Secure Information Dissemination in Heterogeneous Wireless Sensor Networks

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

of

DOCTOR OF PHILOSOPHY

by

Kamal Kumar
(90703509)

Under the guidance of
Dr. A. K. Verma
Associate Professor, CSED
Thapar University, Patiala

and

Dr. R. B. Patel
Associate Professor, CSE
G. B. Pant Engineering College, Pauri

Computer Science & Engineering Department

Thapar University, Patiala – 147004 (India)

July 2014

Secure Information Dissemination in Heterogeneous Wireless Sensor Networks

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

of

DOCTOR OF PHILOSOPHY

by

Kamal Kumar
(90703509)

Under the guidance of
Dr. A. K. Verma
Associate Professor, CSED
Thapar University, Patiala

and

Dr. R. B. Patel
Associate Professor, CSE
G. B. Pant Engineering College, Pauri

Computer Science & Engineering Department

Thapar University, Patiala – 147004 (India)

July 2014

Candidate's Declaration

I hereby certify that the work which is being presented in the thesis entitled **"Secure Information Dissemination in Heterogeneous Wireless Sensor Networks"** in partial fulfilment of the requirements for the award of the Degree of Doctor of Philosophy and submitted in the department of Computer Science and Engineering of Thapar University, Patiala is an authentic record of my own work carried out during a period of September 2008 to June 2014 under the supervision of Dr. Anil Kumar Verma, Thapar University, Patiala and Dr. R.B. Patel, G.B. Pant Engineering College, Pauri, Garhwal.

The matter presented in this thesis has not been submitted by me for the award of any other degree of this or any other institute/university.

(Kamal Kumar)
Reg. No. 90703509

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

(Dr. R.B. Patel)
Associate Professor,
Computer Science & Engineering
G. B. Pant Engineering College,
Pauri, Garhwal

(Dr. Anil Kumar Verma)
Associate Professor,
Computer Science & Engineering
Thapar University,
Patiala

ABSTRACT

With wide spread of sensor technology in every sphere of life and ever increasing digitization one can imagine that soon world will be patched with small sized devices all around. These devices are capable of monitoring and surveillance including an access to vast digital world of information. Seamless transmission using wireless medium, based on anywhere, anytime, anyhow paradigm is a boon for searching data and information as well as processing queries. Deployments of such sensor nodes are not easy, it may range from underwater to mountain, from large dessert to dense forests it is difficult to setup infrastructure for communication. With miniaturization of wireless devices which can receive, send and process information and commands, sensor networks came into existence, inheriting most of features, applications and limitations from ad hoc networks, the sensor networks exhibit their own area of applications. Primarily useful for surveillance and monitoring activities sensor networks face security challenges in the form of open wireless channel, physical compromise and reprogramming. Due to small sizes and open deployment, compromise attacks are most destructive kind of attacks in Wireless Sensor Networks (WSNs). With applications of WSNs growing from physical surveillance to applications in medical sciences and health monitoring, it is important to investigate specialized security solutions for WSNs. In this thesis we tried to address security challenge by devising key management and secure routing scheme.

In this thesis we are using deployment driven localization of security information for the development of scalable key management schemes which are resilient to node compromise and node replication attacks. Using security aware selection of next hop towards destination we designed secure routing schemes. We suggested use of mobile sensors for secure data collection in large sensor networks and addressed authentication and re-authentication of mobile sensors. To meet the requirement of multiple and equally secure paths in a query oriented WSNs, we developed a secure multipath routing scheme. The parameter considered for routing protocols is inclusive resilience, which is improved by increasing link keys on each hop in route. We consider Heterogeneous Wireless Sensor Networks (HWSNs) in which few sensors equipped for high end processing. Computation intensive and organizational activities of HWSNs are

categorically assigned to high end sensors. The developed schemes/protocols are validated through simulation and analytical modeling.

Keywords: Heterogeneous, Multipath, Resilience, Localization, Compromise Attacks.

To my beloved wife Mamta, who always stood by me,

To my kids, Manthan and Shivay who always inspires me,

ACKNOWLEDGEMENT

A few sublime human experiences defy expression of any kind, and a feeling of true gratitude is one of them. I, therefore, find words quite inadequate to express my indebtness to my supervisors Dr. Anil Kumar Verma, Associate Professor, Thapar University, Patiala and Dr. R. B. Patel, Associate Professor, G. B. Pant Engineering College, Pauri, Garhwal, for their virtuous guidance, encouragement and help throughout this work. Their deep insight into problem and the ability to provide solution has been immense value in improving the quality of research at all stages. This experience of working with them shall ever remain a source of inspiration and encouragement for me. I learned a great deal from them, not only about research but also matters touching many other aspects that will benefit me in my future endeavours.

My sincere thanks are due to Sh. Tarsem Garg, Chancellor, M. M. University and Dr. P. Gopalan, Director, Thapar University, for providing me necessary administrative assistance in completion of the work.

I express my heartfelt thank to Dr. Deepak Garg, Head, Computer Science & Engineering Department, for his guidance and supportive attitude. I am thankful to my Doctoral Committee members Dr. Maninder Singh, Dr. S. S. Bhatia, for their constructive comments and ensuring the progress of my research work in right direction. I extend my thanks to Dr. (Mrs.) Seema Bawa and Dr. Neeraj Kumar for their generous support and invaluable suggestions throughout the research work. I thank all faculty members of Department of Computer Science and Engineering, Thapar University for their kind hearted support.

I am extremely grateful to the celebrated authors whose previous works have been consulted and referred in my research work.

Special thanks are due to my parents whose love and affectionate blessings have been a constant source of inspiration in making this manuscript a reality.

I express my deep sense of appreciation to my wife Mamta and children Manthan and Shivay for their cooperation and patience during the completion of my research work.

All the thanks are, however, only fraction of what is due to Almighty for granting me an opportunity and the divine grace to successfully accomplish this assignment.

KAMAL KUMAR

Table of Contents

Abbreviations and Acronyms

AN	Anchor Node
AODV	Ad hoc On-Demand Distance Vector
APTEEN	Adaptive Periodic Threshold-sensitive Energy Efficient sensor Network
BS	Base Station
BVGF	Bounded Voronoi Greedy Forwarding
CARPY	ContrAined Random Perturbation based pair-wise keY
CBAH	Clustering-Based Aggregation Heuristic
CC	Care-of Cluster
COMM	Common Broadcast Vector
CTR	Counter
DC	Data Centric
DD	Directed Diffusion
DES-CBC	Digital Encryption Standard-Cyber Block Chaining
DH	Diffie-Hellman
DSR	Dynamic Source Routing
ECDH	Elliptical Curve Diffie-Hellmen
EG	Eschenauer and Gligor
EKA	Expected Key Average
GEAR	Geographic and Energy-Aware Routing
GeRaF	Geographic Random Forwarding
GK	Generating Key
HC	Home Cluster
HEED	Hybrid, Energy-Efficient Distributed Clustering
HF	Hashing Function
H-Sensor	High end Sensor
HWSN	Heterogeneous Wireless Sensor Networks
KC	Key Chain
KDC	Key Distribution Centre
LEACH	Low Energy Adaptive Clustering Hierarchy
LGK	Localized Generating Key
LKH	Logical Key Hierarchy
LKHW	Logical Key Hierarchy for WSNs
L-Sensor	Low end Sensor
MAC	MAC
MAKM	Modular Arithmetic based Key Management scheme
MECN	Minimum Energy Communication Network
MN	Mobile Node
NR	Neighbour List

PDF	Probability Density Functions
PEGASIS	Power-Efficient Gathering in Sensor Information Systems
PKC	Public Key Cryptography
PKI	Public Key Infrastructure
RAM	Random Access Memory
RR	Rumor Routing
RSSI	Received Signal Strength Indicator
SAR	Sequential Assignment Routing
SGNF	Stateless Geographic Non-Deterministic forwarding
SINK	Sink in WSN
SMECN	Small Minimum Energy Communication Network
SN	Sensor Node
SNEP	Secure Network Encryption Protocol
SPIN	Sensor Protocols for Information via Negotiation
TBF	Trajectory-Based Forwarding
TEEN	Threshold-sensitive Energy Efficient sensor Network
TESLA	Timed, Efficient, Streaming, Loss-Tolerant, Authentication
WSN	Wireless Sensor Network

List of Tables

List of Figures

Chapter 1

Introduction

A Wireless Sensor Network (WSN) [1] in its most generic form is a group of specialized small sized devices with communication resources intended monitoring, surveillance and tracking and recording in diverse and inaccessible locations. A WSN maintains large number of sensing station, called Sensor Nodes (SNs). SNs are resource scarce devices and must communicate sensed data from the sensing fields to a safely located remote Base Station (BS), by using multi-hop routes through wireless links and intermediated SNs. Possibly BS can process it locally, or may be connected to remote processing capability, in other networks. Sensors may be stationary or mobile. SNs may be equipped with devices for location identification or may not. WSNs may form homogeneous WSNs or heterogeneous WSNs. Rarely SNs are assigned individual global sensor identifiers [1]. WSNs are data centric networks. Any form of communication in WSNs requires that interests should be targeted to a well defined group of nodes or defined attributes of data. The inclusion of few High-end Sensors (H-Sensors) in WSNs allows leveraging heterogeneity for assignment of complex computation to H-Sensors. This class of WSNs is known as Heterogeneous Wireless Sensor Networks (HWSNs) {Figure 1.1}.

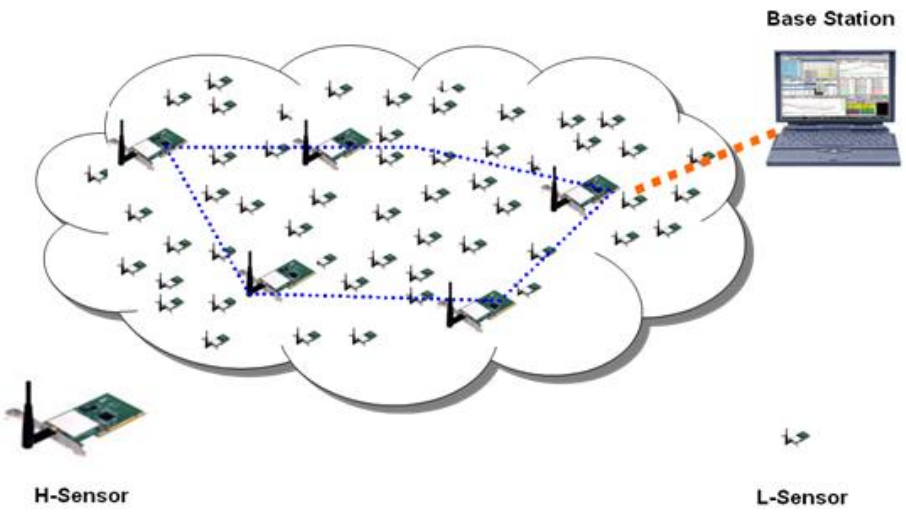


Figure 1.1 Generic View of HWSN [2]

HWSN are designed for specific applications in which computation or communication intensive activities may be transferred or subjected to H-Sensors. H-Sensors are resource rich, capable

sensor nodes. Extra capability may be available in the form of large storage space to support multiple applications, high energy banks for longer life, large transmission range for long distance one-hop communications. H-Sensors might be equipped with higher processing power for meeting timing constraints in time critical applications. In some cases H-Sensors are equipped with GPS (Global Positioning System) and augment applications with deployment or location related information. Mobility of H-Sensor is another paradigm which is being explored in mobile data collection activities and helps in preventing sensors from sending data to long distances. To overcome replications in sensed data from collocated sensors, data must be aggregated for maintaining optimal or no redundancy. Such activities may also be assigned to H-Sensors.

1.1 Wireless Sensor Networks: An Overview

WSNs are deployed to perform a specific task. Environment sensing and data collection remains primary application areas for sensor networks. In typical WSNs, node platforms are error-prone due to harsh, unattended and hostile operating conditions. Communication links between nodes are not stable and durable due to node errors, unreliable modulations, node mobility and external interferences. Due to random deployment of WSNs in unattended and hostile surroundings, sensor networks are prone to attacks. Due to limited resources in WSNs many wire-line solutions remains useless in WSNs. Due to absence of any central authority, sensors must be able to organize themselves into connected network. These limitations greatly affect the system, applications and security designs [2] [3].

1.1.1 Characteristics of WSN

WSNs may differ from ad hoc networks in many dimensions. For example, SNs are resource constrained devices with no global identification. SNs are prone to failures due to energy constraints, malicious attacks, and dynamic topology. SNs are densely deployed and large in numbers when compared to an ad hoc network. Here we give a brief of WSN characteristic:

- Resource Limitations: Sensors are small devices designed for data collections in local surroundings only. Small size limits resource supports in terms of transmission range, storage and processing capability.
- Scale of Network: Compared to other wireless networks, the number of nodes in any WSN may be huge and density of nodes can be high.
- Self Organization: Due to absence of central authority and limited bandwidth, it is required that sensors must be able to organize themselves into a connected network with limited communication overhead and perform routing of application related data.
- Dynamic Topology: Sensors use their battery for sensing, configuring and data reporting. Due to limited battery resources, battery of sensors may fail after deployment. This causes a change in topology and is a frequent activity in WSNs.
- Multi-hop Communication: Due to limited bandwidth in WSNs and remote localization of BS, data must be relayed through neighbours. Sensors network's communication thus resort to multi-hop communication.

1.1.2 Applications

WSNs find their use in wide range of applications. Two most applicable areas where WSNs plays key roles are monitoring and tracking. Well known applications of WSNs in monitoring and tracking are listed below {Figure 1.2}.

Military applications: This includes border area monitoring, force movements, battle damage assessment, intrusion detection, chemical, biological or nuclear attack detection, enemy tracking, infiltration tracking, military vehicle tracking, leakage tracking in gas and petroleum pipelines and mines tracking.

Habitat/environment applications: It includes monitoring in given surroundings like, pollution monitoring, water quality monitoring, landslide detection, flood detection, acoustic detection, precision agriculture, wild fire detection, volcanic monitoring and animal's migration.

Business/industrial application: Includes inventory monitoring for decision makings, structural monitoring, factory monitoring, machine health monitoring, fatigue monitoring, chemical monitoring and human tracking in buildings.

Health applications: This includes patient monitoring, vital parameters monitoring, remote monitoring of physiological data, infant monitoring elderly assistance, deaf assistance.

Home Applications: Monitoring of smart homes, instrumentation monitoring, automated meter readings etc.

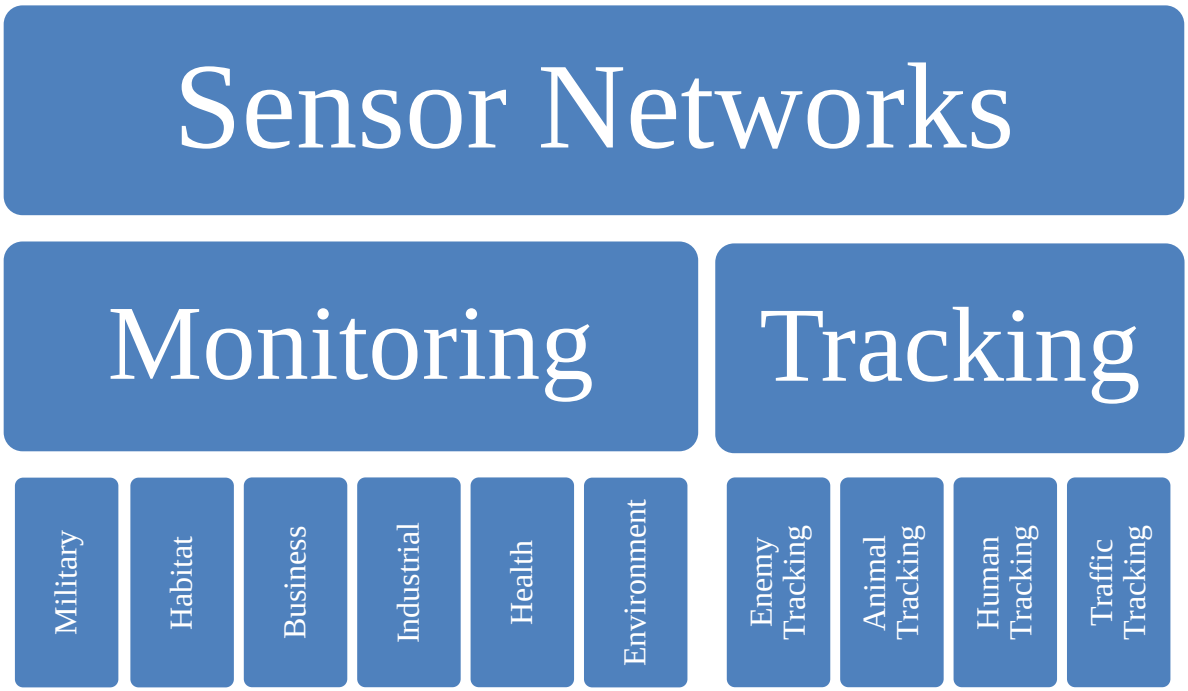


Figure 1.2 Applications of WSNs

1.2 Security Concerns in WSNs

WSNs are envisioned to be future networks of communications. Inaccessible locations, cost effectiveness, flexible and self organization, remote monitoring and control are to name a few inherent features of future networks. WSNs fit most suitably in this definition of communication. WSNs consist of inexpensive, small sized, random deployed, remotely manageable and self configurable SNs. In near future, we can imagine that SNs are liberally spread on defense borders, defense fencing, roads, inside industrial units, machines, forests, river banks, under water deployments, deep seas etc. to develop a wirelessly connected digital communication paradigm that can sense surroundings and detect events of interests like monitoring of traffic congestions, habitat, industrial units, detection of forest fire, seismic activities, emergency requirements etc. Data being relayed in WSNs contains private or confidential information [1]. The need of security services in WSNs is thus a must.

WSNs evolved as monitoring tool in adverse and dynamically changing environment [4]. Time-critical and delay sensitive applications in WSNs press for need to consider security provisions at the time of design, implementation and deployment of application [3]. Privacy of data being reported in WSNs is addressed through security provisioning through key management and keying aware routing protocols.

1.2.1 Security Goals in WSNs

Similar to other communication networks in existence, we can indentify security goals in WSNs. Applications development for security provisioning must focus some or all security goals:

- Confidentiality: Confidentiality is described as accessibility of information to authorized users only [5], [6].

- Availability: Availability property guarantees the persistent survival and access to communication network and its services to authorized users [5] in a WSN.

- Integrity: Integrity property fulfils the requirement that data being received is not altered while in transit [5], [6].

- Authentication: Authentication procedures ensure that communicating nodes can authenticate each others, directly or through authentication servers [5], [6].

- Non-repudiation: Non-repudiation ensures that the sender can't deny from sent messages.

- Authorization: To ensure that only authorized nodes could access networks services in a communication networks, is called authorization property.

- Freshness: This could mean data freshness and key freshness. Since all sensor networks provide some forms of time varying measurements, we must ensure each message is fresh. Data freshness implies that each data is recent, and it ensures that no adversary replayed old messages.

- Forward secrecy: a sensor should not be allowed to know future messages after it leaves the network.
- Backward secrecy: a newly joining sensor should not be able to know any previously transmitted message.

1.2.2 Security Challenges in WSNs

Due to limitation in capabilities WSNs pose severe security challenges that must be understood while implementing any security solution for information dissemination through nodes of WNS. We identify security and routing design challenges particular in WSNs from [7]as follows:

- Resource Limitation: Any security application or solutions must minimize resource consumption and maximize security performance.
- Unattended Operations: WSNs deployment in unattended and hostile surroundings renders more link level attacks ranging from passive eavesdropping to active interfering.
- In Network Processing: Sensed data often contains replications, which must be reduced or removed. Data from different applications requires fusion. Thereby in-network processing becomes a necessity in WSNs during relay through intermediate nodes in end-to-end information transfer.
- Wireless Medium: WSNs operate in wireless bands and wireless communication characteristics render traditional wire-line security schemes unsuitable for WSNs.
- Large Scale: Number of nodes in WSNs is huge when compared with other wireless networks.
- Dynamic Topology: Node mobility, node joining, node failures and network partitioning make the affair more complex.

1.2.3 Security Parameters

Besides implementing the security goal explained above, solutions and schemes must be evaluated for seamless applicability in WSNs [9], [10]. Following metrics are important in WSNs:

- Resilience: Resilience may be defined as effort vested by intruders while trying to break into security provisions. Resilience may also be defined as the ability of the network to provide an acceptable level of security service in case some nodes are compromised.
- Resistance: Resistance may be defined as the ability to prevent the adversary from gaining full control of the network by means node replication attack [11]. Open unattended and hostile surrounding is real cause for resistance requirements.
- Scalability, self-organization and flexibility: Huge number of sensor nodes in WSNs than general ad hoc networks, make it compulsory to consider scalability while designing WSNs. Due to its deployment condition, dynamic topology and flexible mission goals, self-organization and flexibility (nodes leaving and joining) are also important factors.

- Robustness: Robustness may be defined as the ability to operate in adverse conditions. A robust solution ensures continuity in operation despite abnormalities, such as attacks, failed nodes, etc.
- Energy efficiency: Any application/solution design for WSNs is useless if it don't consider energy efficient approach. Application must try to minimize energy expenses and maximize network lifetime.
- Assurance: It is an ability to disseminate different information at different assurance levels to the end-user.
- Self configurable: Any security scheme must be able to configure itself so as to deliver appropriate level information with regard to different desired reliability, latency, etc. with different cost.

1.3 Background: Security Provisioning in WSN

Security provision in WSNs is achieved through cryptographic solutions; secure routing scheme, key agreements and intrusion detections and trust management [12] approaches. Key management schemes and secure routing schemes using key management schemes is important method for achieving security provisions in WSNs. As secure routing has to utilize underlying key management scheme, majority of discussion here relates to key management. A brief of key management schemes is discussed below.

1.3.1 Key Management Schemes: Description and Importance

Need of Key Management: WSN is infrastructure-less networks and mostly deployed in unattended and hostile environment. It leaves such networks prone to much different kind of attacks which may affect Integrity, authenticity and privacy of communication. Attacks varies from eavesdropping on transmissions including traffic analysis or disclosure of message contents, to modification, fabrication and interruption of the transmissions through node capturing, routing attacks, or flooding [13].

Inclusive Definition: Key management or key agreement is the management of cryptographic materials and information in a cryptosystem. Key management includes the generation of keys, exchange of keys among SNs, storage of keys in SNs, uses and replacements of keys. It includes cryptographic protocol design, key servers, user procedures and other relevant protocols [14]. Key management consider keys to be used at user level, i.e., either between users or systems. A supportive key management is critical to the success of a cryptosystem. Key Management is the most difficult aspect in a cryptosystem because it involves system policy draft, user training needs, organizational and departmental interactions, and established coordination among all of these elements.

Types of Keys: Cryptosystems may use symmetric keys or asymmetric keys. In a symmetric key based algorithm keys are identical for both ends of secure channel, i.e., encryption and decryption algorithms use same keys [14]. Keys must be generated and assigned carefully, and pre deployed or distributed securely and stored efficiently. Asymmetric keys based algorithms use two distinct keys (public key and private key) which are related by some mathematical relation.

Prior to any secured communication instances cryptosystem requires exchange of shared keys or public keys. Public keys is known to public and may be exchanged openly (maintaining private key secret) where as symmetric keys must be pre-deployed or exchanged after deployment by using secure channels.

1.3.2 Brief Overview of Key Management Schemes in WSN

Key management schemes in WSN are classified into several classes like, network wide, pair-wise, trusted base station based, random key pre-distribution, public key infrastructure and location based key management schemes. Several solutions suitable to wire-line networks like RSA [15], ECC[16] , AES [17], DES[18], and other promising research proposals seems unavailable in WSNs. Key management schemes for other wireless networks are hard to apply the constrained circumstances in WSNs. Many Characteristics of WSNs requires that key management must be developed especially for WSNs.

Network Wide Key Management: In network wide and trusted base station based schemes, single key is point of failure and is bottleneck to the approach. The compromise and exposure of single key may let whole network down.

Key Pre-distribution: Key pre-distribution based schemes often seen as most viable security solution for secure bootstrapping of the network. The random pre-loading of keying material complements the random deployment and random neighbourhood. Often nodes in WSNs are in communication with small group of SNs and probabilistic key sharing between neighbour nodes results in low degree of connectivity. The storage requirement in key pre-distribution is inversely proportional to the number of keys in the network. The lack of cooperation between nodes far away proves boon for attackers as compromise of one or more nodes exposes link keys used for secure communication by non-compromised keys. The degradation in security is faster than the rate at which compromised nodes increases.

Public Key Infrastructure: The PKI based schemes are seen as safest way for secure bootstrapping. The requirement of Central Authority (CAs) in PKI is infeasible in constrained environment of WSNs. The communication is secured using encryption with public key and decryption using private keys introduces asymmetry in encryption and decryption. The encryption, decryption and verification are major operation in PKI. All these operations require reasonably faster processing and larger storage. Limited storage and computational capability of sensor nodes proves a demonization in using PKI for WSNs. Some customised PKI based solutions based on ECC prove applicable to WSN but with limited scope.

Location Based Key Management: Location based key management schemes uses post deployment information, in virtual or actual exploits actual or virtual neighbourhood for secure communication. The neighbourhood information improves the storage efficiency of the schemes as key material sufficient for secure communication with neighbours is loaded or deployed in SNs. The limited connectivity with respect to complete networks causes such network resort to only multi-hop networks. The number of nodes in routes is equivalent of number of exposure points. Longer routes are weakness of the proposals and wish of the attackers.

Key Management Scheme in HWSNs: The applicability of heterogeneity in WSN is explored in some solutions recently. Often homogeneous networks suffer from low resource availability due to low end SNs in homogeneous WSNs. The scalability in homogeneous networks is burden as scale directly affects the communication, storage and computation overheads on SNs in homogeneous networks. Heterogeneity lends comparatively better resource for computations and communications in HWSNs. Several research projects and communications establish the viability of HWSN [19], [20], [21], [22], [23] to address multiple dimensions [24] simultaneously. The usage of heterogeneity in WSNs may provide default organization as hierarchical networks as opposed to flat networks organizations considered in some promising key management and secure routing solutions. HWSN promise better suitability in dynamic topology, demanding applications and survivable WSNs.

1.3.3 Secure Routing in WSNs

Secure routing ensures that underlying key management schemes is used to establish routing tables and routes to neighbours and distant nodes in WSN. Without a promising key management scheme a secure routing scheme can't be implemented. Several secure routing schemes in WSN rely and implemented in hierarchical WSNs.

Secure Routing and information dissemination approaches in WSNs are proposed in several proposal like LHA-SP [25], SHEER [26], F-LEACH [27], SLEACH [28], AC [29], NHRPA [30], Sec Leach [31], SSLEACH [32] and RLEACH [33] etc. All these solutions are based on some key management schemes and ensure either authentication or/and integrity of sensors and messages respectively. Most secure routing solutions in WSN conclude that security comes at the cost of life of network.

Several secure routing solutions in ad hoc networks [34], [35], [36], [37], [38], [39], Secure Distance Vector [40], SEAD [41], Aridane [42], S-BGP [43], and SAODV [44] addressed the privacy issue using key aware routing schemes. Some of the secure routing designs have been adapted for WSNs with varied level of degradation in performance of schemes. With specialized solution for WSNs privacy of data being reported and routed can be better ensured.

1.4 Contributions of Thesis

The taxonomy of attacks and challenges motivate us to formulate the research questions investigated in this thesis. It has been identified that key management and secure routing for information dissemination are two most important security challenges in WSNs. There is a need to design key management schemes that counter the problem of node compromise attack and scalability issue in random key pre-distribution schemes. Further it is important that routing schemes must be integrated with key management schemes to realize the secure communication in WSNs. Security solutions must consider deployment and static relationships between nodes in close neighbourhood during designing phase.

1.4.1 Motivations

Security solutions for WSNs require efficient key management scheme and a secure routing scheme which can exploit key management schemes while identifying secure routes towards

destination. Besides many solutions proposed by researchers most seem unavailable due to following issues:

Key Connectivity: In most of key management schemes keys are randomly pre-distributed in each node. With limited storage and small number of keys per node, nodes are able to connect to only subset of their neighbours.

Resilience: Resilience is the ability to maintain desired level of security services, in case when several SNs in network are compromised. In most of proposals similar keys are distributed to many SNs in other parts of the network. This phenomenon leaves links between uncompromised nodes prone to attacks.

Scalability: Sensors are energy constrained devices. After deployment nodes may die due to exhausting battery or node error. Also nodes in WSN are huge in number. Most of the solutions don't consider these requirements and are applicable to small scale and de-motivate node joining after deployment.

Node Capture: Open environment and unattended operations in WSN expose small sized nodes to attackers. Nodes can be physically captured and reprogrammed. Scheme must exhibit resistance against node capture attacks.

Node Replications: Node may be captured and replicated for use in other parts of networks. Most schemes lacks to localize the keying materials in the absence of location and deployment knowledge.

Energy Efficiency: SNs are battery operated or the energy is harvested from the surrounding environment and their maintenance after deployment is difficult. Thus, energy saving and load balancing must be taken into account in the design and implementation of WSN platforms, protocols, and applications.

Lack of hardware heterogeneity: In WSNs, node's functions are heterogeneous but node's capabilities are homogeneous. Several computation and communication intensive activities should be performed by high end sensors. Most schemes don't consider heterogeneity in node's capability aspect.

1.4.2 Objectives of Thesis

After a thorough review of state of art in key management in WSN and routing protocols in WSNs we came across several open challenges in WSNs. We propose to introduce heterogeneity in WSN using a small number of H-Sensors besides large number of generic L-Sensors. As the deployment of WSNs is always a random deployment, we suggest to use deployment based key management scheme in HWSNs. To ensure security of data being reported through secure routes in WSN, secure routing protocols must route data efficiently and ensure maximum resilience on the optimally selected routes. In keyed network, where network connectivity greatly depends upon the keying material in trade-off with resilience measures, is big and real life challenge. Routing schemes must exploit underlying key management scheme and guarantee secure routes

for every packet. Solutions with multi-problem addressing capabilities need to be explored and applied. Use of heterogeneity to perform complex and organizational activities in WSN needs to be explored. In other words we can identify the most common security goals that should be achieved in security solution in WSNs. Stating in brief the objectives of the dissertation are finalized as follows:

1. To propose a framework for Heterogeneous Wireless Sensor Network deployment scheme and Key Management approach.
2. To develop a secure data dissemination/accessibility model for WSN using above developed key management framework.
3. Verification and Validation of results through simulation.

1.4.3 Overview of Contribution(s)

In this thesis we have designed several solutions to address the security issue using HWSNs as work field. As per objectives finalized for this thesis work, we designed two key management schemes for hierarchical HWSN and four secure routing solutions for flat and hierarchical HWSN. Major contributions of this thesis in line with objectives of thesis, are discussed briefly as follows:

- **Key Management Schemes:** We have proposed two key management schemes for HWSNs.
    - First key management scheme exploits underlying deployment and local node relationship. Scheme is designed for hierarchical architecture in HWSN. Scheme ensures connectivity in probabilistic environment, but needs intermediation by CH. The localization effect enables the scheme tolerant of node compromise and node replication attack. Scheme uses tree based key generation to achieve randomness at much lower computational overhead.
    - Second key management scheme is a localized matrix based pair-wise key scheme, with low storage overhead. Pair-wise key establishment is ensured without active intervention by CH. Localization provided tolerance to compromise attacks and matrix based design provides complete connectivity through localized pair-wise keys. Scheme is highly scalable and storage efficient in its class.

- **Secure Routing Schemes:** We have suggested four secure routing schemes for HWSNs.
    - First routing scheme utilizes underlying key management schemes in HWSN. First scheme is applicable to flat networks in HWSN. We investigate the impact of local and static relationship among collocated SNs. Scheme performs better in terms of resilience when underlying key management is augmented by local geographic relation among SNs.
    - Second scheme considers limiting variance in number of keys in links using least square approach. Next hop selection is optimal and offers minimum variation with respect to running average number of keys the on partially complete and being extended routes. More than 50% routes results better variance (reduced) than scenario

without variance control approach. The scheme was analyzed for flat architecture in HWSNs.

- As third scheme, we designed a secure data collection paradigm for hierarchical HWSNs using Mobile Nodes (MNs). We have proposed a novel Authentication and re-authentication protocol for MNs using Two-Hop online Authentication (THA) protocol. Scheme considers energy conscious secure data collection and ensures that maximum energy of a SN's is available for data delivery rather than organizational activities.
- Lastly, a multipath secure routing solution was proposed for flat architecture in HWSNs. Scheme exploits underlying random key pre-distribution to induce multicast environment. Scheme suggests Expected Key Average (EKA) as novel tool to prioritize and scrutinize one-hop SNs in a front, towards BS. Scheme finds application in scenarios where WSNs are viewed as large database, and offers equally secure and multiple paths for both, query and replies.

1.5 Organization of Thesis

Including introductory chapter this thesis is organized into six chapters.

Chapter 2 presents a critical review of state of the art in key management and routing schemes in WSN and HWSNs. The chapter primarily identifies the gaps in key management scheme and routing schemes in WSNs. Identified gaps are taken as opportunities for work in next chapters.

In Chapter 3 we presented key management schemes which are based upon underlying deployment and local node level relationship. We presented two key management schemes for HWSN using hierarchical structure. First scheme ensure connectivity to every SN in network with the help of CHs. Both schemes are scalable and storage efficient. Both schemes use a tree based key generation.

Chapter 4 presents secure routing schemes based on random key pre-distribution of keys. Chapter explains four schemes that are applicable in flat and hierarchical HWSNs. Heterogeneity using MNs for secure data collection was suggested. Schemes for flat HWSN strive to improve resilience of routes using different approaches. A multipath secure routing solution is also presented in this chapter.

Finally, chapter 5 summarize the contributions of thesis and identifies future scope of work. In the last research contribution of this work is also provided.

1.6 Summary

In this chapter we define WSNs and HWSNs. We studied general feature, applications and challenges for secure information dissemination in WSNs. A brief look at the background signifies the importance of specialized solutions and introduction of heterogeneity. Section 1.1 introduced WSN, HWSN and discussed characteristics and applications of WSNs. Section 1.2 reviews security concerns in WSNs. Section 1.3 looks into related work into key management and secure routing schemes. In Section 1.4 we presented brief description, motivations, objectives and contribution of this thesis. Section 1.5 describes organization of thesis with

Section 1.6 finally summarises this chapter. In the next chapter we will present a review of key management schemes and routing scheme in WSNs.

Chapter 2

Literature Review

WSN is a communication facility derived from low cost autonomous and randomly distributed small devices equipped with communication infrastructure for sensing local surroundings and relay sensed data cooperatively through neighbours in multi-hop communication paradigm to a remotely situated safely managed highly capable device called BS. These small devices are called sensors and operate under proactive control of BS. The design of WSNs is conceived from surveillance requirement in battle fields, volcanic zones, traffic congestion prone areas, unattended self-organization and flexibility driven applications. With ever increasing applications WSNs crept into day to day monitoring in smart homes, hospitals, precision agriculture, deep sea explorations, seismic activity monitoring, unattended baby care, are to name a few[1].

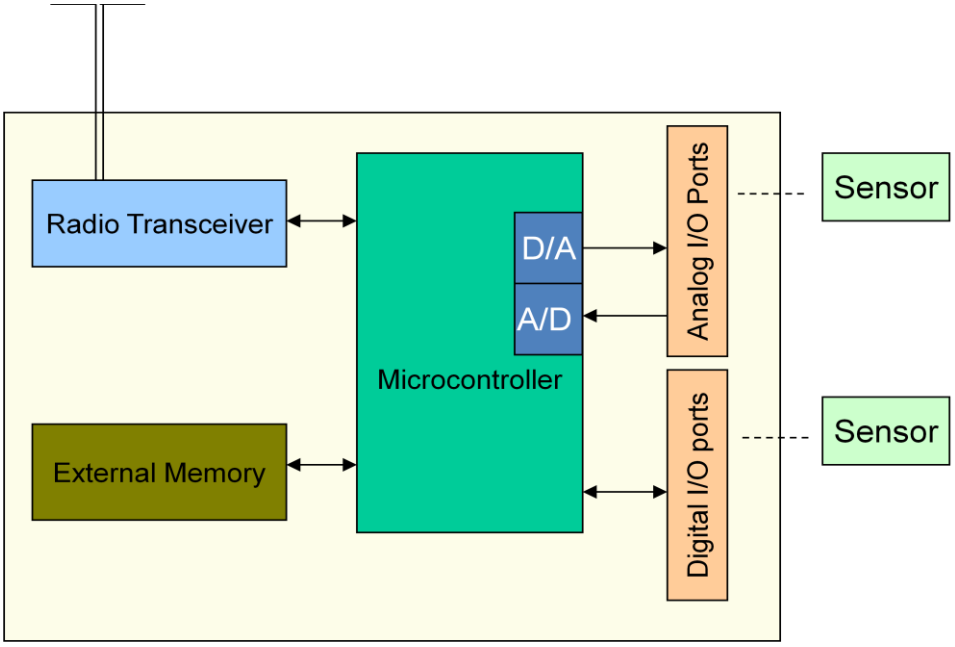


Figure 2.1 Typical Sensor Node's Components [2]

[1]The major findings of this chapter have been published

- "*Promising Key Management in Wireless Sensor Networks: A Review*," of IEEE International Advance Computing Conference (IACC'09), pp. pp. 1061 – 1066, March 6-7, Thapar Institute of Engineering and Technology, Patiala, India, 2009.

WSNs are distinct from other wireless networks in scale and density as the number of sensors that setup WSN is huge and highly dense. Large scale and higher density implies large neighbourhood. Sensors in WSN are connected to one or sometimes several sensors in neighbourhood. With random and uncontrolled deployment and flexibility in connections, topology of the WSNs may take the forms of a star or multi-hop wireless networks. In the absence of global identification and small bandwidth in available communication bands, routing in WSNs takes form of broadcasting or flooding [45], [46].

This chapter presents an architectural view of a sensor node in Section 2.1. Section 2.2 introduce a brief of application and identifies importance of security provisioning. Section 2.3 presents a review of key management scheme. Section 2.4 presents a review of routing schemes in WSN. Section 2.5 presents a review on available secure routing protocols in WSNs. Section 2.6 presents brief analysis on literature. Finally, chapter is summarized in Section 2.7.

Table 2.1: Comparison of Sensor Platforms

	TelosB/Tmote Sky	**Mica2/MicaZ**	**SHIMMER**	**IRIS**	**Sun SPOT**	**EZ430-RF2480/2500**
Microprocessor Specification						
Microprocessor	T1MSP430F1611	Atmel ATmega 128L	T1MSP430F1611	Atmel ATmega 128L	Atmel AT91RM9200	T1 MSP430F2274
Bus	16 bit	8 bit	16 bit	8 bit	32 bit	16 bit
Clock	4-8 MHz	8 MHz	4-8 MHz	8 MHz	180 MHz	16 MHz
Memory Specification(Bytes)						
RAM	10K	4K	10K	8K	512K	1K
Flash	48K	128K	48K	640K	4M	32K
EEPROM	1M	512K	none	4K	none	None
Radio Chip Specification						
Radio Module	T1 CC1000	T1 CC2420	T1 CC2500	T1 CC2480	Atmel AT86RF230	Mitsumi WML-C46
Frequency(MHz)	300-1000	2400-2483.5	2400-2483.5	2400-2483.5	2405-2480	2400-2483.5
Modulation	FSK	OQPSK	OOK, 2-FSK, GFSK, MSK	OQPSK	OQPSK	GFSK
Data Rate	76.8KBaud	250kbps	500kBaud	250kbps	250kbps	721kbps
Tx Power(dBm)	-20 -10	-24 - 0	-30 - 1	-55.8 - 0	-17 - 3	- 6 - 14
Rx Sensitivity(dBm)	-110(at 2.4 kBaud)	-95	-108(at 2.4 kBaud)	-92	-101	-82
Radio Chip Power Consumption						
Sleep	0.2 µA	0.2 -426µA	400 nA - 160µA	0.3 - 190µA	20nA	50µA-1.4mA
Idle(Rx)	74 µA to 7.4 mA	18.8 mA	13.3 – 19.6 mA	26.7 mA	15.5 mA	40 mA
Tx(mA)	10.4 (0 dBm)	17.4 (0 dBm)	21.2 (0 dBm)	26.9 (0 dBm)	16.5 (3 dBm)	60 (0 dBm)

2.1 Architectural View of SN

Each SN in WSN support infrastructure for local sensing, reception and small distance transmission. A generic SN consists of a radio transceiver circuit attached to an internal antenna or provision to connect to an external antenna, a microcontroller chip, an integrated electronic circuit chip for interconnection to sensors, and an energy source {Figure 2.1}. SNs are battery powered or have capability of small scale energy harvesting from surroundings. Sizes of SNs may vary from tablet to the size of a wheat grain. The cost of SNs is dictated from strength of infrastructures available for communication. Constrained size and small cost of SNs derives corresponding constraints on resources of SNs. SNs express limitation in energy, storage, processing speed and available bandwidth for communication. Table 2.1 provides a glimpse of components in popularly available sensor platforms.

