil nodes
- To evaluate the performance of opportunistic networks with the proposed algorithm by comparing the parameters of the three modes; Ideal, Vulnerable and Detection Mode

CHAPTER 5

THE ONE SIMULATOR

5.1 Overview

The Opportunistic Network Environment (ONE) simulator is a java based simulator. It can run on any platform that supports java such as Linux, Windows etc. It can be customized to Delay Tolerant Environment (DTN) or Opportunistic Network Environment. However it is best suited for opportunistic network environment therefore for the implementation of this thesis work, the ONE simulator has been used. The ONE simulator has three main functions:

- It utilises different movement models to generate node movement
- It can send and receive messages using several DTN routing algorithms
- It has graphical user interface where the mobility and message passing in real time among the nodes in a network can be visualized easily.

5.2 Working of ONE Simulator

The ONE simulator works with different inbuilt routing algorithms described in chapter 2. The movement models are divided into two categories such as synthetic models and the existing models. Random Walk Model, Random Waypoint Model and many more are examples of synthetic models. Then it also features various algorithms for routing such as MaxProp routing, Spray and Wait Routing and so on. Moreover, one can also attempt to touch real-time mobility through a kind of text file that is known as external movement and allows the user to create practical scenarios rather than an artificial one. Further it is a great visual aid tool and user friendly graphical representations encourage the user to establish the model parameters (even dynamically in some cases) with the help of GUI. Being an open source package, the ONE simulator enables the user to modify various modules in accordance with their own explicit requirements. The ability of ONE to avail a number of specialised metrics to analyse simulations such as overhead, latency and many more adds up to make it an even more attractive developmental tool. For instance, one can always utilise a map of any geographical location as a work field for the simulation and create an appropriate design. In addition this, with every upgraded version of ONE, there is an introduction to a number of new algorithms for routing as well as mobility

models. Apparently, the provision of extensive documentation provides a great ease of access to the software and ultimately makes it development friendly.

5.3 Description of ONE Simulator

It is a well-known fact that every a node is one of the basic entities of each and every network. ONE simulator is a no exception to this and hence gives the authority to act as its most fundamental agents. In a simulation scenario, specific groups are created by certain nodes to deliver messages to another group of nodes belonging to different communities. As an illustration, let us consider a group of pedestrians and cars, where each group is assigned a single routing practice (say Prophet or Epidemic or any other) but varying number of nodes as well as different rate of acceleration. The user may define as many groups and number of nodes as desired.

Nodes are the basic agents of ONE simulator. Certain nodes form a particular group in the simulation scenario in order to carry the messages to different nodes of various communities. For example, the node group is of pedestrians, cars or trams. Each group can be assigned different number of nodes and different amount of speed. The movement models of each node can be different too. But all the groups are assigned only one routing protocol. It could be epidemic, prophet or HiBOp or any other. It is up to the user to assign as many groups as he wants. Moreover up to what number of nodes to be assigned to each group is also in user's hands.

GUI (Graphic User Interface) enables the user to extract the logs of simulated trials such as number of contacts or transfer of messages. The task of filters is to depict the remarkable events and sometimes to stop the process in case if a specific error occurs. For more intimate inspection of the node it can either be nominated from a list or a log message can be referred. It also enables the user to explore data regarding the state of routing module as well as about the messages that are carried by the node. Although, an overall scenario of the processes during the simulation is very efficiently obtained through GUI, yet a set of performance parameters and message paths generated by post processed report files enables a more vivid scenario of node relations. There are some reports files included in the ONE that can create graph files compatible to GraphViz12. Similarly, in order to check out the spread mechanism of the messages as a time function there is a report module called message location. Also, there is an animator list that represents the data in the form of GIF animation. Then, there is a message parameter report module which collects the statistics of

overall performance (such as message delivery ratio or number of messages created or duration for messages reside in node buffers). Finally, the output of report module is contained in a post processing script.

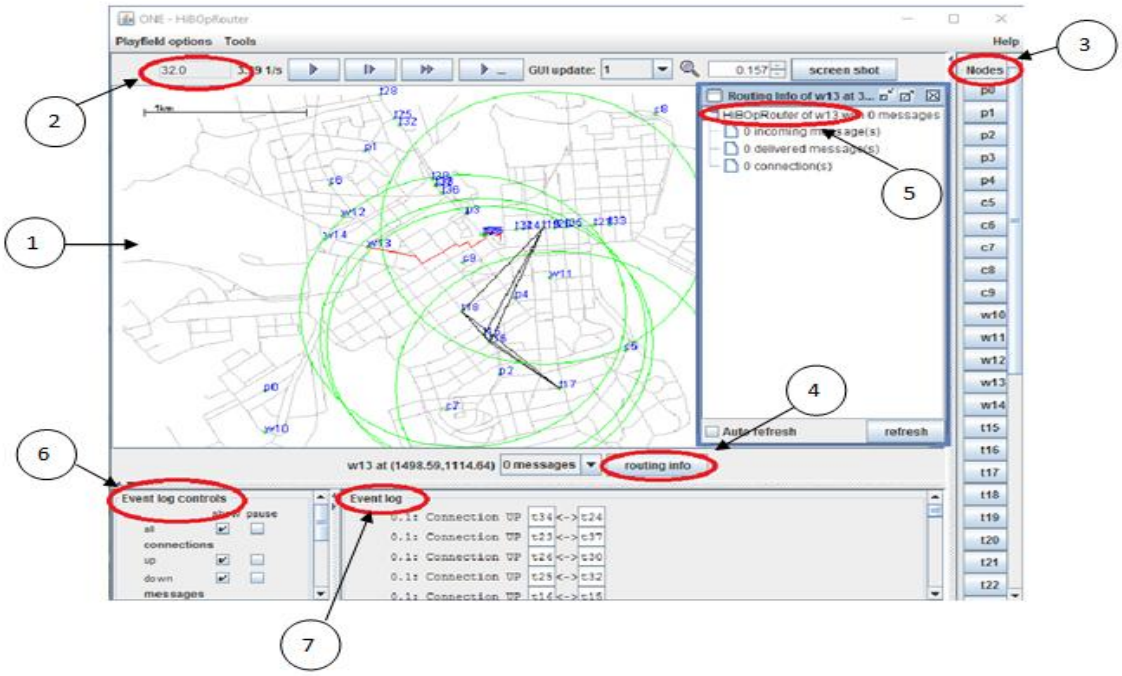

Fig 5.1: ONE Simulator GUI

In the above figure, the important labels are marked from 1 to 7. Label 1 presents the GUI of ONE simulator where Helsinki City map by default sets the simulation scenario where nodes are able to move freely depending up on the movement model defined on them. Label 2 specifies the Simulation time which can be varied from the simulation settings in the ONE Simulator. Label 3 describes the total number of nodes present in the network in ONE simulator. The nodes can be defined under different groups with varying speeds and interfaces. Also the routing information of each and every node can be obtained by clicking on the routing info box marked as label 4 in the Fig 5.1. The information of w13 node is depicted as HiBOp routing protocol by the label 5. Label 6 and 7 represent the event log controls and event logs, respectively routing information, event logs of nodes etc.