2.2 Application and Characteristics: Security Drives in WSNs

We can see plenty of applications of sensors in widely ranging fields from daily life to industries, from health services to traffic monitoring, from agriculture to defence applications. Sensors are used for area monitoring in military for detecting any enemy infiltration, monitoring geo-fencing of any oil or gas pipeline. Environmental Monitoring in the form of sensing magnitudes of temperature, pressure, light and humidity, monitoring gas or particle concentration, ambient monitoring like rainfall, UV levels, wind direction and wind speed, air-pollution, forest fire detection, water quality monitoring, land slide detection/prevention, natural disaster detection and monitoring ,and habitat monitoring. Industrial application of WSNs takes the forms of factory automation and process control, machine's health, detecting leakage of gas/liquid, remote detection of contaminated area and real-time inventory management. Data logging in a nuclear reactor; water/waste-water monitoring; real time water inflow monitoring in water reservoir of a dam; moisture measurement/monitoring in soil; structural health monitoring by monitoring the effect of load, fatigue, chemical erosion, environmental pollution, traffic and weather effects; sensing fires in offices; smart-home monitoring; passive localization and tracking. List is endless so are the issues. One of the alarming issues is the security of information being received or sent. To manage trust in WSNs [46] and make available correct data and information; key management schemes and secure routing are widely used approach.

Key management is the management of keys. Key management include creation; secure bootstrapping, exchanging keys between users, managing storage for key material, usage, revocation and refreshing of keys. Secure routing utilise underlying keying material in SNs while selecting next hop on routes towards destination. Secure routing may optimize route construction such that each link on route is strongest in comparison to available alternates.

Many characteristics of WSNs like constrained resource in terms of energy, storage and communication range requires that key management must be developed specially for WSNs.
Key Management must overcome the storage limitation at the same time maintaining strong security strength. Thus a key management must be efficient in terms key-distribution, key-refresh and key-revocation besides being efficient on storage requirements. As WSNs are Infrastructure-less networks and mostly deployed in unattended and hostile environment leaving such networks prone to many different kind of attacks which may affect Integrity, authenticity and privacy of communication. Attacks varies from eavesdropping on transmissions including traffic analysis or disclosure of message contents, to modification, fabrication, and interruption

of the transmissions through node capturing, routing attacks, or flooding [13]. Attacks may be classified into passive and active attacks depending upon the operational characteristics. Passive attacks affect privacy of the communication by listening and monitoring the communication. More common kind of passive attacks include eavesdropping, traffic analysis and camouflage adversaries. Using passive attacks information can be gathered involving very low risk of being detected. Active attacks are initiated by monitoring, listening and modifying the data stream in communication and thus may lead to severe destruction in normal functioning of WSNs. Routing attacks, denial of service attacks, node subversion, node malfunction, node outage, physical attacks, message corruption, false node and node replication attacks are most commonly launched attacks in WSNs [47].

2.3 Key Management Schemes in WSN

Several key management schemes have been proposed in literature and have been classified into several classes. In this chapter we will review representative key management schemes in its class with special stress on key management schemes in heterogeneous wireless sensor networks. Key management schemes are classified into;

- Single Network-wide Key
- Pair Wise Key
- Trusted Base Station
- Public Key Schemes
- Key Pre-distribution
- Location Based Key Management Schemes
- Key management schemes for HWSNs

2.3.1 Single Network-wide Key

This is simplest in terms of functional complexity as all SNs in WSN use same key for encrypting information being exchanged with other SNs. To ensure the integrity of the message all the messages need to be embedded with MAC of the massage. Unless this single network wide key is known, integrity of massages is ensured. Replay attacks can be avoided by including source, destination and timestamp in the massages. Illegitimate SNs can never join the WSN unless they possess key. Once key is compromised whole of the WSN gets compromised.

S. Basagni et al. [48] suggested a proposal for network wide key using symmetric key management. Key management supports efficient update and exchange of keys. Instead of individual SN, a group of SNs was considered feasible for network as it helps save a lot of space per node. A Traffic Encryption Key (TEK) was used as global key for secure communication in the network. The update in TEK was realized using Cluster Heads (CHs), where CHs are selected using a distributed clustering mechanism. This ensures both forward and backward secrecy. Out of CHs selected that formed backbone; CHs with largest weight among neighbours became Probable Key Manager (PKM). PKMs start generating TEK; t_i for i^{th} round/period of the protocol operation and start distribution after waiting for a random delay governed by large Δ for exponential distribution. The possibility of tie in two or more PKMs becoming Key Manager for the period is broken in favour of PKM with larger weight. The proposal is highly complex and suffers from high communication overheads.

Table 2.2 Classification of Key Management Schemes in WSN

Sr. No.	SUPER-CLASS	MEMBERS
1	Network Wide Key	S. Basagni et al. [48]
		S. Zhu et al. [49]
2	Pair Wise Key	S. Zhu et al. [49]
3	Trusted Base Station	A. Perrig et al. [50]
		R. Pietro et al. [51]
		H. Chan and A. Perrig [52]
4	Public Key based Key Management Schemes	Nils Gura et al. [53]
		G. Gaubatz et al. [54]
		R. Watro et al. [55]
		Blab et al. [57]
		Wenliang Du et al. [58]
5	Key Pre-distribution Schemes	Eschenauer and Gligor [60]
		H. Chan et al. [61]
		B. Lai et al. [62]
		B. Dutertre et al. [63]
		H. Chan et al. [61]
		W. Du, et al. [64]
		D. Liu and P. Ning [65]
		W. Zhang et al. [66]
		D. Huang et al. [68]
		Z. Yu and Y. Guan [69]
		W. Du et al. [70]
		C. Yu et al. [71]
		J. Lee and D. R. Stinson [72]
		S. Camtepe and B. Yener [73]
		M. F. Younis et al. [74]
		M. Eltoweissy et al. [75]
6	Location Based Key Management Schemes	D. Liu and P. Ning [76]
		D. Liu et al. [77]
		Du et al. [64]
		D. Liu and P. Ning [78]
		Yu and Guan [79]
		J. Lee and T. Kwon [80]
7	Key Management in HWSN	Dahai Du et al. [81]
		Patrick Traynor et al. [84]
		Patrick Traynor et al. [24]
		F. Kausar's [85]
		F. Anjum's Scheme [86]
		V. Bulusu et al. [87]
		S. Jiang et al. [88]
		S. Khan et al. [91]

S. Zhu et al. proposed a key management scheme named LEAP in [49] to use network wide keys to establish secure routing of the information and data. LEAP was proposed to address different kind of communication patterns. LEAP used individual key for secure communication between Node and BS, Group Key, a network wide key for global broadcast, Cluster Key for authenticated secure local broadcast and pair-wise key for secure communication between a SN and its neighbours for one-to-one secure communication. Having generated pair-wise keys, nodes erase master keys of their neighbours. The proposal as a whole tried to provide possible solutions against Clone attack, Sybil Attack, Wormhole attack, Forward-backward secrecy and node addition attack. To achieve authenticated local broadcast scheme used one-way hashing with commitment exposed to neighbours using pair-wise key. This is used as AUTH key and is exposed in reverse manner. LEAP provides resilience to almost every attack and is JACK of ALL Trades.

2.3.2 Pair Wise Key

Pair wise concept is derived from its meaning itself. This approach recommends that every node shares unique distinct symmetric key with every other node in the network. For a network of size n each node is assigned $n-1$ keys to be shared secretly with $n-1$ remaining nodes in the network. This enhances the storage requirement per node to $n-1$ at least. Capturing any single SN doesn't affect the security of communications undertaken by remaining SNs in the network. The scheme is perfectly resilient to node compromise or node capture attacks. Pair-wise offers security equivalent of asymmetric key cryptography but at the cost of huge storage for $n-1$ keys. To remove $n-1$ keys of compromised node from whole network, a single broadcast of $n-1$ keys or key's IDs is sufficient. SNs receiving broadcast can delete the keys from their key rings. This approach completes the node revocation effectively. Benefits of symmetric key management schemes are enjoyed without need of dedicated hardware or software. The most preventing issue in pair-wise keys is poor scalability. The storage requirements in SN as well network increases in proportion to network size.

S. Zhu et al.'s scheme LEAP in [49] support pair-wise key for secure communication between a SN and its neighbours in one-to-one communication. Pair-wise is also exploited for secure communication with the aggregation node for achieving energy savings. After discovering neighbour, SN can establish pair-wise key with each of its neighbour after generating their master keys. Having generated Pair-wise keys nodes erase master keys of their neighbours. To establish pair-wise keys with sleeping nodes in dense large sensor nodes IDs of the sleeping nodes are obtained from active nodes and node establishes pair-wise keys for each such node. To achieve authenticated local broadcast, scheme used one-way hashing with commitment exposed to neighbours using pair-wise key. With provision for all other kind of keys LEAP is communication intensive scheme for constrained WSNs.

2.3.3 Trusted Base Station

In this class of schemes, a trusted, securely situated BS is used as generator and distributor to provide pre-deployed or post deployment link encryption keys to SNs in network. SNs share an individual key with BS. BS plays the role of a Key Distribution Centre (KDC). The individual keys may be used for authentication by SNs to KDC. After establishing authorization of both sensors, KDC generates and distributes link keys securely. KDC based approach results in

smaller storage requirements as link keys are generated and distributed dynamically. Scheme offers perfect resilience to node replication and node capture attacks. KDC has full control to revoke any keys and ensures availability of network services to surviving nodes. Due to single point of management scheme is not scalable. Key management schemes proposed in [50] is a representative of this category of key management schemes.

A. Perrig et al. proposed basic building blocks for scarce resources popularly known as SPIN's in [50]. Two protocols were proposed; first of which is Secure Network Encryption Protocol (SNEP) and another one Timed, Efficient, Streaming, Loss-Tolerant, Authentication (µTESLA). Using SNEP and µTESLA, an authenticated routing protocol was proposed. SPIN'S achieved confidentiality, integrity, data authentication, data Freshness (weak and strong) using SNEP. µTESLA is specially designed for broadcast authentication. SPINs was evaluated for code size, RAM requirements, processor and communication overhead. In terms of storage requirement SPINS works well within 4KB RAM limitation. Energy consumption due to addition of MAC for authentication and integrity cost 20% of total energy consumption in transmission.

R. Pietro et al. proposed a Logical Key Hierarchy (LKHW) based proposal in [51]. LKHW is a secure group communication scheme which is based on DD [88]. It is used to provide security in DD. LKHW maintains a tree structure where SNs represent leaf and BS represent root. SNs hold keys for the route between SN and BS. LKHW integrates security and routing in a single framework.

H. Chan and A. Perrig suggested a variation from purely base station based KDC approach in [52]. A peer SN from neighbourhood performs as a trusted intermediate while establishing a shared symmetric key between pair of SNs. The scheme is highly scalable. Scheme results in lesser communication overhead compared to KDC approach.

2.3.4 Public Key based Key Management Schemes

Public key cryptography or asymmetric key cryptography had been in use for security since security requirements are identified. Public Key Cryptography uses a pair of public/private key for encryption/decryption. Any of Public Key Cryptography algorithms like RSA [15] or ECC [16] can be used for encryption/decryption. For wired networks operations meant for public key cryptography like encryption, decryption, signature generation, signature verification and key agreement. All these operations require resource rich platforms. In WSN energy, storage and communication range are very scarce resource. What may seem a boon for wired network may prove fatal for constrained devices like WSNs. Wired network's PKC has to be customized for constrained environments of WSN's. Proposal in [53] and [54] explored the feasibility study PKC in WSNs.

Nils Gura et al. compared performances of RSA [15] and ECC [16] on 8-bit Atmel ATmega128 at 8 MHz in [53] and concluded that RSA which seems only practical solution in asymmetric key based protocols proves to be storage and energy hungry for constrained WSNs. Authors in [53] outlined the importance of operations in RSA and ECC which if implemented using optimizing techniques/optimal algorithms; could bring a significant improvement in computation times of RSA [15] and ECC [16] related operations. Proposal recommends optimization in modular exponentiation for RSA and point multiplication for ECC; for a possible reduction in computation time. Moreover ECC-160 provides security comparable to RSA-1024

and ECC-224 provides security comparable to RSA-2048. Results endorse ECC as practically feasible public key cryptosystem for WSNs.

G. Gaubatz et al., also studied the feasibility of public key cryptosystem is established by comparing the performance of Rabin's and NtruEncrypt for WSNs. Study recommend for custom hardware based approach provided right selection of algorithms and associated parameters, careful optimization and low power design technique. ECC earns negative support due to arithmetic primitives/operations and large number of temporary operands. ECC lacks scalability and rendered less attractive for energy efficient low power designs/implementations. In [54] author instead investigated an approach where encryption is to be done on constrained devices like sensors and decryption shifted to more capable nodes. On the basis of using low power design both Rabin's and NtruEncrypt improved upon throughput and at the same time NtruEncrypt outperforms Rabin's which a specialization of RSA.

R. Watro et al. proposed a protocol called TinyPk in [55] with emphasis on data confidentiality and sender's authentication for sensor networks traffic. Proposal was implemented on UC Berkley MICA2 mote using TinyOS development environment. Public key is widely used tool to support symmetric key management. RSA cryptosystem [15] and Diffie-Hellman [56] can be deployed on sensor networks. TinyPk proposed as security mechanism for providing authentication and key exchange between an external party and sensor networks using signed certificates. Signature verification and encryption which are lighter operations for RSA [15] are used by the nodes in the WSN. RSA was a choice of implementation in [55].

Blab et al. proposed a custom implementation of ECC to achieve maximum performance while preserving main memory in [57]. Proposal was to move constant multiplication matrix from RAM to ROM along with field inversion operation requirement of two arrays of constants. These respectively resulted in saving of 22% and 28% of RAM. A collection of algorithms based on ECC; namely ECDH, El-Gamal and ECDSA algorithms by using a pre computation of points. A faster and memory efficient way to harness ECC for WSN was thus recommended.

Wenliang Du et al. in [58] discussed the issue of verification of public key issued to any random node. Traditional approach of signed certificate results into a lot of overhead. Architecture of the network was exploited to devise an alternate. An alternate using Merkle Tree [59] has been proposed to reduce the communication overhead. A Merkle tree was used to compute public keys of the nodes. Height of the Merkle tree was one of the limiting factors. Instead; Merkle tree was trimmed down to down to Merkle trees of different heights. The deployment knowledge of sensor network's nodes was used to decide upon trimming of the Merkle Tree.

2.3.5 Key Pre-distribution Schemes

Eschenauer and Gligor (EG) proposed a random pre distributed key management scheme for distributed sensor network in [60]. The scheme proposed to distribute a key ring of size k in each node and IDs of the keys in key ring, a key shared with controller. Key are chosen randomly from a key pool of size P, generated offline. Keys are assigned to nodes in offline mode. Key management scheme executes in three steps namely, key distribution, shared key discovery and path key establishment. After deployment nodes identify neighbours with which node's shares a direct key. Path key establishment phase is meant for reaching a neighbour through other neighbours or nodes which shares key with the concerned neighbour. Scheme suffers from low usage of keys suffers from high compromise ration. The limitation of the protocol is the

communication overhead during initial broadcast and key revocation. The size of key ring depends upon the limit imposed by storage available in a node.

H. Chan et al. in [61] proposed a random key pre-distribution based pair-wise keying scheme with distinct pair wise keys loaded into the SNs; before deployment. SNs are pre-deployed with pair-wise keys in their key rings and Ids of other nodes which also know the pair-key between a pair of nodes. Nodes are allocated pair-wise keys with several other randomly selected nodes. The discovery of pair-wise keys proceeds like in [60]. Scheme proposed a distributed revocation method with flexibility of choosing a threshold number of nodes which votes to revoke a node in the networks. The scheme is highly resilient to node capture attack. The scheme is highly scalable but lacks the connectivity.

Master key based pre distribution: Few schemes based on master-key pre-distribution in [62] and [63] were proposed. In this approach, a single or master key is preloaded into all SNs. These schemes result into minimum storage requirements and avoid complex shared key discoveries. Schemes ensure full connectivity in the network.

B. Lai et al., proposed scheme, BROadcast Session Key (BROSK) negotiation in [62] performs negotiations using messages to construct link dependent keys within each pair of neighbour nodes. The scheme adopts the trust level based methods to authenticate the nodes in the neighbourhood.

B. Dutertre et al. designed a scheme based on bootstrapping protocol in [63]. Secure links were established between SNs which are deployed in different phases. Authentication and secure local links are established using initial trust levels which is computed from small set of pre-deployed shared keys. A group authentication and key generation key is also stored in each SN. The authentication key is used for authentication between two SNs which are from same generation of SNs. The same key is also used for exchanging random nonce required for establishment of session keys between pair of SNs or group of SNs. The scheme offers storage efficiency and less computation. The scheme offers very low resilience and capture of single nodes brings whole network down.

Pure probabilistic key pre-distribution: To overcome the resilience limitation of key based and pair wise keying based approaches, pure probabilistic key pre-distribution schemes were proposed. In this class of key management schemes nodes connectivity is compromised against high resilience towards node capture attacks.

E-G scheme [60] is representative random key pre-distribution scheme. The scheme offers addition and deletion of nodes while focussing on solution to bootstrapping problems in sensor networks.

H. Chan et al. proposed a scheme called Q-Composite in [61]. A pair of nodes can communicate only if they share more than one key, i.e., q keys. Increasing minimum number of keys to be shared in key rings, which are pre-deployed in each node before deployment, increases the resilience of the links. Connectivity in Q-composite is lower than in E-G [60] and also increase the impact of node capture attack. Capture of few nodes in the networks reveals the keys distributed in the network and causes network level destruction.

H. Chan et al. also suggested a multipath reinforcement scheme in [61] and was used to strengthen security of link by using multiple paths to establish a pair-wise key. Multiple paths are secured using randomly pre-distributed shared keys. Multiple paths are used to transmit multiple

shares of a pair-wise key between a pair of SNs. Scheme is resource and communication intensive.

W. Du, et al. implemented deployment knowledge based random pre-distribution key management schemes uses likely location information of nodes that may be the neighbours in [64]. Deployment knowledge is modelled using non-uniform probability density function like normal distribution, which helps to compute the ratio of total number nodes in given area around a deployment point. It improves the pair-wise keying environment by using small number of pre-distributed keys in each sensor node. Scheme offers reduced communication overhead while ensuring high resilience. The scheme is complex to realize.

Polynomial pre-distribution: Polynomial based key management schemes offer high resilience and connectivity with low communication overheads. Any node can establish shared pair-wise key with any SN in the network. Even when certain nodes in the networks are compromised networks are ensured of high connectivity.

D. Liu and P. Ning, proposed a scheme in [65] which is polynomial based scheme used to secure communication between pair of SNs using pair wise keys. Nodes used ID of other node to evaluate the polynomial pre-deployed in node's memory. Scheme offers a reasonable resilience but suffers from poor key connectivity. The degree of polynomial determines the resilience against node capture attack. Another scheme in [65] is based on polynomial pool to generate pair-wise keys used randomly generated bivariate polynomials. Scheme also suffers weak key connectivity and storage overheads. A random subset [65] key assignment scheme uses a strategy to identify subset of polynomials to be allocated in setup phase. Nodes are assigned their shares. The scheme offers good scalability but suffers from node level targeted attacks.

W. Zhang et al. suggested a scheme in [66] uses polynomials pre-distribution for pair-wise key establishment. Polynomials are defined over a finite field f_q where q is a prime number. The scheme is highly secure as well as storage and computationally efficient. The scheme suffers from high energy requirements due to high communication costs.

Matrix Pre-distribution: Several proposals based on Blom's concept [67] used $n \times n$ matrix to represent link keys in a network of n nodes. Such schemes need very small amount of storage to store information in each SN, so that each pair of sensor nodes can compute and calculate the link key.

D. Huang et al. developed a scheme using Grid-Group based deployment of sensor in a large area was proposed in [68]. SNs were deployed uniformly. Scheme devised a novel approach for distribution of secret keys to SNs from a structured key pool. This improved storage efficiency of scheme as only few keys needs to install in each SN for secure communication with SNs in neighbouring cells of grid. The random capture assumption used to assign keys is very weak.

Z. Yu and Y. Guan proposed a similar scheme based on Robust-Group in [69] and exploit deployment information. The deployment field was assumed to be divided into hexagonal grids. Scheme ensures very high degree of key connectivity in-spite of low storage overhead. Localization of key usage has improved the resilience of the scheme. Instead of distributing secret keys, secret information for link establishment was distributed. Scheme was highly successful but suffers from capture targeted at grid centres.

W. Du et al. designed a unification of E-G and Blom's Scheme, in [70]. Scheme offers improved resilience. Scheme proposed to convert complete deployment graph into connected graph so that sensors nodes in neighbourhoods can communicate with very small amount of

keying information. Scheme is highly storage efficient. Scheme is highly scalable and offers the flexibility of deployment in phases. Scheme fails to qualify the optimal resilience requirements.

C. Yu et al. proposed ContrAined Random Perturbation based pair-wise keY (CARPY) establishment scheme in [71] which requires to exchange the columns of the key matrix to establish pair-wise key. The scheme offers poor resilience as column being exchanged may become known to adversaries. An improved variant which did not require communication for key establishment was also proposed. Scheme was first non-interactive scheme and offers a good resilience as no communication is required. Scheme has shown high energy consumptions.

Tree based Pre-Distribution: Few schemes used tree based key distribution for secure communication. The topology is visualized as tree with nodes performing child and parent in the tree. Only nodes that are in child-parent relation can communicate. This has drastically reduced the key storage requirements. Schemes allowed the dynamic addition by using authentication from two or more existing nodes in the tree. Newly joined nodes create pair-wise keys to be shared with its parent after node authentication. Pair-wise key is divided into shares and shares are sent to those nodes which authenticated the node on request from BS. Concerned nodes then send the shares to the parent of the newly joined node.

J. Lee and D. R. Stinson explored an ID based one-way hash function scheme in [72] to reduce the number of keys that needs to be stored in the sensor nodes. Each sensor node is assigned a unique ID. ID of node is used to determine the secret keys to be allotted to the sensor nodes. Scheme is not suitable for large sensor networks. It supports only small sized networks. The size of network is highly dependent upon the keys allotted in each sensor nodes. For a network with k keys in each sensor's memory the maximum size is $O(k)$. Another approach to improve the resilience of multiple IOS in tree based scheme was introduced in [72]. The idea was to reduce the connectivity in the network connectivity graph. Instead of using complete graph a bi-partite graph was used. It overcame the limitations of ID based scheme.

Hierarchical Architecture based Pre-distribution: Few proposals were proposed that brings the network in a virtual or physical hierarchy. Such schemes are called hierarchical key management schemes. Keys at a level in hierarchical scheme are distributed to the nodes of a particular class. The keys for lower level can be generated using the keys at higher level but not vice-versa. The major issue solved using hierarchical schemes are data aggregation and easier management with topology control in hostile environment.

S. Zhu et al. scheme for clustered hierarchical sensor network, called LEAP, was proposed to cater the group pair-wise, cluster based communication and authentications issues [49]. LEAP uses master key based approach for bootstrapping. Due to clustering LEAP can to limit the impact of node compromise to local group of nodes. LEAP uses a cluster key for authenticated secure local broadcast and pair-wise key for secure communication between a SN and its neighbours for one-to-one secure communication. LEAP is highly appreciated proposal for its all round approach. Being very complex and bootstrapping period vulnerability, makes LEAP a difficult choice.

Combinatorial Design based Pre-distribution: S. Camtepe and B. Yener proposed a combinatorial design based key management in [73]. The scheme decides how many keys to assign each key chain. The decisions are taken before deployment. It was proposed to increase the probability to share a key a pair of nodes. It was able to reduce the key path length to very low value. Increase in the complexity in distribution resulted in low key sharing probability.

Exclusion Basis System (EBS) based pre-distribution: EBS based schemes used combinatorial design based schemes to devise efficient key management schemes. Scheme in [74] and [75] uses a trade off between number of administrative keys deployed and number of key refreshing or rekeying messages.

M. F. Younis et al. scheme called SHELL [74] supports rekeying and thus ensures survivability against node capture attack. Scheme uses post deployment information for allocating keys by cluster gateways. The compromise of cluster gateway node command node is notified and takes care of revocation and refreshing. Similarly; a node compromise is taken care of by cluster gateway nodes. The scheme offers a limited scalability with reasonable degree of flexibility. Structure of scheme is highly complex which involves heterogeneous node role structure and multiple types of keys

M. Eltoweissy et al. scheme in [75] called LOCK uses localized rekeying to reduce the communication overhead. The protocol don't uses any expected location information while remains location dependent. The scheme assumes a hierarchical structure in three tiers. LOCK preferred key polynomials over location based keys in SHELL [74].

2.3.6 Location Based Key Management Schemes

D. Liu and P. Ning proposed the use Pseudo Random Function (PRF) in [76]. SNs are preloaded with a master key shared with the setup station. Nodes also shares pair-wise keys with expected neighbours. The scheme offers a high resilience to node capture attack as compromise of any node don't expose direct pair-wise key between any other SN's pair. The scheme is highly storage efficient and allows the dynamic deployment of new sensor nodes. The scheme suffers from extra overhead on master nodes. The nodes are not only distributed in the network and communications overhead to cater newly added nodes is considerable large. A location dependent pair-wise key management scheme in [76] divided the target deployment field into cells where each cell is associated to a specific bivariate polynomial. Scheme offers high neighbourhood connectivity. The scheme uses ANs to utilize location factor but these are soft targets for capture and results in denial of service attack.

D. Liu et al. generalized grid based key management scheme and it called Hypercube based [77] key management scheme to guarantee that any pair of sensors can establish pair wise keys only when network is free from compromised attacks.

Du et al. proposed a key management schemes in [64] which use deployment knowledge, assuming that a particular order in deployment can help to obtain deployment knowledge to some extent. Deployment knowledge is modelled using Probability Density Functions (PDFs). Considering non-uniform PDFs, positions of SNs to be at certain areas can be assumed. Generally nodes are deployed in groups. By choosing an optimal distance between collocated deployment points, we can achieve equality in probabilities of locating a SN in small areas. In a key pre-distribution scheme based on the deployment model, N SNs assumed to be divided into $t \times n$ equal size groups along with dividing key pool into $t \times n$ key pools with objective that to

ensure that collocated key pools have maximum common keys; followed by assigning a sub pool to a group of SNs. Neighbours key pools can be identified on the basis distance between resident points. Scheme follows a grid deployment pattern. Utilization of deployment knowledge minimized storage and communication overhead. An improvement in resilience against node capture and network connectivity was observed. Scheme is highly complex.

D. Liu and P. Ning proposed a scheme in [78] which used post deployment knowledge based key pre-distribution and performs even better than W. Du, et al. scheme in [64]. The scheme improves pair-wise key pre-distribution in WSNs. Pre-distributed keys get priority where priority is computed using post deployment knowledge. Nodes are assigned large sized key rings before deployment. Low priority keys are discarded and removed from sensor node's memory. This step helps to recover memory in the network while simultaneously reducing the extent of compromise attack due to low priority keys. The scheme is highly complex as scheme requires the management of pre and post-deployment locations of the nodes.

Yu and Guan considered a location dependent key management scheme and partitioned target field into hexagon shape grids [79]. Similarly, SNs are assigned to as many groups as there are hexagonal grids. Each group of SNs is deployed into distinct grid. Authors proposed group based deployment model. Scheme investigated the establishment of pair wise keys. Scheme divided the links of WSNs in two classes and constructs two classes of matrices called; A & B. Scheme proceeds two phases. In first phase, each sensor is assigned one secret matrix A, one public matrix G and few secret matrices of type B. SNs from same group use matrix A to establish a shared pair-wise key. Inter-group communication is established using secret matrix B. Scheme exhibits resilience to node capture attack and achieved better network connectivity using small amount of storage. Performance of scheme improves further by using more memory.

J. Lee and T. Kwon proposed a location aware key management scheme (GENDEP) for general deployment in WSNs [80]. Scheme consider true deployment information for real time sensing geography. Scheme proceeds in two steps namely, group placement plan and key management scheme. Scheme evaluated the efficacy of pre-distribution key management in location aware approach. Scheme presented a true numerical analysis and simulation of the scheme. Scheme considered controlled deployment of sensors, which makes it ineffective.

2.3.7 Key Management Schemes in HWSNs

Dahai Du et al. in [81] has proposed a key management scheme for HWSN named MAKM (Modular Arithmetic based Key Management). MAKM was compared for energy efficiency and storage efficiency with E-G [60], C4W [82] and IBC-KM (Identity Based Cryptography-Key Management) [83]. CHs were deployed uniformly in deployment region. CHs complete the bootstrapping of member nodes during first phase of key establishment. CHs are provided with Authentication Key, a pair of public/private keys using underlying ECC defined over undisclosed field. A unique separate key between CH and its member SNs is established using modular arithmetic. Also a group key is generated for group communication in hierarchical WSN. MAKM is scalable and node joining procedures ensure forward secrecy. Having established mutual authentication member SNs delete their authentication and BS's public key. After mutual authentication SNs receives a seed from CH for generation of group key and shared key with CH. With the increase in network size the network wide storage space requirements increase very slowly compared to E-G [60] and C4W [82]. Probability of compromising links remains constant and is almost zero with the increase in the network size, where as for E-G [60]

and C4W [82] it increases with the increase in the network size. Time consumed in establishing shared secure channel with neighbours is more for MAKM when compared with E-G [60] but remains constant. MAKM seems to overtake C4W [82] and IBC-KM [83] for any network size. For Large scale networks MAKM is more energy efficient compared with E-G [60], C4W [82] and IBC-KM (Identity Based Cryptography-Key Management) [83].

Patrick Traynor et al. in [84], proposed pair wise key establishing approach in HWSN. Scheme used a novel unbalanced key pre distribution approach in WSN. Network in HWSN consists of L1 and L2 sensors. L1 is capable of low storage while L2 can support large storage. Scheme considered three different trust models (Backhaul, P2P and P2P with Liberal Trust) for application in balanced and unbalanced key pre-distribution scenario. The Backhaul trust model represents a case when L1 can trust only an L2. P2P works similar to E-G [60] and may use intermediate L1 or L2 while setting up shared-key. In P2P with liberal trust model L1 can trust other neighbouring L1s in indirect key establishment. Analysis of scheme reveals reduced number of hops in indirect keys using non-uniform key pre distribution. With reduced transmission range of transmission both balanced and unbalanced pre distribution cases suffers poor connectivity. With large transmission range unbalanced scheme outperforms balanced scheme. Compromise of L2 node causes more harm in non-uniform pre-distribution scheme.

Patrick Traynor et al. extended their work in [24] from that of [84]. Proposal consider non-uniform scheme. SNs are assigned keying materials on the basis of their capabilities; in HWSN. Proposal examines the probabilities of connectivity, under three trust models (Backhaul, P2P and P2P with Liberal Trust). Proposal suggested three protocols; first is LION for infrastructure less environment. Proposal also considered a protocol for KDC based environment called TIGER. A hybrid of TIGER and LION, i.e., LIGER was also considered. LION implements E-G [60] scheme, TIGER ensures better authentication probability, due to access to KDC and LIGER allows operation to switch between LION and TIGER, and exploit available resources when they are available. Proposal concludes the strength of non-uniform pre-distribution in case of, authentication probability, bootstrapping time and eavesdropping.

F. Kausar's proposal in [85] for HWSNs categorically allocated keying materials on the basis of storage and processing capabilities. H-Sensors assumed the roles of CHs and L-Sensors function as cluster members. Scheme functions as hierarchical scheme with CHs responsible for communications among SNs. SNs are allocated Generation Seeds instead of usable keys. With Non-uniform key distribution of Generation Seeds, and hashing based key chain generation dynamically; scheme is scalable, storage efficient and resistant to node capture attacks. The scheme fails against node replication attacks.

F. Anjum proposed a scheme for WSN in [86], which is location dependent. Scheme introduced a special kind of heterogeneity, by using Anchor Nodes (ANs) which are capable of transmitting in multiple ranges. Each transmission level correspond to distinct nonce, SNs receive multiple nonce from different ANs deployed in controlled manner. Nonce set received by SNs are strictly bound to SNs location. Storage requirements and communication overhead in proposal are extremely low. The impact of varying transmission radius of a transmission level and varying transmission level was investigated and concludes that compromise ratio increases with decrease of number of power levels and vice-versa. Scheme is poorly scalable.

V. Bulusu et al. proposed a key distribution scheme for WSN consisting of both mobile and stationary nodes in [87]. Two distinguished key distribution approaches using a key pool were proposed. In first scheme different sensor networks of stationary nodes are given disjoint key pools. Mobile nodes are given m keys and stationary nodes are given e keys such that $e \ll m$. In

second scheme a large key pool is segmented into multiple sub key pools called segments. Each segment acts as a key pool for different sensor network consisting of stationary nodes. Mobiles nodes are given same number of keys as stationary nodes from aggregated key pool. Mathematical modelling and simulation study of the proposal proved that scheme with segmented key pools performs better than scheme with disjoint key pools. The parameter studied included communication overhead, compromise ratio and storage overhead.

S. Jiang et al. proposed a special kind of heterogeneity of Mobile and Static Sensor nodes in [88]. An issue of re-authentication of Mobile Nodes (MNs) in the clustered WSN was dealt in privacy preserving way. MNs enter the static sensor networks after obtaining initial information from offline BS. The cluster to begin with becomes Home Cluster (HC). MN achieves authentication using information from BS. The movement of MN from HC to other cluster called Care of Cluster (CC) and requires the authentication of both the CH of care of cluster and the MN itself. New cluster knows nothing about MN and thus involvement of HC is exploited and after authentication in new cluster, new cluster becomes HC. The previous HC should not be able to trace the messages sent by the MN. To achieve this concept of Pseudonyms proposed in [89] [90] was used. Besides; BS can always track the location of MN in the deployed static sensor networks.

S. Khan et al. proposed a key management scheme for HWSN in [91]. Scheme used more capable nodes for local certification agency (CA) and less capable as Mobile Nodes (MNs). More capable nodes remain stationary and called Fixed Nodes (FN). The network is assumed to be clustered hierarchical. FNs are provided with six keys and MNs are also pre-deployed with two prime numbers besides two keys namely. Authentication of MNs is established with help of BS. Communication between a pair of MNs is co-ordinated by FNs and generate communication key. Scheme was simulated for storage, communication and computational analysis. In terms of storage scheme proved better than [60] [92]. Also on computational cost; scheme was better than [93], [94].

2.4 Routing Schemes in WSN

WSNs are data centric networks and require that queries must be targeted to an area in deployment zone or data with specific attribute values. Most of the routing schemes proposed in WSNs; either consider WSNs as large data base or digital monitoring/surveillance skin. Considering limited transmission capabilities and absence of global node identifiers in WSNs; most of the routing models in WSN resort to simple flooding. Based on different views on node's roles and deployment models routing may be classified into flat network, hierarchical or location based routing. All these classes are network structure driven. Few routing schemes in WSN may be classified on the basis of QoS parameter qualified by them. These protocols consider different routing criterion. On the basis of brief discussion on routing strategy, we can classify routing schemes proposed in WSN into two major classes, namely network structure oriented routing schemes and operational characteristics driven routing schemes. A brief overview of routing schemes in WSN is presented in this section.

Table 2.3 Classification of Routing Schemes in WSNs

Sr. No.	SUPER-CLASS	SUB-CLASS	MEMBERS
1	Network Structure Driven Routing Schemes	Flat Architecture based Routing	A. Perrig, at al. [50] (SPINs)
			C. Intanagonwiwat et al. [95] (Directed Diffusion)
			D. Braginsky and D. Estrin [96] (Rumor Routing)
			Y. Yao and J. Gehrke [97] (CAUGAR)
		Hierarchical Architecture Driven Routing	W. R. Heinzelman et al. [99] (LEACH)
			S. Lindsey and C. Raghavendra [100] (PEGASIS)
			Ossama Younis and Sonia Fahmy [101] (HEED)
			A. Manjeshwar and D. P. Agarwal [102] (TEEN)
			A. Manjeshwar and D. P. Agarwal [103] (APTEEN)
			W.R. Heinzelman et al. [104]
			J. N. Al-Karaki et al. [105]
			J. N. Al-Karaki et al. [106]
			F. Ye et al. [108] (TTDD)
			R. N. Enam et al. [109]
			H. L. Chen et al. [110]
			H. Lee et al. [111]
		Location Augmented Routing	Y. Xu et al. [112] (GAF)
			Y. Yu et al. [113] (GEAR)
			L. Li and J. Y. Halpern [115] (MECN)
			V. Rodoplu and T. H. Meng [116] (SMECN)
			Zorzi and Rao [117] (GeRaF)
			B. Nath and D. Niculescu [118] (TBF)
			G. Xing et al. [119] (BVGF)
2	Routing Strategy Driven Routing Schemes	Multi-path Routing Protocols	C. Intanagonwiwat et al. [95] (Directed Diffusion)
			X. Mao et al. [120] (Opportunistic Routing)
		Query Driven Routing	C. Intanagonwiwat et al. [95] (Directed Diffusion)
			D. Braginsky and D. Estrin [96] (Rumor Routing)
		Negotiation Based Routing Protocols	A. Perrig et al. [50] (SPINs)
		QoS Based Routing	T. He et al. [121] (SPEED)
			I. F. Akyildiz et al. [124] (SAR)
			K. Akkaya and M. Younis [125]
3	Secure Routing Scheme	Secure Variants of LEACH	B. Parno et al. [25] (LHA-SP)
			J. Ibriq and I. Mahgoub [26] (SHEER)
			M. Tubaishat et al. [127]
			L. B. Oliveria et al. [27] (FLEACH)
			A. C. Ferreira et al. [128] (SLEACH)
			R. Srinath et al. [29] (AC)
			C. Hong-bing et al. [30] (NHRPA)
			L. B. Oliveira et al. [31] (Sec-LEACH)
			Di Wu et al. [32] (SSLEACH)
		Recent Secure Routing Scheme	J. Zhang et al. [129]
			H. Rong-hua et al. [130]
			E. K. Wang et al. [131] (LSDD)
			M. Bohge and W. Trappe [141]

Classification of Routing Protocols {Table 2.3}

1. Network Structure Driven Routing Schemes
    - Flat Architecture based Routing
    - Hierarchical Architecture based Routing
    - Location augmented Routing
2. Routing Strategy Driven Routing Schemes

- Multi-path Oriented Routing Schemes
- Query Driven Routing Schemes
- Negotiation and Meta Data Driven Routing Schemes
- QoS Driven Routing Schemes

3. Secure Routing Schemes
   - LEACH
   - Secure Variants of LEACH
   - Recent Secure Routing Schemes

2.4.1 Network Structure Driven Routing Schemes

The performance characteristics and operational complexity derives the evolution of routing schemes in this class. We present an informative review of routing schemes in this category of routing schemes.

2.4.1.1 Flat Architecture Driven Routing

Multi-hop date forwarding and homogeneous operation of SNs is determining characteristics of routing schemes in this class. SNs are not globally identified due to huge numbers. SNs perform sensing task in cooperative manner. To squeeze out sensed data from network, query should be targeted either to an area or data with specific attribute-value pair. This kind of paradigm is known as Data Centric (DC). BS view network as large data base and launch queries in the network.

A. Perrig, at al. proposed a family of protocols for data collection using negotiations was in [50]. Before any SN can send sensed data to BS, a sequence of meta-data based negotiations is satisfied. Data qualifying a particular query is routed cooperatively using multi-hops in the network. Protocol is able to overcome redundancy through negotiations. Proposal recommends a change in protocol being run, to best suit current energy levels in SNs.

C. Intanagonwiwat et al. proposed a routing scheme called Directed Diffusion (DD)[95]. Similar to SPIN's data is managed in attribute-value pairs. Queries take the form of interest directed towards data source. The interests are flooded into the network and gradients are setup towards interest source. Data may travel through multiple paths and requires in-network processing to remove redundancy en-route; was major contribution of the proposal. DD reports improvements in energy characteristics and network life time.

D. Braginsky and D. Estrin suggested Rumor Routing (RR)[96]; an extension to idea proposed in Directed Diffusion. In order to advertise events of interests RR employs long-lived specialized packets. Performance of RR is better than mere event advertisements based data centric protocol. RR achieves longer network lifetime.

Y. Yao and J. Gehrke proposed a routing scheme called COUGAR in [97] which considered network as data base and proposed a query layer to better address the issue. Similar to other schemes in data centric paradigm, COUGAR imbibed in-network processing to overcome redundancy. Another proposal by Sadagopan et al. in [98] known as ACtive QUery forwarding In sensoR nEtworks (ACQUIRE). ACQUIRE extends database view further by dividing a query into sub-queries. SN on the query path tries to reply query partially from its cached information and then forwards query.

2.4.1.2 Hierarchical Architecture Driven Routing

Hierarchical architecture or clustering approach organizes SNs in multiple layers where each layer is assigned a distinct role. SNs in lower layer performs basic sensing while sensors in upper layer perform sensing and coordinates the data and query routing, from and to, sensors governed by them. Depending upon the organizational requirements nodes may be organized into multiple tiers. A form of routing strategy in which data travels across tiers, refines the quality of data and offers efficiency in operation; is called hierarchical driven routing. Hierarchy of SNs organizes nodes in clusters, where CHs performs organizational activities and cluster members perform data sensing and relaying.

W. R. Heinzelman et al. designed a hierarchical paradigm in WSNs called Low Energy Adaptive Clustering Hierarchy (LEACH) [99]. No global knowledge of network was exploited in LEACH. In LEACH, the cluster-head (CH) nodes perform data aggregation and report data to SINK/BS. Using distributed CH selection, LEACH ensures uniform energy usage across the network. LEACH operates in round and any node can't be selected CH twice in a single round. The massive improvement in network's life time which was measured in terms of event called first node dead was reported. The protocol suffers from energy consumption in reclustering after every round and delay in reporting data to BS.

S. Lindsey and C. Raghavendra, extended the LEACH protocol by using near optimal, chaining based protocol in [100]. Power-Efficient Gathering in Sensor Information Systems (PEGASIS) employs greedy based approach. Data traverse through chain, hop by hop. Nodes send data to neighbours in chain. One of the nodes in chain takes turn to send data to BS. Simulation established uniform energy consumption across the nodes in network in comparison to LEACH.

Ossama Younis and Sonia Fahmy proposed HEED [101], which was another extension to LEACH by incorporating node's energy and degree as decision metrics, as primary and secondary parameters respectively, for CH election and achieved uniform energy usage. It considers the network as graph and operates as multi-hop networks. HEED proposed an adjustable and adaptive transmission level the long distance inter-clustering communication. HEED overcomes the control overheads, uniform clusters in geography aspect and short lifetime of LEACH. HEED results in compact clusters. Secondary parameter is used to break tie due to first parameter. HEED only improved energy characteristics of the network, rather than being a total solution in WSNs.

A. Manjeshwar and D. P. Agarwal, proposed TEEN (Threshold-sensitive Energy Efficient sensor Network protocol), and APTEEN (Adaptive Periodic Threshold-sensitive Energy Efficient sensor Network protocol) in [102] and [103], respectively. With time-critical applications as objective, these protocols were designed. By using hard-threshold to define maximum value of parameter being sensed and using soft-threshold to decide upon data reporting, both TEEN and APTEEN reduced number of transmissions to BS. Threshold based approach prolong network's lifetime and adaptive periodicity and threshold values in APTEEN, energy dissipation was further reduced.

W.R. Heinzelman et al. considered certain application in which aggregates of sensors were required to collectively monitor and track activities, a collection of procedures were proposed in [104].

J. N. Al-Karaki et al. made a proposal in [105] suggested a square cluster based hierarchical routing scheme. CH selection is optimal and utilizes aggregation and in-network processing for removing redundancy, both locally and globally. J. N. Al-Karaki et al. considered a heuristic for aggregation [106] in WSN. Both proposal improved network life-time and energy efficiency.

F. Ye et al. considered Two-Tier Data Dissemination (TTDD) in [108] by assuming that stationary nodes were location aware and mobile sinks collect data from grids located in deployment region. One of the nodes in each grid delivered data on behalf of grid members. Proposal required location awareness equipment on SNs, which is impractical for inexpensive devices.

R. N. Enam et al. proposed a Distributed Uniform Clustering Algorithm for WSNs [109]. Instead of location dependent clustering approach, which causes irregular shaped clusters, a new approach based on virtual grid and sensors transmission range is suggested. Another motivation is suggested from variability of size and number of packets in different clusters. CHs are selected on the basis of proximity to virtual grids and sensors join clusters on the basis of distance from clusters. The overall distribution of the scheme is at least twice better and energy consumption improved by 50%.

H. L. Chen et al. proposed an energy efficient clustering approach with clustering in each round [110]. Each round consists of setup phase and data delivery phase. Setup phase identifies CHs for the current round, in two sub phases. First sub phase identifies CHs in far regions using their remaining energy. Second sub phase identifies CHs in near regions on the basis of residual energy. To reduce collision among contenders in near region, controller used a estimation concept and overcomes the need to collect information on remaining energies. In case of collision, controller resolves by using broadcasting. Energy characteristics of the proposal show improvements over LEACH by 7% and network life time by 49%.

H. Lee et al. proposed an energy efficient clustering based routing algorithm for prolonging network lifetime and better distribution of CHs in deployment area [111]. Based on message success rate and representative paths BS identifies CHs in centralized manner. A reliable multi-hop routing scheme is also proposed that supports inter and intra-cluster communication paradigms. Scheme performs 2 times better than LEACH.

2.4.1.3 Location Augmented Routing

In this class of routing, distance between nodes or location of nodes in network plays a vital role. To obtain the distance between a pair of nodes, RSSI or GPS based localization is preferred. Location augmentation reduces number of transmissions, potential neighbours and uses sleep-awake patterns to decide turns while communicating collected data. Proposals in [107] and [74] investigated many approaches for designing sleep cycles.

Y. Xu et al. proposed Geographic Adaptive Fidelity (GAF) in [112], a location augmented approach and resulted in improved energy efficiency. Deployment area was segmented into multiple virtual grids of small sizes. Nodes used GPS to associate themselves with most close point in virtual grid. GAF adopted sleep-awake cycles for improved performance. GPS is must requirement in GAF.

Y. Yu et al. made a proposal called Geographic and Energy Aware Routing (GEAR) in [113], which was an energy efficient routing scheme. GEAR exploited location information of neighbours to decide upon forwarder towards BS. GEAR obtains fine grained geographic information using GPS. A collection of localized routing schemes were discussed in [114].

L. Li and J. Y. Halpern designed Minimum Energy Communication Network (MECN) [115], a location-augmented protocol for ad hoc networks, which overcame the mobility of SNs and maintained low energy network. The protocol was based upon minimum energy graph. Protocol constructed a SINK rooted spanning tree with minimum energy requirement paths and obtains a sub graph. The sub optimal edges have been removed from network graph. Data transmission through this sub graph (spanning tree) results in minimum energy consumptions. MECN is best when applied to mobile SNs and loose its shine applied to static networks. MECN suffers from a severe battery depletion problem in that case. MECN resulted in scenarios where SNs will always use same SNs for relaying its data to SINK. Network becomes partitioned in that case.

V. Rodoplu and T. H. Meng proposed SMECN [116] which was an improvement to MECN by incorporating a neighbour discovery approach. SNs in question will broadcast neighbour discovery packets at increasing power levels. A reply from neighbours' at a given power level is compared with theoretical neighbour set. If these set were same SN in question will transmit at given power level. Otherwise, SN increment its power level for neighbour discovery packets. This approach helped overcome the limitation of partitioned networks in MECN.

GeRaF by Zorzi and Rao in [117] suggested a dynamic and opportunist selection of forwarder towards SINK. Each node on the relay path towards acts a new source and performs same steps as done by original source. SNs near to SINK are in high priority delivery zone than SNs that are farther. The SNs are not aware of locations and sleep awake patterns of neighbours. SNs know only location of self and SINK. A SN with data must request for channel through RTS and waits for CTS from awake SN in lower level priority. If CTS is received, packet is forwarded towards the node, otherwise RTS is resent for possible reply form comparatively higher priority zone. This process continues as long as packet is not timed out. Timeout for a packet is defined in terms of number of times RTS is sent. After expiry of timeout period packet may be dropped by the SN. As SN has tried multiple times its is said to be best effort routing approach.

B. Nath and D. Niculescu's proposal Trajectory-Based Forwarding (TBF) [118] is applicable for dense and location aware networks. SNs are aware of their locations using some coordinate system. The sender of packets specifies the trajectory instead of SNs on the path towards destination. The trajectory specification is coordinate by coordinate. The path was fixed not the forwarders. Sender node makes greedy decision to forward packet to a next hop neighbour, which is closest to next point on the trajectory. The movement of SNs in the region was well supported using trajectory not the SNs Ids. TBM finds its application in network management.

G. Xing et al. considered Bounded Voronoi Greedy Forwarding (BVGF) [119] which exploited Voronoi diagram. In Voronoi diagram, SNs are location-aware. In BVGF, network was seen as Voronoi diagram with SNs considered as sites. Sender SN always forwarded a packet to a neighbour which resulted in farthest/longest movement of packet towards SINK. The SNs in the regions which were intersected by the segment line joining sender and SINK. The selection of same neighbour as forwarder each time resulted in unbalanced energy consumption among SNs in region.

2.4.2 Routing Strategy Driven Routing Schemes

This section reviews strategy driven routing protocols in WSN. For example, multipath routing schemes uses multipath strategy to improve fault tolerance.

2.4.2.1 Multi-path Routing Protocols

In the dynamic topology of WSN and to share the relay overhead among multiple one-hop neighbours towards destination, several proposals suggested the use of multipath routing strategy.

C. Intanagonwiwat et al. proposed Directed Diffusion in [95], was most suitable example in this class of routing schemes. A travelling query established multiple gradients towards source of query. These gradients are as good as multiple paths along which reply corresponding to a query traversed through network.

X. Mao et al. considered list of forward nodes was identified in [120] for selecting nodes out of one hop neighbours towards a particular destination. Nodes were homogeneous in nature and had fixed transmission range. Each link cost some energy to sender and receiver. With error prone environment each link suffers some error. Node u has selected nodes $\{v_1, v_2, \dots, v_n\}$ as possible set of forwarding nodes. This is treated as priority list and node $v_1$considered to most preferred node. Opportunistically nodes forward message sent by u towards BS. There is possibility of multiple copies of message being forwarded by forwarder nodes because of hidden node problems. Opportunistic routing may suffer from duplicated packets as there is no solution for schedule for nodes forwarding packets via forwarder nodes and security is not considered and thus prone threats.

2.4.2.2 Query Driven Routing

Data can also be obtained by querying the network about an event of interest. Source nodes initiates query and nodes in network replies query fully or partially, from cached information. Directed Diffusion and Rumor Routing discussed above are query driven routing schemes.

2.4.2.3 Negotiation Based Routing Protocols

Meta-data, attribute-value naming or data naming may be used filter and reduce the data volumes being transmitted from within networks to BS. Before; any data can be delivered it has to be negotiated. SPIN's [50] described earlier is suitable example in this class of routing schemes.

2.4.2.4 QoS Based Routing

Routing protocol may consider one or more parameters for qualifying certain requirements. Such protocols are classified in QoS based routing protocols. Parameters like energy efficiency, rekeying messages, frequency of updates, delivery ratio and throughput etc may be considered for QoS.

T. He et al. considered a QoS driven routing protocol for WSNs in [121] named SPEED. SPEED guaranteed end-to-end delay by ensuring that each packet must travel at a specified speed through the network. SPEED [121] used speed of packet as QoS for admission decision. SPEED provided soft speed guarantees. Nodes used geography based decision to find the paths. Protocol was also able to overcome congestion in the network. A special routing module was proposed in SPEED called Stateless Geographic Non-Deterministic forwarding (SGNF). SGNF coordinate with few other modules at the n/w layer. SNs can compute delay incurred in packet delivery. ACK to packet contained delay values and SGNF module at packet sender selects the

node on the basis of delay. If it failed to satisfy speed requirements neighbour's miss ratio is fed to SGNF module. The control overhead of SPEED is less compared to Ad hoc On-Demand Distance Vector (AODV) [122] and Dynamic Source Routing (DSR) [123]. Moreover AODV and DSR lose to SPEED when it comes to end-to-end delay and miss ratio.

I. F. Akyildiz et al. proposed Sequential Assignment Routing (SAR) [124] which was the first QoS based routing protocol in WSNs. The protocol is table driven and each node maintained a table size dictated by network size. The routing decision was based on complex of three factors namely energy resource, packet priority and QoS on each path. Based upon these parameters creates routing tree rooted at one-hop neighbours of SINK. The periodic updates due to node's failure require reconstruction of tree. A periodic update was in place to accommodate any such circumstances. The loss of inconsistency in routing table entries between the nodes upstream and downstream is handled locally without any global involvement of SNs in network. The protocol is improvement from energy efficient protocols and performs better many such proposals. The storage requirement may be a limitation in large sized networks.

K. Akkaya and M. Younis proposed an Energy aware protocol for real-time image traffic in [125]. Scheme considered energy efficient least cost paths. The selected path also meets end-to-end delay criteria. The cost was measured using complex of many parameters. A queuing model was also exploited to support both; real time and non-real time traffic. Protocol used a greedy approach to find the least cost path from the list of paths that meet QoS criteria. The protocol seems to lack on bandwidth sharing aspect among different links.

2.5 Secure Routing Scheme

LEACH is most widely acceptable routing protocols in WSN using homogeneous sensors. Before we present discussion on secure variants of LEACH, we presented a detailed review of LEACH here.

2.5.1 LEACH

W. R. Heinzelman et al. proposed LEACH in [99]. LEACH scheme used WSN with 100 uniformly deployed sensor nodes. LEACH [99] provided one of the most studied clustering techniques. LEACH identified Cluster Heads (CHs) in a network or network component. The protocol classified the network into 2-tier hierarchy. Tier-1 consists of CHs and tier-2 consists of SN. Each CH and member governed by CH forms cluster.

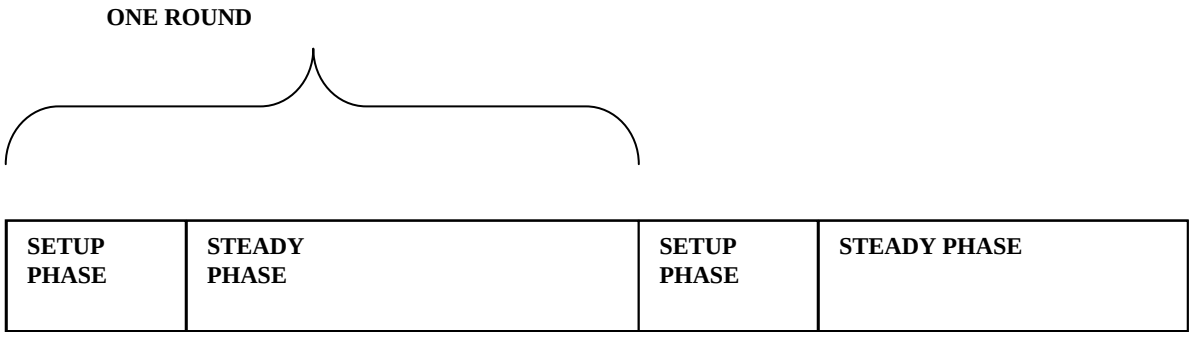


Figure 2.2 Protocol Operations in LEACH

CH receives the data sent from SNs and may aggregates and then transmits them to the BS. CHs communicate with BS on behalf of SNs. This communication pattern has reduced the burden of communication in constrained WSNs. As a result the life-time of the network was improved. Sensor-to-CH signal used Time Division Multiple Access (TDMA). The operation of protocol was mainly divided into repeats of setup and steady state operations with one pair of setup-steady states defining one round of operation. The diagram in Figure 2.2 describes the operations of LEACH in simplest form.

In the setup phase, clusters and CHs are identified. TDMA schedule is dispatched to cluster members. During this phase each node generates a random number between 0 and 1 and if random number's value is smaller than threshold $T(n)$, the node will be a new CH; otherwise, it performs as cluster member.

The value of $T(n)$ is computed as follows:

$$T(n) = \begin{cases} \frac{p}{1-p(r \bmod 1/p)} & if\ n \in G \\ 0 & otherwise, \end{cases} \quad (2.1)$$

where p is the percentage of CHs desired out of total number of nodes. Variable r is the identifier value for current round, and *G* is the set of nodes that have not clustered in the last $1/p$ rounds [99]. After the election of CHs, all the nodes in a network perform the operation as shown in Figure 2.2. The setup phase in Figure 2.2 represents the behaviours of CHs, while the steady phase represents the behaviour of cluster members.

After CHs selection, CHs broadcast their existence in whole the network. SNs can hear these advertisements and select one of the nearest CHs as their own CH. SNs needs to join the corresponding CH by sending cluster join message. After this stage, CHs know all of their members. CH creates and dispatch TDMA schedule for use during steady-state phase in broadcast manner.

As setup phase is performed during each round, SNs spends a lot of energy in Join-Request message to its CH. Moreover CHs has to process all Join-Request received from its member nodes. This results into unavoidable delays and energy overheads.

During next phase called steady-state phase, members in clusters sense and monitor the surroundings. Members send the sensed data to their CH during the time-slot assigned to node as per latest TDMA schedule. SNs may opt to save energy by switching to sleep mode before their turn. Moreover, CH aggregates the received data and transmits it to the BS.

Re-clustering in LEACH adds to undesirable delays and energy overhead. This limitation has been taken care of in Shin's [126] scheme using one-time clustering. The first round is same as in basic LEACH. After first round; a predetermined sequence/order of CH selection is followed. The order to be followed is deployed offline in nodes. The proposal in [126] proposed 35% improvement in network's lifetime against that of LEACH [99].

2.5.2 Secure Variants of LEACH

Several works in WSNs suggested secure variants of popular routing protocol for clustered hierarchical WSNs. This section presents a brief overview of promising solutions.

B. Parno et al. proposed one of the beginning work on secure routing in HWSNs with arbitrary number of levels in hierarchy in [25] under the name LHA-SP. Symmetric key based group key is used for providing confidentiality with assumption that adversary will not be able to

complete tempering jobs during network setup. Network setup time is assumed to be very small compared to time required for tempring bootstrapping in HWSN. LHA-SP overcame the problem of orphan
nodes in WSN.

J. Ibriq and I. Mahgoub proposed a Secure Hierarchical Energy Efficient Routing Protocol (SHEER) to provide secure communication network layer in [26]. With the proposed use of random broadcast and 3-tier hierarchy; life time of network show improvement. Secure routing in SHEER is implemented using HIKES. SHEER uses symmetric key based cryptography. The performance comparison with LEACH using HIKES favors SHEER as a better secure routing scheme.

M. Tubaishat et al. suggested a routing scheme for hierarchical WSNs in [127]. The objective of the proposal was energy efficiency. The generic approach of selecting a safe and secure path towards BS was used with the help of underlying symmetric key management scheme. The proposal also discussed a group key management scheme. Group key is generated from shares contributed by group members. Rotation of CHs role compels to change all kinds of keys in the network and brings network operation to a halt.

L. B. Oliveria et al. [27] proposed to secure LEACH by using symmetric key management (FLEACH). The security of communication between CH-SN is not addressed by FLEACH. FLEACH addresses most common goals of security but fails to address node-capture attacks. Node authentication is performed by BS only. SN-SN level communication is not secured.

A. C. Ferreira et al. proposal SLEACH [28] investigated security provisioning in LEACH protocol for homogeneous wireless sensor networks. SLEACH consider confidentiality, authentication and integrity. SLEACH ensure secure broadcast. To ensure of integrity MAC based on symmetric keys was considered. SLEACH is resilient against many attacks. DoS attack is unaddressed and may result in reducing the throughput of the CH. SLEACH fails to ensure confidentiality. Only outsider attacks were addressed.

R. Srinath et al. considered an approach to secure LEACH named Authentication-Confidentiality (AC) in [29]. It used PKI. The protocol protected against insider attacks and compromised node attack. PKI is not suitable for WSNs and render this proposal energy inefficient scheme to secure WSNs. Similarly a scheme in [128] uses public key base cryptography to provide security in WSNs. Efficient Security Model of Routing (ESMR) protocol in [128] showed very poor energy characteristics in the absence of compromised nods and improved in performance only in the presence of compromised nodes.

C. Hong-bing et al. proposed NHRPA in [30], which was an adaptive routing protocol and adapted protocol operation as per residual energy node density and node distribution and distance to BS. No specific cryptographic scheme was used to secure routing. By virtue of its routing technique NHRPA is more resilient to node compromise attack and was compared with PEGASIS and LEACH. The energy and throughput characteristics of NHRPA are much better than PEGASIS and LEACH in the presence of compromised nodes. NHRPA is adaptive routing scheme and adjust its routing method according to distance between SN and BS. Without use of any cryptographic technique, NHRPA provided secure routing environment with low overhead. Node capture attack is left in-effective in NHRPA.

L. B. Oliveira et al. proposed a secure routing Sec-LEACH [31], based on key management for hierarchical clustered sensor network. The clustering protocol used was LEACH. The proposal addressed communication between a node to CH using pre-distributed random keying. LEACH is vulnerable to attacks like DoS, spoofing, replay attacks, to name a few. Attacks on

CHs may result in sinkhole or selective forwarding attacks. Sec LEACH assigned a key ring of fixed size (m), key IDs and pairwise key shared with BS. Nodes sharing keys with nearest CH, elect its CH. Elected CHs broadcast their key IDs during adv massage and nodes can compute the IDs of keys in the key ring held by CH, using a RNG deployed at each node. Nodes revert with MAC of the join-req & ID of the key used to create MAC. This can be verified at CH and this key in particular will be used to secure link node-CH. A nonce is also sent by CH to avoid any replay attacks. CH-BS communication is protected using pairwise key shared between CH-BS. Scheme also resulted in orphan nodes that do-not share key with CHs. The scheme simulated for different number of CHs, security level and energy consumption and memory usage by keying. Scheme offers trade-off between energy consumption and memory usage. Scheme fails to authenticate broadcast from CHs and could not provide solution against rising compromise ratio with increasing number of compromised nodes.

Di Wu et al. designed SSLEACH [32], which is a secure implementation of LEACH. SSLEACH considered an efficient clustering approach. Using multi-paths CH's chains for communication with BS, energy characteristic and network lifetime of WSN improved reasonably. Key pre distribution and self-localization was the key to success of SSLEACH. SSLEACH effectively prevented compromised nodes from becoming part of routes. SS-LEACH resilient to all attacks that can be launched by compromised nodes.

K. Zhang et al. considered a secure routing solution for LEACH in [33] called RLEACH. By using LEACH like clustering, improved pair-wise keying for handling orphan nodes and hashing based integrity, RLEACH is able to deliver efficient performance with strong resilience against all kind of attacks.

2.5.3 Recent Secure Routing Scheme

J. Zhang et al., proposed a WSN with mobile sink as data collector [129]. Authentication of mobile sink was established using two party mutual authentications, without any intermediation by BS. Secure data delivery between CHs and mobile sink is ensured by using a session key, generated at BS. The resilience of scheme against insider compromise attacks and various other anomalies, established the performance of scheme. Scheme also performs computationally efficient.

H. Rong-hua et al. designed and implemented a scheme for secure data aggregation for an environment poisoned either by sensors which inject false data or compromised/captured aggregating node [130]. A scheme called secure sort group filter was proposed to overcome the false data injection. To protect against modification or alteration of data by captured aggregator is handled using a secure packet delivery mechanism. Scheme is resilient against modifications, low overhead and high accuracy in the aggregation results.

E. K. Wang et al. suggested a Lightweight Secure Directed Diffusion (LSDD) scheme for security provisioning in Directed Diffusion [131]. LSDD is resilient against DoS and sinkhole attack by providing authentication and integrity in routing process. A one way chain based procedure is utilized for key management in LSDD. Compared to other secure variant LSDD improved upon node wise energy consumption due to security provision. Scheme show improvements in average packet delay in lossy environment.

M. Bohge and W. Trappe proposed a secure routing protocol for 3-tier hierarchical ADHOC network in [141]. Scheme uses SPINS building block TESLA for authentication. MAC was employed to ensure integrity of messages being routed. The proposal presented a framework for

authentication especially for application inspired multi-tier networks. Scheme doesn't discuss any approach for prevention against packets by intruders and no protections is presented against eavesdropping.

2.6 Analysis

This section summarises a look on challenges few of which are considered as motive behind the development of this thesis. Most of the solutions we reviewed in this chapter; lacks in defence against node compromise attacks and node replication attacks. With most of secure routing confined to one or two promising proposals, a plenty of opportunities are identified.

In brief, redundancy in data reported by SNs, lack of research works using tiered architectures, global and local time and location synchronization in WSNs, localization of event pr target SN, periodic self-organization, self-configuration and reconfiguration of WSNs, and secure routing are open challenges in routing domain.

In key management schemes passive and active attacks, heterogeneous operation and function of SNs, adversarial conditions due unattended mode of operation, resource aware specialized solutions, need of scalable solutions due to dynamic topology, density and strength of SNs in WSNs, Rekeying and Revocation of compromised SNs, are challenges.

2.7 Summary

This chapter presented a review of key management and routing schemes. In next chapter we considers key management scheme for HWSN, using a small number of H-Sensors and large numbers of L-Sensors.

Chapter 3

Key Management

This chapter presents two key management proposals. Schemes rely upon dynamic generation of usable keys from pre-loaded key information. By considering a variant of binary tree; schemes considered computationally efficient procedure for key generation. Both schemes are scalable and resilient against node level compromise attacks. Section 3.1 presents issue addressed in this chapter. Section 3.2 details a key management scheme based on localization and generating keys. Section 3.3 presents a key management scheme based on localized key matrix. Finally, Section 3.4 summarises the chapter.

3.1 Issues

Key management is an important tool for security provision in any network. Inheriting several characteristics from ad hoc networks, WSNs contrast themselves in many dimensions. Inevitable face off with active and passive attacks in wireless medium, resource limitations due to small sizes, categorical difference in activities related to data collection and network organization are few challenges faced in hostile, unattended operating conditions in WSNs. Physical compromise attacks, node replication attacks and inability to exploit group deployment and huge neighbourhood are few issues for developments in this chapter. We suggest key management schemes as one of the possible solution to vibrant security challenges. Opportunistically one should exploit post deployment location information to make it harder for any kind of compromise attack in WSNs. We have suggested two key management solutions in this chapter. First scheme is based on dynamic generation of keys by SNs after deployment, using HBT on preloaded Generating Keys (GKs). Proposed key generation is location based and provides strong resilience to node compromise and node replication attacks. Second scheme is localized matrix based pair wise key management scheme. The scheme allows each pair of SNs in cluster to establish unique shared pair wise key. Full pair wise keying scheme provided node capture resilience, while localization enhanced resilience against node replication attack. Both scheme are scalable, storage efficient and supports seamless revocation of compromised nodes[1] [2].

---

[1]The major findings of this chapter have been published

- "*A Location Dependent Connectivity Guarantee Key Management Scheme for Heterogeneous Wireless Sensor Networks*," Journal of Advances in Information Technology (JAIT), Vol. 1, No. 3, pp. 105-115, August 2010

[2]The major findings of this chapter have been published

- "*An Inexpensive Key Management Scheme for Heterogeneous Wireless Sensor Networks*," Proceedings of WECON 2009, pp. 302-308, 23rd - 24th October, 2009.

3.2 An Inexpensive Key Management Scheme for HWSN

Key management scheme in this section address two important parameters namely computation and storage efficiency; along with resilience against node compromise attack. To realize computational efficiency we utilized a variant of binary tree called Hash Binary Tree (HBT). Each SN in the network can generate their own HBT as per requirements. Scheme uses non-uniform key pre-distribution for SNs of two different classes namely H-Sensors and L-Sensors in HWSN. Instead of allocating keys from large pool we allocate few GKs to each SN. Usable pair-wise keys can be generated from GKs, by individual SN under the supervision of CH. Although we didn't quantify the percentage of H and L-Sensors in HWSN but we have assigned functional responsibility clearly based upon their capability. The scheme is good improvement from scheme in [132] and [60] while considering storage efficiency, computational complexity and resistance against node compromise attacks. Scheme also ensures authentication of SNs and integrity of messages being transmitted.

3.2.1 Network Elements and Network Setup

Proposal considers a generic HWSN with four different kinds of wireless devices on the basis of functionality; SINK/Base Station (BS), Cluster Head (CH), Anchor Node (AN) and Sensor Nodes (SN).

- **Sensor Node (SN):** HWSNs consist of two classes of sensors, i.e., L-Sensors and H-Sensors. L-Sensors are low cost, low processing power, generic wireless communication devices. Each L-Sensor has limited battery bank, storage capacity, computing facility and short radio transmission range. L-Sensors communicate with their CH, L-Sensors and BS. H-Sensor possesses considerably more resources than the L-Sensor. H-Sensors are capability rich wireless communication device, equipped with powerful batteries, sufficiently large storage, powerful radio antenna and reasonable processing capabilities.
- **Cluster Head (CH):** CH is a role played by H-Sensor. CHs can perform computation intensive operations, organizational activities and have longer radio transmission range than L-Sensors. CHs can communicate with other network directly using single-hop communication and data forwarder for its cluster members and BS.
- **Anchor Nodes (ANs):** ANs are H-Sensors with multiple power level for transmission. ANs are placed at Triangular/Hexagonal points to realize a novel clustering/localization approach. This approach transforms this scheme into location dependent.
- **Sink/Base Station (SINK/BS):** BS is controller of WSN. It is a device with all infrastructures for wired and wireless communication paradigm in WSN. It is a computing facility for simultaneous processing capabilities, multiband and multichannel radio signaling, huge storage capacities and radio transmission range. BS can communicate with every network element in a WSN. BS supervises functioning of WSN from safe a location either at centre or corner of network as specified by the application requirements.

3.2.2 Localization based Network Setup

Network model consider large number of SNs (consisting of large number of L-Sensors and small number of H-Sensors) which are randomly distributed in an area. BS is located at a protected location within network and supervises the network's operation. SNs monitor surrounding environment and relays sensed readings to BS via CH. Each L-Sensor has small

radius of transmission. L-Sensors are static and possess limited battery life. Battery cannot be replaced or charged after deployment. ANs are deployed uniformly and in controlled manner using a manned or unmanned deployment vehicle which is equipped with GPS system to connect with satellite to retrieve exact location for ANs positioning. Using hexagonal deployment of ANs in the deployment field; the network deployment field is roughly into Hexagonal field/zones {Figure 3.1}. In Figure 3.1, the dark lines are transmission radius of ANs placed at triangular points. At higher transmission level ANs transmits in larger transmission radius. Depending upon number of ANs whose transmission ranges are aligned/covering a small area completely, SNs in that area/cell will receive similar and equivalent number of nonce. We consider that at ANs transmits an entirely different nonce at each distinct transmission level. For e.g. SNs in blue cluster (central cluster) receives selected nonce but from all ANs. SNs in triangular cells in blue color receives different set of nonce. SNs in triangular cell closer to AN2 receives N_{24}, N_{25}, N_{26} from AN2, N_{15}, N_{16} from AN1, N_{34}, N_{35}, $N_{36}$from AN3, N_{45}, N_{46} from AN4 , N_{55}, N_{56} from AN5 and N_{65}, N_{66}, from AN6. SNs in the same area/cell receive the same set of nonce thus got grouped into same geographical cell. Moreover SNs which receive same set of nonce are assigned the common cell ID (assumption). ANs are able to transmit at six distinct power levels.

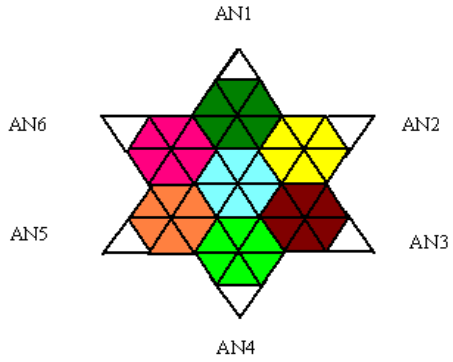


Figure 3.1 Hexagonal Deployments of ANs and Resultant Cells.

3.2.3 Basic Elements of Scheme

Scheme is based on pre-distribution of GKs to SNs nodes from set of GKs. Key pool can be generated from GKs at requirements. Each GK generates a Key Chain (KC). The aggregation of all KCs derivable from GKs defines key pool. Key management scheme relies upon symmetric key mechanism. Before discussing phases in this scheme, we outline some definitions applicable to scheme. Various definitions and terms that are used to describe scheme are:

- **Key Pool (K)** is a large pool of randomly generated symmetric keys.
- **Key Generation Set (G):** G is the set of Generating Keys (GKs). Keys from G are used to define contents of K. The numbers of keys in G are very small as compared to keys in K.
- **Hash Function (HF):** HF satisfies the conditions that the result $HF(x,k)$ has fixed length when the argument x can be of arbitrary length and HF is one way hash function in the sense that produces a y as the image of HF. It is computationally impractical to predict or compute a message x such that $HF(x) = y$. HF is collision free hashing function.
- **Key Chain (KC):** KCs are subset of K (i.e. $KC \subset K$). Each KC is generated from a unique GK. Key chains are derived by applying a sequence of hashing using HF repeatedly on a seed.

Table 3.1 Notation Used

Notations	Description
BS	Base Station
CH	Cluster Head
AN_i	Id of i^{th}Anchor Node
K	A pool of keys
KC_i	i^{th}Key Chain
GK_i	GK of i^{th} key chain and Id of i^{th} GK
L_i	Identity of i^{th} L-Sensor
K_M	Master Key
$K_{L_i,M}$	Authentication Key of SN L_i
N_{ij}	Nonce from AN_iat j^{th} transmission level
G	Set of all the Generating Keys
S	Set of Generation Keys given to SNs
H	Set of Generation Keys given to H-sensor
r	Set of Generation Keys given to L-sensor
C	Total number of Key Chains
K_r	Refresh Key
HF	Hashing Function
$COMM$	Common Broadcast Vector
S^{Local}	Set of Localized Generation Keys obtained at SNs
$S_{L_i}^{Local}$	Set of Localized Generation Keys obtained at SN with Id L_i
GK_i^{Local}	Localized Generating Key with Id i
RN_i	Random nonce from SN with Id L_i
NR_i	Neighbour Set of SN with Id L_i
K_{CH_i}	Cluster key for cluster id CH_i
k	Common setup key

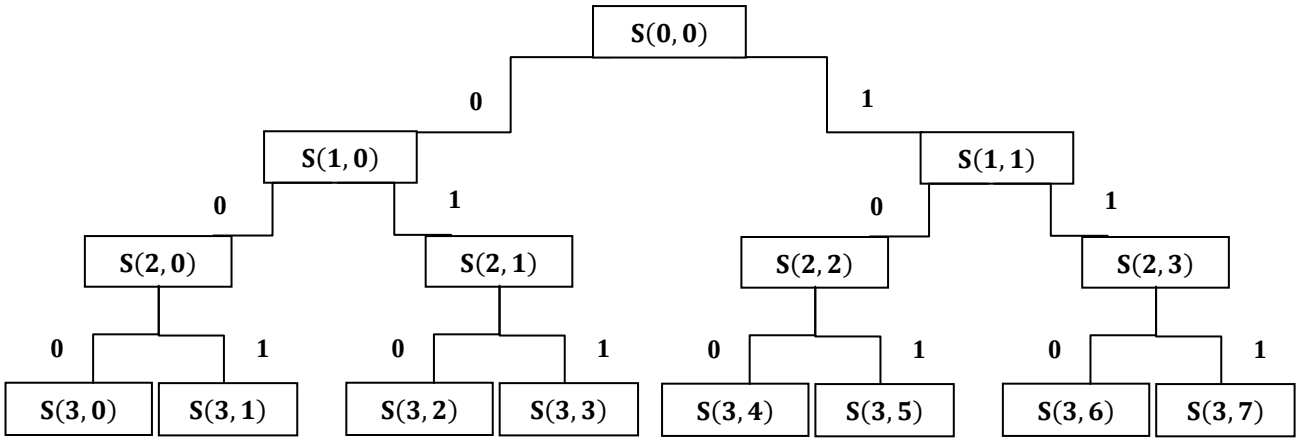


Figure 3.2 Hash Binary Tree

Each KC is represented as HBT rooted at the corresponding GK. Each key chain is uniquely identifiable as KC_i. K consist of all key chains obtainable from GKs in G such that $K = KC_0 \cup KC_1 \cup KC_2 \cup ... \cup KC_{|G|}$.

- **Key Set (**S) is the subset of GKs from G. Each SN is allocated S where cardinality of S depends upon the role of SN.
- **Localized Generating Key Set (S_{Local}):** LGK is defined as set of Localized Generating Keys (LGKs). This is obtained from S after location based modification; and is described ahead. H-Sensors maintain two sets of GKs i.e., preloaded GKs and LGKs. L-Sensor maintain only LGKs.

3.2.4 Key Management Scheme

Key Management scheme proceeds through several phases namely; pre-distribution phase, cluster formation phase, key discovery phase and steady data communication phase.

3.2.4.1 Key Pre-Distribution

The key pre-distribution consists generation of K and assigning subset S from G to each SN in HWSN. The allocated set is called S. To complete this stage we proceed in following steps.

- **Key pool generation:** It refers to generation of all possible keys in K with help of GKs in G. The cardinality of K, i.e., $|K|$and G, i.e., $|G|$ are based on the network size to be supported. Key pool generation can be described in two parts namely formation of GKs and KCs generation. Besides GKs, BS also generates a network wide key (K_M) called Master Key.
- **Formation of GKs:** It is performed by BS. BS generates an HBT {Figure 3.2} by applying HF on randomly selected large seed value. To get left child of a tree node, left shift operation followed by hashing is applied on the tree node. Similarly, right shift followed by hashing is applied to get the right child. These operations are applied to obtain HBT of sufficient height. Leaves of HBT thus obtained at BS serve as GKs. Master Key may be used for generation of Authentication Key by BS and CHs.
- **Formation of KCs:** This step is performed by SNs. For each GK a KC can be generated by using HBT. Further, there are no common keys between any two KCs because of collision free HF i.e. $KC_i \cap KC_j = \phi, \forall i \neq j$. SNs also use HBT to generate KCs{Figure 3.2}. The root of HBT is defined by GK values in set S, for example generation key GK_i in S may perform as root node of HBT. To obtain the j^{th} key in the key chain KC_i, we need to go down to n^{th} level in the HBT rooted at the generation key GK_i. Values n and j are related as $n = log_2(j)$.
- **Key Set Assignment:** In this phase we consider the assignment of GKs, i.e., S from pool of GKs, i.e., G, to each SN, on the basis of their Ids. Node Ids for a node (both H-sensor and L-sensor nodes) is generated using a Pseudo Random Function (PRF). Each L-Sensor and H-Sensor node is allocated and pre loaded with a set S of GKs. For L-Sensor nodes, Id of the L-Sensor is input as seed into a Pseudo Random Number Generator (PRNG) of a large number of periods to obtain r numbers. These r numbers represent indices of GKs in the set G. These marked GKs are assigned to the given SN. This forms its key set S with r GKs. Each L-sensor is also preloaded with an authentication key $K_{L_i,M,}$ which is calculated by

applying HF on K_M and node Id. Similarly, each H-Sensor node is preloaded with H GKs in the manner as described above, such that $H \gg r$. In addition to the GKs, H-Sensors are also loaded with Master Key K_M. SNs obtain common setup key (k) as a part of pre-allocation.

3.2.4.2 Cluster Formation

In this phase geographical clusters are identified and created. All the H-Sensors broadcast HELLO messages to nearby L-Sensor nodes, with some delay. H-Sensors assume the role of CHs. HELLO message contains Id of the H-Sensor. L-Sensors may receive multiple HELLO messages from same or distinct H-Sensors. HELLO message from an H-Sensor having best Received Signal Strength Indicator (RSSI) is replied using HELLO-REPLY. Corresponding H-Sensor is chosen as its CH by an L-Sensor. HELLO messages from other H-Sensors are also stored by the L-Sensors. Those H-Sensors are considered as backup CHs.

3.2.4.3 Key Discovery Phase

Key discovery phase begins after cluster formation. This phase can be described in various parts: neighbourhood discovery, the pair wise shared key discovery and the formation of group key. Pair wise keys for inter-cluster and intra-cluster communications are generated in this section. The pair wise key establishment requires active participation and intermediation by CH of concerned pair of L-Sensors.