Modelling of a mobile endpoint that is adept of acting as a carry forward and store router is done by a node (a pedestrian or a car as an instance along with essential hardware). In ONE data from real world scenarios can be imported along with a set of distinguished reports based on node movement and other required statistics. The dynamic configuration all the report mot modules with routing algorithms and

movement models makes it an easy to use tool for extending the simulator with new and evolving modules.

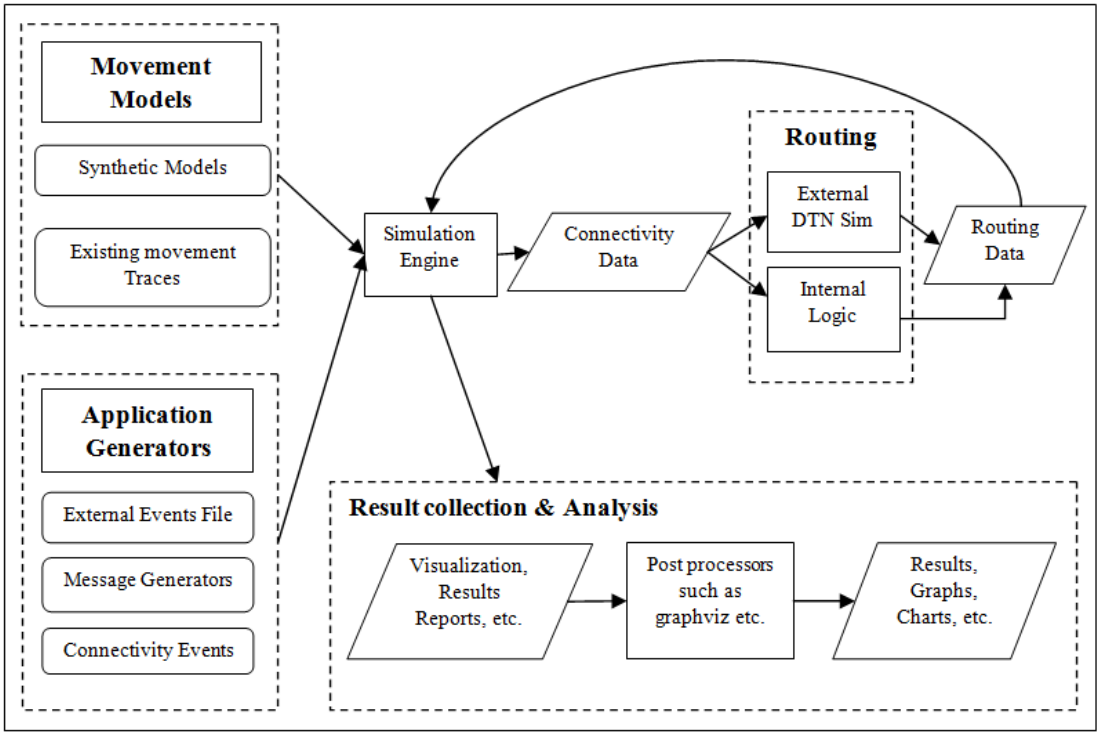

Fig. 5.2: Brief overview of the ONE simulator

- **Mobility Modelling:** Presently, ONE supports map-based movement models that acquire their feedback from well-known text (.wkt) files. WKT files are edited and generated utilising Geographic Information Systems (GIS) like OpenJUMP. The map-based movement models provide a platform for the nodes to move on the real-time road and walkway framework of the map. Further, a number of node groups may be called to use a specific region on the map. As a result, a road is discriminated from the walkway and thus prevents any accidents like car running over a walkway. A casual map-based movement model contains nodes moving on roads specified by the map data but to indiscriminately determined locations. In the shortest map based movement model, nodes use Dijkstra algorithm to move on shortest path rather than moving unsystematically.
    - Another highlight of a map based model is the presence of Points of Interest (POIs) that may be used to model some specific shops or cinema halls etc. and some nodes are equipped with pre-determined map routes. In this case, the destination node is always the next

destination of the route being travelled. Both routes and POIs may be defined with the help of wkt-compatible GIS program.

- **Routing Simulation:** Although a number of inbuilt routing modules are present to serve message for routing, there are also many external simulators like NS2 that can be utilised for this purpose. However, to import from an external source the message needs to be converted into the events comprehensible by ONE by employing a separate program. If ONE is applied to generate connection programmes for an outward router, the subsequent routing decisions can be studied in the GUI corresponding to the node movement. Some of the inbuilt modules are direct delivery, spray and wait (normal and binary), epidemic and PRoPHET. All procedures transfer messages to the last receiver whenever they meet it, but vary in terms of method regarding handling of other messages are handled.
- **Visualisation:** The results in ONE can be visualised either in real-time or using map based movement model. In the former case the whole GUI represents the whole scenario in the real-time and node locations, current paths etc. are depicted in the main window whereas in the latter the map paths along with an image that is depicted as a background. A user enjoys the freedom to select nodes for closer inspection, zoom-in or zoom- out the view, adjust the speed of simulation and so on.

Further for simulation work, the ONE simulator can be integrated with Netbeans IDE as well as Eclipse IDE. In this thesis, it is integrated with Eclipse IDE.

CHAPTER 6

PROPOSED WORK

6.1 Proposed Algorithm

In any network it is difficult to detect the malicious behaviour of any node. The efforts have been applied to mitigate the effects of Sybil attack in opportunistic networks through the proposed algorithm. The use of HiBOp routing protocol [14] is advantageous as it provides the historic information of each and every node. Further it also prevents occurring of higher overhead as in opportunistic networks this protocol needs not to send the multiple copies of the messages. However, it becomes difficult for HiBOp to store the path information of each node within itself, which leads to the introduction of Sybil nodes. The proposed algorithm uses the concept of betweenness centrality and ant colony optimization technique to detect the Sybil nodes.

6.1.1 Shapely Value using Centrality

It is essential to determine the degree of critical nodes and edges in any network in order to provide an efficient network. Centrality can be applied in different scenarios depending upon its nature in many different ways. For instance, identification of the most imperative hubs on the road, most influential people on a social networking site, or quantification of the value of nodes or edges are applied in some noted works [20].
In general, consistent ranking of nodes is built to apply centrality. As an instance, shortest paths are required to measure the betweenness centrality. Like betweenness centrality the other accepted methods utilised for calculating centrality are degree centrality, closeness centrality and page rank centrality. These methods are more commonly referred to as conventional or standard centrality.

- **Betweenness centrality:** It depends upon the shortest path (or the path that requires least number of links). Higher the betweenness centrality i.e. higher the number of shortest path through a node, the more significantly it acts as a link between the different node pairs. It is generally the preferred method to be used through software tools.
- **Degree Centrality:** Degree is assigned to each node on the basis of number of adjacent edges to a node. It helps in determining the single node that is affected by the propagation of any information in the network. Like the

betweenness centrality, the node affected from more number of sources represents the higher degree centrality.