Neighbourhood Discovery and GK Localization

This phase starts after formation of clusters. L-Sensors in each cluster identifies neighbour L-Sensors. Firstly, each L-Sensor broadcast HELLO messages for a short range in order to obtain replies from the neighbouring L-Sensors. Neighbour L-Sensors replies with the HELLO-REPLY message. Each L-Sensor node prepares a Neighbour List (NR). L-Sensor nodes sends NRs to their respective CHs. SN also informs the nonce set received from ANs as Nonce Set (NS). NS contains Ids of received nonce (i.e. N_{ij}). Messages contents are explained in Figure 3.3. MAC is created using authentication key. CHs obtain authentication key of concerned L-Sensor using Master Key and node's Id. As a reply CH informs common broadcast vector (COMM) to respective L-Sensor. CH determines the shared key with SN's neighbour and unicast shared GK information to each of its neighbour. This completes authentication of L-Sensor and CH respectively. L-Sensors are directed for generation of LGKs. LGKs are derived from GKs in set S, after hashing operation as $LGK_i = HF(COMM, GK_i)$. Here COMM is common broadcast vector ($COMM \subseteq NS$). Contents of COMM are computed at respective CHs for their cluster members and on the basis of its cluster members. Sent messages are verified for integrity and senders get authenticated. At the end of neighbourhood discovery L-Sensors constructs S^{Local} as a result.

$$L_i \rightarrow CH : L_i||NR_i||NS_i||RN_i||MAC_{K_M,L_i}(L_i||NR_i||NS_i||\ RN_i)$$
$$CH \rightarrow L_i : L_i||NR_i||COMM||RN_i||MAC_{K_M,L_i}(L_i||NR_i||COMM||RN_i)$$
$$LGK_i = HF(COMM, GK_i)$$
$$K_{CH_i} = HF_k(COMM)$$

Figure 3.3 Neighbourhood Discoveries by Sensor Node and generation of LGKs

Pair wise shared key

Pair wise shared key is considered for secure communication between a pair of L-Sensors. Pair-wise key discovery is discussed under two scenarios. One is the pair-wise key discovery between neighbouring L-Sensor nodes and second is for non-neighbours L-Sensor lying in same or different clusters. Pair-wise key discovery key between far away non-neighbouring SNs, occurs whenever required\requested by one of the L-Sensor in pair of L-Sensors.

Pair-wise key between neighbouring SNs

Pair-wise key between neighbouring SNs is mediated by CH of cluster. Let the pair of L-Sensors be L_i and L_j. CH applies Pseudo Random Number Generator (PRNG) on L-Sensor's Ids. This is the same procedure applied by BS before deployment. CH obtains two sets of GKs that had been allocated to the SNs L_i and L_j. Using this information CH can conclude common LGKs shared between L_i and L_j. Diagram in Figure 3.4(a) and 3.4(b) describe whole procedure neatly. In Figure 3.4(a) step 1 represent requests of L_i to CH.

$$L_i \rightarrow CH : L_i||L_j||\ NR_i||RN_i||MAC_{K_M,L_i}(L_i||L_j||NR_i||\ RN_i)$$
$$CH \rightarrow L_i : L_i||L_j||\ GK_i^{Local}||n||RN_i||MAC_{K_M,L_i}(L_i||L_j||GK_i^{Local}||n||\ RN_i)$$
$$CH \rightarrow L_j : L_i||L_j||\ GK_i^{Local}||n||RN_i||MAC_{K_M,L_j}(L_i||L_j||GK_i^{Local}||n||RN_i)$$

Figure 3.4(a) Pair-wise key between neighbours L-Sensor in same cluster

$$L_i \rightarrow CH : L_i||L_j||RN_i||MAC_{K_M,L_i}(L_i||L_j||\ RN_{L_i})$$
$$CH \rightarrow L_j : L_i||L_j||RN_i||MAC_{K_M,L_j}(L_i||L_j||\ RN_i)$$
$$L_j \rightarrow CH : L_i||L_j||RN_j||MAC_{K_M,L_j}(L_i||L_j||RN_j||\ RN_i)$$
$$CH \rightarrow L_i : L_i||L_j||GK_i^{Local}||n||RN_i||MAC_{K_M,L_j}(L_i||L_j||\ GK_i^{Local}||n||\ RN_i)$$
$$CH \rightarrow L_j : L_i||L_j||GK_i^{Local}||n||RN_j||MAC_{K_M,L_i}(L_i||L_j||\ GK_i^{Local}||n||RN_j)$$

Figure 3.4(b) Pair-wise key between non-neighbours L-Sensor in same cluster

Request messages contents include the node Id of two L-Sensors, NR of initiating L-Sensor Random Nonce (RN) along with the Message Authentication Code (MAC). MAC is obtained using Authentication Key and will help to verify the integrity of data and authentication of L-sensor. CH selects the common LGK, i.e., GK_i^{Local} where $GK_i^{Local} \in S_{L_i}^{Local} \cap S_{L_j}^{Local}$. CH

generates a random number n which acts as index in the key chain that can be generated fromGK_i^{Local} using HBT by concerned pair of L-Sensors, i.e., L_i and L_j. In step 2 and 3 CH sends Id of common LGK (GK_i^{Local}) and index value n to L_i and L_j. Step 2 authenticates CH as legitimate node. Step 3 authenticates $L_j$to CH. Nodes $L_i$and L_j can generate key at index n in KC_i on their own and use this key for their lifetime unless it is required to be changed. Shared pair wise key between pair of L-Sensors is established on request; in case L_i and L_j are not neighbours. As long as L_i and L_j belong to same cluster and governed by common CH the procedure described in the Figure 3.4(b) is applicable. The procedures outlined in Figure 3.4 establish authentication of L-Sensors and CH. Integrity of message is verified in each message using MAC.

Absence of common generation key between L-sensors is handled slightly differently. This scenario arises when CH is not able to find a common LGK between intended SN pair. Also we can say that $S_{L_i}^{Local} \cap S_{L_j}^{Local} = \phi$. To handle this situation, CH tries to obtain a common LGK between CH and L_i and a common LGK between CH and L_j. CH then forms a common key ($K_{L_i-L_j}$) between L_i and L_j. CH encrypts it with the shared keys ($K_{CH-L_i}$and K_{CH-L_j}, obtained using HBT from respective common LGKs) between the CH and the L-Sensors ($L_i$and L_j) {Figure 3.5}.

$$L_i \rightarrow CH: L_i||L_j||NR_i||RN_i||MAC_{K_M,L_i}(L_i||L_j||NR_i||RN_i)$$
$$CH \rightarrow L_j: L_i||L_j||GK_i^{Local}||n||RN_i||MAC_{K_M,L_j}(L_i||L_j||GK_i^{Local}||n||RN_i)$$
$$CH \rightarrow L_i: L_i||L_j||GK_i^{Local}||n||RN_i||MAC_{K_M,L_i}(L_i||L_j||GK_i^{Local}||n||RN_i)$$
$$CH \rightarrow L_i: \left(K_{L_i-L_j}\right)_{K_{CH-L_i}}$$
$$CH \rightarrow L_j: \left(K_{L_i-L_j}\right)_{K_{CH-L_j}}$$

Figure 3.5 Pair Wise Key Generation on when Sensor Pair don't share Generating Key

Absence of common generation key between CH and L-sensor i.e., $S_{CH_i}^{Local} \cap S_{L_i}^{Local} = \phi$ and/or $S_{CH_j}^{Local} \cap S_{L_j}^{Local} = \phi$. CHs of respective cluster, CH_i and CH_j generates key K_{CH_i,L_i} and K_{CH_j,L_j} respectively. CHs send these keys to L-Sensors encrypted using respective L-sensor's authentication key. Onwards steps as shown in Figure 3.4(a) or 3.4(b) or 3.5 may be followed.

Group key discovery

Group key plays vital role in WSN and allows member of a group to communicate in multicast manner. Any random SN may float a group. Group need not be coordinated and thus behaves as on-air group. Let one of the L-Sensor want to float a group. L-Sensor must now request its CH to broadcast Id of LGK's and index in the corresponding KC which can be generated from concerned LGK. In case other nodes want to enter into group and to have a secure communication session in local geography, must possess the identified LGK. SNs possessing the concerned LGK may enter group without any organizational hustle. We don't consider

authentication of the group members. The members of group may be CH and cluster members. Groups will always stay within clusters and each SN may be part of multiple overlapping groups.

3.2.4.4 Inter-cluster communication (3-hop Communication)

Inter cluster communication is required either when one L-Sensor communicates with a remote L-Sensor via corresponding CHs or when two CHs enter into a communication due to various security reasons. CH-CH communication is established using preloaded GKs. Communication between two CHs is realized using shared preloaded GK discovery in S; followed by pair wise key generation in the key chain derivable from corresponding shared GK. A CH can obtain the contents of S for other CH, using PRNG. There is very high probability of finding shared GK between CHs. The reason is attributed to high cardinality of set S in CHs. The L-Sensor pair in two clusters uses LGKs in respective clusters. Due to threats from adversary and to mitigate node replication outside cluster, L-Sensors maintain only S^{Local}. In this communication end-to-end encryption cannot be considered. The communication is 3-hop communication i.e., $L_i - CH_i$, $CH_i - CH_j$ and $CH_j - L_j$. Cluster head CH_i and L_i enter into secure communication using shared LGKs from their S^{Local} set. Both CH_i (CH for the node L_i) and CH_j (CH for the node L_j) may use common GK from preloaded GKs (i.e. S). Now CH_i and L_i or L_j and CH_j may enter in secure communication {Figure 3.6}.

$$L_i \rightarrow CH_i: L_i||L_j||\ RN_i||MAC_{K_M,L_i}(L_i||L_j||\ RN_i)$$
$$CH_i \rightarrow L_i: L_i||L_j||\ GK_m^{Local}||n||RN_i||MAC_{K_M,L_i}(L_i||L_j||GK_m^{Local}||n||\ RN_i)$$
$$CH_i \rightarrow CH_j: CH_i||CH_j||L_i||L_j||\ GK_t||n||RN_i||MAC_{K_M,CH_j}(CH_i||CH_j||L_i||L_j||GK_t||n||\ RN_i)$$
$$CH_j \rightarrow L_j: L_i||L_j||\ GK_m^{Local}||n||RN_i||MAC_{K_M,L_j}(L_i||L_j||GK_m^{Local}||n||\ RN_i)$$

Figure 3.6 Pair Wise Key Establishment during Inter Cluster Communication

3.2.4.5 Addition of New Sensor Nodes

In WSN there can be a requirement to enhance the established network by considering addition of the new SNs. In this scheme new SNs can be deployed in existing networks. It must be ensured that the newly joined SN is not an adversary node. Newly deployed SN discovers its neighbours using process outlined in Section 3.2.4.3. Newly deployed SN chooses its CH using RSSI value as selection parameter. SN must send the request message to the chosen CH.

$$L_{new} \rightarrow CH: L_{new} \parallel S_{new} \parallel RN_{new} \parallel NR_{new} \parallel MAC_{K_M,L_{new}}(L_{new} \parallel RN_{new} \parallel S_{new} \parallel NR_{new})$$
$$CH \rightarrow L_{new}: L_{new} \parallel COMM \parallel RN_{new} \parallel NR_{new} \parallel MAC_{K_M,L_{new}}(L_{new} \parallel COMM \parallel RN_{new} \parallel S_{new})$$

Figure 3.7 New L-Sensor Joining existing WSN

CH determines GKs set, i.e., S pre-deployed in new SN; using PRNG. If contents in S_{new} match the expected ones SNs is verified for authentication. If MAC is found correct integrity of message is established. Equations in Figure 3.7 describes the format of request by new SN, sent

to CH. SN is allowed to join after successful authentication by CH. CH determines the shared key with new SN's neighbour and unicast shared GK information to each of its neighbour and new SN. CH also directs new L-Sensor to generate LGKs from S to obtain S^{Local}.

3.2.4.6 Revocation and Refreshing Process

Revocation process is the process of reformation of keys whenever any compromised L-Sensor is detected in the network. BS is assumed to keep an eye over the whole network and if it detects that a node has been captured by an adversary then it informs the CH to revoke the keys. The scale of revocation depends upon extent of problem. Single cluster issue can be handled by corresponding CH under supervision of BS. In this scenario, CH sends a message to all its cluster members for performing fresh localization of LGKs. CHs obtain a new COMM (i.e. $COMM^{new}$) for its cluster using random seed and old value of COMM ($COMM^{new} = HF(COMM^{old}, Seed)$). CHs unicasts $COMM^{new}$ to each of its cluster member by using authentication key for encryption. CH directs its cluster members to update K_{CH_i} (cluster key). SNs update their LGKs and K_{CH_i} using eqn. {3.1 and 3.2}.

$$LGK_i^{new} = HF(LGK_i, COMM^{new}) \quad (3.1)$$

$$K_{CH_i}^{new} = HF(K_{CH_i}, COMM^{new}) \quad (3.2)$$

Network level node revocation is performed using new broadcast from one or more ANs. Revoked SNs will not be able to participate in clustering and GK localization process. Similarly network level key refreshing is performed by using new broadcast from ANs and repeat all post deployment activities.

3.2.5 Performance and Security Evaluation

We have evaluated this scheme on few performance and security parameters. These include computational complexity, storage requirement, node compromise attack, node replication attack, connectivity ratio and compromise ratio.

3.2.5.1 Performance Evaluation

Performance evaluation is evaluated for computational complexity and storage requirements in scheme.

Computational Complexity

We have defined computational complexity in terms of number of hash operations performed to generate key at given index in the key chains derivable from GKs. We have compared the computational complexity against a proposal in [132]. It is shown that the proposed scheme proves to be very efficient in terms of computational complexity. Graph in Figure 3.8 shows that the number of hash operations required in our proposal are extremely low in comparison to scheme in [132]. The improvement in our proposal is attributed to the use of HBT. To find the j^{th} key in a key chain KC, we need to go to n^{th} level in the binary tree, such that inequality; $2^{n-1} > j \geq 2^n$ holds.

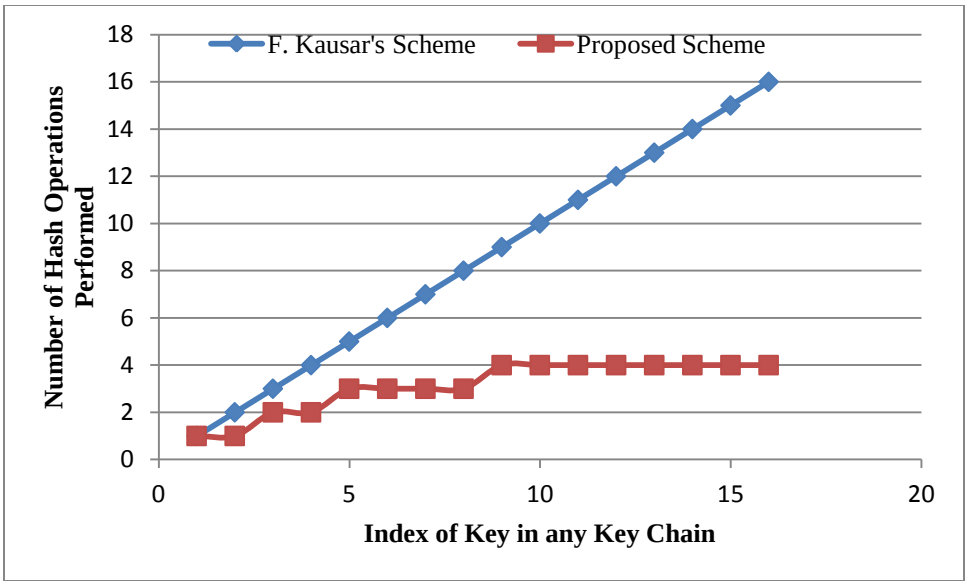


Figure 3.8 Comparison of Computational Efficiency in terms of Hashing Operations

Thus; the number of hash operations required to find the j^{th} key is n, whereas in [132], the number of hash operations needed to generate j^{th} key in the key chain is equal to j. Roughly we can say that $n = log_2(j)$. Longer key chain ensures more randomness in selection of shared key. This result in higher resilience towards various security attacks. As shown above {Figure 3.8}, the number of hash operations required for generation of a large key chain is exceptionally smaller, thus it provides very less complexity even if we want to increase randomness of keys to provide higher security level, by increasing the key chain length. Scheme is a novel proposal in the light of computational efficiency and increasing randomness for key selection.

Storage Efficiency

Firstly, we will evaluate the probability of having common shared generation key between two L-Sensors as well as between an L-Sensor and H-Sensor. One important observation while studying storage requirement is that if key set size is fixed in the network and then varying sizes of G affects the connectivity in the network. Increasing the size of G reduces the probability of sharing a key between pair of nodes. Similarly, decreasing the size of G increases the probability of key sharing between SNs. We want to find the largest value of G such that the probability of number of common generation key between any two sensors is greater than some constant ($p \leq 1$). Second important observation is that there exist a relationship between the key pool size and the probability of a link being compromised. It can be stated that on increasing the key pool size, the probability of a randomly chosen link being compromised is decreased, such that the compromised node is not at either end of the chosen link. If we assume that the probability of sharing of GK key is 1, i.e., there should be at least one common GK between two nodes then the probability of not compromising an un-captured link is expressed in eqn. {3.3}.

$$\bar{X} = 1 - \frac{G!}{r! \times (G-r)} \times \frac{G!}{H! \times (G-H)} \tag{3.3}$$

Quantity X represents the probability that there is at least one common generation key between nodes. G represents total number of KCs or total number of GKs. Using eqn. {3.3} we can compute the size of G for fixed sizes of S for L-Sensors and H-Sensors. For H=100 and r=2 it can be concluded that quantity X, has same value, i.e., the probability of sharing at least one key is same as with 100 keys in the basic random key pre-distribution scheme [60].

3.2.5.2 Security Evaluation

We consider compromise ratio, resilience to node capture and node replication attacks for security evaluations in this scheme.

Compromise Ratio

We compared the proposed scheme against the basic scheme [60] in terms of security. The proposed scheme provides a very high level of security when we evaluate the protocol against compromised node attack. The probability of a key not residing in a sensor node is given by $1 - r/G$. Therefore the probability of a key not present in n compromised nodes can be written as $(1 - r/G)^n$. The probability of total number of compromised keys when n nodes are compromised can be given by $\bar{t} = 1 - (1 - r/G)^n$.

Node Capture and Node Replication Attack

Node Capture and Node Replication Attack is most severe attack in WSNs due to its deployment in hostile and unattended environments. Captured nodes may be moved somewhere else within same cluster or outside the cluster. The relocation of captured node within same cluster offers resistance as SNs has to request CH with neighbour lists. Any change in NR will be detected by CH and node revocation may be initiated. Replication of captured node outside the cluster is harmless as SN can't localize its GKs with respect to new locations. Any request as pretending new node will not result in major deterioration because localization needs preloaded GKs. Localization has improved resilience against node capture attack.

3.2.6 Discussion

In this proposal we presented a location dependent, storage and computationally efficient key management scheme for HWSNs. A small set of keys is generated and assigned to the SNs before deployment of WSN. Proposed scheme allows secure communication by using pair-wise keys between every pair of nodes. Localization of generation materials after deployment improved resilience against node level physical attacks. Scheme supports efficient revocation of keys, refreshing of keys and addition of new SNs. The analysis of the scheme against schemes in [60] and [132] shows that the proposed scheme is very efficient in terms of computational complexity. The results show that the scheme requires extremely less number of hash operations as compared to that required in [132]. The scheme is efficient in terms of storage requirements at L-Sensor as compared to basic random pre-distributed key management in [60]. Proposed scheme offers more resistance to node capture and node replication attacks than schemes in [60] and [132].

3.3 A Location Dependent Connectivity Guarantee Key Management Scheme for HWSN (LOCK)

Another key management scheme considered in this chapter is LOcation dependent Connectivity guarantee Key management (LOCK) scheme for hierarchical HWSN without using deployment knowledge. Location based approach coupled with matrix based scheme significantly reduced the number of keys stored at each SN. LOCK is a pair-wise key management scheme and ensures that every pair of SNs in a cluster can communicate without active intermediation by CH. CHs organize geographical clusters. Scheme supports pair-wise, group wise and cluster key among SNs. Similar to proposal in Section 3.1 LOCK also uses ANs based localization and is an improvement over scheme in Section 3.1, in the sense that every pair of SNs can establish pair-wise key without intermediation of CHs. LOCK reduces storage overhead and communication overhead on CHs in the presence of full pair-wise key connectivity. Similar to earlier scheme node compromise and node replication or node usage outside its location are rendered in-effective. Scheme is based on matrix of keys and proved to support large network using smallest storage overhead as compared to existing key management schemes.

3.3.1 Network Elements and Network Setup

We considered a generic HWSN with four different kinds of wireless devices on the basis of their functionality; SINK/Base Station (BS), Cluster Head (CH), Anchor Node (AN) and Sensor Nodes (SN). Detail of network elements is given in Section 3.1.1.

3.3.2 Clustering Approach

Clustering approach is given in Section 3.1.2. Besides other activities CH informs $2e$ values to each cluster member.

3.3.3 LOCK

LOCK suggested an efficient approach for setting up pair-wise shared but unique keys between each pair of communicating sensors. In contrast to several random pre-distribution keying schemes LOCK rely upon a semi random pre-distribution scheme. LOCK guarantees connectivity between every pair of SNs by dynamic generation of key matrix from small set of generating keys. LOCK assumes that each node in network is preloaded with network wide common generating keys. Further, localization of network wide common generating keys limits the usability of keys within specified zones in deployment area. Node capture attack in pre-distribution approaches is most deteriorating attack. The reason for this may be attributed to multi-node assignment of same key in the network. Pre-distribution scheme can't survive if same key is not assigned to at least one node in each sensor's neighbourhood. What may feel a boon for achievement of high network connectivity in pre-distribution approach; is leading cause of biggest threat in WSNs. Usage of same keys in multiple sensors of network leaves network prone to compromise attack. The extent of compromise attack depends upon the extent of reuse. Connectivity and compromise ratio are tradeoffs in pre-distribution schemes. We augment key pre-distribution with post deployment location information. Localization with pseudo random

keying scheme adds to high resilience against node capture, node replication and eavesdropping. In LOCK scheme we proceed through two phases,

- Setup keys assignment phase,
- Location dependent Keys Generation Phase

Location dependent key generation phase includes the generation of group key, cluster key and pair-wise key between SNs. An off-line authority called BS is in-charge of the initialization in LOCK.

3.3.3.1 Setup Key Assignment Phase

BS is responsible for assigning setup key to each SN. Setup key pre-loaded into SNs before deployment. Each SN is assigned same set of network wide common setup keys. Each SN is assigned a unique Id; generated by BS using PRF. Besides this each SN is also assigned Ids of two CHs which are assigned the part of the information required to generate pair wise key with its post deployment CH. BS also generates a key pool of symmetric keys. BS assigns a unique key from key pool to each SN before deployment. This is known as direct key (semantic key) and is the shared pair-wise key between SN and BS (K_{SN_i-BS}). Direct key is used to exchange encrypted data between SN and BS. Besides these a common key k is preloaded as a common setup key into the memory of each SN.

To achieve semi random pre-distribution, network wide common keys are arranged as diagonal of a key matrix M. Each sensor is assigned $2e$ values, of which first e values denote row numbers and remaining e values denote column numbers. SNs can generate contents of e rows and e columns using an extended HBT {Figure 3.2} called Dual skewed Hash Binary Tree (DHBT) {Figure 3.10}. Each row of matrix is a single DHBT, generated from diagonal value. Each key matrix is thus represented as a collection of DHBTs. In a $m \times m$ key matrix, each sensor maintains only m values, in the form of diagonal elements. For convenience, we use R_i and C_j such that$(i, j = 1,2, \dots, m)$, to denote i^{th} row and the j^{th} column respectively, in key matrix M, respectively. Before we can generate the complete rows of the matrix we need to localize key matrix with respect to SN's Location. CHs compute the common content of the ANs broadcast received by all SNs in its cluster. CHs informs the common received broadcast vector (COMM in Section 3.1.3.2) to each SN in its cluster using a plain broadcast message or by encrypting using cluster key{Section 3.3.3.2}.

$$k_{i,i}^{j} = HF\left(COMM_j, k_{i,i}\right) \quad (3.4)$$

Eqn. {3.4} is used to localize the diagonal elements in M, where $k_{i,i}^{j}$ is the localized diagonal element of i^{th} row and i^{th}column with respect to location of j^{th} CH. $COMM_j$is defined as COMM for j^{th} cluster and is computed as $COMM_j = N_{ij} \oplus N_{jk} \oplus \dots$. In this equation N_{ij}, N_{jk} etcetera represents nonce received by all the SN in j^{th}cluster. Now each SN is provided with localized diagonal values of M. Next we use Dual skewed Hash Binary Tree (DHBT). Matrix M can be generated by applying DHBT. This is novel alternative against the use of e rows and e columns and storage overhead of $2 \times e \times m$ values per SN in [133]. This is where LOCK performs better in terms of memory requirements as it requires only m diagonal values in the memory. LOCK performs even better for higher values of e. For higher values of e saving in memory requirements is even higher. Any two SNs share at least $2e^2$ value in their memories. Setup key assignment which is deployment knowledge independent but location dependent, guarantees the connectivity between any two nodes in the network. Compared to scheme

proposed in [132] and scheme in Section 3.1, LOCK ensures 100 percent connectivity among nodes of HWSN even without storing complete key matrix.

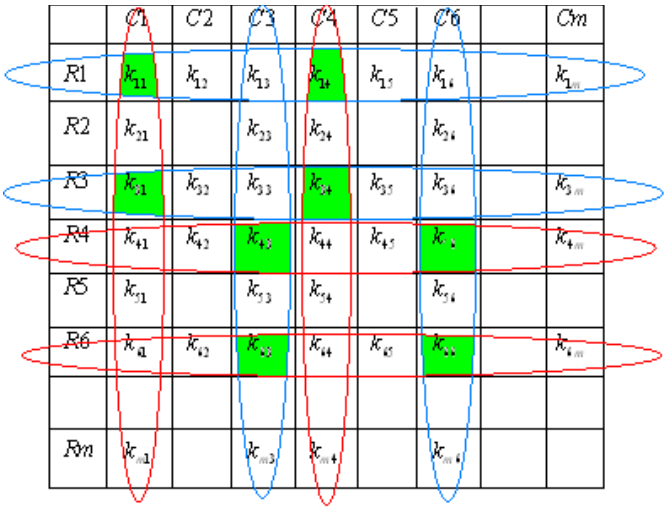


Figure 3.9 Setup key Matrix and Keys Assignment

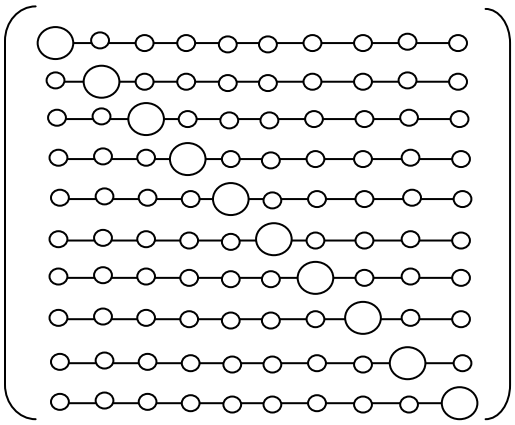


Figure 3.10 Dual Skewed Hash Binary Tree Representation of Key Matrix

3.3.3.2 Location Dependent Keys Generation Phase

During this phase LOCK executes procedures for generation of Inter Cluster, Administrative keys, Cluster key and pair-wise symmetric keys.

Inter Cluster Key ($K_{CH_i-CH_j}$) is established between a pair of CHs. Let CH_i and CH_j are the participating CHs. Both CH_i and CH_j can generate the pair-wise key between them using eqn.

{3.5} where $sh_1$and sh_2 are shares exchanged between participating for generation of the symmetric key where k is pre-loaded common setup key.

$$K_{CH_A-CH_B} = HF_k(sh_1 \oplus sh_2) \quad (3.5)$$

CHs will use inter-cluster key for providing a secure channel between corresponding CHs, when any SN requires communication with some remote SN.

Administrative Key ($K_{CH_i-SN_j}$): Administrative key is preloaded in each SN. CH has to construct this pair wise symmetric key using the information stored in SNs. Each SN is provided with Ids of two CHs. SN send these Ids to its CH. CH will receives the shares k_1 and k_2 from two CHs whose Ids is sent to CH by SN. Eqn. {3.6} is used to set up $K_{CH_i-SN_j}$, where k is pre-loaded common set up key.

$$K_{CH_i-SN_j} = HF_k(k_1 \oplus k_2) \quad (3.6)$$

Pair-wise Key Generation Phase

In this phase we establish pair-wise key to provide secure the communication between two neighboring SNs in a cluster. For secure communications between any pair of SNs within a cluster, a pair-wise key needs to be established. We complete this process in three steps. Let L_i and L_j denote two SNs. In first step, L_i randomly selects $l(1 < l < e)$rows and $l(1 < l < e)$ column's Ids from stored $2e$ values. Now L_i generate a random nonce RN_i. Then, node L_i broadcast a handshaking message including its Id, i.e., L_i, RN_i and indices of selected rows and columns to L_j using k for encrypting the handshaking message. Handshaking is followed by pair wise key setup. Consider an example that L_i stores 3^{rd} and 6^{th} column and $1^{st}$and 4^{th}row indices of key matrix M in its memory and L_j stores $1^{st}$and 4^{th} column's, and 3^{rd} and 6^{th}row's indices of key matrix M. Now L_i broadcasts a handshaking message $\{L_i, R_1, R_4, C_3, C_6, RN_i\}$ to node L_j. Similarly, L_j generates a random nonce RN_i, and broadcasts $\{L_j, R_3, R_6, C_1, C_4, RN_j\}$ to node L_i. Nodes exchange random nonce during handshaking. Node pair can identify shared keys indices and thus generates shared keys individually at their sites {Figure 3.9}, i.e., $\left(k^j_{1,1}, k^j_{1,4}, k^j_{3,3}\ k^j_{6,3}, k^j_{4,1}, k^j_{4,4}, k^j_{3,6}, k^j_{6,6}\right)$. Now, nodes L_i and L_j can compute a pair-wise key between them by eqn. {3.7}:

$$pk_{L_i-L_j} = RN_i \oplus k^j_{1,1} \oplus k^j_{1,4} \oplus k^j_{3,3} \oplus k^j_{4,1} \oplus k^j_{4,4} \oplus k^j_{3,6} \oplus k^j_{6,6} \oplus RN_j \quad (3.7)$$

A pair of SNs can set up shared pair wise key without CHs or third node participation. LOCK can survive without using path-key establishment. Due to this approach LOCK exhibit low communication overhead and reduced exposure of keying process. Pair-wise key is outcome of randomness of nonce, randomness of row and column assignment and deterministic key matches in row-column cross-points. Uniqueness of pair-wise keys between every pair of sensors is guaranteed. Single or multiple node capture attack doesn't expose pair-wise keys of uncompromised links. Further customizing the diagonal elements to a cluster results in

strengthening the resilience against node capture attack; same node or replicated node may never be used outside the cluster.

Geographical Group Key Generation (k_{GoG}): This key is derived by all SNs lying in the same geographical cell. This group of neighbours can construct a group keyk_{GoG} using the broadcast received from ANs and membership information computed at CHs. SNs in the identified cell of a cluster proceed to set up k_{GoG} as follows:

$$k_{GoG} = H_{K_{CH_i}}(N_{11}, N_{12}, \dots N_{ij}, \dots, list\_of\_IDs) \tag{3.8}$$

In eqn. {3.8} N_{ij}'s are nonce broadcast from AN_i and transmitting at j^{th} power or transmission level, $list\_of\_IDs$ is unique value obtained as a result of X-OR operation on the IDs of the nodes residing in a cell. Value of $list\_of\_IDs$ can be computed as in eqn. {3.9}

$$list\_of\_IDs = L_1^i \oplus L_2^i \oplus \dots \oplus L_n^i \tag{3.9}$$

In eqn. {3.9} L_j^i is the j^{th} Node's Id in i^{th}cell. $list\_of\_IDs$ is securely sent to the SNs using administrative key, i.e., $K_{CH_i-SN_j}$.

Cluster Key Generation (K_{CH_i}) is performed by CHs using eqn. {3.10}

$$K_{CH_i} = H_k(COMM_i) \tag{3.10}$$

Here $COMM_i = N_{ij} \oplus N_{jk} \oplus \dots$. In this equation N_{ij}, N_{jk} etcetera represents nonce shared by all the SN in the i^{th}cluster. Common key k is pre deployed in SNs as described earlier. Successive uses of k is replaced by K_{CH_i} and k can be purged after bootstrapping is over. In case CHs requires revoking a SN; CHs compute $COMM_i^{new}$ and unicast it to other members of cluster by using $K_{CH_i-SN_j}$for encryption. This will revoke the target SN.

3.3.4 Security Analysis and Performance Evaluation

We analyze the security property and performance over vital parameters in this section. Simulation of scheme was performed by using programs developed in MATLAB, on Windows platform. Hardware platform used was Pentium 4, 3GHz and 512MB RAM.

3.3.4.1 Security Analysis

Security analysis presents resilience against node capture attacks, node replication attacks and compromise ratio.

Node Capture and Replication Attack

Node Capture and Replication Attack is most annoying attack in WSNs. It is due to the unattended mode of operation in hostile environments. Some SNs could be physically captured

by an adversary after initialization period. Captured node may be used inside or outside the cluster and may even replicate the captured node. Node replication can't be prevented in WSNS, but its deteriorating effects can be reduced or neutralized. In [60] and [11] pair-wise keys are identified and used from only preloaded key ring. Replication of captured node and deployment of replicates in WSNs leaves networks compromised.

In LOCK the keys are not same throughout the operational life of the SNs. Cluster key is updated as and when needed using most recent broadcast from the ANs. Geographical group key is updated using new and remaining list of nodes from cluster head and new broadcast from the ANs. Diagonal entries of the matrix are customized with respect to the corresponding cluster's location using the common part of the broadcast received by the nodes in the cluster head's coverage range. Uniqueness of pair-wise key may be used to establish mutual authentication of pair of sensors during steady phase. Capture of single SN affects the integrity of single SN. Communication between other pair of SNs is completely protected. Consequently node capture and node replication attack are handled graciously by LOCK.

Compromise Ratio

Compromise ratio is defined as percentage of communications exposed between non-captured [60]. Considering simulations for an environment with key pool size K=10000, key ring =200 keys, neighbourhood degree = 60, number of nodes =1000, for simulation we conclude that more than 30% communication in uncompromised node pairs is compromised if 200 nodes are captured. Increasing the number of captured nodes to 500 leads compromise of 60% uncompromised links.

In LOCK, localization of diagonal elements and unique pair-wise keys between each pair of nodes reduces the impact of compromise. In a network of n nodes, capturing one node exposes the communication in links with compromised node as one of the two ends. Any other communication involving only uncompromised sensors is safe from compromise. Compromise of one node affects n communications of captured node. Second node's capture affects $n-1$ more communications. With capture of m nodes $m!$ communications in total are exposed.

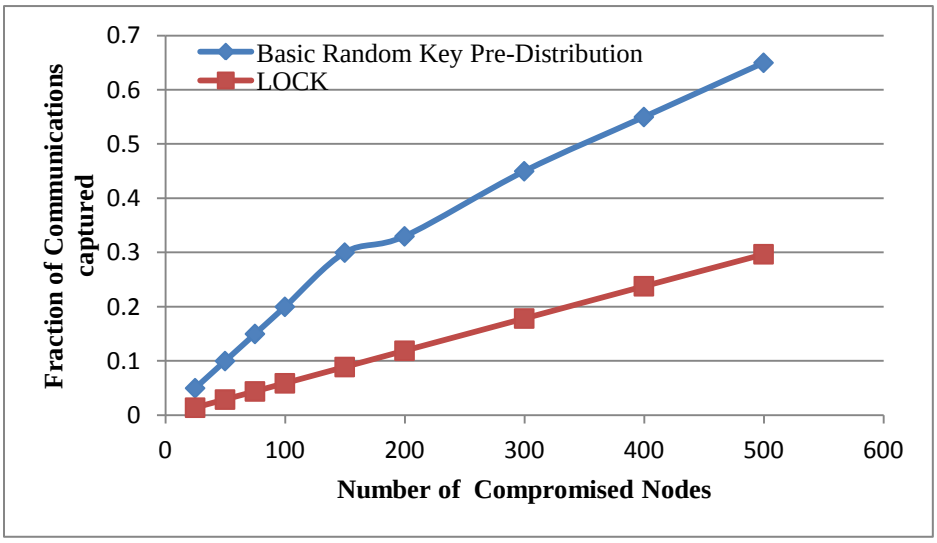


Figure 3.11 Fractions of Compromised Communications

To compromise 30% of total communication more than 50% of total number of sensors must be captured. To surprise, links between uncompromised sensors remains intact. Figure 3.11 plots the compromise ratio.

3.3.4.2 Performance Study

In this section we will discuss scheme's performance using network size, storage efficiency, network connectivity and communication overhead.

Network Size Support

Figure 3.12 shows the LOCK cluster size supported. As a result of localization the network size supported is much larger than any existing key management scheme. Scheme is applicable to large sensor networks without any modification. If we assume the number of clusters is 7 and the size of the network is almost 7 times of cluster, the cluster size supported {Figure 3.12}. In LOCK, the maximum supported cluster size exponentially increases when the key ring size increases linearly. Think of the network size that can be supported in LOCK. In LOCK the same matrix got localized for each cluster and the equation which earlier denoted the size of network, represent the size of cluster.

Storage Efficiency

Random key pre-distribution key management [60] scheme can support a network of size 200 nodes using 50 keys per node for 5 to 9 connectivity. Q-composite [11] key distribution is not much better than Random key pre-distribution key management scheme. In our proposal we store only diagonal entries of key matrix and reduced memory requirements. Compared to matrix based schemes as in [133], storage requirements in LOCK are only 25%.

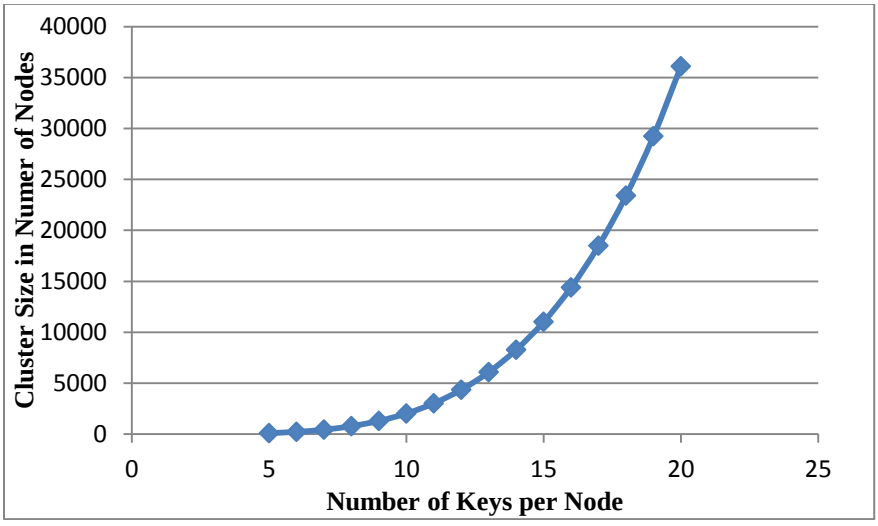


Figure 3.12 Cluster Size Support in LOCK

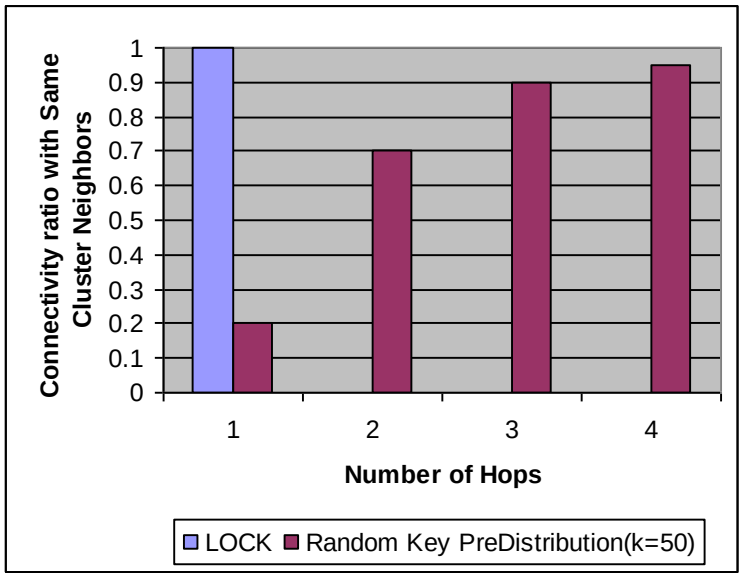


Figure 3.13 Network Connectivity vs. Number of hops needed for pair wise keys

Network Connectivity

Key ring size determines the network connectivity in [60] [11]. Only 20% nodes can be reached in one-hop in [60]. Remaining nodes can be reached by using two or more hopes. Figure 3.13 compares the network connectivity in LOCK (ring size is irrelevant) and random key pre-distribution scheme in [60].

Communication Overhead

Communication overhead is the measure of energy efficiency in key management scheme. Basic pre-distribution scheme in [60] may require more than one-hop to reach 80% of the nodes before a direct key could be established. This scenario increases the communication overhead by large amount. In LOCK any neighbour or non-neighbour sensor pair can connect after direct handshaking without any need of path key setup.

3.3.5 Discussion

In LOCK we are able to highlight the effect of heterogeneity on the performance of key management scheme in WSNs. We considered a special kind of heterogeneity, i.e., the number of power levels and were able to draw the effect on performance in terms of memory requirements and size of the network supported by LOCK. Average number of nuances/keys received depend not only the maximum transmission radius but also on number of power levels. SNs can setup a unique pair wise key without any intermediation by CHs. This affects the number of messages exchanged for key setup. Communication overhead in LOCK is much lower than the scheme in [60] and [61]. Ability to setup direct key in one-hop by all SNs has improved network connectivity compared to schemes in [60] [11]. As a result LOCK doesn't need path key

setup. Storage requirement in LOCK is considerably low due to dynamic key generation during key setup. Compared to scheme in [133] LOCK requires only 25% storage requirement. Similarly, schemes in [60] and [61] need about 200 keys per node to achieve considerable network connectivity.

3.5 Summary

In this chapter we suggested two location dependent key management schemes. First scheme is storage efficient scheme with reasonable connectivity and resilient against node compromise and node replication attack. Another scheme is a matrix based key management scheme which ensure benefits of full pair-wise key at sufficiently low storage overhead. In the next chapter we will present secure routing solution for flat and hierarchical architecture in HWSN.

Chapter 4

Routing Protocols

This chapter presents suggestions on secure routing schemes[1, 2, 3]. Two of the schemes exploit underlying key management for security provisioning in a route and designed efficient approaches which ensure that resilience of link being considered is maximized. Use of MNs for secure data collection is also explored and presented in third scheme. Security of multiple paths between two ends of a communication is addressed by a secure multipath routing scheme is presented in fourth scheme. Section 4.1 briefly identifies key issues to be addressed by secure routing schemes. Section 4.2 and 4.3 presents two secure routing schemes based on random key pre-distribution of keys to SNs. Both schemes strive to improve resilience of routes towards BS. Section 4.4 present a secure data collection using MNs and addressed issue of authentication and re-authentication of MNs. In Section 4.5 we present a secure multicast routing scheme using random pre-distribution of keys to each SN. Finally, Section 4.6 summarises this chapter.

4.1 Issues

Routing protocols lay down the paths and determine trajectory of each data packet in underlying network. With varied range of parameters, different mode of operation and different architectures; routing protocols must perform correct and select optimal route for each packet. Due to unattended mode of operations and low resources WSNs offers play ground for secure and optimally secure routing approach; resilient to physical and software attacks. The use underlying key management and incorporate security as vital parameter during selection of next hop; often addressed through secure routing schemes.

---

[1]The major findings of this chapter have been are published

- "*Variance Aware Secure Routing for Heterogeneous Wireless Sensor Networks*," Malaysian Journal of Computer Science, Vol. 26, No. 2, pp. 159-169 (SCI indexed, Impact Factor 0.20), Malaysia.

[2]The major findings of this chapter have been accepted for publication

- "*Secure Multipath Routing Scheme using Key Pre-Distribution in Wireless Sensor Networks*," In International Journal of Foundation in Computer Science, Australia.

[3]Major contribution of this chapter are communicated in International Journal

- "*Secure Data Collection using Mobile Sensors in Statically Deployed Sensor Networks*," In Malaysian Journal of Computer Science (SCI indexed, Impact Factor 0.2).
- "*Evaluating Location Augmentation Key Pre-distribution Scheme in Heterogeneous Wireless Sensor Networks*," Wireless Personal Communications, Springer (SCI Indexed, Impact Factor 0.7).

WSNs are often deployed for surveillance and monitoring purposes. Events related data must be routed to BS for further processing and decision making. Some times WSNs are viewed as large data bases, which may be queried for some event tracking. Distinct views require distinct solutions. We have designed four distinct solutions for varied requirements[1 2 3].

First solution exploits random key pre-distributed keys and localization, to derive most resilient paths towards BS. Scheme applies security in GPSR. Second scheme ensures that newly added hop should maintain the resilience of being established route. A novel variance aware next hop selection approach is developed in this proposal. Third solution provides a new paradigm for data collection using MNs. Authentication of MN is established using a novel THA protocol. Multi path traversal of query and data using secure routes is proposed as fourth scheme. Scheme is a novel secure multipath routing scheme.

4.2 Location Augmented Secure Routing in HWSN

There is growing demand for provision of end to end security in communication between sensors and their designated BS. Mostly the issue related to local relationships among sensors after deployment is largely ignored and thus design of most of key distribution schemes is limited only to pre-deployment pre-distribution of keys among the sensors in WSNs. The proposal in this section makes use of uniform and non-uniform key pre-distribution scenarios in HWSN and post-deployment key ring derivation. To derive location based key ring we use location information gathered using ANs {Section 3.2.2}. This scheme incorporates end-to-end resilience in routing scheme GPSR using local geographic relationship among SNs; and constructs secure routes toward BS.

4.2.1 Network Elements and Network Model

This section elaborates network elements and network model for flat architecture in HWSN. HWSN is realized by using heterogeneous elements.

4.2.1.1 Network Elements

Large-scale HWSNs with the flat architecture is considered in this proposal. SNs are divided into two categories namely H-Sensors and L-Sensors. H-Sensors are small number of SNs possessing higher memory, large transmission range, multiple transmission ranges, high processing power and battery life than generic L-Sensors. Network model has three different kinds of wireless devices on the basis of functionality; Sink Node/Base Station (SINK/BS) and SNs.

- **Sensor Node (SN):** HWSNs consist of two classes of sensors, i.e., L-Sensors and H-Sensors. L-Sensors are low cost, low processing power, generic wireless communication devices. Each L-Sensor has limited battery bank, storage capacity, computing facility and short radio transmission range. L-Sensors communicate with their CH, L-Sensors and BS. H-Sensor possesses considerably more resources than the L-Sensor. H-Sensors are capability rich wireless communication device, equipped with powerful batteries, sufficiently large storage, powerful radio antenna and reasonable processing capabilities.

- **Anchor Nodes (ANs):** ANs are H-Sensors with multiple power level for transmission. ANs are placed at Triangular/Hexagonal points to realize a novel clustering/localization approach. This approach transforms this scheme into location dependent {Section 3.2.2}
- **Sink/Base Station (SINK/BS):** BS is controller of WSN. It is a device with all infrastructures for wired and wireless communication paradigm in WSN. It is a computing facility for simultaneous processing capabilities, multiband and multichannel radio signaling, huge storage capacities and radio transmission range. BS can communicate with every network element in a WSN. BS supervises functioning of WSN from safe a location either at centre or corner of network as specified by the application requirements.

4.2.1.2 Network Model and Cells

Network model used in this scheme is given in Section 3.3.2, Figure 3.1. As this scheme considers flat network, no CHs is assumed in this scheme.

4.2.1.3 Geographical Cell Key Generation (K_G)

SNs which receive same set of nonce are said to belong to same cell. For each SN in a particular cell, we can construct a cell key (K_G) using the common broadcast received from all ANs. Without using any deployment information we are able to classify SNs in groups/cell. Without detailing the message exchange, we proceed to set up cell key as follows.

$$K_G = Hash\left(\bigcup_{i,j}^{m,n}\left(N_{ij}\right)\right) \quad (4.1)$$

In eqn. {4.1}, $\{i,j|i = 1..m \,\&\, j = 1..n\}$ variables m,n correspond to Id number of ANs and Id of power levels respectively. Also N_{ij} is nonce broadcast by i^{th} AN transmitting at j^{th}power or transmission level.

4.2.2 Network Initialization

To establish secure communication we proceed in two steps namely: Key Management Scheme for HWSNs and Security Aware Route establishment in GPSR [134]. Routing and key management go hand in hand and cannot be distinguished from each other. Table 4.1 lists the parameters in protocol with their notations and description.

4.2.3 Key Management

Key management consists of multiple stages: Key pre distribution, pair wise key establishment, establishing routing paths.

4.2.3.1 Key pre-distribution

Consider a HWSN with N sensors, consists of L-Sensors and H-Sensors. One BS is assumed for networks management. To quantify numbers of L-Sensors and H-Sensors we use n_1 and n_2 respectively. Scheme pre-distribute k_1 and k_2 unique keys such that $k_1 \leq k_2$ chosen randomly

from a large key pool of size K respectively to L-Sensor and H-Sensors. BS maintains all K keys but uses only k_2 keys like an H-Sensor.

Table 4.1 Notations Used

Symbols Used	Exploits
n_2	Number of H-Sensors
K	Key Pool Size
N_c	Number of Captured SNs
N	Number of SNs
k_1	Keys Allotted to L-Sensors
k_2	Keys Allotted to H-Sensors
n_1	Number of L-Sensors
c	Number of Classes
HF	Hash Function
K_G	Cell Key
K_{G_i}	i^{th}Key in cell wise key ring obtained from K_i
K_i	Pre-distributed key with Id i
I_m	Intermediary Node
P_r	Protection Keys

4.2.3.2 Cell wise Key Ring Generation

SNs in each cell can proceed to compute another key ring on the basis of their location. To obtain new key ring SNs in a cell member first compute common pre-distributed content. Pre-distributed keys are predeployed in SNs by BS. Although it seems a difficult proposition but with multi level transmission by ANs extremely small sized cells are obtained. The possibility of obtaining common pre-distributed key is more in small sized cells than in larger cells. Cell wise key ring is obtained by applying HF on common pre-distributed keys and cell key, i.e. K_G. Each SN now generate cell-wise key ring. Cell wise key ring can be used provide end-to-end confidentiality and to identify the cell in which event occurred. Any member from cell may communicate sensed data using one or more key from cell-wise key ring. Pre-distributed keys are maintained intact while generating cell wise key ring.

$$K_{G_i} = HF(K_G, K_i) \tag{4.2}$$

Cell wise key ring may be generated as in eqn. {4.2} where K_i is one of common key among pre-distributed keys. Similarly other keys of cell wise key ring can be derived from other common pre-distributed keys. At the end of this phase each SN possess two key rings i.e., pre-distributed key ring and cell based key ring.

4.2.3.3 Pair-wise Key Establishment

SNs may exchange handshaking messages and be aware of key-IDs in key ring of one-hop neighbours. Also each SN is aware of key values in cell wise key ring of SNs in same cell. Now SNs may proceed to establish all the one-hop and two-hop key paths to all its one-hop neighbours. SN's pair L_i and L_j may share all keys in cell wise key ring if both belong to same cell. Beside this there are keys from pre-distributed key rings which are used to generate cell wise key ring. Major contribution may come from other shared pre-distributed key in pair of SNs. Cell key $K_G$is always available between SNs of same cell. It can also be said that there is possibility that one-hop direct key path may exist between them. Sensor L_i may now proceed to establish all two-hop key paths with each of its neighbours. This is improvement from proposal in [24] which quotes that there is possibility that SNs pair may not have direct path. In this scheme cell key, i.e. K_G has ruled out such possibility. We use two-hop paths to enhance the link resilience [24] [135] (the attacker has to compromise all key paths for a link between two SNs in order to compromise this link). There is a high probability that L_i and L_j are neighbour in same cell. Moreover intermediary on two-hop key path may belong to same cell or different cell. Cell wise key rings certainly may improve keys shared with one-hop neighbours on one-hop and two-hop key paths.

Participation of cell key, cell-wise keys along with other pre-distributed keys in one-hop and two-hop key paths will help us further enhance the resilience of any link between L_i and L_j by increasing the number of protection keys and subsiding cases of no-common keys. Intermediate SNs on two-hop paths receives id's of L_i and L_j. By virtue of cell memberships and some pre-distributed keys we have large ratio (almost-all-neighbours) of neighbours which can be intermediates on two-hop key paths. Intermediate SN (I_m) prefers to use all the common keys which include cell key, cell wise keys and pre-distributed keys on two hop key path between L_i and L_j. I_m sends a reply back to L_i.

In this way, a two-hop key path $L_i - I_m - L_j$ is constructed. All two-hop key paths are constructed as above. After L_i constructs all two hop key paths to L_j, node L_i generates multiple key shares and transmits each on disjoint two-hop and one-hop key path. Encrypted key-shares are dispatched between L_i and L_j, hop-by-hop using all common keys of respective hops. SNs need not store the number of protection keys for each link on two hop paths and reduce memory requirement in this key management scheme.

Assuming that there are p two-hop key paths between L_i and L_j, each with the help of proxy $I_m(1 \leq I_m \leq p)$, and denote $K(i\,,j)$ as the number of shared keys between L_i and L_j. The number of protection keys between L_i and L_j can be denoted by $P_r(i\,,j)$:

$$P_r(i\,,j) = K(i,j) + \sum_1^p \min(K(i,I_m), K(I_m,j)) \tag{4.3}$$

Protection keys determine the resilience of link. Scheme doesn't compute resilience and conclude the same by computing an enhancement in average keys on routes from SNs to BS.

4.2.4 Performance Study

Performance Study is performed using a probability based performance model and simulation based analytical study.

4.2.4.1 Performance Model

Performance model is based on probabilistic modelling and uses the fact that end-to-end resilience on routes is scripted by number of keys (or average number of keys) in the links on the routes. We have proposed a location augmented keying mechanism which resulted in co-located SNs to share some keys for use in encryption/decryptions over links. We have established simulation set-up using GPSR [134] as underlying routing protocol. During simulation a routing tree is established using metric of interest. Routing tree is rooted at BS. We evaluate the impact of location augmented keying on the average number of keys in the routes from SN to BS.

By definition resilience is measured as the probability that at least one of the key in the link is not disclosed to the attacker. If we can increase the keys in the links we can expect that resistance against attacks will increase. An increase in resistance will improve end-to-end resilience. We will evaluate the protection keys for say average number of keys on the routes from SNs to BS.

We assume the number of captured SNs (N_c) is known. SNs at any distance can reach the BS by at most $N-1$ hops and avoid any loop. For a specific communication route from any random SN to BS with h hopes the resilience can be expresses as probability and denote by $eRESe(h)$. The probability value $eRESe(h)$ can be expressed as the product of probabilities of links in routing path with h hops.

In eqn. {4.4}, $eRESe(h)$ is calculated as product of probabilities that all SNs and links are un-captured /uncompromised in the path with h hops.

$$eRESe(h) = \frac{\binom{N-h}{N_c}}{\binom{N}{N_c}} \times (RES_{link})^h \tag{4.4}$$

In eqn. {4.4} RES_{link} is the resilience of link and denote probability that a link between two uncaptured SNs is uncompromised. In eqn. {4.4}, the value of $\binom{N-h}{N_c}/\binom{N}{N_c}$ represents the probability of ways by which a SN can be captured provided none of SNs in h hopes used for communication is captured. For evaluation scheme used probabilistic model and demonstrate to enhance the value of RES_{link} as established using some of equation as given in [135] which are applicable only to homogeneous environment and overlooked heterogeneity and geographic relations among SNs.

Computation of Q_i : Before computing value of RES_{link} we compute the probability value $Q_i\{i = LorH\}$ which is the probability that a SN on the path between a SN and BS is either of H-Sensor and L-Sensor class. In homogeneous WSN all SNs are L-Sensors and thus Q_i refer to probability of selection of i^{th}SN as next hope. During route construction next link should be more or equally resilient. Such requirement will add SNs with more total number of shared keys. The shared keys may come from pre-distributed key rings or and cell-wise key rings.

Derivation of Q_i will follow after computation of $p_{common}(i,j,l)$ which is defined as the probability of any i class SN shares l keys with a j class SN where as in homogeneous WSN i & j refers to sensor i and sensor j respectively. Consider p_i as percentage of class i SNs in the network and is given by $p_i = {n_i}/{N}$.

If $P_{common|same}(i,j,l)$ denotes conditional probability of sharing keys given that SNs are from same cell. Similarly, $P_{common|diff}(i,j,l)$ denotes the conditional probability that any class

i sensor SN shares l keys with a class j sensor SN given that SNs are from neighbouring but distinct cells. The equations are as under:

$$p_{common}(i,j,l) = P_{common|same}(i,j,l)P_{common|diff}(i,j,l) \tag{4.5a}$$

$$p_{common|same}(i,j,l) = \binom{K}{l/2}\frac{\binom{K-l/2}{K_i}}{\binom{K}{K_i}}\frac{\binom{K-K_i}{K_j-l/2}}{\binom{K}{K_j}} \tag{4.5b}$$

$$p_{common|diff}(i,j,l) = \binom{K}{l}\frac{\binom{K-l}{K_i-l}}{\binom{K}{K_i}}\frac{\binom{K-K_i}{K_j-l}}{\binom{K}{K_j}} \tag{4.5c}$$

If P_{same} denote the probability of next hop j being same cell's member of as of i by then the probability of being member of different cell is given by

$$P_{Diff} = 1 - P_{same} \tag{4.5d}$$

Here $P_{same} = \frac{1}{2}$. Similarly define $P_{diff} = Q_{same} = 0.5$. If ANs are heterogeneous in the sense that each can support different number of transmission levels, P_{same} and P_{Diff} may differ. Scheme has considered homogeneity in transmission levels of ANs.

$$\begin{aligned} &P_{prefer}(j,l) \\ &= \sum_{j=1}^{2} P_j \left(\sum_{u=1}^{Z} P_{comm|same}(i,j,u) \left(\sum_{v=1}^{u-1} P_{comm|same}(i,l,v) + \sum_{v=1}^{2u-1} P_{comm|diff}(i,l,v) \right) \right. \\ &+ \frac{1}{2} \left(\sum_{u=1}^{Z} P_{comm|same}(i,j,u)\, P_{comm|same}(i\,,l,u) \right. \\ &\left. \left. + \sum_{u=1}^{Z} P_{comm|diff}(i,j,u)\, P_{comm|diff}(i\,,l,u) \right) \right) \end{aligned} \tag{4.6}$$

Although there is greater probability of intermediate SNs being members of same cell if next-hop SN j of SN i are both same cell members. If $P_{prefer}(j,l)$ is defined as the probability of j SN is preferred over l SN as next-hop on routing path, the effect of belongingness to same or different cells should also be incorporated. Scheme rely upon location based cell's contributions and use equation as per new dimension in eqn. {4.6}, where u is the number of pre-distributed keys. Finally, the expression of Q_i is as follows where $f(j)$ equals 1 when $i = j$, otherwise 0.

$$Q_i = \binom{N_{nei}}{1} \prod_{j=1}^{2} \left(P_{prefer}(i,j) \right)^{N_{nei} * P_i - f(j)} \tag{4.7}$$

In eqn. {4.7}, N_{nei} is the average number of physical neighbours of a SN, which is given by $N_{nei} = N * (\pi r^2/Area)$.

Derivation of RES_{link}: Given the expressions of Q_i as in eqn. {4.7} which is equally applicable to homogeneous and heterogeneous WSN; we can now the expressions for RES_{link} [135] in this section where denote $RES_{link}(i,j)$ is resilience of the pair-wise key between a SN of i class and j class SN:

$$RES_{link} = \sum_{i=1}^{2}\sum_{j=1}^{2} Q_i * Q_j * RES_{link}(i,j) \tag{4.8}$$

Where expressions for $RES_{link}(i,j)$ is as follows:

$$RES_{link}(i,j) = (1 - \mathrm{U}) \tag{4.9a}$$

$$U = \left(1 - P_{res}\left(K_{avg}(i,j)\right)\right)\left(1 - (1 - \mathrm{N_c/N})P_{res}\left(K_{avg}(i,j)\right)P_{res}\left(K_{avg}(\mathrm{i})\right)\right)^{n_{path}} \tag{4.9b}$$

Here $P_{res}\left(K_{avg}(i,j)\right)$ is probability that the direct one-hop key path between a class i SN and a class j SN is uncompromised, $\mathrm{N_c/N}$ is probability that the proxy SN on one of the two-hop key paths is captured, and is the probability that the link on a two-hop key path between a class i SN and the proxy is un-compromised. $K_{avg}(i,j)$ as the average number of shared pre-distributed keys between a class i SN and a class j SN, $K_{avg}(i)$ as the average number of shared pre-distributed keys between a class i SN and one of its physical neighbours, and denote $n_{path}(i,j)$ as the number of two-hop key paths between a class i SN and a class j SN.
Thus, the expressions for $RES_{link}(i,j)$ can be given by eqn. {4.9}. We now can derive the expressions for $P_{res}(i)$, $K_{avg}(i,j)$ and $K_{avg}(i)$. Given the number of captured SNs N_c, the average number of disclosed pre-distributed keys, denoted by K_{dis} is given by,

$$K_{dis} = \left(1 - \left(1 - \frac{K_{avg}}{K}\right)^{N_c}\right) \tag{4.10}$$

, where K_{avg} is the average number of keys pre-distributed in sensor SNs. The expression of K_{avg} is given by,

$$K_{avg} = \sum_{i=1}^{2} p_i * k_i \tag{4.11}$$

Given the expression of K_{dis} above, expression of $P_{res}(i)$ is as follows,

$$P_{res}(i) = 1 - \frac{\binom{K-i}{K_{dis}-i}}{\binom{K}{K_{dis}}} \tag{4.12}$$

Recall the expression of $P_{comm}(i,j,l)$ in eqn. {4.4} above, the expressions of $K_{avg}(i,j)$ and $K_{avg}(i)$ can be given by,

$$K_{avg}(i,j) = \sum_{l=1}^{min(K_i,K_j)} l * P_{comm}(i,j,l) \tag{4.13}$$

$$K_{avg}(i) = \sum_{j=1}^{c} p_j * K_{avg}(i,j) \quad (4.14)$$

Finally, the expression of $n_{path}(i,j)$is as follows:

$$n_{path}(i,j) = 0.5865 * N_{nei} \sum_{l=1}^{2}\big(1 - P_{comm}(i,l,0)\big)\big(1 - P_{comm}(j,l,0)\big) \quad (4.15)$$

where $0.5865 * N_{nei}$ is the average number of common neighbours of two neighbouring SNs [61].

Scheme focuses on the quality and don't quantify resilience which in-fact is probability of not disclosing when compromised. As per eqn. {4.5} above, resilience of route depends upon resilience of links on the route. Further resilience of link depends upon the number of keys in the link used for encryption and decryption while routing as can be concluded from eqn. {4.9}. Eqn. {4.5} is improved from [135] and improvement reported is tremendous nearly 300%. The impact of eqn. {4.5} is incorporated in eqn. {4.6} for homogeneous and heterogeneous key distribution respectively. Eqn. {4.6} helps uniquely finalize the next SN on routes from SNs to BS. Here scheme try to select the SN if it maximizes the computation in eqn. {4.5} without much-ado in terms of memory consumption. Eqn. {4.6} establishes the probability of preferring one SN over other in the light of local neighbour-hood. Incorporating the local neighbourhood in eqn. {4.5} and eqn. {4.6} improved upon the number of keys in each of one-hop and two-hop key paths. This selection criterion is modification with a view that SN on the routes should maximise the number of protection keys on links.

4.2.4.2 Simulation Study

In an effort to realize the effect of location based key augmentation method a simulation environment using MATLAB was established. Simulation's objective is to prove that new mechanism is able to bring an improvement in number of keys in links on routes if alternates are available and thereby increasing the effort of intruders.

Simulation Set-up for uniform key pre-distribution

Simulated was performed using simple scenario where routes are formed using GPSR taking geographic distance as metric of concern. Scheme then used key-shares between SNs as their distance metric. A SN is preferred over others if share more keys. GPSR under uniform key distribution scheme finds routes form BS to SNs with effort to maximize keys on the routes between BS and SNs. Finally GPSR is simulated under uniform key management using local cell based relationships which tries to maximize the keys in the routes as well limits the variance in number of key values on the routes.

Simulation considers following values for various protocol parameters $k_1 = 45$, $N = 45$, $n_1 = 45$ and $K = 1000$.

The network to be studied is deployed in 100x100 area with transmission range = 20. Figure 4.1 draws deployment pattern. SNs are numbered from 1 to 45 with SN 1 acting as BS. The SNs are pre distributed with keys by BS and deployed thereafter.

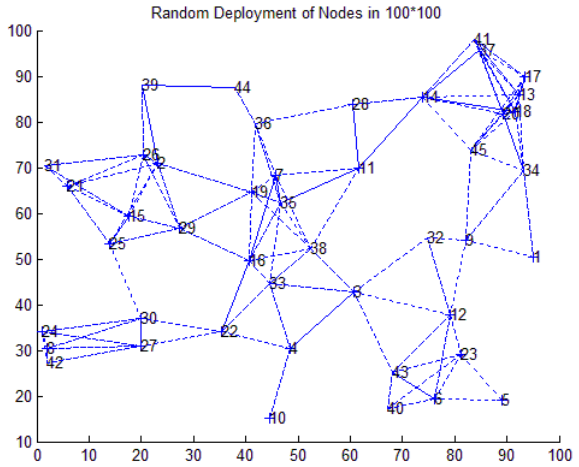


Figure 4.1 Random Deployments of WSN SNs

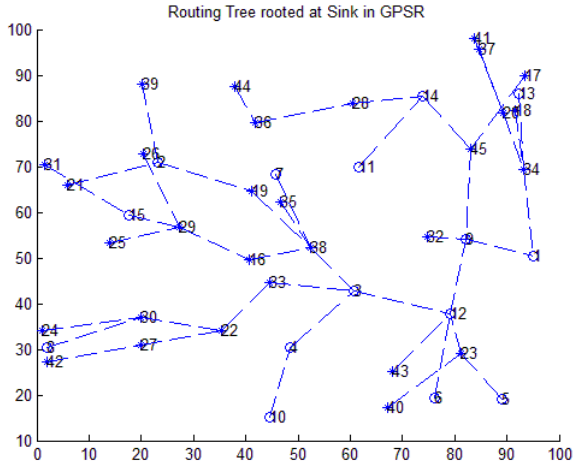


Figure 4.2 Spanning Tree in GPSR rooted at BS.

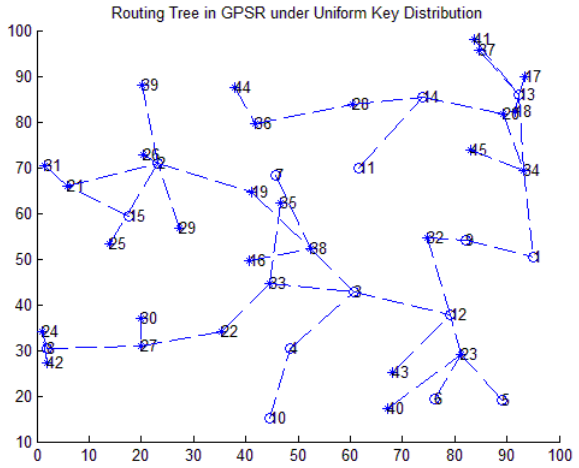


Figure 4.3 Routing Tree in GPSR under UNIFORM distribution

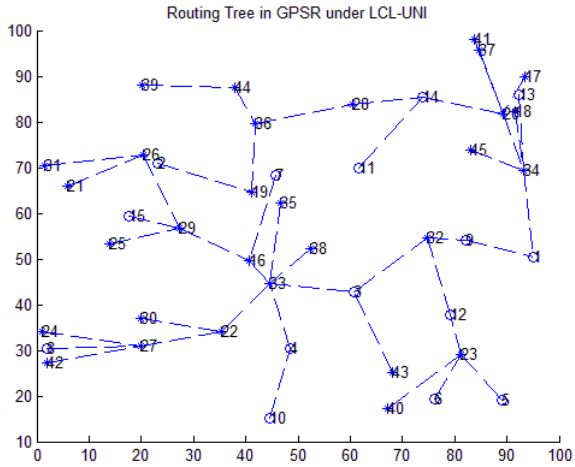


Figure 4.4 Routing Tree in GPSR LCL-UNIFORM key distribution

Figure 4.2, 4.3 and 4.4, shows the routing trees in GPSR, GPSR-UNIFORM and GPSR-LCL-UNIFORM scenarios respectively. In Figures 4.2, 4.3 and 4.4 above; routes in three scenarios differs from others to some extent as per distance metric. Figure 4.2 has been drawn for distance as metric where as Figure 4.3 and 4.4 are drawn using link keys as metric. It must be understood that next-hop SNs are limited by the neighbourhood and key ring matches. This limitation is even more pronounced in keyed paths. The graph in Figure 4.5 exhibits a comparison of route lengths in keyed variants of GPSR. The average keys on routes from SNs are shown in Figure 4.6 under uniform and uniform-local key distribution. Visibly the average keys in this proposal for secure version of GPSR have improved by about 40-400% with respect to uniform pre distribution. For example route no. 10 in graph possesses 4 keys on average in uniform distribution while same route in uniform local key distribution possess 8 keys (100% improvement). Again route no. 17 possesses 7 keys in uniform pre distribution while same route in uniform local pre distribution possess 37 keys (400%). This multi-fold improvement in certain routes is due their passage through dense area or routes starting in dense area. As dense areas are critical areas; which should offer more resilience and so is exhibited in Figure 4.6.

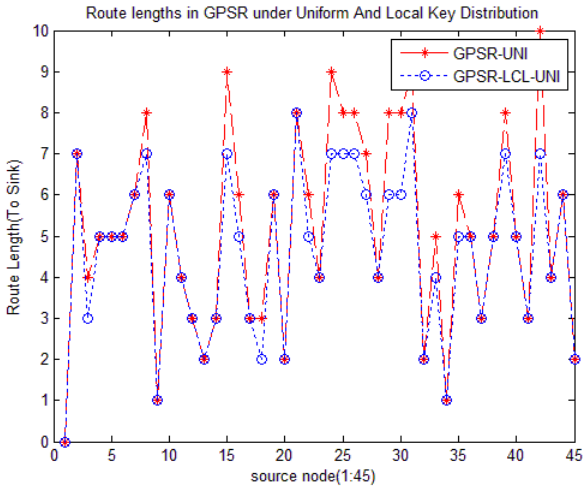


Figure 4.5 Route lengths comparison in GPSR under Uniform and Local Uniform Keying

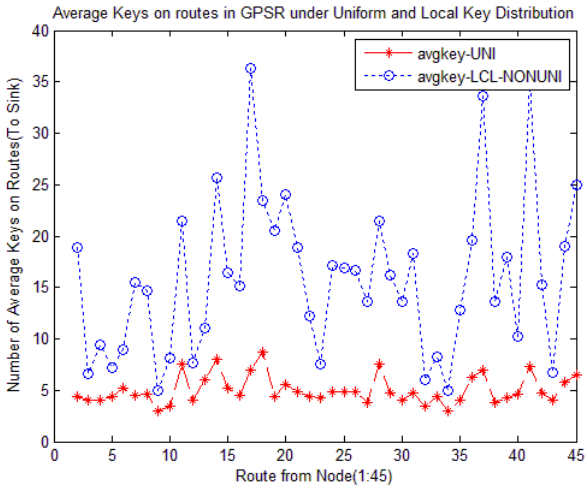


Figure 4.6 Average keys comparison on routes in GPSR and GPSR-LCL-UNIFORM Key

Simulation Set-up for non-uniform key pre-distribution

Next simulation is performed using GPSR under non-uniform key management and augmentation by Local Cell based connectivity which tries to maximize the keys in the routes. Simulation considered following values for various protocol parameters $c = 2,\ k_1 = 45,\ k_2 = 90, N = 45,\ n_1 = 30, n_2 = 15$ and $K = 1000$.

The network to be studied is deployed in 100x100 area with transmission range = 20. HWSN has considered two classes ($c = 2$) of SNs and deployment of SNs is as shown in Figure 4.1.

SNs are numbered from 1 to 45 with SN 1 acting as BS. SNs are pre distributed with keys by BS. Figure 4.7 and 4.8 show routing trees in GPSR-NONUNIFORM, and GPSR-LCL-NONUNIFORM scenarios respectively. The graph in Figure 4.9 draws a comparison of route lengths in GPSR-UNIFORM and GPSR-NONUNIFORM. Figure 4.10 show route length comparison in GPSR-NONUNI and GPSR-LCL-NONUNI. Finally Figure 4.11 describes a combined route length comparisons.

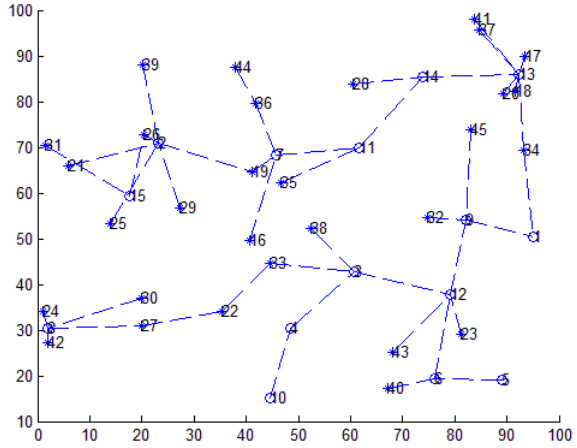


Figure 4.7 Routing Tree in GPSR NON-UNIFORM key distribution

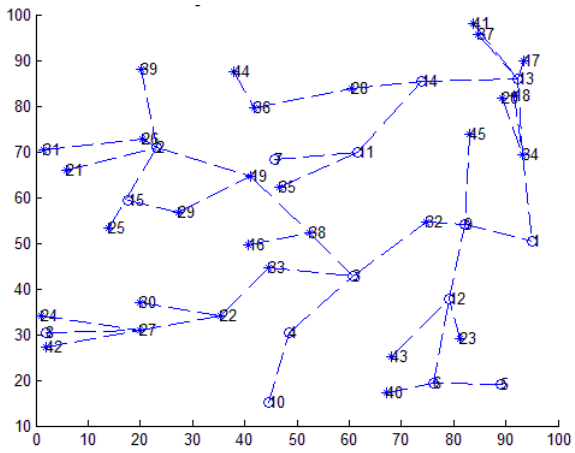


Figure 4.8 Routing Tree in GPSR under Local NON-UNIFORM key distribution

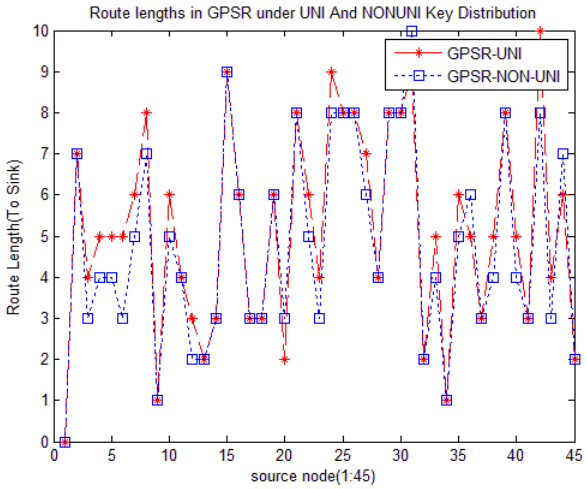


Figure 4.9 Route Length comparisons in GPSR-UNI and GPSR-NONUNI Key Scheme

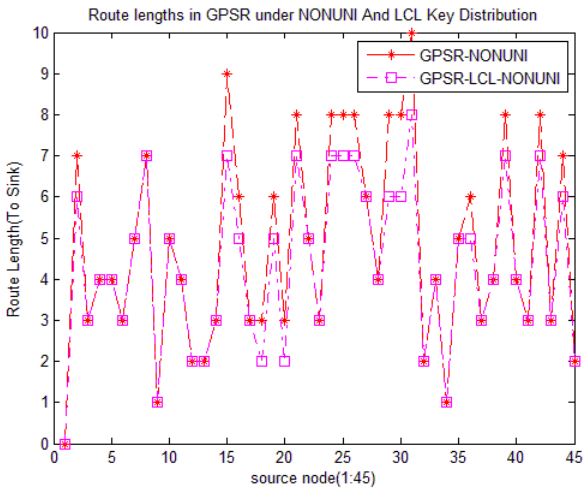


Figure 4.10: Comparison of Route Lengths GPSR-NONUNI and GPSR-LCL-NONUNI

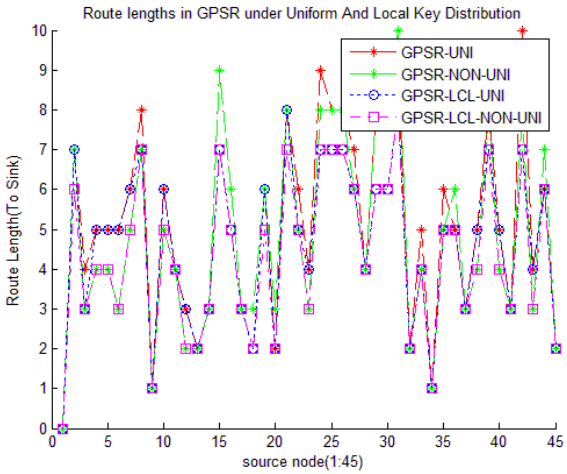


Figure 4.11 Route lengths comparison in UNI, NONUNI, LCL-UNI, LCL-NONUNI

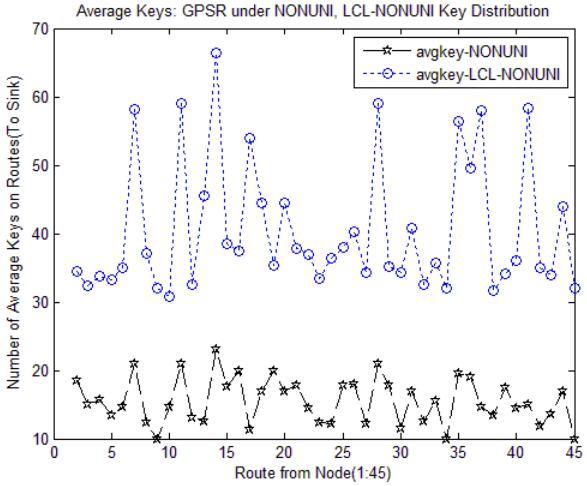


Figure 4.12 Average Keys on routes in NONUNI, LCL-NONUNI Keying Scheme

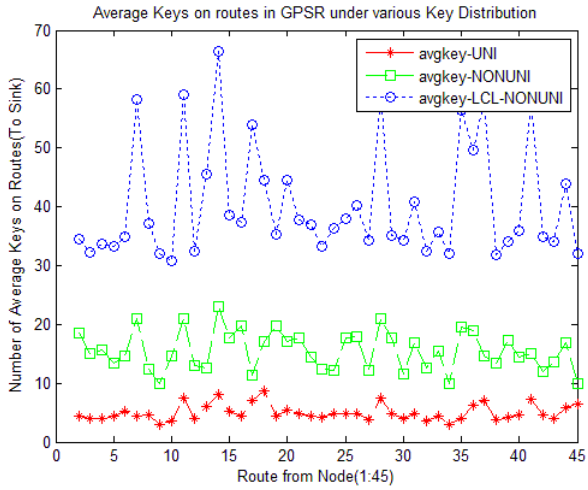


Figure 4.13 Average keys on routes in UNI, NONUNI and GPSR-LCL-NONUNIFORM

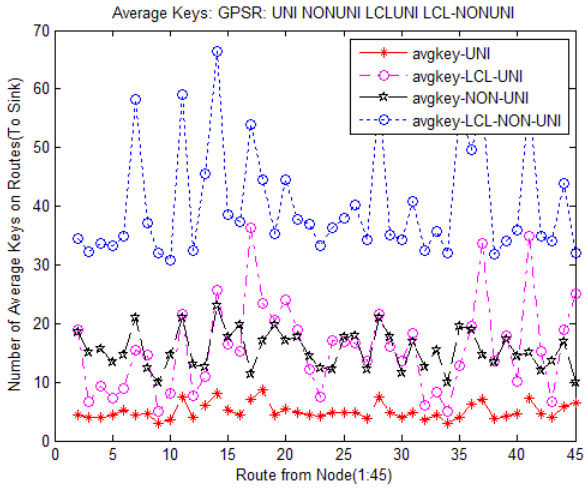


Figure 4.14: Average Keys on routes in UNI, NONUNI, LCL-UNI, LCL-NONUNI Keying

Average keys on routes from SNs are shown in Figure 4.12 under GPSR-NONUNI and GPSR-LCL-NONUNI key distribution. Figure 4.13 describes comparison of average keys on routes in UNI, NONUNI and LCL-NONUNI keying schemes. Figure 4.14 describes comparison of average keys on routes in UNI, NONUNI, LCL-UNI and LCL-NONUNI key pre distribution schemes. Visibly the average keys in this proposal for secure version of GPSR has improved by about 400-600% with respect to uniform and about 100% with respect to non uniform key distribution.