- **Closeness Centrality:** In this the inverse of the shortest distance from a particular node to the other nodes is calculated and then added. The resultant sum of inverse distances is called closeness centrality. Closer the nodes are, more is the closeness centrality.
- **Page Rank Centrality:** It is the count and worth of neighbours linked to the node. Ruling out an appropriate page from the web is the most popular application of page rank centrality. It is determined in three steps. First of all, a random page rank value is supposed for all the web pages and then it is divided equally among all the links going out from every web page. Then the values obtained from the links arriving towards that web page are summed up to give the final page rank value. The process is repeated iteratively until there is an outsized scope in the alteration of page rank values of all web pages between two consequent iterations.

The concept of shapely value was introduced by Shapely in 1953 [20], according to which the division in the concept of theoretic centrality is done in such a manner that certain desirable normative properties are obtained. The four desirable properties are efficiency, null player, symmetry and additivity. These properties are combined to calculate the weighted average of subsidiary contributions of a particular agent to all possible coalitions he belongs to. Shapely values can be considered as one of the centrality measures in order to spread the information.

Following is the pseudocode for shapely values calculation for shortest path.

Algorithm 1: Shapely Value for calculating centrality of nodes

Input: Source Node N_i, Distance Vector D, Path P, $d_{cutoff}>0$
Output: Centrality values of all nodes for all $n \in N_i(P)$

```
for each n ∈ N_i(P)
{
 D= Dijkstra (n,P);
extNeighbours(n) = ∅;
extDegree(n) = 0;
  for each m ∈ N_i(P)  such that m ≠ n
   {
     If(D(m)≤ d_cutoff)
      {
extNeighbours(n).push(m);
extDegree++;
```

```
      }
  }
}
for each n ∈ N_i(P)
  {
SV(n) = 1/(1+extDegree(n));
    for each m ∈ extNeighbours(n)
      {
SV(n)+= 1/(1+extDegree(m));

      }
}
return SV;
```

In order to compute the centrality values of each node in a region, it is important to find the extNeighbours and the extDegree of each node. The extNeighbours or extended neighbours are formed by all the nodes which are one or two hops away. The idea is that the node A will be inclined to other node B only when the distance between node A and node B is not more than the d_{cutoff} (fixed to a constant value). For this algorithm the d_{cutoff} value is set to 2.

6.1.2 Ant Colony Optimization

Ant Colony Optimization algorithm [38] is inspired from the biological methodology of the ants. Ant colony optimization is a type of a swarm intelligence technique. Here, the network nodes are assumed to work like ants. This technique is originally intended to find the optimal paths based on ants' behaviour to search food.

Initially, the ants move randomly. But when an ant is able to find out about the food source, it reverts back to its colony by spreading the pheromones (a sort of a left behind clue) all over the path to depict the presence of the food. The moment other ants encounter this particular path where such pheromones are present, they will probably move on the same path with a certain probability. In case the ants follow the same path, the ants would populate the passage with their own pheromones when they will bring back the food. Due to this more number of ants is able to find the path due to which at diverse food sources near the colony, the couple streams of ants gather which makes it stronger.

Every time the ants bring the food, they drop the pheromones due to which shorter paths are more liable to be strong, hence optimizing the solution. While in the meantime, nearby food sources are still randomly scouted by some ants. The moment

the food is adequately unavailable, the pheromones on the route begin to evaporate and the route decays slowly.

The following table gives the brief overview of ACO techniques defined so far by different authors.

Table 6.1: ACO Variants as defined by [36]

ACO Variant	**Abbreviation**	**Year**	**Author**
Elitist ACO	EAS	1996	Dorigo
Ant Colony System	ACS	1997	Dorigo & Gambardella
Rank Based Ant System	ASrank	1999	Bullenheimer
Max-Min Ant System	MMAS	2000	Stuzzle & Hoos
Hyper Cube Framework	HCF	2004	Blum & Dorigo

Every ACO variant has its own way to optimize the solution. In this thesis, the basic ACO variant is used. Following is the basic algorithm of ACO

Algorithm 2: ACOProblemSolver

```
procedure ACOProblemSolver
  while (not_end)
generateSolutions()
daemonAction()
pheromoneUpdate()          //if the pheromone gets evaporated in case
                           // the optimized value is obtained on some other path
  end while
end procedure
```

The transition values are calculated in order to determine the convergence of the nodes using the given formula [38]

$$p_k(r,s) = \begin{cases} \frac{[\tau(r,s)].[\eta(r,s)]^{\beta}}{\sum_{u \epsilon J_k(r)}[\tau(r,s)].[\eta(r,s)]^{\beta}} & if\ s \epsilon J_k(r) \\ 0 & otherwise \end{cases} \quad (1)$$

Where, $p_k(r,s) = probability\ of\ k\ node\ from\ r\ to\ s\ path$

$J_k(r) = set\ of\ nodes\ that\ can\ be\ connected\ to\ make\ desirable\ paths$

$\eta = \frac{1}{\delta}, i.e.\ the\ inverse\ of\ distance\ \delta(r,s)$

$$\beta < 0 \; is \; relative \; importance \; of \; path \; w.r.t \; distance$$

and, $$\tau(r,s) \leftarrow (1-\alpha).\tau(r,s) + \sum_{k=1}^{m} \Delta\tau_k(r,s) \qquad (2)$$

Where, $\Delta\tau_k(r,s) = \begin{cases} \frac{1}{L_k} & if \; (r,s) \epsilon suited \; path \\ 0 & otherwise \end{cases}$

$$L_k = length \; of \; path \; followed$$

$0<\alpha<1$ is the pheromone (or path) decay parameter; $m = number \; of \; ants$

6.2 MODES OF PROPOSED ALGORITHM

The proposed work runs under the three modes, namely; Ideal, Vulnerable and the Detection mode. The Ideal mode or normal mode is free of any attack and security. The Vulnerable mode is the mode in which the Sybil attack is launched. While the Detection mode is the mode in which concept of centrality and ACO are applied to detect the Sybil nodes and prevent them from causing any malicious activity in the network.

A. Ideal Mode

In Ideal Mode the opportunistic network scenario in ONE simulator is created. The simulator is integrated with the Eclipse IDE to implement proposed algorithm. The simulation time is set to 6500s. The movement model is set to Shortest Path movement model. The HiBOp routing protocol is set for the whole scenario. The number of nodes will vary from 10 to 30. The total number of groups used in this thesis is 3. Finally this mode is evaluated to calculate the parameters such as number of dropped packets, delivery probability, overhead ratio and throughput.

B. Vulnerable Mode

In this mode the Sybil attack is all set to be launched. The HiBOp routing protocol is used in order to store the history of each node but unfortunately it fails to store the path information in its history table. Due to which it became possible to launch Sybil attack in such scenario.

```
if (batchMode) {
    long startTime = System.currentTimeMillis();
    for (int i=nrofRuns[0]; i<nrofRuns[1]; i++) {
        print("Run " + (i+1) + "/" + nrofRuns[1]);
        Settings.setRunIndex(i);
        new Sybil().startSybil();
        resetForNextRun();
        new DTNSimTextUI().start();
    }
    double duration = (System.currentTimeMillis() - startTime)/1000.0;
    print("---\nAll done in " + String.format("%.2f", duration) + "s");
```

Fig 6.1: Sybil Attack Code Snippet

The two fake nodes have been injected into the network. These nodes are made to attract the packets towards themselves by setting the highest centrality value among the other nodes. Centrality values are assigned to each node on the basis of their path information. As the topology is dynamic these values keep changing. So every time in the network any node acquiring highest centrality value will occur. It is also possible that the nodes acquiring highest centrality value at one time can have the lowest one the other time. The Sybil node would fake the identities of the legitimate nodes with highest centrality values and would advertise its own centrality to be more than that of the legitimate one. As a result, the legitimate nodes would send data to fake nodes, thinking them to be the trusted nodes because of their high centrality values. Consequently, there would be an increase in the packet drop rate, overhead ratio and decrease in the throughput. Further these parameters are noted down and compared with those of the ideal mode which gave the clear justification of the attack launched.

C. Detection Mode

In this mode, the attack launched in the vulnerable mode is prevented using the optimization technique. First, the shortest path is obtained between the source and the destination using Dijkstra's algorithm. Then the betweenness centrality values of each node are calculated using the shapely value algorithm based on the number of shortest paths found. The idea is that centrality values will be assigned according to maximum number of shortest paths linked with a particular node. In normal scenario, more the number of paths linked with a particular node, more will be its centrality value which makes a node more trusted one. It is also assumed that the centrality values of each

node in network would always change. But because it is possible that the fake higher centrality values could be advertised by the Sybil nodes, therefore the use of Ant Colony Optimization (ACO) technique is used to detect Sybil nodes. The shortest path and the centrality values of each node are injected as an input to the ACO. ACO will optimize the path with respect to centrality values of each node. ACO will determine the convergence value of nodes using the state transition rule [38]. The values of trusted nodes will converge to some value. The nodes whose values are not converged will be identified as Sybil nodes and ACO will prevent any messages to be sent through them. Thus, their centrality gets updated to 0 and they get removed from the network. Once the Sybil nodes are detected and removed from the network the parameters are again calculated i.e., the number of dropped packets, delivery probability, the overhead ratio and the throughput and compared with the parameters of ideal and vulnerable mode.

The following vectors have been used to model the proposed scheme

- *Vector P* = <P_1, P_2, P_3…….P_k>, where P_k are the number of shortest paths found using Dijkstra
- *Vector N* = <N_1,N_2,N_3…….N_k>, where k is number of nodes detected in a region
- *Vector C* = <(N_1,C_1), (N_2,C_2), (N_3,C_3)...(N_k,C_k)>, where C_k is the centrality value of nodes N_k.
- S_n to be the Source Node and D to be the Destination Node

Algorithm 3: Proposed Algorithm (P,C,N,D)
Input: Vector P, Vector C , Vector N **Output:** Number of dropped packets, overhead ratio and throughput

if(N_i==D) // *N_i is the node receiving the message in the network*
{ *//D is the Destination node*
Deliver the message
}
else
{
Apply *Dijkstra*;
for each node in a network
{

```
                C= ComputeCentrality (P,N);
                 ACO(C);
               }
          }
    if(values converged)
    {
        Accept as Trusted nodes;
    }
    else
     {
       Update Ci=0;
       Reject as Sybil nodes;
     }
}

ComputeCentrality(Input: P)
    {
         Compute centrality value of each node present in the path P, using shapely value
         Algorithm
         Generate the vector C
         Return C
   }
ACO( Input: C)
    {
          Fetch all the values from Vector C
          Converge the Values of Vector C using equation (1)
          Return Converged Values
  }
```

In the Fig 6.2 mentioned below, the brief overview of the proposed work is explained.