For example route no. 10 in graph possesses 4 keys on average in uniform distribution while same route in non-form key distribution possesses 16 keys. Again same route under local effect in non-uniform key distribution possesses 32 keys.

4.2.4 Discussion

Qualitatively resilience of any path is determined by the number of keys in the link. Any path between two SNs considers not only the keys on direct path but also keys on two-hop paths through intermediate common neighbours. Increasing the number of protection keys in the link which may be achieved only by increasing the number of key shared between a pair of SNs was primary objective. If scheme can achieve higher probability of sharing keys for a link, security aware routing may chose most resilient link as per their requirements.

Graph in Figure 4.5 reveals that route lengths in case of uniform key distribution with local neighbourhood effects has lower values in almost every route compared to that of uniform key distribution. This suggests that the next-hop selection is largely affected as a result of cell based keying. Plots in Figure 4.6 show average number of keys on routes from respective SNs to BS. Analysis of these plots reveal that average keys on the routes in uniform distribution with local neighbourhood effects has maximum possible average number of keys on any route compared to that of uniform key distribution scheme. This gain varies in range of 40-400%. Local cell relationship improved the protection keys in each link and thus each route. Also route length is reduced for almost every route. If average keys on routes considered as quality or quantity of resilience then we improved upon resilience. Moreover the results are under limitation posed by neighbourhood.

Graph in Figure 4.7 and 4.8 correspond to routing tree in non-uniform key distribution. From Figure 4.9 one can reveal that route lengths in case of non-uniform key distribution have lower values than that of uniform key distribution scheme. Extending the comparison of route lengths to non-uniform and non-uniform with local effects in Figure 4.10 establishes that local cell membership can play superbly in non-uniform distribution of keys. Every route in non-uniform with local effects has smaller route lengths compared to that of non-uniform key distribution. Combined conclusions from Figure in 4.5, 4.9, 4.10 and 4.11 are drawn. We conclude that non-uniform key distribution performs better than uniform key distribution and uniform with local effect performs better than uniform and close to non-uniform key distribution scheme. Non-uniform with local effects has performed best of all scenarios. This suggests that the next-hop selection is largely affected as a result of cell based key ring. In Figure 4.12 we plotted average number of keys on routes from respective SNs to BS. From graph we reveal that average keys on the routes in non-uniform distribution with local effects has maximum average number of keys on any route compared to that of non-uniform key distribution scheme. This gain is around 200-250%. For easier comparison see from graph in Figure 4.13 that non-uniform with local effects performed better than non-uniform which in turn performed better than uniform key distribution scheme. Figure 4.14 finally draws combined case which helps us to conclude that uniform with local effects performs as good as non-uniform key pre-distribution and even better than non-uniform key pre distribution scheme in some cases.

4.3 Variance aware Secure Routing Scheme

This scheme is inspired by the fact that route is as strong and resilient as the weakest link in the route. The weaker links are weak with respect to other links in the same route. Most solutions seem of ignoring this fact. Proposal devised a strategy based on variance of number of link keys on routes. Proposal strives to reduce the variance of link keys on the routes being constructed hop-by-hop. Scheme is evaluated under uniform and non-uniform key pre-distribution in HWSNs.

4.3.1 Network Elements and Network Model

Network Elements: This scheme also applicable to is large-scale HWSNs with the flat architecture. SNs are divided into two categories; namely H-Sensors and L-Sensors. H-Sensors are small number of SNs possessing higher memory, transmission range, multiple transmission ranges, processing power and battery life. Network model for this scheme has two different kinds of wireless devices on the basis of functionality; SINK/Base Station (BS) and Sensor SNs (SNs).

- **Sensor Node (SN):** HWSNs consist of two classes of sensors, i.e., L-Sensors and H-Sensors. L-Sensors are low cost, low processing power, generic wireless communication devices. Each L-Sensor has limited battery bank, storage capacity, computing facility and short radio transmission range. L-Sensors communicate with their CH, L-Sensors and BS. H-Sensor possesses considerably more resources than the L-Sensor. H-Sensors are capability rich wireless communication device, equipped with powerful batteries, sufficiently large storage, powerful radio antenna and reasonable processing capabilities.
- **Sink/Base Station (SINK/BS):** BS is controller of WSN. It is a device with all infrastructures for wired and wireless communication paradigm in WSN. It is a computing

facility for simultaneous processing capabilities, multiband and multichannel radio signaling, huge storage capacities and radio transmission range. BS can communicate with every network element in a WSN. BS supervises functioning of WSN from safe a location either at centre or corner of network as specified by the application requirements. In this proposal BS is situated at random location in deployment area.

Network Model

In this scheme, a large number of SNs are randomly distributed in deployment area. BS takes charge of the whole network's operation. SNs monitor the surrounding environment and transmit the sensed readings to their BS via multi-hop relay path. SNs are deployed randomly in the field. BS is situated at random location in deployment area. BS can reach any SN in the deployment area directly is presumed. Each sensor has small radius of transmission i.e. r. SNs are static and possess limited battery life. Battery of SNs cannot be replaced or charged after deployment {Figure 4.1}.

4.3.2 Key Management

Majority of activities during this phase are performed on behalf of Key Management Scheme being used. In Table 4.1 we list the parameters used in protocol with notations and description. Key management consists of multiple stages: Key pre distribution, pair wise key establishment, establishing routing paths.

Key pre-distribution

We study a network with N SNs and one BS. SNs belong to two classes namely L-Sensors and H-Sensors. The strength of L-Sensors and H-Sensors is represented by n_1 and n_2 respectively where $n_1 > n_2$ SNs. We then pre-distribute k_1 and $k_2$unique keys such that $k_1 \leq k_2$ chosen from a large key pool with size K respectively to L-Sensor and H-Sensor. BS is pre-distributed with all K keys but uses only k_2 keys similar to H-Sensor from key pool. After this, BS is deployed at any random position, similar to N SNs in HWSN.

Pair-wise key establishment

After random deployment of SNs in HWSN SNs proceed to establish pair-wise keys with their neighbours. Pair-wise keys ensure secure communication between a pair of SNs. SNs are pre-distributed with key rings and key-Ids of pre-distributed keys. SNs near to BS wait for a beacon from BS. SNs initiate secure path establishment after receiving beacon. This supports push-pull paradigms of communication. TTL (Time-to-Live) of beacons is set to 1, i.e. $TTL = 1$. All one-hop neighbours compute an Illusionary Resilience (IR) towards their BS. This value if denoted by IR and equals sum of IR_{sender} and the square of number of pre-distributed keys shared with the sender of beacon as specified in eqn. {4.16}. As SNs away from BS will receive multiple beacons informing sender's IRs; SNs locally select one of sender as next hop towards BS for which eqn. {4.16} gives minimum. Receiving SNs wisely select a sender as their next-hop towards BS, on the basis of following equation.

$$IR_j = min\{IR_k + (K_{comm}(j,k))^2\} \quad (4.16)$$

If any SN L_j has received IR values from p distinct one hop neighbours then $k = 1..p$. Here $K_{comm}(j,k)$ denote the number of pre-distributed keys that a SN L_j shares with k^{th} sender among p distinct sending neighbours. For routing purposes selection of forwarder towards BS is informed to concerned SN. Having completed the process of computing IRs towards BS, SNs gets arranged like a tree rooted at BS.

4.3.3 Performance Evaluation

As per non-uniform key pre-distribution scheme H-Sensors are given more keys than L-Sensor. Possibility of sharing more keys with H-Sensors is high compared to that of L-Sensors. Process of computing IR continues until all SNs in network have computed IRs toward BS. At the end of route establishment; SNs are aware of which of one-hop neighbours will route information through them.

Probability of sharing common keys with SNs can be computed easily. The resilience of any link between L_i and L_j is dictated by number of shared keys. Key paths can be constructed between any L_i and L_j by sending a request to its neighbours, containing the Ids of L_j and L_j . In this proposal it is obtained while constructing routing tree. L_j can check if it shares pre-distributed keys with L_i only if L_j received the IR_i as well as Ids of all the pre-distributed keys of L_i . L_j prefers to use all the common keys for one-hop direct key path between L_i and L_j . L_j sends an acknowledgement back to L_i with which L_j shares optimal number of keys and proceeds to compute own IR. In this way, a one-hop key path $L_i - L_j$ is constructed. After L_i constructs one-hop key path to L_j , messages are encrypted or decrypted on hop by a combination (e.g., XOR) of all shared keys on that hop. Ultimately, the pair-wise key between L_i and L_j is a combination of all the common keys. SNs must store the number of protection keys for each link. Assuming that $K(i,j)$ denote the number of shared keys between L_i and L_j. The number of protection keys between L_i and L_j is exploited by $P_r(i,j)$ and is defined as follows.

$$P_r(i,j) = K(i,j) \quad (4.17)$$

Not to forget that some of the protection keys between a pair of SNs is maximum possible common keys. With no confusion we conclude that at the most one link is set between any pair of SNs in a routing tree.

4.3.3.1 Analytical Performance Model

The performance analysis in this scheme is again inspired by the evaluations towards resilience computations. An evaluation model was presented in last scheme. The difference in operation has caused change in some equation to incorporate the impact of variance based computation. For common equation this proposal will refer to earlier prescribed evaluation model.

Under similar assumption in two schemes we will refer earlier model. We assume the number of captured SNs (N_c) is known. SNs at any distance can reach the BS in at most $N - 1$ hops and will be able to avoid any loop as routing tree is spanning tree rooted at BS. For a specific

communication from any random SN to BS with h hopes probability can be expressed as $eRESe(h)$ and is the end to end resilience for a path with h hops.

Equation (4.4) above calculate resilience for this scenario i.e., $eRESe(h)$ is calculated as product of probabilities that all SNs and links are un-captured /uncompromised in the path with h hops. Routing tree construction mechanism in this scheme is distributed in nature and proceeds breadth-first way uses underlined pre-distribution to increase the value of RES_{link}. Before computing the value of RES_{link} it is required to compute a probability value Q_i which is the probability that a SN on the path between a sensor and BS is either of i (L or H Sensor) class. SNs get linked to active routes which results in minimization of equation (4.16). Derivation of Q_i will follow after computation of $p_{common}(i,j,l)$ which is defined as the probability of any i class sensor SN shares l keys with a j class sensor SN.

Consider p_i as percentage of class i SNs in the network and is given by $p_i = {}^{n_i}/_{N}$. If $P_{common}(i,j,l)$ denotes the probability that any i class sensor SN shares l keys with a j class sensor SN given that SNs are one hop neighbours. The equation for computation is prescribed in eqn. {4.18} below.

$$p_{common}(i,j,l) = \binom{K}{l} \frac{\binom{K-l}{K_i}}{\binom{K}{K_i}} \frac{\binom{K-K_i}{K_j-l}}{\binom{K}{K_j}} \tag{4.18}$$

If $P_{prefer}(j,l)$ is defined as the probability of class j SN is preferred over class l SN as next-hop on routing path, the equation for $P_{prefer}(j,l)$ can be defined as follows:

$$P_{prefer}(j,l) = \sum_{j=1}^{2} p_j \left(\sum_{u=1}^{min\{k_i,k_j\}} P_{common|P_{parent}=(IR_j+u^2)}(i,j,u) * \left(\sum_{v=1}^{min\{k_i,k_l\}} P_{common|P_{parent}\leq(IR_m+v^2)}(i,l,v) \right) \right) \tag{4.19}$$

$P_{parent} = \{ min\{IR_j + u^2\} \mid j = 1..p \}$; Where u subset of pre-distributed keys.

In eqn. {4.8} p is the average number of SNs from which SN receives IR values. The value of Q_i computed in eqn. {4.8} is applicable here also.

Derivation of RES_{link} Given the expressions of Q_i as in eqn. {4.8} we specify expression for RES_{link} is as shown in eqn. {4.20}, where $RES_{link}(i,j)$ is resilience of the pair-wise key between a SN of i class and j class SN:

$$RES_{link} = \sum_{i=1}^{2} \sum_{j=1}^{2} Q_i * Q_j * RES_{link}(i,j) \tag{4.20}$$

Where expressions for $RES_{link}(i,j)$ is as follows:

$$RES_{link}(i,j) = 1 - \left(1 - P_{res}\left(K_{avg}(i,j)\right)\right) \tag{4.21}$$

Where $P_{res}(i)$ as the probability that at least one of i unique pre-distributed keys is not disclosed to the attacker, $K_{avg}(i,j)$ as the average number of shared pre-distributed keys between a class i SN and a class j SN, $K_{avg}(i)$ as the average number of shared pre-distributed keys between a class i SN and one of its physical neighbours. The eqn. {4.21} is modified from eqn. {4.10} to refer only present scenario. In eqn. {4.20}, $P_{res}\left(K_{avg}(i,j)\right)$ is probability that the direct one-hop key path between a class i SN and a class j SN is uncompromised. To compute the value of $K_{avg}(i,j)$ refer to eqn. {4.11} to eqn. {4.14} derived earlier. There is no possibility of loops as routes are maintained as tree. Selection of parent towards BS is governed by eqn. {4.19}. Only one of potential parents will be announced parent of any SN.

4.3.3.2 Simulation Study

To evaluate the effect of next-hop selection method a simulation is established using MATLAB. Objective is to prove that new approach is able to bring an improvement in number of keys in links on routes if alternates are available and reduce the variance in number of keys in links on the routes. The almost ignored fact that route is as resilient as the weakest link is primary concern in this proposal. A major contribution of this work is to decrease the variance in resilience on the routes. This will increase the resistance against capture attacks . In this proposal, the range of variation in resilience of member links in a path is affected by novelty of next hop selection method. Proposal categorically chose a SN as parent in routing tree construction which minimizes the variation in the IR value of newly added link with respect to already existing links on the paths. The most common way to describe the range of variation is standard deviation or variance (usually denoted by the Greek letter sigma: σ).

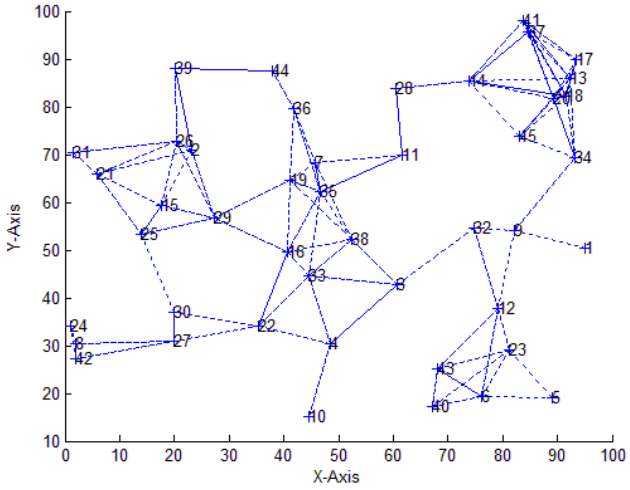


Figure 4.15 Random Deployments of SNs in 100*100

Simulation Setup

To establish the required simulation environment, a simple scenario using GPSR [134] is established where routes are formed taking geographic distance as metric. Next step is to use

key-shares between SNs as their distance metric. In generic keyed scenario a SN is preferred over others if it shares more key than alternates.

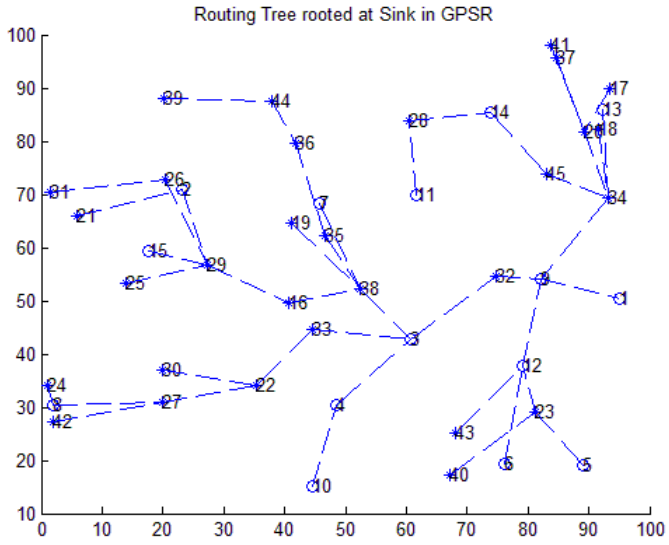


Figure 4.16 Routing Tree in GPSR

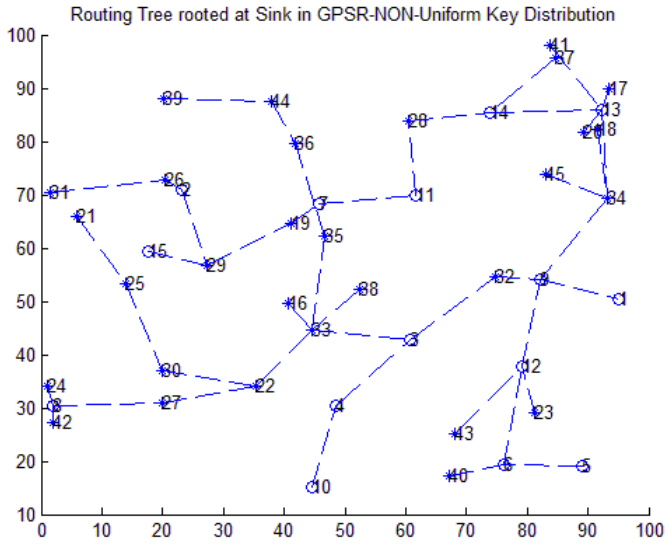


Figure 4.17 Routing Tree in GPSR under Non-uniform key distribution

GPSR under non uniform key distribution scheme finds routes form BS to SNs with effort to maximize keys on the routes between BS and SNs {eqn. 4.16}. Finally GPSR was simulated under non uniform key management using IR values as the distance which tries to minimize the keys in the routes as well limits the variance in number of key values on the routes. Simulation considered following values for various protocol parameters $c = 2$, $k_1 = 45$, $k_2 = 60$, $N = 45$,$n_1 = 30$,$n_2 = 15$ and $K = 1000$. The network to be studied is deployed in 100x100 area with transmission range = 19. HWSN have considered two classes of SNs and deployment of

SNs is as shown in Figure 4.15. SNs are numbered from 1 to 45 with 1 acting as BS. The SNs are pre distributed with keys by BS and deployed thereafter. The neighbourhood of SNs is shown connected. Figure 4.16, 4.17 and 4.18 shows the routing trees in GPSR, GPSR-NONUNIFORM, and GPSR-VAR-NONUNIFORM scenarios respectively.

In Figures 4.16, 4.17 and 4.18 routes in three scenarios are differing from others to some extent as per distance metric. It must be understood that next-hop SNs are limited by the neighbourhood. This limitation is even more pronounced in keyed paths. The graph in Figure 4.19 exhibits a comparison of route lengths in three different scenarios.

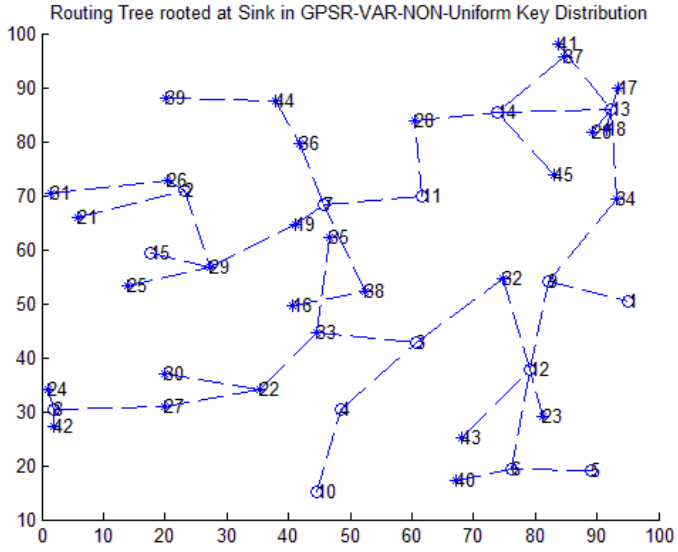


Figure 4.18 Routing Tree in GPSR under VARIANCE non uniform key distribution

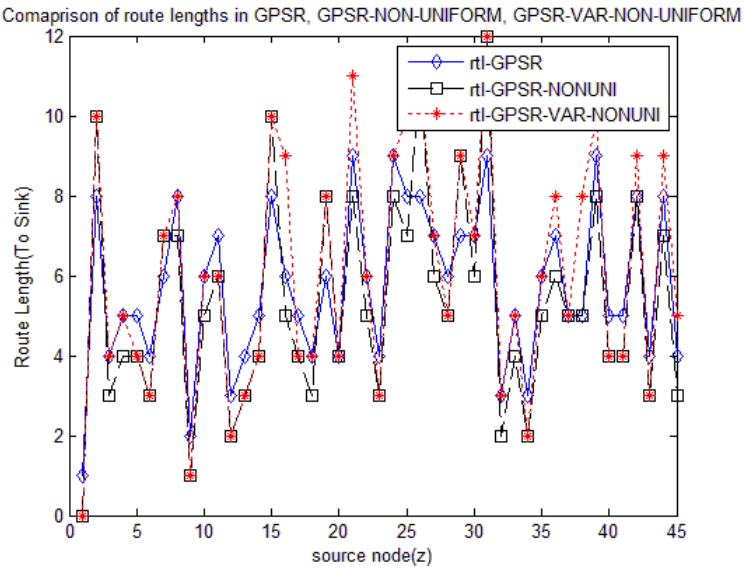


Figure 4.19 Route lengths comparison in three scenarios.

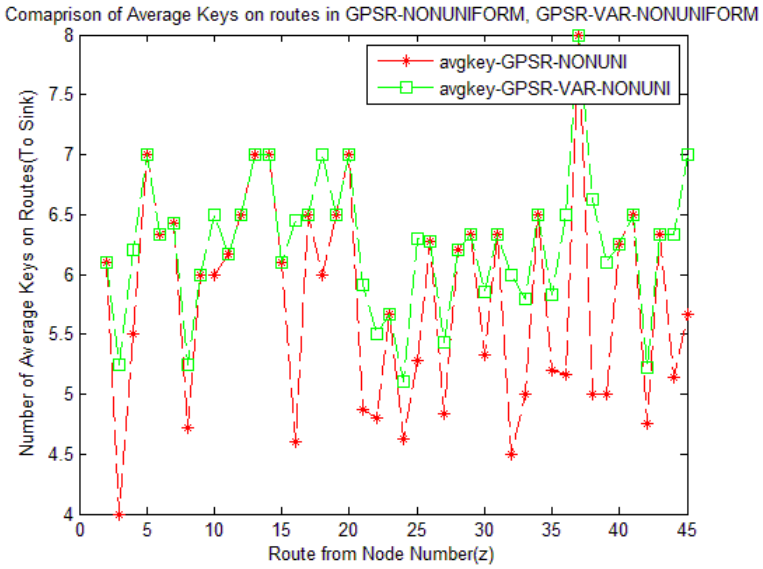


Figure 4.20 Comparison of average keys on routes in GPSR GPSR-NONUNIFORM and GPSR-VAR-NON-UNIFORM

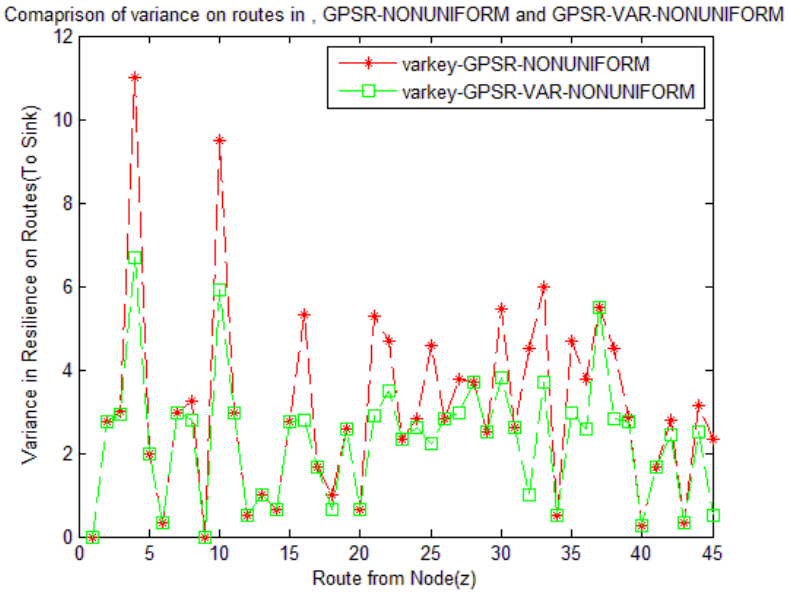


Figure 4.21 Comparison of variance in number of Keys on routes in GPSR-NON-UNIFORM Key distribution and GPSR-VAR-NON-UNIFORM Key distribution

Average keys on routes from SNs are shown in Figure 4.20 under non uniform and variance conscious non-uniform keyed paths. Graph in Figure 4.21 show the variance in keys values on the routes in GPSR under non-uniform and variance conscious scenarios. Visibly the variance in this scheme for secure version of GPSR has reduced in most of the cases under neighbourhood limitation in random key distribution environment. The variance in keys values for hops on each route is drawn in Figure 4.21.

4.3.5 Discussion

The resilience of any path is determined by the resilience of the weakest link. There is huge possibility that newest link added to the route is weakest with respect to resilience of the route being formed. This weakest link decides the resilience of the route. In our proposal we defined a value IR which should be minimized while adding a new link on any route. The mathematical modelling and simulation validate the approach and successfully brings down the variation in the key values in the links. It is perceived in many works that next-hop selection should add maximum possible keys to total keys in the route, but simulation of such scenarios revealed that it may result in adding some link which is weaker with respect to links already added. Graph in Figure 4.20 reveals that average keys on the routes under such perception is not always the highest possible. This perception is even challenged by results on route lengths in Figure 4.20. Route lengths under such perception are smaller than in this proposal but reduced or smaller routes should have more average number of keys on routes. Approach in this proposal has increased the route lengths in most of the cases and simultaneously improved values of average keys on those routes. If average keys on routes considered as quality or quantity of resilience then we improved upon that. Going further approach brought down the variance in resilience of new links being added. The comparison in variance of keys on routes is plotted against the perceptions in literature in Figure 4.20 and if it was possible scheme is able to reduce variance in limitation posed by neighbourhood.

4.4 Secure Data Collection using Mobile Sensors in Statically Deployed SNs

Often security solutions add overhead in terms of extra energy requirements. A secure data collection from statically (immobile) deployed hierarchical HWSNs is developed in this section. MNs introduce heterogeneity to WSN. Movement of MNs in WSN poses issues of authentication, re-authentication, and privacy of MNs. Proposal is evaluated for energy conscious security solution using key management for WSN. Proposal introduced a novel Two Hops online Authentication (THA) scheme for MN's authentication and re-authentication. Proposal exploits asymmetric, symmetric pre-distributed and dynamic key management schemes. Energy efficiency in this proposal is established through simulation. The scheme is based upon a state of art in routing scheme for hierarchical WSN and popularly known as LEACH [99]. The details of LEACH are specified can in Section 2.5.

4.4.1 Mobile Wireless Sensor Networks (MWSN)

In this scheme a new framework for energy conscious and secure data collection in sensor networks has been proposed and is called MWSN. MWSN use MNs for data collection and replaced data sending by CHs to BS in [99] and [126]. To address the authentication and re authentication due to mobility of MN's a novel and WSN customized Two Hop online Authentication (THA) scheme is proposed. THA authenticates MNs in new network component. Authentication of Static Sensor Nodes (SSNs) is ensured using pre-deployed symmetric secret key.

4.4.2 Network Elements and Network Model

Network architecture of MWSN is given in Figure 4.22. MWSN consists of five types of elements:

- **Base Station (BS):** BS is assumed to be situated at secure location and is equipped with protection for physical, cyber and natural disaster. BS is equipped with high bandwidth, large energy and storage space with faster computation capability.
- **Static Sensor Node (SSN):** SSN in MWSN works as data collector. SSNs sense data and relays data to Delivery Points.
- **Delivery Points (DPs):** DP has similar storage, energy and computation capability like normal SSN. DPs are identified by using clustering approach used in [99] and [126]. Transmission range of DPs is fixed at same level as SSNs. DPs work as secure data relay (delivery points) between MNs and group of SSNs. DPs are chosen from within a network component using order/random selection method.

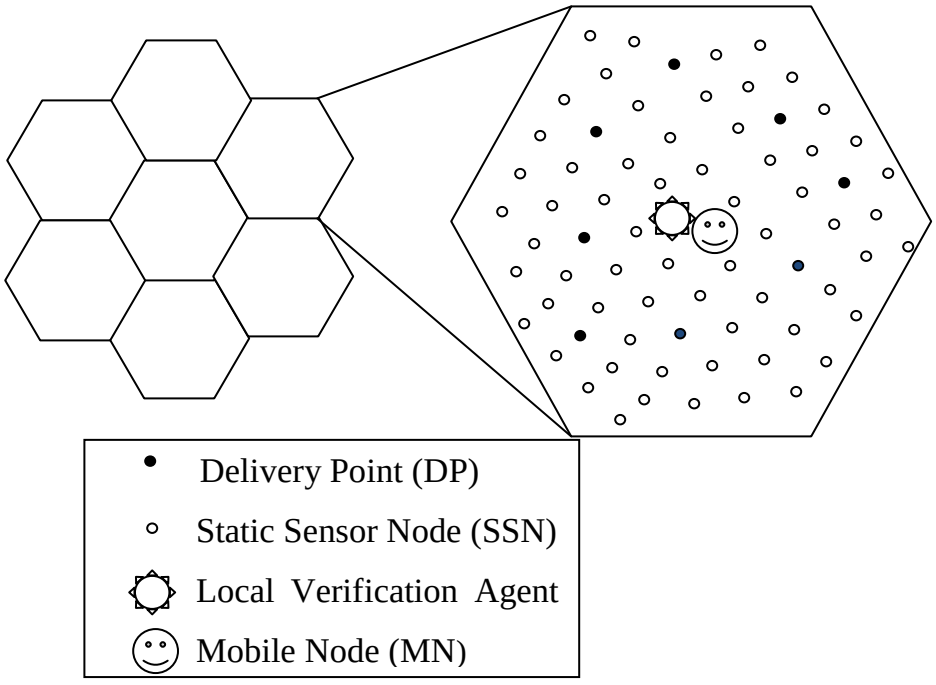


Figure 4.22 Architecture of MWSN framework

- **Local Verification Authority (LVA):** LVA is a special node in each network component. LVA authenticate MNs in MWSN. LVA can synchronize with respect to BS in MWSN and thus provides synchronization to other elements in MWSN.

- **Mobile Node (MNs):** MNs differs on mobility, energy and capacity storage, from SSNs. MN can transition from one cluster to another cluster and get authentication from BS via LVA. MNs receive data collected in the cluster via DPs in the network component.

MWSN concentrates on energy aspects of SSNs and security aspect of SSNs and MNs while collecting data using MN. Network is divided into network components {Figure 4.22}. Each network component consists of 100 SNs and is unit of discussion in MWSN. SSNs in MWSN collects data after sensing and deliver sensed data to nearest DP and ensure integrity. DPs deliver data to MNs after MN has achieved authenticated in network component.

4.4.3 Proposed Scheme

Network is assumed to be pre deployed in a large geographical area. Network is divided into smaller networks called network component or components (for simplicity). Network component is subset of total number of SSNs.

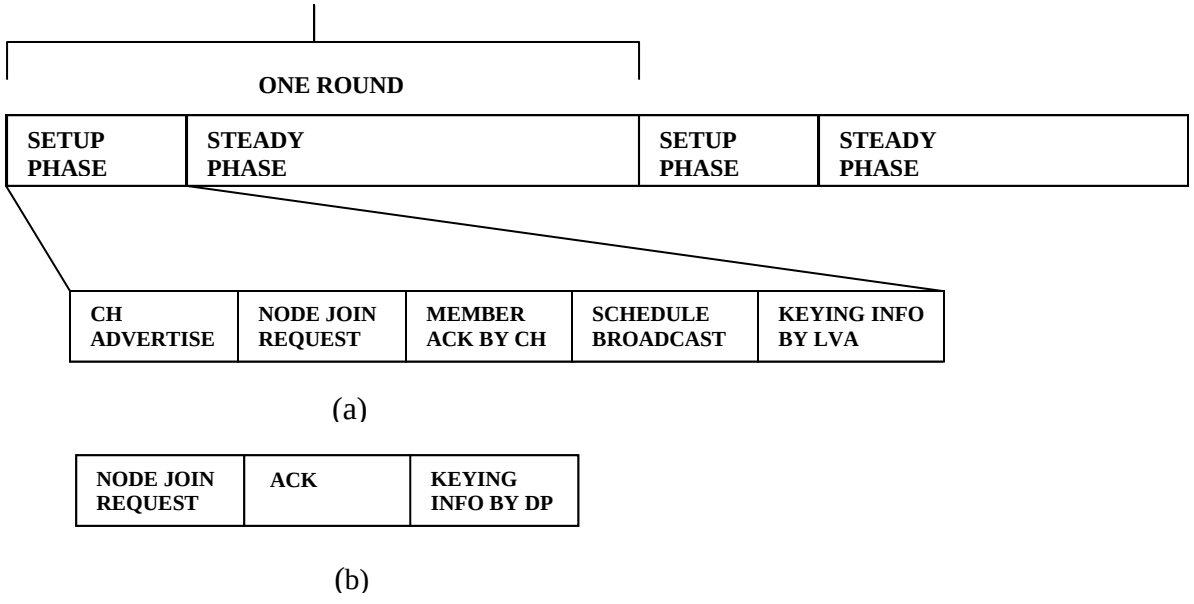


Figure 4.23 (a) Protocol Operation in MWSN (b) Variant SETUP Phase in MWSN

A clustering scheme proposed in Heinzelman's Scheme (LEACH) in [99] and Shin's Scheme in [126] is used for network component level clustering. Using LEACH we identify DPs in each network component. Each network component contains one special node called LVA. The role of LVA in each network component is to authenticate MNs before MNs can request for any data delivery. DPs aggregate data to reduce data redundancy. To ensure integrity; the data has to be encrypted using a group key in its delivery zone. Group key establishment is discussed in Section 4.4.4.4. MNs may transit from one cluster to another to collect data and require re-authentication.

4.4.4 Basic Operation of Proposed Scheme

The operation of protocol for static sensor network consists of SETUP phase and STEADY phase. SETUP phase help identify the DPs in each network component for the following round. STEADY phase is meant for communicating with selected DP for sending sensed data. SETUP phase in MWSN consists of five messages as shown in Figure 4.23. CHs are selected as per criteria explained in [99] and [126]. DP ADVERTISE is used to announce the availability of DP in the transmission range. NODE JOIN REQUEST message is sent by SSN nodes to selected DP for membership. ACK is used for membership confirmation message to member SSN. KEYING INFO message is the information about keying material to be used during following round. After identification of member SSNs DP broadcast schedule using SCHEDULE BROADCAST. SETUP phase messages for round 1 is give in Figure 4.23(a) and for successive rounds in Figure 4.23(b).

4.4.4.1 Key Distribution and Establishment

MWSN used a combination of pre-distribution and dynamic (periodic) key generation. MNs are pre-distributed with a secret key (K_{secret}^{MN}), public key of BS (K_{pub}^{BS}), two large integer prime numbers P_{MN} and Q_{MN}, network public keyK_{pub}^{MWSN}. Each MN stores three keys and two prime numbers. Each LVA is provided with public/private key pairs ($K_{pub}^{LVA_A}$ & $K_{prt}^{LVA_A}$)(where A represents ID of LVA), public key of BS (K_{pub}^{BS}), two large integer prime numbers P_{LVA_A} and Q_{LVA_A}, network public/private key (K_{pub}^{MWSN} & K_{prt}^{MWSN}) and a Random Number Generator (RNG) for secret key generation using $f_{RNG}()$. Each LVA maintains five keys, two large prime numbers and a RNG. LVA also stores value of R, a large prime number deployed offline in every DP and SSN.

SSNs are allocated with one large integer prime number value i.e. R, network public keyK_{pub}^{MWSN}, additive component of group key (C'_{intra} or C_{intra}) and a SN's secret key K_{secret}^{SSN}. LVA are provided with list of SSNs. Each SSN stores two keys and one prime number. Each element in MWSN is able to detect its compromise and can erase its keying material before it is exposed. SNs are pre-deployed with a certificate called Node Compromise Certificate (NCC).

4.4.4.2 Post Deployment Network Start Up

Network component wise DPs are identified in MWSN. DPs are used as data collector and data aggregation points for its delivery zone members. Each network component may have multiple delivery zones. Each delivery zone is controlled by its DP. The number of DPs varies with varying values of p [99]. We assume that each SN of the network component is in the

communication range of one-or-more DP. Each network component is equipped with an LVA. LVA broadcasts an SYN message in its transmission range to synchronize the START/STOP of current delivery round (CDR).

$$SYN: LVA \rightarrow * \tag{4.22}$$

SNs listening SYN message synchronize for CDR. Also LVA deliver the value of Q'_{MN}, P'_{MN} and value of C_{intra} to each SSN in the network component using SSN's secret key K_{secret}^{SSN}. DPs also receive Q'_{MN}, P'_{MN} and value of C_{inter} using secret key DPs. Where Q'_{MN} and P'_{MN} are the current values of MN's prime numbers i.e., P_{MN} and Q_{MN} . Messages are sent in unicast to SSN; and are time-stamped to counter the replay attack. Only legitimate SSNs and DPs can decrypt the messages from LVA. Compromised SNs and programmed SNs will not be able to participate in the following CDR.

$$\mathrm{LVA} \rightarrow *: \mathrm{AUTH}$$
$$\mathrm{MN} \rightarrow \mathrm{LVA}: \mathrm{JOIN}\left(\mathrm{MN_{ID,}LVA_{ID}}, (\mathrm{P_{MN}}, \mathrm{Q_{MN}})_{\mathrm{K_{pub}^{mwsn}}}\right)$$
$$\mathrm{LVA} \rightarrow \mathrm{BS}: \mathrm{VERIFY}\left(\mathrm{LVA_{ID}}, (\mathrm{P_{MN}}, \mathrm{Q_{MN}})_{\mathrm{K_{pub}^{BS}}}\right)$$
$$\mathrm{BS} \rightarrow \mathrm{LVA}: \mathrm{VERIFIED}\left((\mathrm{Q_{MN}\ and\ Q'_{MN}})_{\mathrm{K_{pub}^{LVA_{ID}}}}\right)$$
$$\mathrm{LVA} \rightarrow \mathrm{MN}: \mathrm{CONF}\left((\mathrm{Q_{MN}}, \mathrm{Q'_{MN}}, \mathrm{P_{MN}\ and\ P'_{MN}})_{\mathrm{K_{secret}^{MN}}}\right)$$

Figure 4.24 Mobile Node's Authentication using THA

$$\mathrm{LVA} \rightarrow *: \mathrm{AUTH}$$
$$\mathrm{MN} \rightarrow \mathrm{LVA_{dest}}: \mathrm{TRANS-JOIN}\left(\mathrm{MN_{ID,}LVA_{dest}}, \left(\mathrm{P_{MN}}, \mathrm{Q_{MN}}, \mathrm{P'_{MN}}, \mathrm{Q'_{MN}}, \mathrm{LVA_{src}}\right)_{\mathrm{K_{pub}^{mwsn}}}\right)$$
$$\mathrm{LVA_{dest}} \rightarrow \mathrm{LVA_{src}}: \mathrm{VERI-TRANS}\left(\mathrm{MN_{ID,}LVA_{dest}}, \left(\mathrm{P'_{MN}}, \mathrm{Q'_{MN}}, \mathrm{LVA_{src}}\right)_{\mathrm{K_{trans}}}\right)$$
$$\mathrm{LVA_{src}} \rightarrow \mathrm{BS}: \mathrm{VERIFY}\left(\mathrm{LVA_{dest}}, (\mathrm{P'_{MN}}, \mathrm{Q'_{MN}})_{\mathrm{K_{pub}^{BS}}}\right)$$
$$\mathrm{BS} \rightarrow \mathrm{LVA_{dest}}: \mathrm{VERIFIED}\left((\mathrm{Q'_{MN}\ and\ Q''_{MN}})_{\mathrm{K_{pub}^{LVA_{dest}}}}\right)$$
$$\mathrm{LVA_{dest}} \rightarrow \mathrm{MN}: \mathrm{CONF}\left(\left(\mathrm{Q'_{MN}}, \mathrm{Q''_{MN}}, \mathrm{P'_{MN}\ and\ P''_{MN}}\right)_{\mathrm{K_{secret}^{MN}}}\right)$$

Figure 4.25 Mobile Node's Re Authentication using THA

4.4.4.3 Authenticating Mobile Node: THA Protocol

In this section we detail a novel Two Hop online Authentication (THA) protocol. MNs obtain some keying and authenticating material from BS in offline mode. MNs may enter any network component initially. LVA in the network component has to register MN and verify the credentials of MN. LVA broadcast AUTH message for MNs. Each MN may receive AUTH

message from one-or-more LVA. Depending upon the signal strength; MNs select one of LVA as their Home Network Component (HNC). Steps in THA are given in Figure 4.24. MN replies LVA with JOIN request. LVA decrypts JOIN request with K_{prt}^{mwsn}. LVA dynamically generates $MN's$ secret key by locally available function $f_{RNG}(P_{MN})$. LVA notify/enquire authenticity of MN from BS. BS also concludes on the integrity of LVA and MN by decrypting this message. BS reply/maintain legitimacy/location information to LVA. This is verification completed confirmations message from BS. Only legitimate LVA can decrypt messages from BS. It contains pair of prime numbers, i.e., Q_{MN} and Q'_{MN}, where Q'_{MN} is value of Q_{MN} for new CDR. At this point LVA authenticate MN by sending confirmation (CONF) message to MN. CONF is encrypted using secret key K_{secret}^{SSN} of MN. CONF contains both old and new values of Q_{MN} as well as P_{MN}; i.e., Q_{MN}, Q'_{MN}, P_{MN} and P'_{MN}, where P'_{MN} is locally generated by LVA; P'_{MN}, will be used during transition from present network component to next network component. At this point LVA and MN both achieved authentication from BS. Simultaneously; BS also update/maintain the Data Base for Present Location (DBPL) of MNs. This process involves two hops, MN-LVA and LVA-BS respectively (2 Hop Communication).