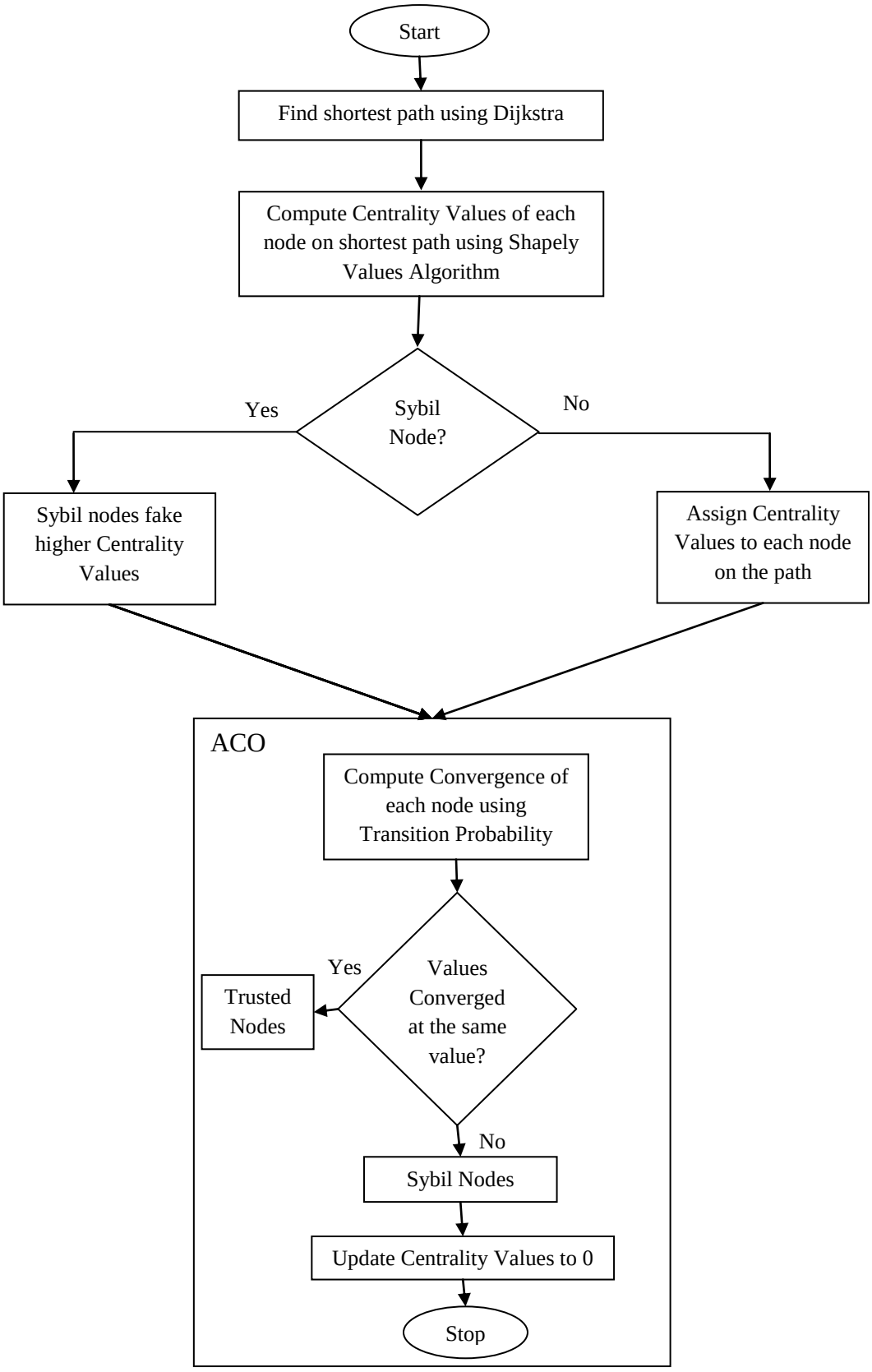

Fig 6.2: Overview of Proposed Work

Following is the table giving the brief comparison of different techniques with the proposed algorithm.

Table 6.2: Comparison of different techniques with the Proposed Algorithm

Properties / **Schemes**	**Centrality**	**Trust**	**Sybil Attack**	**ACO**	**Shapely Values**
MobID [15]	✓	✓	✓		
Sybil ACO [17]			✓	✓	
Trust Centrality [18]	✓	✓			
Sybil Detection [19]	✓		✓		
Game Theory [20]	✓				✓
SNSD & SGA [25]	✓	✓	✓		
Sybil Trust [33]		✓	✓		
CGrAnt [35]	✓			✓	
Proposed Algorithm	✓	✓	✓	✓	✓

CHAPTER 7

SIMULATION & ANALYSIS

7.1 Simulation Scenario

In this section, the proposed scheme is evaluated using the ONE simulator. A dynamic set of mobile nodes is considered in order to establish the opportunistic network environment. The nodes are free to leave and join the network any time. In this simulation scenario of opportunistic network 3 groups of nodes have been considered which consist of pedestrians, cars and trams, each with different speeds. Each group has been assigned the shortest path based movement model. The numbers of nodes are varied in the whole scenario in order to calculate the required parameters such as delivery probability, number of dropped packets, overhead ratio and the throughput. A detailed simulation scenario is depicted in Table 7.1:

Table 7.1: Simulation Environment Setup

Simulation Parameters	**Description**	**Simulation Values**
Simulation Area		$4500 \times 3400\ m^2$
Simulation Time		6500s
Number of Group Nodes	Pedestrians	3
	Cars	
	Trams	
Speed	Pedestrians	0.5- 1.5 m/s
	Cars	2.7-13.9 m/s
	Trams	7-10 m/s
Movement Model	Shortest Path Movement Model	
Transmission Speed/Range	Bluetooth	2 Mbps/10 m
	High-Speed	10 Mbps/1000 m
Packet Size		500kB – 1MB
Initial TTL		300 min
Message Generation Interval		25s-35s
Buffer Size		5M

The opportunistic networks do not have large-scale deployments yet. But the trace-driven simulation is the foremost approach to evaluate routing performance in opportunistic networks. For example, time –ordered encounter lists among the nodes such as mobile phones etc, are the traces used in such simulations. The traces may be generated artificially by an analytic model of human mobility or may be based on empirically measured real-world human movements. Such encounters lists help in simulating the routing protocols and then directly comparing them on the basis of number of performance metrics. Metrics commonly used for evaluating the performance of opportunistic network routing protocols include:

- **Number of Packets Dropped:** This represents number of packets dropped from each node's buffer. It is assumed that some packets may never be delivered even if the Sybil nodes are not involved in forwarding of packets. It is also assumed that the transmission range and the buffer size of a node are limited.
- **Delivery Probability:** This metric is the measure to calculate the number of messages successfully delivered out of the total number of unique messages created. Mathematically it is defined as the ratio of number of messages delivered by the number of messages created.
- **Overhead Ratio:** It can be defined as average number of relays used to deliver one message. Numerically, it can be defined as the ratio of number of packets relayed to the total number of packets delivered [3]. In opportunistic Networks for each message to be a delivered, a message replica is created. In short, the number of replicas created per delivered message.
- **Throughput:** Within a given time period when some amount of data is moved from one place to other during data transmission in a network. It is measured in bits per second or megabits per second or gigabits per second.

7.2 Result Inferences

First the number of nodes is varied in the network and then the impact of this variation is measured on the number of packets dropped from the node's buffer. The results are depicted in Fig 7.1. From Fig 7.1 it is inferred that the packet drop is increasing as the number of nodes are increased. Moreover, the difference of the packet drop among different modes can also be clearly depicted from the figure. The proposed algorithm is able to bring the rate of packet drop down to the optimal

solution. It is noticed that the total increase in the number of packets dropped against the 10 number of nodes increases from 142 to 428 which is approx. 3 times in the vulnerable mode while it decreases from 428 to 288 again in the detection mode.

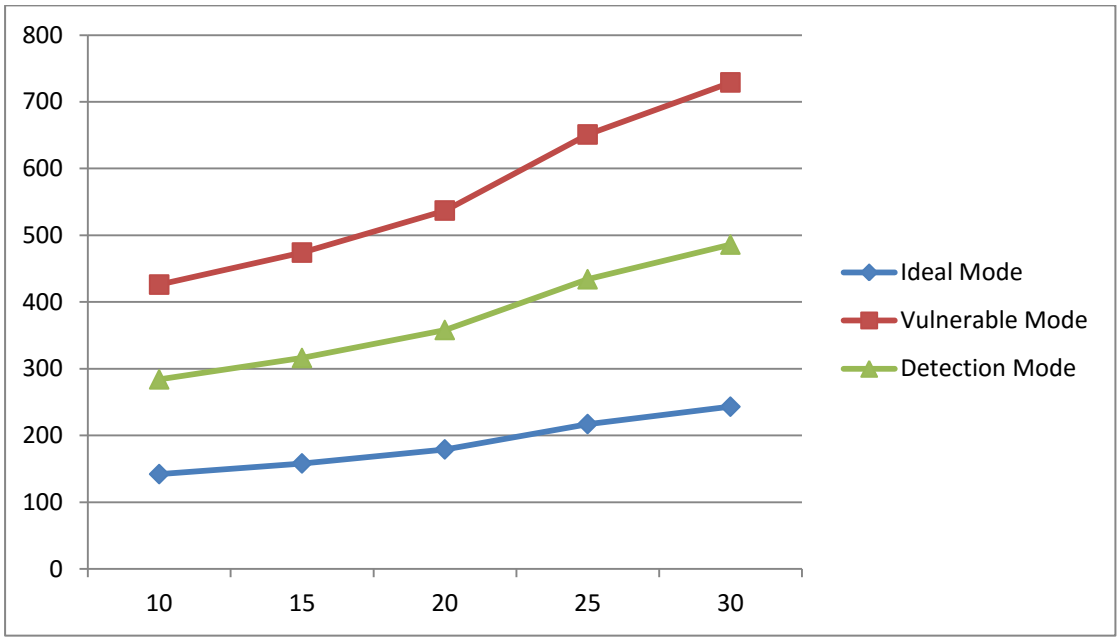

Fig 7.1: Number of Dropped Packets vs Number of nodes

In Fig 7.2, it can be observed that when number of nodes is increased, the delivery probability significantly increases. It is because with the increased number of nodes the message is delivered to each node based on its history as HiBOp routing protocol has been used. Moreover the number of Sybil nodes injected in the network is also two. So when the numbers of nodes are more the delivery probability of each packet is increased. It is inferred that difference in delivery probability of the ideal and the vulnerable mode on an average is equal to 0.0717. While that of the vulnerable and the detection mode is 0.0357. But the difference in the delivery probability of ideal and detection mode on an average is 0.0360.

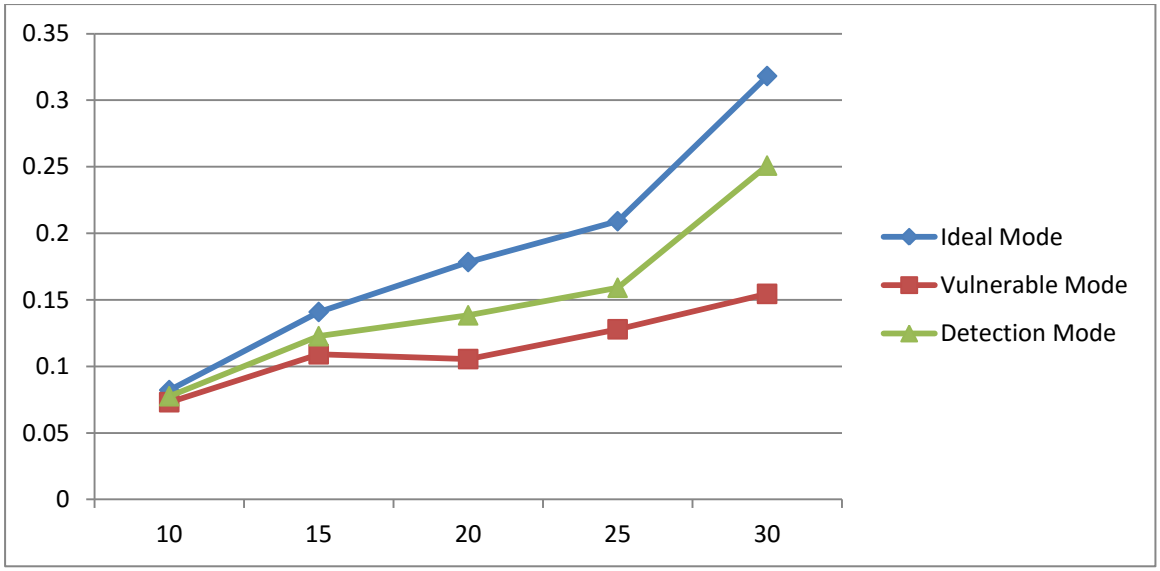

Fig 7.2 Delivery Probability vs Number of nodes

Fig 7.3 reveals the comparison of overhead ratio among the different number of nodes in different modes. The graph gives us the rough idea of increase in the rate of overhead ratio with increase in the number of users in an opportunistic network. From the Fig 7.3, the increase and decrease of overhead ratio among the three modes is depicted. It is noticed that the ideal mode giving the overhead ratio 7.76 at 20 nodes suddenly jumps to 20.3 in vulnerable mode. But it drops to 12.5 when the detection mode is applied. It is noticed that the proposed algorithm is able to considerably reduce rate of overhead ratio but could not have reached the ideal limits.

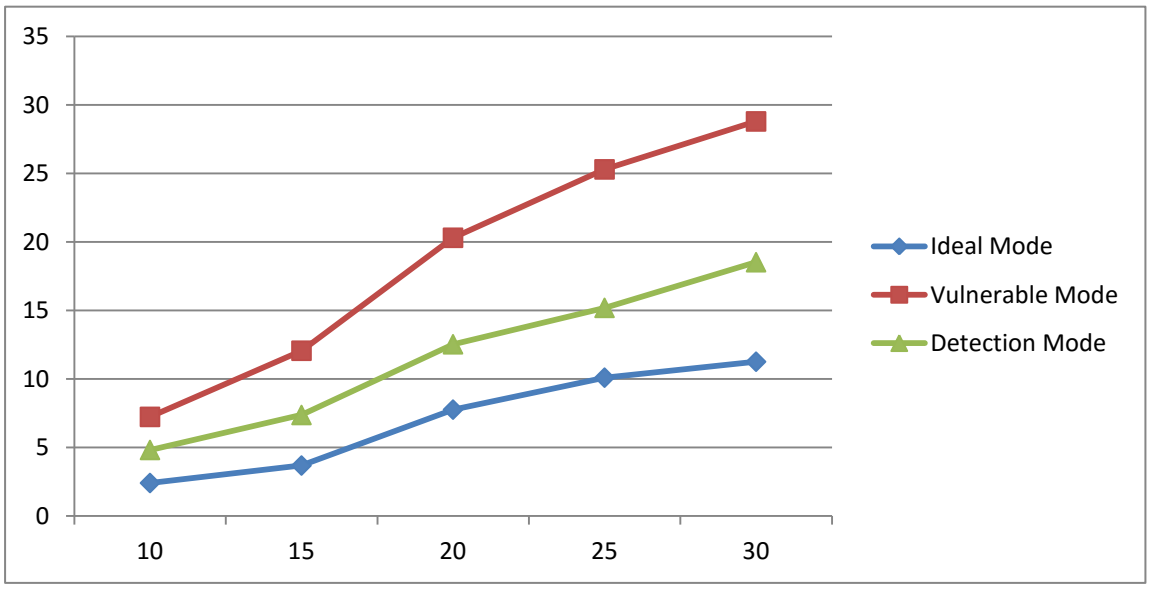

Fig 7.3: Overhead Ratio vs Number of nodes

In Fig 7.4, the throughput of each node is depicted in all the three modes. Here for each packet drop, the throughput decreased when the number of nodes was increased. Increasing number of nodes would increase packet drop that would lead to decrease in the throughput of the network. In the Fig 7.4, a brief comparison of the throughput under the three modes of the proposed algorithm is presented. It is noticed that the ideal mode giving the throughput 6593.7 kbps at 30 nodes suddenly reduced to 3046.8 kbps in vulnerable mode. While the throughput again takes a hike of 5095.8 kbps in the detection mode. Similar is the case with number of other nodes. But the trend is such that with increase in number of nodes the packet drop is increasing due to which throughput is decreasing.