4.4.4.4 MNs Transition

MNs are free to move from one network component to another. Assume that a MN moves to a destination network component (governed by LVA_{dest}) from source network component (governed by LVA_{src}). Reauthentication of MNs during transition is completed using THA {Figure 4.25}. MN must maintain Q_{MN}, Q'_{MN}, P_{MN} and P'_{MN}. MN presents TRANS-JOIN request encrypted with K_{pub}^{mwsn} to LVA_{dest}; with updated both values of pair of prime numbers i.e.,Q_{MN}, Q'_{MN}, P_{MN} and P'_{MN}. TRANS message also contains ID of LVA_{src}. LVA_{dest} uses K_{prt}^{mwsn} to decrypt the message and retrieve prime number's pairs and ID of the LVA_{src}. Now LVA_{dest} creates VERI-TRANS message from TRANS-JOIN. Message is encrypted with dynamically generated key K_{trans} where $K_{trans} = f_{RNG}(P'_{MN})$. We call it transverse key. LVA_{src} can decrypt the message and informs the movement of MN to new BS LVA_{dest}. LVA_{src} inform ID of LVA_{dest} to BS. Now LVA_{src} delete any information pertaining to MN at this moment. BS sends movement confirmation to LCA_{dest}, with message contents Q_{MN} and Q'_{MN}, where Q'_{MN}, is value of Q_{MN} for new CDR. Message is encrypted with $K_{pub}^{LCA_{dest}}$. A CONF message is sent to MN by LVA_{dest}. As every detail pertaining to MN is deleted by LVA_A, no communication can be traced or retrieved by LVA_{src}. MN replaces Q'_{MN} and P'_{MN} with their latest values i.e., Q''_{MN} and P''_{MN}respectively. LVA_{dest} also maintains $\mathrm{P_{MN}}$, $\mathrm{Q_{MN}}$, $\mathrm{P''_{MN}}$ and $\mathrm{Q''_{MN}}$ for CDR.

LVA → SSN: $\left(CDR, TS, (Q'_{MN}, P'_{MN}, C_{inter} or\ \mathrm{C'_{inter}})_{\mathrm{K_{secret}^{SSN}}}\right)$

LVA → DP: $\left(\mathrm{CDR, TS, (Q'_{MN}, P'_{MN}, C_{intra} or\ C'_{intra})_{K_{secret}^{DP}}}\right)$

Figure 4.26 CDR Specific Group Keying/ Refreshing

$$K_{intra}^{DP_i} = (R * Q'_{MN} + C_{intra} + C'_{intra}) \bmod P'_{MN}$$

$$K_{inter}^{LVA_i} = (R * Q'_{MN} + C_{inter} + C'_{inter}) \bmod P'_{MN}$$

$$SSN \rightarrow DP: (Data)_{K_{intra}^{DP_i}}$$

$$DP \rightarrow LVA: (Data)_{K_{inter}^{LVA_i}}$$

$$LVA \rightarrow MN: (Data)_{K_{secret}^{MN}}$$

Figure 4.27 Data Delivery via DPs in Delivery Zones

4.4.4.4 Secure Data Collection

SSNs collected data from local surrounding and should be delivered to DPs as per SN's schedule. Assume that ID of DP under discussion is A. SNs deliver data to nearest DP using group key for DP. We propose to use modular arithmetic based keying scheme for data delivery. MN as well as LVA both knows the values of P'_{MN} and Q'_{MN}. Also; LVA delivers the value of Q'_{MN}, P'_{MN} and value of, C_{intra} to each SSN in the network component using K_{secret}^{SSN} of corresponding SSN. LVA computes K_{secret}^{SSN} and K_{secret}^{DP} using secret key generation function $f_{RNG}(R)$. SSNs compute group key with i^{th} DPs; using modulo P'_{MN} operation and obtain $K_{intra}^{DP_i}$; where $K_{intra}^{DP_i} = (R * Q'_{MN} + C_{intra}) \bmod P'_{MN}$. DPs deliver data to MN using encryption with K_{inter}^{LVA}; where K_{inter}^{LVA} is obtained using moduloP'_{MN} operation as $K_{inter}^{LVA} = (R * Q'_{MN} + C_{inter}) \bmod P'_{MN}$. During next CDR, LVA sends updated value of $P'_{MN}, Q'_{MN}$and increment C'_{inter} and C'_{intra} for SSN and DPs; for use in next CDR. The detail of round wise key refreshing and secure data delivery using group key is given in Figure 4.26 and 4.27.

4.4.4.5 Rekeying or Key Refreshing

Group keys are refreshed as soon as MN enters the cluster and received join confirmation. LVA send only updated value of values of P'_{MN}, Q'_{MN} and increment C'_{intra} to SSNs. Similarly LVA sends only updated value of of P'_{MN}, Q'_{MN} and increment C'_{inter} to DPs and initiate next CDR. As Q'_{MN} is obtained via BS, so refreshing information is maintained simultaneously at BS also. SSNs and DPs generates new group key. Because; new group key is generated for next CDR, thus key refresh mechanism in MWSN is time-limited key refresh mechanism.

4.4.5 Simulation Study

We have simulated MWSN for a large sensor network spread over a large area. The shape of the network is immaterial for large sized WSNs. The network consists of many average sized network components of 100 SNs. The simulation is performed using a MATLAB version 7, on Intel core i5, with 3 GB RAM. The simulation is done in spirit of LEACH [99] with modification as per the operational requirements of MWSN. We consider [99] and [126] as our reference protocol. The simulation was repeated enough to arrive at the results. For simplicity and

feasibility we considered single network component in WSN for simulation and results. Within each network component LVA is situated at centre of the network component. The energy consumed in computation cycles at SNs is considered negligible as compared to energy used in unicast, multicast and broadcast transmission. We assumed that MN moves to a network component and hooks up at LVA. Network component's DPs are selected anew per round; before round's steady phase.

Table 4.2, describes the notation, meaning and the value of various parameter of simulation. MN is equipped with sufficient battery backup and thus energy issues of MN are ignored in our study. The energy spent in movement of MN is out of scope of present study. We ignored energy usage in encryption and decryption for present study. The location of LVA and MN is fixed at the centre of network component; for the round under investigation. We used first-order energy model proposed in [99] and [126], [136] and [137] as is specified in the code available with proposal. The propagation model considers error free wireless channels. Power control can be used to invert this loss by appropriately setting the power amplifier.

If the distance of propagation is within the d_0, the free space (fs) model is used; otherwise, the multipath (mp) model is used [138]. Thus, to transmit a k-bit message along the distance d, radio power consumption is given by

$$\begin{aligned} E_{Tx}(k.d) &= E_{tx-elect}(k) + E_{Tx-amp}(k,d) \\ &= \begin{cases} kE_{elect} + k\varepsilon_{fs}d^2, & d < d_0 \\ kE_{elect} + k\varepsilon_{mp}d^4, & otherwise. \end{cases} \end{aligned} \tag{4.23}$$

The energy consumption in eqn. {4.23} is specified for transmission and amplifier components. First part in eqn. {4.23} express energy spent by the transmission device, and the second part specifies the energy spent by amplifier. Receiving is free from amplification and thus only energy spent is for electronics in receiver module. Eqn. {4.24} specifies the energy spent in receiving k-bit data.

$$E_{Rx}(k,d) = E_{Rx-elec}(k) = kE_{elec} \tag{4.24}$$

In above equations E_{elec} specifies radio electronics transmission/reception energy considering wireless environment factors with ε_{fs}^2 and ε_{mp}^4 represents constant values for amplifier considering the distance to the receiver and accepTable bit-error rate. A part of energy store is spent on aggregation and is specified as E_{da}. For each network component in MWSN, the communication energy parameters are as shown in Table 4.2.

4.4.5.1 Energy Analysis

In this section we present energy analysis of MWSN. We have performed simulation using MATLAB. We assumed uniform SN deployment for each network component. Deployment for one network component is as shown in Figure 4.28. The number of SN per network component is fixed to 100. We have compared MWSN with contribution in Heinzelman's scheme [99] scheme and Shin's scheme [126].

Table 4.2 Simulation Parameters in MWSN framework

Parameter	Description	Value
N	Number of SNs	100
P	SN's election probability as Delivery point	0.5
E_0	Initial Energy	1.0 Joules
L	Packet Length	6400 Bits
CL	Control Packet Length	200 Bits
E_{elec}	Circuit Electronics energy consumption	50×10^{-9}
E_{Tx}	Transmission Energy per Bit	50×10^{-9}
E_{Rx}	Receiving Energy per Bit	50×10^{-9}
E_{fs}	Energy Dissipation in Free Space Model	10×10^{-12}
E_{mp}	Energy Dissipation in Multipath Model	0.0013×10^{-12}
E_{da}	Energy Dissipation in Aggregation	5×10^{-9}

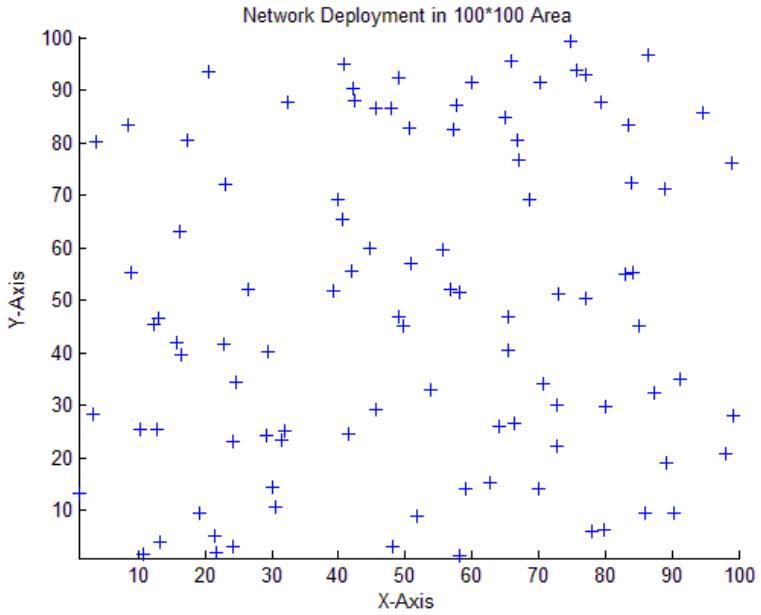
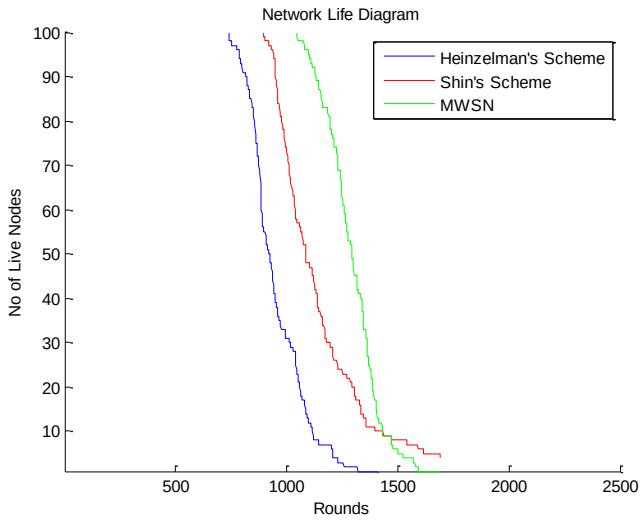
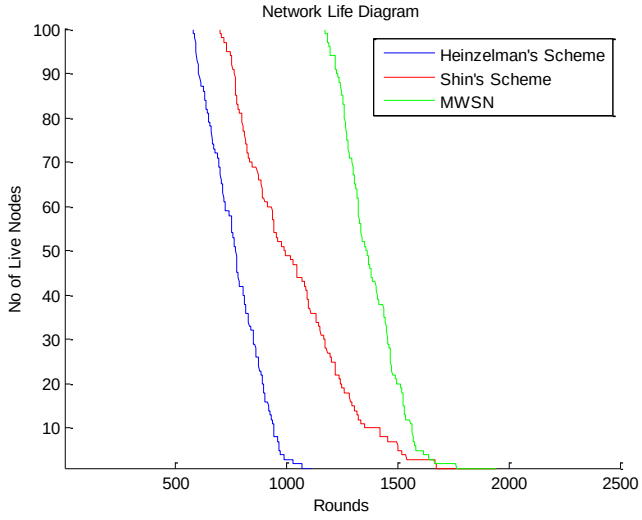


Figure 4.28 Deployment in a Network Component

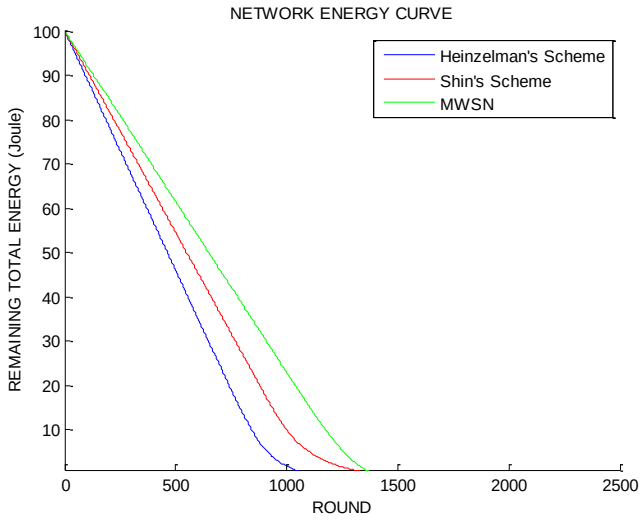
In Heinzelman's scheme and Shin's scheme location of BS is kept fixed to (50,175) and is outside deployment area. In MWSN we have considered the (50, 50) as the hook-up coordinate for MN and fixed co-ordinate position for LVA. In MWSN keying information is delivered using control messages by LVA. The energy spent in receiving keying information is considered in our proposal. The keying distribution is unicast communication between LVA and receiving element in MWSN. The energy spent in receiving keying information is considered as part of energy spent in SETUP phase (round initialization).


Network Life Diagram
Heinzelman's Scheme
Shin's Scheme
MWSN
No of Live Nodes
Rounds
100
90
80
70
60
50
40
30
20
10
500
1000
1500
2000
2500

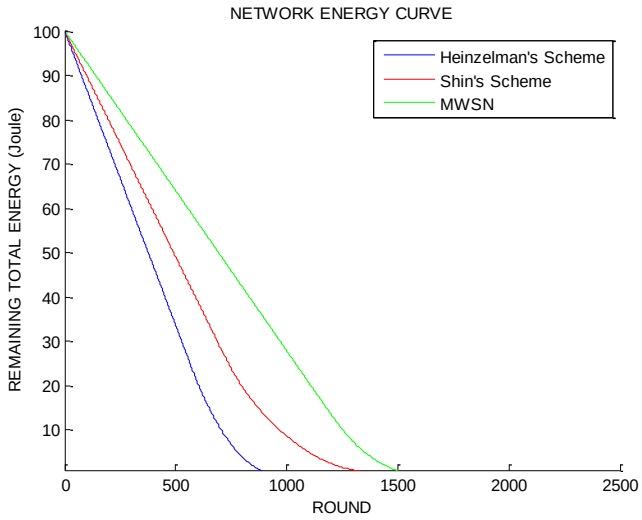
(a)


Network Life Diagram
Heinzelman's Scheme
Shin's Scheme
MWSN
No of Live Nodes
Rounds
100
90
80
70
60
50
40
30
20
10
500
1000
1500
2000
2500

(b)


NETWORK ENERGY CURVE
Heinzelman's Scheme
Shin's Scheme
MWSN
REMAINING TOTAL ENERGY (Joule)
ROUND
100
90
80
70
60
50
40
30
20
10
0
500
1000
1500
2000
2500

(c)



(d)

Figure 4.29 Network Life Time Curve (a) p=0.05 (b) p = 0.10 Network Energy Curve (c) p=0.05 (d) p=0.10

In Figure 4.29 we plot the network life time and network total energy consumption under two different clustering probabilities. Graph in Figure 4.29(a) and 4.29(b) show that in Heinzelman's scheme first SN dies earlier than that of Shin's and MWSN. In MWSN availability of MN within network component has resulted in slower energy usage among SSNs and DPs. In MWSN, DPs deliver data to MN instead of BS. It saved a considerable energy during each transmission to MN. The fixed and within location of MNs results a short distance communication. This prevented some SNs from quickly draining their energy. MWSN's key management cause energy overhead in SSNs. Overhead of key reception by network elements can be seen in Figure 4.29(c) and 4.29(d).

As network continues to decrease in number of SNs, key reception overhead becomes even more pronounced. Thus slope of curve in MWSN is higher than that of Shin's scheme. Output in Table 4.3 also conveys the same fact.

The percentage of initialization energy i.e. the energy spent in setup phase across the life-time of the network is highest in Heinzelman's Scheme. Shin's scheme proves to be most energy efficient in SETUP phase. Higher initialization energy in MWSN is attributed to key reception during setup phase.

Absence of clustering in Shin scheme delayed the death of first SN. In MWSN keying process is accompanied with absence of re-clustering after each round and in-network localization of hooked-MN. This delayed first SN death in MWSN when compared to Heinzelman's scheme and Shin's scheme. Life time curves for MWSN exhibits delayed death of first SN and last SNs. MWSN shows improvement over Heinzelman's [99] and Shin's [126] scheme at $p = 0.05$ and $p = 0.10$. With increasing value of p more DPs are selected per round. This will reduce overhead on each individual DP. With increasing values of p this benefit is available to more DPs.

The graphs in Figure 4.29(c) and 4.29(d); plots the remaining network energy after each round. Initially; SNs are given same amount of energy (1.0 Joule) and with progress of rounds

network's total energy drops slowly. In MWSN, remaining energy falls slowest in comparison to among [99] and [126]. This is attributed to absence of reclustering after each round and short distance communication with MN during data delivery. At higher p values more energy is spent in initialization per round. With the increase in p number of DPs per round also increase. Higher p value results faster depletion of remaining network energy in Heinzelman's [99] scheme compared to Shin's [126] schemes, than at lower p values.

Table 4.3 Energy analysis in MWSN

	Heinzelman's scheme[9]		**Shin's scheme [10]**		**MWSN**	
	P=.05%	P=.10%	P=.05%	P=.10%	P=.05%	P=.10%
First SN Dead (Round)	797	579	854	680	1013	1161
Last SN Dead (Round)	1355	1147	1914	2756	2332	2889
Initialization Energy (% of Total Energy)	18	28	1	1	3	3
Packets to CHs (Discrete Number)	89246	68802	106072	90987	120773	122756
Packets to BS (Discrete Number) or MN	4862	7764	5856	10409	6533	13776

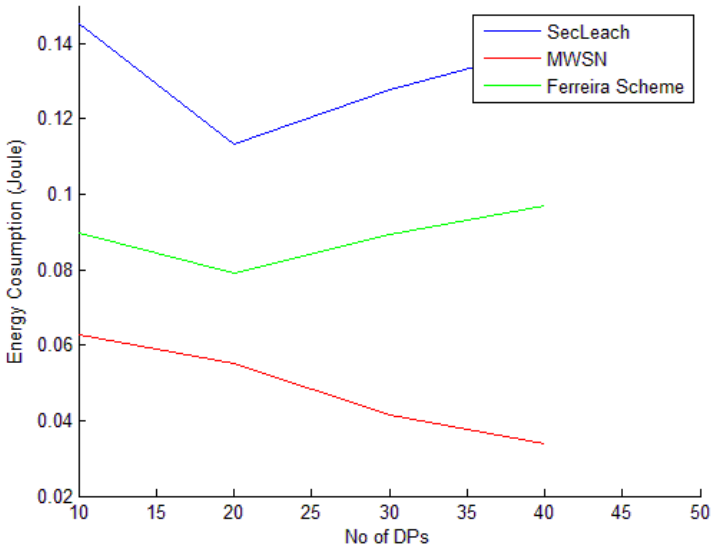


Figure 4.30 Energy Consumption per Steady Cycle

In MWSN, more DPs in each round cause more energy expenses in set-up phase. Shin's [126] scheme spends noting during setup phase which results minimum expenses in setup phase. In MWSN, setup phase includes only key refreshing. MWSN is a secure variant with enhanced life-time.

Figure 4.30 gives effect on energy in MWSN, SecLeach [126] and Ferreira Scheme [28] (all secure variants of LEACH). Schemes in [28] and [27] are representative secure variants of Heinzelman's [60] scheme. MWSN has performed better than both schemes. The improvement is due to MN based data delivery and absence of reclustering in each setup phase. In SecLeach

[119] authors exploit random key distribution with varied key ring sizes and security level. Smaller ring sizes resulted in orphan SNs and reduced actual network size. We studied SecLeach [27] at security level .99 and ring size 100. From Figure 4.30 we can conclude that higher number of DPs results in more energy expense by DPs during data delivery to BS in [27]. Similarly F-Leach [28] supports authentication along with reclustering in each round. The energy expenses in [28] during steady phase are due to long distance data delivery to BS.

4.4.5.2 Performance Analysis

The performance parameters considered for MWSN are storage requirement, communication overhead, resilience and connectivity.

Storage Requirement: The number of keys stored per element in MWSN for security provisions. We also considered memory overhead as number of bytes consumed. The storage requirement of different network elements is based on their distinguished roles. BS is service provider and maintains all keying and location information. The location information is updated with the help of LVA. SSNs sense the data and delivers data to respective DPs. To support encrypted data and updated keying information network elements must store keying information. Part of the information is acquired offline and part after deployment in online mode.

In MWSN, SSNs store one large prime number (R) (20 bytes) [139], public key of network $\left(K_{pub}^{MWSN}\right)$(40 bytes) ([139]), Secret key (K_{secret})(20 bytes) ([139]) and additive component of hybrid congruential generator C_{intra}(20 bytes) and most recent $P'_{MN}$and Q'_{MN} (20 bytes each). Mobile Nodes (MNs) store old value of two large prime numbers $(P \,\&\, Q)$ (20 bytes each), new values of two large prime numbers$(P'_{MN} \,\&\, Q'_{MN})$ (20 bytes each), public key of network $\left(K_{pub}^{MWSN}\right)$ (40 bytes) and secret key (K_{secret}) (20 bytes) and ID information of last visited network component (4 bytes).

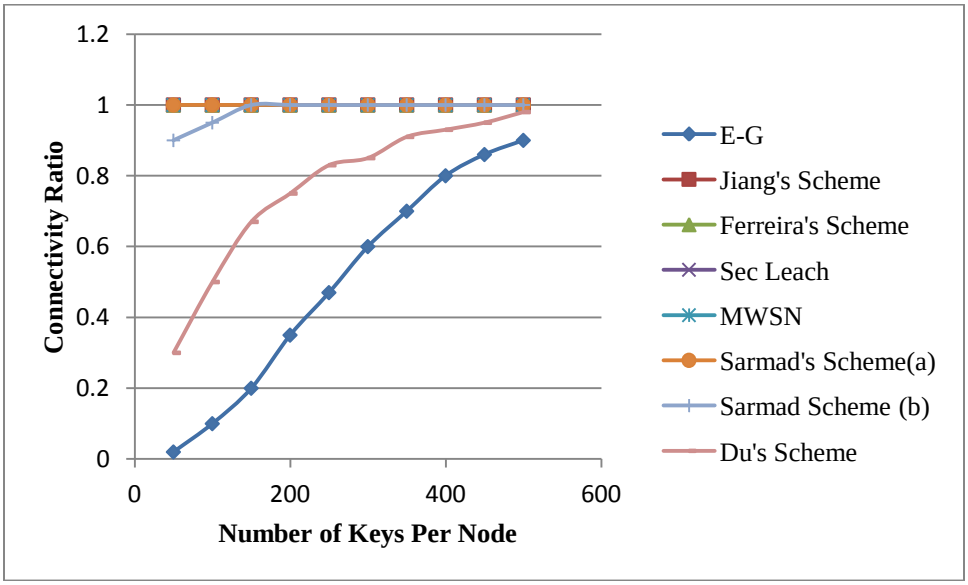


Figure 4.31 Connectivity Ratios vs. Number of Keys per SN

LVA is equipped with network's public/private key pairs $\left(K_{pub}^{MWSN} \,\&\, K_{prt}^{MWSN}\right)$ (40/20 bytes)([139]), BS's public key $\left(K_{pub}^{BS}\right)$(40 bytes)([139]), Two large prime numbers$(P_{MN} \& Q_{MN})$ (20 bytes each), one large prime number (P_{MN})(20 bytes) for most recent authentic MN that moved out of source LVA, one large prime number (P'_{MN})(20 bytes) for authentic MN with-in network component, Secret key generation function (f) and own public/private $\left(K_{pub} \,\&\, K_{prt}\right)$(40/20 bytes)[139] key pairs. This is minimal requirement in secure data dissemination.

We have brought the storage requirement to minimum. Table 4.4 presents the number of keys in each element of MWSN. If the value of $(p = 0.10)$, possible number of DPs in our network component is 10%. For a given network component the storage space requirement can be computed as follows:

$COMP_{storage} = 220 \times N_{LCA} + 144 \times N_{MN} + 140 \times N_{SSN} + 120 \times N_{DP}$, where N_{LCA} , N_{MN} N_{SSN} and N_{DP}represents number of LVA, number of MN, number of SSNs and number of DPs in any network component.

The computation of storage space in [81] exhibits that our security mechanism i.e. MWSN requires only one-third of that of [81], for same network configuration.

In [60], SNs are pre-allocated m keys (20 bytes) from a large key pool. For higher connectivity the value of m should be large. For a network with N SNs the storage space requirements are $20 \times N \times m$. For various values of m we have varying space requirements. For $m = 100$ and $N = 100$ [60] could connect with 60% neighbours using 1-hop. Storage requirement in MWSN is only 10% of the requirement in [60].

A graph in Figure 4.31 demonstrates storage requirement and impact on connectivity ratio. Connectivity ratio in Ferreira's scheme [28], SecLeach [27], along with Jiang's Scheme [88] match connectivity performance of MWSN. Scheme in Ferreira's scheme [28], SecLeach [27] and Jiang's Scheme [88] require only fixed two, hundred and six keys respectively, achieving connectivity ratio equal to 1. Schemes namely E-G [60], Sarmad's Scheme (a) [140] and Sarmad's Scheme (b) [91] and Du's Scheme [81] improve upon connectivity ratio with increase in number of keys per SN. MWSN performs equally acceptable with Ferreira's scheme [28], [91] and Jiang's Scheme [88]. MWSN needs six keys and increasing number of keys is irrelevant in MWSN. MWSN needs more keys than Ferreira's scheme [28]. MWSN also support SN-to-DP authentication. Ferreira's scheme [28] lacks in SN-to-DP authentication. Scheme in Jiang's Scheme [88] lacks to cite any clustering approach. SecLeach [27] requires at least hundred keys for connectivity ratio equal to 1. MWSN is most storage and energy efficient secure variant of LEACH [99].

Table 4.4 Storage requirements in MWSN Framework

Network Element	Number of Keys and Time Stamp	Number of Function Codes	Storage Space
LVA(Source)	09	01	220 bytes
MN	07	-	144 bytes
BS	-	-	-
DP	05	-	120 bytes
SSN	06	-	140 bytes

Table 4.5 Communication Overhead in MWSN framework

Network Element	MN Authentication	MN Transition	Data Delivery	DP Selection/ Round Initialization		
				Heinzelman's Scheme	Shin's Scheme	MWSN
LVA(Source)	3	1	1	-	-	-
MN	1	1	0	-	-	-
BS	1	1	0	-	-	-
DP	0	0	1	2/2	2/0	3/0
SSN	0	0	1	1/1	1/1s	1/1
LVA(Target)	-	2	-	-	-	-

Communication Overhead: It considers number of messages required per round, per element in MWSN during setup and steady phases. It includes messages exchanged for key establishment and secure data delivery by the network elements. The communication overhead is studied for single round. The beginning of round is linked with the movement of MN. We could identify few scenarios that add to communication overhead in MWSN. We considered MN Authentication, MN Transition and Data Delivery to DPs by SSN and DP Selection. DP Selection is varied in MWSN based scheme from that of Heinzelman's Scheme [99] and Shin's Scheme [126]. Table 4.5, describes number of messages per round. Number of message dictates that energy of SSN and DPs has no overhead. Low messaging by DPs and SSN under data delivery concludes that they are least burdened in MWSN. In MN authentication the overhead of communication lies with LVA, MN and BS. MNs and LVA elements of MWSN are free from the concern of energy contentions. The burden of establishing keys and making the information delivery secure, least bothers DPs and SSNs. Similarly MN Transition also requires involvement of LVAs, BS and MN. DP Selection adds communication overhead in DPs and SSNs. As per specification, MWSN {Figure 4.23} requires four messages in total. Three of these messages are sent by DP and one by SSN. The overhead of DP selection is carried in majority by DPs.

In Heinzelman's the DP-ADVERTISE and SCHDEULE are broadcast by DP. In MWSN we broadcast schedule information and DP advertisement only during first round. In remaining rounds we selected DPs using pre determined order stored offline in all SNs. The repeated transmission of schedule and DP advertisement is avoided in MWSN. It reduced the communication cost incurred by DPs in every round.

Energy usage in SETUP and STEADY phase is drawn in Figure 23 (b) and Figure 23 (d). Table 4.4 describes that in Heinzelman's a considerable portion is spent on initialization i.e. SETUP phase. Nearly 18% -34% of energy is spent in SETUP phase in Heinzelman' Scheme [99], for varying values of p. In Shin's Scheme (a non secure variant of LEACH) merely1-2% energy is spent in setup phase. MWSN spends 3% of network's energy in DP selection and key reception. This exhibits that communication overhead in MWSN is less than that of [99] but more than that in Shin's Scheme [126].

4.4.5.3. Security Analysis

Adversary Model: Adversary is equipped with cryptanalysis tools and can perform eavesdropping, fabrication and modification of messages. Adversary can replay old messages and result Denial of Service attack. Adversary can compromise a SN by physically capturing the

SN. It can replace legitimate SNs with programmed SNs and disrupt the normal functioning of WSNs. Adversary can create replications of SSN and place elsewhere in large WSNs.

Resilience: Resilience is the measure of difficulty in breaking into the security. In MWSN pre-deployed content is distributed offline and post deployment content is distributed by LVA. Post deployment information is delivered using SN's secret key, which can be dynamically generated by LVA using secret key generation function $(\boldsymbol{f})$. The prime number to be used is sent by encrypting with network public key ($\boldsymbol{K_{pub}^{MWSN}}$). This message can be decrypted only by LVA and keying information for current round is delivered using encryption with SSNs secret key. LVA is assumed resilient to capture and thus secret key generation function $(\boldsymbol{f})$ is difficult to expose. No one else except concerned SNcan decrypt the information. Moreover the keying information carries time-stamp to help avoid replay of stale messages or efforts to partition the network by providing SNs with old information.

While considering MN; the messages are encrypted using network public key, and are time stamped. The replay of old messages is thus checked using time-stamp information. During authentication and transition most of the communication is between BS and LVAs. The communication between BS and LVA is using PKI and thus offers the resilience of ECC equivalent. Data is encrypted using group key for the round. Group key is updated per round. With no confusion group keys are refreshed after each round and thus SN which are allowed to participate in the current round are provided fresh keying information. To be revoked SNs are not delivered round specific keying information. It helps in time-limited SN revocation.

Attack Analysis: To analyse attack profile of a routing scheme we discuss performance against some significant attacks in WSNs.

Node Compromise attack: Security in MWSN relies mainly on the prime numbers deployed in SSN, MN and LVA. Prime numbers in LVA, SSN are deployed offline and thus safe from online threats of being captured. The mobility of MN requires a fresh pair of prime numbers for use in new network component. Use of ECC based PKI is used for encryption of update messages. BS public key (K_{pub}^{BS}) is deployed in LVA using offline mode. Unless LVA is compromised, (K_{pub}^{BS}) cannot be exposed.

The delivery of new pair of prime numbers to MN is encrypted using secret key of (K_{Secret}^{MN}) MN. MN's secret key (K_{Secret}^{MN}) is deployed offline. SSNs secret key (K_{Secret}^{SSN}) is deployed offline. LVA can generate the secret key of any SN using secret key generation function (f). The messages sent by MN are encrypted using (K_{pub}^{MWSN}) public key of MWSN, which is deployed offline. Node capture attack at LVAs, MNs and SSNs are nullified using NCCs. A compromised SN replaces its keying material with NCC. The communication between SSN and LVA takes place using K_{pub}^{BS} and K_{Secret}^{SSN}. Both these keys are difficult to obtain as these are deployed offline. Data delivery in delivery zones is protected using group key, which is updated after each round. Compromised SNs are not delivered fresh update on group keying material and thus remain ineffective. The periodic update of group keying helps us achieve time-limited node revocation.

Replay Attack: To deliver fresh key in each round messages are timestamped. To overcome replay attack, SSNs and DPs maintain timestamp information of last round. A probabilistic value of next time-stamp can be computed by adding the total schedule duration to last received

timestamp. Even if the probabilistic value of new timestamp can be computed by intruders also; but the fresh value of Q' is difficult to compute. If any SSN has received fabricated message containing fabricated values of Q' and time-stamp; message delivered by SSN can't be decrypted at DPs. This subside the possibilities of fabrication and replay attack.

Node Replication Attack: The location information being updated at BS after each transition helps avoid SN replication attack. LVA of destination network component enquires LVA of source network component for authentication information of MN. Source LVA confirms destination LVA as well as BS for location update of MN concerned. Any conflicting updates at BS can be detected immediately.

4.4.6 Discussion

We have proposed a novel Two Hop online Authentication scheme in MWSN. MWSN addresses authentication, re-authentication and energy efficiency. The hierarchical network organization results in distributed and evenly energy usage. The absence of reclustering and in-network hooked-MN has compensated the overhead due to round wise keying. Our proposal show considerable gains in life-time, energy-usage curve and delayed death of first SN. We compared MWSN with schemes in [99], [126], [27] and [28]. MWSN performs better than each of the scheme in [99], [126], [27] and [28]. The storage and connectivity characteristics of our scheme has also compared with [27], [28], [88], [60], [140], [91] and [81]. Authentication using THA results in minimum storage overhead. Data delivery is secured using group key and secret keys. The time limited node revocation and time-stamping during key refresh process helped us to overcome compromised SN and message replay attacks. The extension using efficient sleep-awake cycles in dynamic clustering is possible extension to this work.

4.5 Secure Multipath Routing Scheme

Multipath routing in WSN has been a long wish in security scenario. Many proposals of Multipath routing has been proposed in ADHOC Networks but under constrained from pre-distributed keying environment most seems ignorant. In WSN where crucial data is reported by SNs in deployment area to their securely located BS, route security has to be guaranteed. Under dynamic load and selective attacks, availability of multiple secure paths is a boon and increases the attacker efforts by many folds. We build a subset of neighbours as front towards destination SN. We also identified forwarders for query by base station. The front is optimally calculated to maintain the security credential and avail multiple paths. In this section we present our proposal with network elements and network model. We could address the query and data routing in our proposal using Query Relays (QR) and Data Relays (DR). QR relays the query from BS to a deployment area or single SN. DR routes replies back to BS using data relays. The routes for query and reply may have same or disjoint routes and ensures minimum delay.

We consider a list of forward SNs as proposed in [120] for selecting SNs out of one hop neighbours towards a particular destination. This is as shown in Figure 4.32. Single destination in WSN happens to be Base Station. We consider HWSN and have fixed transmission range. Diagram in Figure represents an example scenario. Each link in Figure 4.32 cost some energy/security to sender and receiver. With error prone environment each link suffers some error.

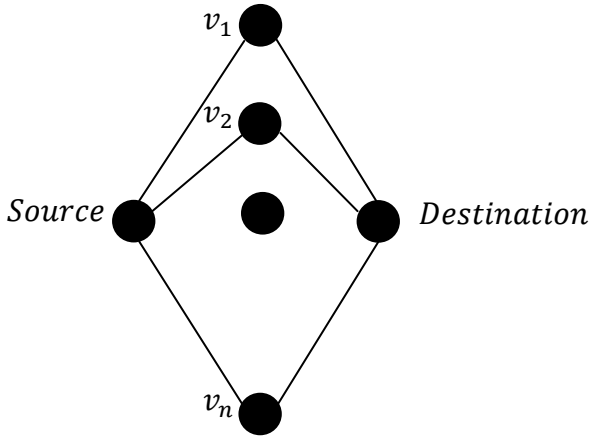


Figure 4.32 Wireless Environment Scenario

Each SN u has selected SNs $\{v_1, v_2, \ldots, v_n\}$ as possible set of forwarding SNs. This is treated as priority list and SN $v_1$considered the most preferred SN in this case. Opportunistically; SNs in forward list forward message sent by u towards BS. There is possibility of multiple copies of message being forwarded by forwarder SNs because of hidden node problems. Opportunistic routing in [120] may suffer from duplicate packets as there is no solution for schedule for SNs forwarding packets via forwarder SNs and security is not considered and an open security challenge. Our proposal is a novel secure multipath routing protocol for WSN. We established effectiveness of our proposal with mathematical analysis.

4.5.1 Network Model and Elements

We consider an HWSN consisting of Large Number of L-Sensors and small numbers of H-Sensors. SNs are assigned unique IDs and are assigned by BS. Each SN has fixed transmission range. We may assume that H-Sensor has comparatively more storage capacity to cater larger number of keys. The resultant network is modelled as multi-hop network. An edge between a pair of SNs implies connectivity between concerned SN pair. Table 4.6 describes notations and their description for this scheme.

Consider $HWSN = \{A, H, L, K, k_1, k_2, E, V\}$, where A denotes deployment area dimension, H denotes number of H-Sensors, L describes the strength of L-Sensors, K is the key pool, $k_1$denotes number of keys given to L-Sensors, $k_2$denotes number of keys pre-distributed to H-Sensors. E denotes the undirected/undirected edge set and V denotes SNs set respectively. Each directed link $u \longrightarrow v$ has a nonnegative weight, denoted by $k(u, v)$ which is the number of shared randomly pre-distributed keys and to be used by SN u together to send a packet to SN v for encryption during forwarding. In addition, each link has a failure probability, denoted by $f(u, v)$, which is the probability that a transmission over link (u, v) is not successful because of unavailability or schedule, i.e., to have a chance of $1 - f(u, v)$ for successful secure transmission a packet to SN v; SN v must be active or not simultaneously receiving other transmission. No transmission is possible if SN's shares no key. To illustrate the idea let us consider a network example in Figure 4.33.