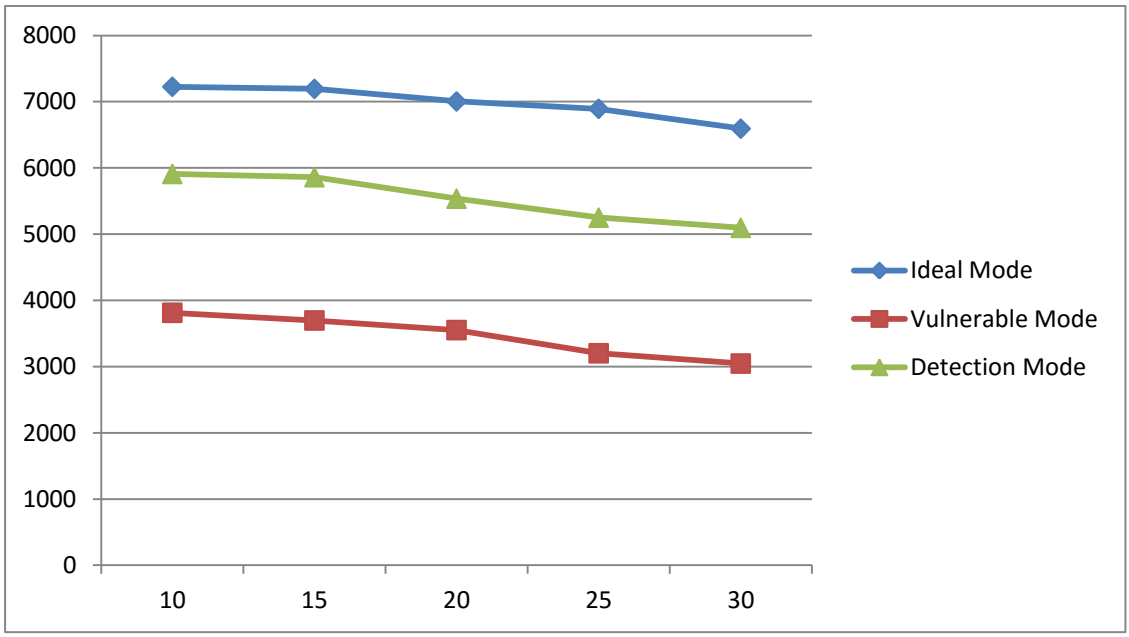

Fig 7.4: Throughput vs Number of nodes

CHAPTER 8

CONCLUSION & FUTURE SCOPE

8.1 Conclusion

The opportunistic networks being the most dynamic network by nature tend to possess many security threats. Sybil attack is the one of the most harmful attack in the networks. In recent literature, the concept of centrality and ACO has been used for routing in OppNets. This thesis has featured the research performed in this area by designing, implementing and experimenting with a novel method i.e, the combination of Centrality and ACO in order to determine an optimal and secure route against the Sybil attack. This work has focused over the main parameters that are reflected in almost every research work such as dropping of packets, delivery probability, overhead ratio and the throughput of a network. Applying centrality efficiently detects Sybil nodes in a network. With the help of ACO, the Sybil nodes are effectively identified and eliminated from OppNet and the optimal path is obtained. Although HiBOp routing protocol has been initially applied as it acts as a reliable tool to prevent the high overhead in the network of 30 nodes yet overhead ratio further gets improved from 20.33 to 12.53, as a consequence to the proposed algorithm. The number of dropped packets considerably gets reduced on an average from 537 to 358 after applying the proposed algorithm. Delivery probability is found to have enhanced value from 0.1055 to 0.1384 after taking the prevention measures. Finally, the throughput of an ACO secured network 5536.26 kbps is significantly higher than that of the vulnerable network which is 3552.19 kbps. This work in the long run provides a valuable framework for further exploration of utilising opportunistic networks in ever growing field of wireless communication.

8.2 Future Scope

The research presented in this thesis could always be used in future to make improvements or new discoveries. Combination of Centrality and ACO is a novel method to defend against the Sybil attack. In future, the scalability of the networks can be addressed in order to significantly perk up the efficiency of this method. The schemes used in this work can be used to counter the effects of any other kind of attack such as. Computing the delay in message transmission can add up to recognise

the efficacy of the technique. Also, other parameters can be worked upon in order to apprehend the effectiveness of the proposed algorithm to prevent other attacks such as blackhole attack, sinkhole attack etc in opportunistic networks. Also, a blend of the mentioned schemes with other variants of ACO or any other optimization schemes such as Particle Swarm Optimization (PSO), can be applied as a hybridised method to obtain the higher levels of reliability among the nodes and security in the network.

REFERENCES

[1] A. Heinemann, "Opportunistic Networks," in *Handbook of Research in Ubiquitous Computing Technology For Real Time Enerprises*. New York, USA: IGI Global, chapter 9, pp. 190-191, 2008.

[2] I. Parris, G. Bigwood and T. Henderson, "Privacy-enhanced social network routing in opportunistic networks," in *Pervasive Computing and Communications Workshops (PERCOM Workshops), 2010 8th IEEE International Conference* , Mannheim, pp. 624-629, 2010.

[3] D.Pan et al., "A comprehensive-integrated buffer management strategy for opportunistic networks," *EURASIP Journal on Wireless Communication and Networking*, vol. 2013, no. 1, pp. 1-10, 2013.

[4] J. Cho, A.Swami and I. Chen, "A Survey on Trust Management for Mobile Ad Hoc Networks," *IEEE Communications Survey & Tutorials*, vol. 13, no. 4, pp. 562-583, 2010.

[5] E. Jones et al., "Practical Routing in Delay-Tolerant Networks," *IEEE Transaction in Mobile Computing*, vol. 6, no. 8, pp. 943-959, 2007.

[6] K. Sharma and M. Ghose, "Wireless Sensor Networks: An Overview on its Security Threats," *International Journal of Computer and Applications- Mobile ad-hoc networks*, pp. 42-47, 2010.

[7] G. Kulkarni et al., "Wireless sensor network security threats ," in *5th International Conference on Advances in Recent Technologies in Communication and Computing(ARTCom 2013)*, Bangalore, pp. 131-135, 2013.

[8] J. Douceur, "The Sybil Attack," in *Peer to Peer Systems*. Cambridge, USA: Springer Berlin Heidelberg, vol. 2429, pp. 251-260, 2002.

[9] A. Vahdat and D. Becker, "Epidemic routing for partially-connected ad hoc networks," Duke University, Durham, Technical Report CS-2000-06 2000.

[10] J. Budit, D. Norman and A. Hamid, "PRoPHET Routing Protocol Based on Neighbor Node Distance Using a Community Mobility Model in Delay Tolerant Networks," in *High Performance Computing and Communications & 2013 IEEE International Conference on Embedded & Ubiquitous Computing (HPCC_EUC)*,

Chicago, pp. 356-374, 2013.

[11] A. Lindgren, A. Doria, and O. Schelen, "Probabilistic routing in intermittently connected networks," in *Workshop on Service Assurance with Partial and Intermittent Resources (SAPIR)*, USA, pp. 239-254, 2004.

[12] N. Derakhshanfard, M. Sabei and M. Rahmani, "Sharing spray and wait routing algorithm in opportunistic networks," *Wireless Networks*, pp. 1-12, 2015.

[13] M. Saadat and M. Mohuiddin, "An improved MaxProp based on neighborhood contact history for Delay Tolerant Networks," in *2013 16th conference on Computer and Information Technology(ICCIT)*, Khulna, pp. 287-291, 2014.

[14] C. Boldrini, M. Conti, J. Jacopini and A. Passarella, "HiBOp: A History Based Routing Protocol for Opportunistic Networks," in *2007 IEEE International Symposium on a Word of Wireless, Mobile and Multimedia Networks*, Finland, pp. 1-12, 2007.

[15] D. Quercia and S. Hailes, "Sybil Attacks Against Mobile Users: Friends and Foes to the Rescue," in *Proc. INFOCOM'10*, San Diego, pp. 1-5, 2010.

[16] K. Xu, V. Li and J. Chung, "Exploring Centrality for Message Forwarding inOpportunistic Networks," in *Wireless Communications and Networking(WCNC), 2010 IEEE Conference*, Sydney, pp. 1-6, 2010.

[17] B. Zeng and B. Chen, "SybilACO: Ant Colony Optimization in defending Sybil Attacks in Wireless Sensor Networks," in *2010 International Conference on Computer and Communication Technologies in Agriculture Engineering*, Chengdu, pp. 357-360, 2010.

[18] G. Barbian, "Trust Centrality in Online Social Networks," in *2011 European Intelligence and Security Informatics Conference(EISIC)*, Athens, pp. 327-377, 2011.

[19] F. Ahmad and M. Abulaish, "Identification of Sybil Communities Generating Context-AwareSpam on Online Social Networks," in *Proceedings of the 15th Asia-Pacific Web Conference (APWeb'13)*, Sydney, pp. 268-279, 2013.

[20] T. Michalak et al.,"Efficient Computation of the Shapley Value for Game-Theoretic Network Centrality," *Journal of Artificial Intelligence Research* , vol. 46, pp. 607-650, 2013.

[21] W. Zang et al., "Detecting Sybil Nodes in Anonymous Communication Systems," *Procedia Computer Science*, vol. 17, pp. 861-869, 2013.

[22] B. Yu, C. Xu and B. Xiao, "Detecting Sybil attacks in VANETs," *Journal of Parallel and Distributed Computing*, vol. 73, no. 6, pp. 746-756, 2013.

[23] S. Abbas et al., "Lightweight Sybil Attack Detection in MANETs," *IEEE Systems Journal*, vol. 7, no. 2, pp. 236-248, 2013.

[24] B. Tian et al., "A novel sybil attack detection scheme for wireless sensor network," in *Broadband Network and Multimedia Technology(IC-BNMT), 2013 5th IEEE conference*, pp. 294-297, Guilin, 2013.

[25] W.Chang, J. Wu, C. Tan and F. Li, "Sybil defences in mobile social networks," in *Global Communication Conference (GLOBECOM), 2013 IEEE*, Atlanta, pp. 641-643, 2013.

[26] I.Parris and T.Henderson, "Friend or Flood? Social Prevention of Flooding attack in Mobile Opportunistic Networks," in *34th IEEE International Conference on Distributed Computing Systems Workshops (ICDCSW), 2014 IEEE*, Madrid, pp. 16-21, 2014.

[27] X.Cao and Y.Yin, "An Identity Authentication Scheme for Opportunistic Network based on Multidimensional Scaling," in *Cyber-Enabled Distributed Computing and Knowledge Discovery(CyberC), 2014 International Conference*, Shanghai, pp. 87-93, 2014.

[28] G. Noh et al., "Robust Sybil attack defense with information level in onlineRecommender Systems," *Expert Systems with Applications*, vol. 41, no. 4, pp. 1781-1791, 2014.

[29] Z. Trifa and M. Khemakhem, "Sybil Nodes as a Mitigation Strategy against Sybil Attack," *Procedia Computer Science*, vol. 34, pp. 1135-1140, 2014.

[30] Y. Lin et al., "Secure Routing based on Social Similarity in Opportunistic Networks," *IEEE Communication Society*, vol. 15, no. 1, pp. 595-605, 2015.

[31] R.Ciobanu et al., "SPRINT-SELF: Social-based routing and selfish node detection in Opportunistic Networks," *Mobile Information Systems*, vol. 2015, pp. 1-12, 2015.

[32] S. Liang, M. Jianfeng and M. Zhuo C.Xi, "A Trust Management Scheme based

on Behavior Feedback for Opportunistic Networks," *Communications*, vol. 12, no. 4, pp. 117-129, 2015.

[33] G. Wang et al., "Neighbor Similarity Trust against Sybil Attack in P2P E-Commerce," *IEEE Transaction on Parallel Distributed Systems*, vol. 26, no. 3, pp. 824-833, 2015.

[34] S. Trifunovic and A. Picu, "Stalk and lie—The cost of Sybil attacks in opportunistic networks," *Computer Communications*, vol. 73, pp. 66-79, 2016.

[35] A. Vendramin et al., "A social-aware routing protocol for opportunistic networks," *Expert Systems With Applications*, vol. 54, pp. 351-363, 2016.

[36] C. Blum, "Ant colony optimization: Introduction and recent trends," *Physics of Life Reviews*, vol. 2, no. 4, pp. 354-371, 2005.

[37] A. Keranen, J. Ott, T. Karkkainen, "The ONE Simulator for DTN Protocol Evaluation," in *SimuTools'09, Proceedings of 2nd International Conference on Simulation Tools And Techniques*, Belgium, 2009.

[38] M. Dorigo, "Ant Colony System: A Cooperative Learning Approach to the Traveling Salesman Problem," *IEEE Trnsaction on Evolutionary Computation*, vol. 1, no. 1, pp. 53-66, 1997.

LIST OF PUBLICATIONS

[1] G. Kaur and T. Bhatia, "Trust Based Security in Opportunistic Networks: A Survey," in *2nd IEEE International Conference on Computer & Technology (ICETECH)*, Coimbatore, pp. 634-638, 17th& 18th March 2016.

[2] G. Kaur and T. Bhatia, "Detection of Sybil Attack using Centrality & ACO in Opportunistic Networks", (Communicated).

Link for the Video

[1] https://www.youtube.com/channel/UCAicZDB86Gdz2KFuphIYJjA

thesis

ORIGINALITY REPORT

9%	4%	7%	0%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Routing in Opportunistic Networks, 2013. Publication	1%
2	etd.lsu.edu Internet Source	<1%
3	Dhurandher, Sanjay K., Deepak Kumar Sharma, Isaac Woungang, and Aakanksha Saini. "Efficient routing based on past information to predict the future location for message passing in infrastructure-less	<1%