Table 4.6 Notations Used

Notation	Description
u	Source Node
v_i	i^{th} vertex (node) in Node's Graph
$k(u,v)$	Keys between node u and node v
f	Probability of Error
$f(u,v)$	Error Probability between node u and node v
SH_i	Share contributed by i^{th}node
fR_{key}	Forward Key
bR_{key}	Backward Key
M	Member Message
FR	Forward Key Establishment Message
K	Key Pool
k_1	Keys allocated to L-Sensors
k_2	Keys allocated to H-Sensors
$EKA_u^{v_i}$	Expected Key Average of node u to BS through v_i
$NHList(u)$	One hop Neighbour list of node u towards BS
$NHList^{\#}(u)$	One hop Neighbour list of node u towards BS sorted by EKA
S	Selector Set
s_i	Selector node numbered i
EKA_{v_i}	Expected Key Average of node v_i
ID_i	Identity of i^{th}SN

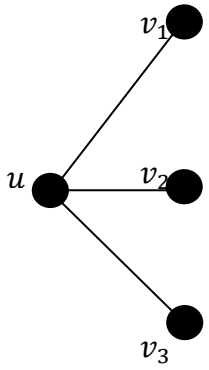


Figure 4.33 Example Scenario

The unavailability probability from the source SN to each SN v_i is f and is same for all links. In our proposal instead of relaying through one SN, say v_i; we propose to use a set of SNs forming a forwarding relays which is a priority list for routing packets towards a fixed destination i.e. SINK/BS. We call such SNs forward relays (fR). We can compute that the expected number of transmissions will be $\frac{1}{1-f}$ for the intended SN v_i to receive the packet correctly. Let SN v_i is selected as member of fR by v_j, $v_k$and v_l SNs, such set of SNs i.e. $\{v_j, v_k, v_l\}$ is Selectors Set

and we will use them as query relays and named as backward relays(bRs) on reverse path from BS to SNs. On the other hand, by having multiple fR to counter for unavailability or outage and considering multiple one-hop SNs in the role of fR, in symmetric-paired-key environment, the expected numbers of transmissions for at least one SN to receive the packet by fRs increase to $\frac{1}{(1-f)^n}$. The denominator term is raised to power n, because of paired keying environment in random key pre-distribution which contrasts from broadcast environment. Assume that fR are maintained as priority list. The fR list is prioritized to indicate which SNs have higher priority to forward the packet. The SN in fR list, which received the packet successfully, will act as new source SNs and route the packet to the target SN via its fR. Finally; main idea of our secure forwarding which we named as Expected Secure Relaying (ESR) is as follows: we let $EAK_u(fR(u))$ denote the Effective Average Key harnessed on the route from SN u to BS, where $fR(u)$ is chosen by u as fR. During initial step EAK_{BS} is initialized to 0 along with all other SNs. The updates on EAK_u, $fR(u)$ and $bR(u)$ are computed periodically.

4.5.2 Setting up Forward Relay Key (fR_{key}): Eqn. $\frac{1}{(1-f)^n}$ specifies the number of retransmissions to be performed for at least one in fRs receive and forward the packet from its selector. If we can increase the denominator to $(1-f^n)$ by providing a broadcast environment with SNs in fR we can reduce number of broadcast for at least one SN in fR receive packet successfully. In case of encryption using all pair-wise keys obtained it is difficult to have broadcast environment. We strive to establish a secure broadcast key between SN and its fR using following method. Let we identify SNs i, j as SNs in fR of SN s. Figure 4.34 and 4.35 shows the steps for establishing fR_{key} .

1: $s \rightarrow i : ID_i || Member\ message\{MAC(M)||M\}_{K_{is}}$
2: $s \rightarrow j : ID_j || Member\ message\{MAC(M)||M\}_{K_{js}}$
3: $i \rightarrow s : ID_s || My\ Share\{MAC(SH_i)||SH_i\}_{K_{is}}$
4: $j \rightarrow s : ID_s || My\ Share\{MAC(SH_j)||SH_j\}_{K_{js}}$
5: $s \rightarrow i : ID_i ||\ FR\{MAC(SH_i \oplus SH_j \oplus SH_s)||SH_j \oplus SH_s\}_{K_{is}}$
6: $s \rightarrow j : ID_j || FR\{MAC(SH_i \oplus SH_j \oplus SH_s)||SH_i \oplus SH_s\}_{K_{js}}$
7: $fR_{key} = SH_s \oplus SH_i \oplus SH_j$

Figure 4.34 Steps for Establishing Forward Key from shares

Consider SN s being selector sends encrypted messages to members i & j in steps 1 to 6 are performed in sequence as shown in Figure 4.34.

Messages in step 1 and 2 are encrypted using all pre-distributed shared keys between $i-s$ and $j-s$ pairs. On verifying the integrity of messages; i & j compute their shares (SHs) individually and sends messages to s encrypted using all pre-distributed shared keys between $i-s$ and $j-s$ in steps 3 and 4 respectively. Having received all shares from $fR(s)$ selector SN s generates its unique share and using X-OR of all shares with its own share generates a unique fR_{key} for communication with DRs only. In step 5 and 6 selector SN s dispatches fR_{key} key

message destined for i & j. Now i &j can generate fR_{key} key using the contents from $fR\ Key$ message and own share there by verify the identity of sender and integrity of message. Following eqn. {4.25} gives an insight of operation:

$$fR_{key} = SH_s \oplus SH_i \oplus SH_j \tag{4.25}$$

Thus fR_{key} key is established using shares from contributors. As the numbers of forwarders are one or more so are the contributions. To compromise the fR_{key}every path between selector and it's fRs has to be compromised. As fR_{key} is common among selectors and fRs; we now are able to exploit the broadcast advantage in wireless medium and reduce the number of trials for at least one of forwarders receive and forward the packet. Increasing the denominator in equation from $(1-f)^n$to $1-f^n$will decrease the number of trials for successful receiving and forwarding of message.

4.5.3 Setting up backward Relay Key (bR_{key})

Consider that a particular SN has obtained distinct fR_{key} for use with distinct selector. Assume that a SN i was in fRs of set S where $S = \{s_1, s_2, s_3\}$. We identify set $\{s_1, s_2, s_3\}$ as possible backward Relay (bR) set of SN i. Let $bR(i)$ denotes bR set of SN i and $bR(i) = \{s_1, s_2, s_3\}$.

1: $i \rightarrow s_1 : ID_i || bR\ SetUp\{MAC(Q)||Q\}_{fR_{key}^{s_1,i}}$

2: $i \rightarrow s_2 : ID_i || bR\ SetUp\{MAC(Q)||Q\}_{fR_{key}^{s_2,i}}$

3: $i \rightarrow s_3 : ID_i || bR\ SetUp\{MAC(Q)||Q\}_{fR_{key}^{s_3,i}}$

4: $i \rightarrow s_1 : ID_i || Shares\left\{MAC\left(fR_{key}^{s_2,i} \oplus fR_{key}^{s_3,i}\right)||fR_{key}^{s_2,i} \oplus fR_{key}^{s_3,i}\right\}_{fR_{key}^{s_1,i}}$

5: $i \rightarrow s_2 : ID_i || Shares\left\{MAC\left(fR_{key}^{s_1,i} \oplus fR_{key}^{s_3,i}\right)||fR_{key}^{s_1,i} \oplus fR_{key}^{s_3,i}\right\}_{fR_{key}^{s_2,i}}$

6: $i \rightarrow s_3 : ID_i || Shares\left\{MAC\left(fR_{key}^{s_1,i} \oplus fR_{key}^{s_2,i}\right)||fR_{key}^{s_1,i} \oplus fR_{key}^{s_2,i}\right\}_{fR_{key}^{s_3,i}}$

7: $bR_{key}^{bR(i),i} = \left(fR_{key}^{s_1,i} \oplus fR_{key}^{s_2,i} \oplus fR_{key}^{s_3,i}\right)$

Figure 4.35 Steps for Establishing Backward Key

Assuming $fR_{key}^{s_1,i}$, $fR_{key}^{s_2,i}$and $fR_{key}^{s_3,i}$ denotes fR_{key}between $s_1 - i$, $s_2 - i$ and $s_3 - i$, SN i can now compute bR_{key} for use as query broadcast key by SN i. Following steps outline the generation and distribution of bR_{key}.

Figure 4.35 shows the steps for establishing backward key. Step 1 to step 3 is encrypted communication from SN i to each of it's $bR(i)$ for bR_{key} key setup. Step 4 to step 6 results into dispatch of partial key to selectors. Step 7 finally; establishes bR_{key} at SN i and selectors $\{s_1, s_2, s_3\}$.

4.5.4 Expected Key Average

Here we present the main idea of calculating the Effective Key Average (EKA) for each SN and selecting the forward Relays (fR). We define EKA as the average keys used to provide a broadcast environment in pre-distributed keying environment. As in above section fR_{key} has been established using all shared pre-distributed keys on links between selectors and fR SNs, which implies that effectiveness of routing in our customised broadcast environment using $fR_{key}$is as effective as is the average number of keys used in setting up of fR_{key}.

Consider a SN u and its one-hop neighbours. We will compute the, EKA and $NHList(u)$ of SN u based on the EKA of its neighbours whose EKA of sending data to the BS has already been computed. We want to choose a subset of neighbouring SNs $N(u)$ as $NHList(u)$of SN u such that the EKA on the route from SN u to send a packet to BS is maximized.

Consider BS as our destination SN. Given a set of SNs U, let $U^{\#}$ defines the sorted list of U based on EKA to send data (via possible relay) to $Sink$.

If $NHList(u)$ denote the priority next hop list of SN u then $NHList^{\#}(u)$ represents sorted next hop list on EKA in decreasing order. i.e, $NHList^{\#}(u) = \{v_1, v_2, \dots, v_{|NHList(u)|}\}$ where $i < j \Longrightarrow EKA_{v_i} \leq EKA_{v_j}$ .Using the theory of probability let F denotes the probability of total failure i.e. a packet sent by SN u is not received by any SN in $NHList^{\#}(u)$. Clearly,

$$F = \prod_{i=1}^{|NHList^{\#}(u)|} f_{uv_i} \tag{4.26}$$

The probability of at least one SN in $NHList^{\#}(u)$ will receive packets successfully, can be computed as $R = 1 - F$. We can compute the number of trials that SN u must perform in order to achieve first success by $1/R$. For e.g. if probability of success is 0.5 then number of trial to have first success can be given by $1/0.5 = 2$. If $1/R$ gives the number of trials that a SN must perform to send a packet which is received by at least one in the $NHList^{\#}(u)$ then using trials information for SNs $NHList^{\#}(u)$ we can compute possible delay incurred to get the packet at $Sink$.

Let, $EKA_u^{v_i}(NHList^{\#})$ denote the expected key average on next hop from u through one of the SN $v_i$in $NHList^{\#}$ then $EKA_u^{v_i}$ that will be used can be computed as:

$$EKA_u^{v_i}\left(v_i \in NHList^{\#}(u)\right) = \frac{k_{uv_1} * \left(p_{uv_1}\right) + k_{uv_2} * \left(p_{uv_2}\right) + \cdots + k_{uv_{|NHList^{\#}(u)|}} * \left(p_{uv_{|NHList^{\#}(u)|}}\right)}{1 - f^{|NHList^{\#}(u)|}} \tag{4.27}$$

Where p_{uv_i}represent the probability of forwarding to v_i in$NHList^{\#}(u)$. As one of the forwarder has to forward ultimately (may require many trials) requires that $\sum_{i=1}^{|NHList^{\#}(u)|} p_{uv_i} = 1$.

For example, if $|NHList^{\#}(u)| = 3$ then $NHList^{\#}(u) = \{v_1, v_2, v_3\}$. If forwarder $v_1$has been assigned highest priority of among three forwarders with $v_2$assigned second then we have

$4X + 2X + 1X = 1$ where $p_{uv_i} = 2 * (i-1) * X$. This implies $p_{uv_1} = 4 * X, p_{uv_2} = 2 * X$, $p_{uv_3} = 1 * X$. This leads to $p_{uv_1} = 0.57, p_{uv_2} = .29,\ p_{uv_3} = .14$. If $f(u, v_i) = .5$
If we assume that $k_{uv_1} = 30, k_{uv_2} = 27,\ k_{uv_3} = 22$ then $C_u^{v_i}(NHList^*) = 54$.

When at least one SN in the forwarder list of SN u received the packet successfully, we need to calculate the expected cost to forward the packet sent by SN u. Let $EKA_u^{BS}\left(NHList^{\#}(u)\right)$ denotes $EKA$for u to forward (using some SNs in the forwarder list of u) the packet to the $Sink$.If $EKA_u^{BS}\left(NHList^{\#}(u)\right)$ represent Effective Average Keys of route through $NHList^{\#}(u)$ can be calculated as follows: assume the relays list is$NHList^{\#} = \{v_1, v_2, \dots, v_{|NHList(u)|}\}$. The probability that SN v_1 forwards the packet is $1 - f(u, v_1)$ and Effective Keys Average of $v_1$is $EAK_{v_1}^{BS}$; then SN v_2 will forward the packet with probability $f(u, v_1) * (1 - f(u, v_2)$ and the Effective Keys Average will be $EAK_{v_2}^{BS}$. Basically, SN v_i forwards the packet if it receives the packet and SNs $v_j;\ 0 < j < i$ did not receive the packet, and in this case, the Effective Average Keys will be $EAK_{v_i}^{BS}$. Hence, $EKA_{v_i}^{BS}$ can be computed as follows:

$$EAK_u^{BS}\left(v_i \in NHList^{\#}(u)\right) = \left(1 - f_{uv_1}\right) * EAK_{v_1}^{BS} + \sum_{i=2}^{|NHList^{\#}|} \left(\prod_{j=1}^{i-1} f_{uv_j}\right) * \left(1 - f_{uv_i}\right) * EAK_{v_i}^{BS} \quad (4.28a)$$

Finally; $EAK_u(NHList^{\#})$ the on route from u to BS is computed as follows:

$$EAK_u\left(NHList^{\#}(u)\right) = \frac{EAK_{v_i}^{BS}\left(v_i \in NHList^{\#}(u)\right)}{1 - f^{|NHList^{\#}(u)|}} \quad (4.28b)$$

$$EAK_u^{BS} = EAK_u^{v_i}\left(v_i \in NHList^{\#}(u)\right) + EAK_u\left(NHList^{\#}(u)\right) \quad (4.28c)$$

Eqn. {4.28} illustrated how to compute EAK of a sender to broadcast a packet if the current chosen forwarder list is $NHList^{\#}(u)$. Eqn. {4.28b} computes tentative EAK which finalizes $NHList^{\#}(u)$ and eqn. {4.28c} computes real EAK by augmenting tentative EAK with last-hop cost computed in eqn. {4.27}. Thus first part i.e. eqn. {4.28b} is EAK for the sender to successfully transmit a packet to at least one receiver in $NHList^{\#}$. The second part i.e. eqn. {4.28c} corresponds to EAK that one of SN in the $NHList^{\#}$ finally to relays the packet to the final destination SN.

4.5.5 Finding the $NHList$

Instead of random selection of SNs from $N(u)$, we choose a prefix of sorted neighbour list $N^{\#}(u)$ as result i.e. $NHList^{\#}(u)$. For a given $N^{\#}(u)$ there can be at the most $|N^{\#}(u)| + 1$

prefixes. Selecting SNs from $N^{\#}(u)$, one at each step provided $EAK_{v_i} > EAK_u$. If v_i fails to satisfy the required condition; every SN ahead of v_i in $N^{\#}(u)$fails to satisfy the said condition.

4.5.6 Routing Algorithm

How SNs will select their forwarder list and how to use expected cost is highlighted in previous section. Now we are able standardize the steps as collection of three algorithms, i.e., $Update\_EAK$, $Compute\_EAK\_to\_BS$ and $Dispatch\_NHList$. These algorithms are presumed to be hardcoded and can be executed as per their requirements. After execution of $Compute\_Cost\_to\_BS$ BS has information of about selectors and Relays. Each selector may have multiple relays and each SN may possess multiple selectors. In each case we have a subset of one-hop neighbours as selector or relays or selectors-relays combined. Using the information received from SNs in deployment area BS is able to compute routes from BS to SNs. BS may use these routes to periodically diffuse query in the network, whereas SNs may use their forwarders towards BS to report any urgent event. The algorithm's pseudo code is described in Figure 4.36.

4.5.6.1 Exchanging $NHList$ List Information

Each SN prioritized their relays in $NHList$. Selection along with priority is informed to relays by selectors. This process may be initiated by SNs after completing the execution of $Compute\_EAK\_to\_BS$.

$Update\_EAK\left(EAK_u\left(NHList^{\#}(u)\right), N(u)\right)$

1: $BEGIN\ \{Update\_EAK\}$
2: Sort the neighbouring SNs $N(u) = \{v_1, v_2, \dots, v_{|N(u)|}\}$ based on their EAK in decreasing order and get $N^{\#}(u)$.
3: $for(i = 1; i < |N^{\#}(u)|; i++)$
4: $if\left(EAK_u\left(NHList^{\#}(u)\right) < EAK_{v_i}^{BS}\left(v_i \notin NHList^{\#}(u)\right)\right) then$
5: $NHList^{\#}(u) = NHList^{\#}(u) \cup \{v_i\}$ and update p_{uv_i}
6: Update $EAK_u\left(NHList^{\#}(u)\right)$ using equation(5) in steps (5.1) and (5.2)
7: $return\left(EAK_u\left(NHList^{\#}(u)\right)\right)$
8: $End\ \{Update\_EAK\}$

$Compute\_EAK\_to\_BS\left(BS, V, EAK_u\left(NHList^{\#}(u)\right)\right)$

1: $BEGIN\ \{Compute\_EAK\_to\_BS\}$
2: $BS\_Broadcast\_Initialize$
3: $Node\_Initialize: EAK_u\left(NHList^{\#}(u)\right) = 0\ , NHList^{\#}(u) = \phi$
4: $Node\_Broadcast\_IDS + EAK$
5: $Node\ Sort\ Neighbour\ List\ on\ EAK$ in decreasing order to get $N^{\#}$
6: $Nodes\ Executes: EAK_u\left(NHList^{\#}(u)\right) = Update\_EAK\left(EAK_u\left(NHList^{\#}(u)\right), N(u)\right)$
7: $u \in V,\ EAK_u\left(NHList^{\#}(u)\right) = 0\ ,\ EAK_{BS}^{BS}\left(NHList^{\#}(Sink)\right) = 0$
8: $Sink\_Limited\_Broadcast\{EAK_{BS}^{BS}\}$
9: $\forall u \in N(BS) Executes:\ EAK_u^{BS}\left(NHList^{\#}(u)\right) =$
$Update\_EAK\left(EAK_u^{BS}\left(NHList^{\#}(u)\right), N(u)\right)$
10: $repeat$
11: $let\ S_1 = V - \{BS\}\ and\ S_2 = \{BS\}$
12: $repeat$
13: $v = min\_cost\{S_1\}$
14: $S_1 = S_1 \cup \{v\}\ and\ S_2 = S_2 - \{v\}$
15: $\forall u \in N(v) \cap S_1 : EAK_{TEMP} = EAK_u^{BS}\left(NHList^{\#}(u)\right)$
16: $\forall u \in N(v) \cap S_1 : NHList^{\#}(u)_{TEMP} = NHList^{\#}(u)$
17: $\forall u \in N(v) \cap S_1\ Executes: EAK_u\left(NHList^{\#}(u)\right) =$
$Update\_EAK\left(EAK_u\left(NHList^{\#}(u)\right), N(u)\right)$
18: $until\ \ S_1 = \emptyset$
19: $\forall u \in V, Node\_Broadcast\_to\_N(u): EAK_u^{BS}\left(NHList^{\#}(u)\right)$
20: $\forall u \in V\ Executes: EAK_u\left(NHList^{\#}(u)\right) =$
$Update\_EAK\left(EAK_u\left(NHList^{\#}(u)\right), N(u)\right)$
21: $until\ \ No\ Change\ in\ EAK\ \ and\ NHList^{\#}$
22: $Dispatch\_NHList^{\#};$
23: $End\ \{Compute\_EAK\_to\_BS\}$

$Dispatch\_NHList^{\#}()$

1. $BEGIN\ \{Dispatch\_NHList^{\#}\}$
2. $u \in V\ , u\ \Rrightarrow NHList^{\#}(u)$
3. $End\{Dispatch\_NHList^{\#}\}$

Figure 4.36 Routing Scheme

Relay SN in $NHList$ are like vectors disclosing direction towards BS. Reverse channel is always available. Now relays have information of their relays and selectors. This information is propagated to BS using unicast messages through relays in $NHList$. Aggregating the information by relays SNs help reduce the number of messages. Selectors are proposed to be used for routing any query towards a region or SN and path through relays to route a reply to destination BS respectively. We have classified the Selector SNs as Query Forwarder and Relay SNs as Data Forwarders.

4.5.6.2 Route Construction

SINK has information of SN wise selectors and relays. For query forwarding SINK constructs query route using pairs like:

$(D, \{Fwd(D)\}),$
$(\{Fwd(D)\},\ \{Fwd(\{Fwd(D)\})\})$
…
$\left(Fwd\left(\{\ldots\{Fwd(\{Fwd(D)\})\}\right), Sink\right)$ (4.29)

Each such pair gives a possible hop on the respective paths. As a result sink may obtain all possible paths towards a specific SN i.e. D or vice-versa. SINK may choose any of such paths for propagation of query. SINK may choose any of the route on the basis of optimization criterion which may be delay, energy, hop count or else. Query with specified route is encrypted /decrypted on the path as it travels from SINK to D.

4.5.7 Performance Analysis

In this section we present a simple and effective validation of this scheme using theorems.

Theorem 4.1: $NHList^{\#}(u)$ of SN u must be a prefix of $N^{*}(u)$.
Proof: we proof this theorem by contradiction. Let v_k, v_{k+1} are two SNs such that SN $v_{k+1}$is in $L^{\#} = L \cup \{v_{k+1}\}$ and $v_k$is not. Let $EAK_u(L^{\#})$is expected key value after and $EAK_u(L)$is expected key values before considering v_{k+1}. Let Δ_{k+1} represent the increment achieved, i.e. $EAK_u(L^{\#}) = EAK_u(L) + \Delta_{k+1}$. Had it been v_{k+1} then $L^{\wedge} = L \cup \{v_k\}$. In $N^{\#}(u)$, v_k comes earlier than v_{k+1}as $N^{\#}(u)$is sorted on effective key averages. This implies $\Delta_k \geq \Delta_{k+1}$ and$EAK_u(L^{\wedge}) \geq EAK_u(L^{\#})$. Thus selection of v_{k+1} ahead of v_k contradicts our selection criterion. Hence $NHList^{\#}(u)$ is prefix of $N^{\#}(u)$.

We further study the properties of forwarder list by introducing another three theorems. The first theorem, Theorem 4.2, shows that if a SN, whose expected cost is less than the expected cost of a prefix forwarder list, is added to the forwarder list, then the expected cost of the newly created forwarder list will decrease while it will still be greater than the expected cost of the newly added SN. The second theorem, Theorem 4.3, shows that if a SN, whose expected cost is greater than the expected cost of a prefix forwarder list, is added to the forwarder list, then the expected cost of the newly created forwarder list will increase. Theorem 4.4 establishes connectivity issues.

Theorem 4.2: Consider a SN u, a prefix $NHList^{\#}$ and a SN $v_k \in N(u)/NHList^{\#}$. if $EAK_{v_k} > EAK_u(NHList^{\#})$ then $EAK_u(NHList^{\#} \cup \{v_k\}) > EAK_u(NHList^{\#})$ and $EAK_u(NHList^{\#})$ is monotonically non-decreasing.

Proof: We can prove above theorem by induction. Let us assume that SN to be considered first from $N^{\#}(u)$, is v_1 and $L^{\#} = L \cup \{v_1\}$. Let us assume that $|L| = 0$ and $EAK_u(L) = 0$. Using eqn. {4.28.a} $EAK_u(L^{\#}) = EAK_u(L) + \Delta$ where $\Delta = (1-f) * EAK_{v_1}\left(L^{\#}(v_{k+1})\right)$ and f represents non-negative error probability. This implies $EAK_u(L^{\#}) \geq EAK_u(L)$.

Induction step: Considering v_k next from $N^{\#}(u)$, is v_k and $L^{\#} = L \cup \{v_k\}$. Let us assume that $|L| = k-1$ and $EAK_u(L)$ is expected key average earned. $EAK_u(L^{\#}) = EAK_u(L) + \Delta$ Where $\Delta = f * f * \ldots (k-1\ terms) * (1-f) * EAK_{v_k}\left(L^{\#}(v_k)\right)$ and e represents non-negative error probability. This implies $EAK_u(L^{\#}) \geq EAK_u(L)$. Hence, adding next SN increments EAK in case v_k is qualifies feasibility criterion of being a member in $NHList^{\#}$.

Considering next from $N^{\#}(u)$, is v_{k+1} provided $EAK_{v_{k+1}} \geq EAK_u$ and$L^{\#} = L \cup \{v_{k+1}\}$. Let us assume that $|L| = k$ and $EAK_u(L)$ is expected key average earned. $EAK_u(L^{\#}) = EAK_u(L) + \Delta$ where $\Delta = f * f * \ldots (k\ terms) * (1-f) * EAK_{v_{k+1}}\left(L^{\#}(v_{k+1})\right)$ and $e$represents non-negative error probability. This implies $EAK_u(L^{\#}) \geq EAK_u(L)$. Hence, adding next SN increments EAK in any case.

Theorem 4.3: Querying any SN $u \in V$ will reach concerned u in O (n) time.

Proof: As BS has information about relays and selectors in the network. BS computes all possible paths towards u. BS unicast the query consisting of route to u to SN at one-hop. One hop SNs sends query to one of his selectors mentioned in the path. During query forwarding process relay SNs (selectively) forwards query to selector mentioned in the path of query. Query follows specified path in the network, and reaches u in limited number of hops. As in the worst case path length is $(N-1)$. Reply SN becomes new source of reply and will route reply on encrypted paths through its Data-Relays.

Theorem 4.4: All SNs $(\forall u \in V)$ in the network are reachable.

Proof: Let we prove theorem by contradiction. Let there be a SN u which is unreachable as there is no route to u at BS. This implies u is not selector of any SN. It implies$NHList(u) = \emptyset$. With no doubt we can be concluded that $N(u) = \emptyset$. This suggests a partitioned network. Otherwise; in a connected network $\forall u \in V,\ N(u) \neq \emptyset$ and eqn. {4.27} ensures that only neighbour will be in $NHList(u)$. Thus, in a connected network we have $NHList(u) \neq \emptyset$. As a fact BS will have routes to $\forall u \in V$.

4.5.8 Discussion

We have proposed a new kind of multi path secure routing which distinguishes relays for query and reply, classified as Data-Relays (DRs) and Query-Relays (QRs). With provision of multiple DRs and QRs we have reduced the number of trials for successful traversal of packets from source to BS. The optimal selection of DRs in the network has been proposed, with objective of maximizing the Effective Average Keys on the routes from random SN to BS. As the route was specified by BS and forwarders are selected by SNs on the path, any masquerading and modification attack rendered ineffective. The analytical modelling supported the objectives and

supports the strength of proposal. The scheme may be specialized for study of different parameters in demanding environments.

4.6 Summary

Four different secure routing proposals have been discussed in this chapter. First two routing protocols realized secure routing using random key pre-distribution of keys to SNs. Both protocols achieved improvement in resilience by improving strength of links. A secure data collection paradigm using MNs has been suggested. Issues like authentication and re-authentication of MNs has been achieved through a novel THA protocol for authentication. Finally, chapter concludes with a proposal on secure multicast routing scheme. The schemes in this chapter are evaluated through simulation and analytical models.

In next chapter we presented contributions and future scope of this thesis work.

Chapter 5

Conclusions

Openly deployed WSNs are difficult challenge for security provisioning. Resource limitation in WSNs has further complicated the scenario. In the absence of WSN aware security solutions and inability of applying wire-line security solutions, research area in secure information dissemination is an opportunity and challenge for research communities. With little storage at disposal; keying information and keying material must be concise and precise enough for constrained SNs. To provide security for routing and data; routing scheme must exploit underlying keying scheme. To propose secure routing, usable key management scheme is implied requirement. The security solution must maintain the network connectivity. Node compromise in WSNs is inevitable threat in unattended WSNs. To propose a viable security solution, key management scheme must ensure that the compromise of single or multiple nodes in keyed environment must not expose links due to non-compromised nodes in the network. In this manuscript several security solutions using key management and secure routing using underlying key management schemes are proposed which partially meet the objectives finalized in the research work. Section 5.1 presents the contributions of this thesis work. Section 5.2 presents a brief on future scope of this thesis.

5.1 Contributions

Novelty factors for our work includes as follows:

I. We proposed a key management scheme for HWSN, using generating keys instead of keys from key pool. Scheme used non-uniform pre-distribution of generating keys. With high probability of sharing of generating keys non-uniform distribution achieves high connectivity and at the same time minimizing the compromise ratio. H-sensor, identified as CHs and intermediate secure conversions between pair of Low-end Sensors (L-Sensors). We proposed to use binary tree called HBT to derive keys from generating keys. The computational complexity of generation of any key is $log\,(n)$ where n represent the length of chain. The localization of generation keys using multi range broadcast from ANs has reduced the impact of node compromise and node replication. Scheme addresses limited storage by using only small number of generating keys in L-Sensors. Scheme supports revocation, rekeying and addition of new nodes.

II. Another security solution called LOCK is considered for HWSN. LOCK exploits location information to localize the keys to be used for communication. LOCK is applicable for hierarchical topology with H-Sensors performing as CHs. L-Sensor acts as cluster members. Multiple transmission range of ANs allows each SN receives a subset of total

broadcast. Received subset is dependent upon location of SN. LOCK is a matrix based key management scheme. Each SN maintains only diagonal of key matrix. SNs localize diagonal of matrix using broadcast from ANs. To obtain complete key matrix HBT was extended into Dual skewed Hash Binary Tree and carved out rows and columns of matrix as and when needed. The storage requirement of the scheme is very low as only diagonal elements are stored in each SN. Due to pair-wise keys, compromise of node affects the security of those links which begin or terminate at compromised node. The replication and usage of SNs outside its cluster becomes ineffective as SNs possess localized key matrix. Scheme supports secure communication patterns using different kind of keys. Key refresh is performed at network level by using new broadcast from ANs.

III. A novel variance aware secure routing protocol is considered for HWSN. Using non-uniform random key pre-distribution as underlying key management scheme, and a variance aware next hop selection method, protocol generates secure routes from every SN to BS. Hop selection criteria overcomes weaker links and select next hop that is as strong or resilient as partial route in making. Scheme could avoid steep variation in average number of keys on each route. Because the route is as strong as the weakest link in the route, we obtained sufficiently strong links, every time we add a new hope. Few paths had more hops than non-uniform keyed scenario. Sixty percent (60%) paths show an improvement in average number of keys on the route with fifty percent (50%) routes show lower variance in average number of keys than non-uniform keyed scenario.

IV. To evaluate the impact of location on average number of keys on secure routes in GPSR, secure GPSR using uniform and non-uniform key pre-distribution was suggested. Local cell based relationship show tremendous impact on security parameter while selecting next hop in GPSR. Using local relationship in uniform key distribution scenario average number of keys on the route improved by hundred percent (100%) against simple uniform keyed scenario. Similarly in non-uniform key distribution scenario the effect of local relationships resulted in improvement ranging from 40-400%. More keys in each link imply more resilience.

V. We considered extension to secure LEACH protocol in WSN by using secure data collection by mobile nodes. Extended LEACH avoids distributed re-clustering. Authentication of mobile nodes is achieved by using a novel authentication protocol called Two Hop online Authentication (THA). Communications within cluster are secured by using group keys established using congruent generator (Chinese remainder theorem). Group key shared between CH and cluster members. Group key is updated at the beginning of each round. The scheme proved energy efficient secure variant of basic clustering scheme.

VI. We considered a multipath secure routing scheme for HWSN. Multicast environment is realized by inducing a multicast environment with help of random pre-distributed key. We proposed a novel approach for selection of subset from one-hop neighbours towards BS. The routing scheme offers equally secure multiple paths towards a destination, with high resilience. Both query and replies, are supported and both travels using multiple paths. The strength of protocol is established with help of mathematical theorems.

5.2 Future Scope

This work opens opportunities and challenges in Heterogeneous Wireless Sensor Networks. We summarize few of them here.

I. Heterogeneity in SN's storage is considered in this work. Heterogeneity in transmission range of SNs is left un addressed in this work. Considering varying transmission range is more promising research dimension.

II. Considering other parameters ranging from attack analysis against newer forms of attacks and performance evaluation using other substantial performance parameters may be considered for future works.

III. Considering secure routing with the help of underlying key management scheme is considered in this work. To propose a routing protocol which can overcome several or specific attacks by virtue of its operating characteristics may be considered newer approach in secure routing.

IV. BS is most commonly used assumption and considered controller of WSNs. By distributing functionalities of BS among SNs and using cooperative routing techniques is area of research which needs attention.

V. Synchronization of WSNs is major issue and several works make strong assumptions of synchronized operations. With strict timing constraints of the application in WSN, achieving tight and weak synchronization is still open research area.

VI. Mobility of SNs was considered in this work and addressed several related issues. Authentication of mobile nodes using offline technique and synchronize the operation of WSNs simultaneously is possible extension of our work.

VII. Mobility of H-Sensor could be considered to add another level of heterogeneity where mobile H-Sensor performs as distributed BS and propose a routing protocol for dynamic topology under various mobility models.

Bibliography:

[1] Salvatore La Malfa, "Wireless Sensor Networks", available at http://www.dees.unict.it/users/bando/files/wsn.pdf, retrieved on June 16, 2014.

[2] WSN IMAGE, AVAIALBLE AT http://www.powershow.com/view/98673-Y2Q5Y/Wireless_Sensor_Networks_powerpoint_ppt_presentation, ACCESSED ON JUNE 22, 2014.

[3] X. Chen, K. Makki, K. Yen and N. Pissinou, "Sensor Network Security: A Survey," In IEEE Communications Surveys & Tutorials, Vol. 11, No. 2, pp. 52-73, IEEE, Second Quarter 2009.

[4] J. Newsome, E. Shi, D. Song and A. Perrig, "The Sybil Attack in Sensor Networks: Analysis and Defenses," In Proceedings of 3rd International Symposium on Information Processing in Sensor Networks, pp. 259-268, 2004.

[5] A. S. Tanenbaum, Computer Networks, 4th ed. NJ: Prentice Hall, 2003.

[6] W. Stallings, Cryptography and Network Security- Principles and Practices, 3rd ed. Upper Saddle River, NJ: Prentice Hall, 2003.

[7] D. W. Carman, P. S. Kruus, and B. J. Matt, "Constraints and Approaches for Distributed Sensor Network Security," NAI Labs Technical Report 00-010, 2000.

[8] D. Djenouri, L. Khelladi and N. Badache, "A Survey of Security Issues in Mobile Adhoc and Sensor Networks," In IEEE Communications Surveys & Tutorials, Vol. 7, pp. 2-28, 2005.

[9] Y. Wang, G. Attebury and B. Ramamurthy, "A Survey of Security Issues in Mobile Adhoc and Sensor Networks," In IEEE Communications Surveys & Tutorials, Vol. 8, pp. 2-23, 2006.

[10] B. Deb, S. Bhatnagar and B. Nath, "Information Assurance in Sensor Networks," In Proceedings of 2nd ACM International Conference on Wireless Sensor Networks and Applications, pp. 160-168, ACM, 2003.

[11] H. Chan, A. Perrig, and D. Song, "Random Key Predistribution Schemes for Sensor Networks", In Proceedings of IEEE Symposium on Security and Privacy, May 11-14, pp. 197- 213, 2003.

[12] S. Bala, G. Sharma and A. K. Verma, "Classification of Symmetric Key Management Schemes for Wireless Sensor Networks," In International Journal of Security & Its Applications, Vol. 7, No. 2, pp. 177-38, 2013.

[13] V. C. Gungor and G. P. Hancke, "Industrial Wireless Sensor Networks: Challenges, Design Principles, and Technical approaches," IEEE Transactions on Industrial Electronics, Vol. 56, No. 10, pp. 4285-4265, October 2009.

[14] "Key Management", available at http://en.wikipedia.org/wiki/Key_management, retrieved on June 16, 2014.

[15] R. L. Rivest, A. Shamir, and L. Adleman, "A Method for obtaining Digital Signatures and Public-key Cryptosystems," In Communications of the ACM, Vol. 21, No. 2, pp. 120-126, February 1978.

[16] V. Miller, "Use of Elliptic Curves in Cryptography," In Proceedings of Advances in Cryptology (CRYPTO'85), pp. 417-426, Springer Berlin Heidelberg, 1986.

[17] National Institute of Standards and Technology, "Announcing the ADVANCED ENCRYPTION STANDARD (AES)," Federal Information Processing Standard Publication 197, November 26, 2001, Retrieved June 16, 2014.

[18] W. Diffie and M. E. Hellman, "Exhaustive Cryptanalysis of the NBS Data Encryption Standard," Computer, Vol. 10, No. 6, pp. 74-84, 1977.

[19] D. Gesbert, M. Shafi, D. shan Shiu, P. Smith and A. Naguib, "From Theory to Practice: An overview of MIMO Space-time Coded Wireless Systems," In IEEE Journal of Selected Areas in Communication, Vol. 21, No. 3, pp. 281-302, April 2003.

[20] R. Ramanathan, J. Redi, C. Santivanez, D. Wiggins, and S. Polit, "Ad hoc Networking with Directional Antennas: A Complete System Solution," In IEEE Journal of Selected Areas in Communication, Vol. 23, No. 3, pp. 496-506, March 2005.

[21] S. Cui, A. Goldsmith, and A. Bahai, "Energy-efficiency of MIMO and Cooperative MIMO Techniques in Sensor Networks," In IEEE Journal of Selected Areas in Communication, Vol. 22, No. 6, pp. 1089-1098, Aug. 2004.

[22] M. Yarvis, N. Kushalnagar, H. Singh, A. Rangarajan, Y. Liu, and S. Singh, "Exploiting Heterogeneity in Sensor Networks," In the Proceedings of IEEE INFOCOM, vol. 2, pp. 878-890, March 2005.

[23] W. Luo, and Y. Fang., "A Survey of wireless Security in Mobile Ad Hoc Networks:Challenges and Available Solutions", Kluwer Academic Publishers, pp-319-364, 2003.

[24] P. Traynor, R. Kumar, H. Choi, G. Cao, S. Zhu and T. L. Porta, "Efficient Hybrid Security Mechanisms for Heterogeneous Sensor Networks", In IEEE Transactions on Mobile Computing, Vol. 6, No. 6, pp. 663-77, June 2007.

[25] B. Parno, M. Luk, E. Gaustad and A. Perrig, "LHA-SP: Secure Protocols for Hierarchical Wireless Sensor Networks," In Proceedings of 9th IFIP/IEEE International Symposium on Integrated Network Management, pp. 31-44, May 2005.

[26] J. Ibriq and I. Mahgoub, "A Secure Hierarchical Routing Protocol for Wireless Sensor Networks," In Proceedings of 10th IEEE International Conference on Communication Systems, Singapore, pp. 1-6, October 2006.

[27] L. B. Oliveira, H. C. Wong, M. Bern, R. Dahab, and A. F. Loureiro, "Secleach - A Random key Distribution Solution for Securing Clustered Sensor Networks," In Proceedings of Fifth IEEE International Symposium on Network Computing and Applications (NCA 2006), IEEE, pp. 145-154, 2006.

[28] A. C. Ferreira, M. A. Vilacia, L. B. Oliveira, E. Habib, H. C. Wong and A. A. F. Loureiro, "On the security of cluster-based communication protocols for wireless sensor networks," In Proceedings of 4th IEEE International Conference on Networking (ICN'05), Vol. 3420, Lecture Notes in Computer Science, pp. 449-458, Reunion Island, April 2005.

[29] R. Srinath, A. V. Reddy and R. Srinivasan, "A Cluster based Secure Routing Protocol for WSN," In Proceedings of Third International Conference on Networking and Services, Washington, DC, USA, pp. 45, IEEE Computer Society, 2007.

[30] C. Hong-bing, Y. Geng and H. Su-jun, "NHRPA: a Novel Hierarchical Routing Protocol Algorithm for Wireless Sensor Networks, In The Journal of China

Universities of Posts and Telecommunications, Vol. 15, No. 3, pp. 75-81, September 2008.

[31] L. B. Oliveira, A. Ferreira, M. A. Vilaca, H. C. Wong, M. Bern, R. Dahab and A. A. F. Loureiro, "Secleach-On the Security of Clustered Sensor Networks," In Signal Processing, Vol. 87, No. 12, pp. 2882-2895, December 2007.

[32] D.Wu, G. Hu and G. Ni, "Research and Improve on Secure Routing Protocols in Wireless Sensor Networks," In 4th IEEE International Conference on Circuits and Systems for Communications (ICCSC 2008), pp. 853-856, May 2008.

[33] K. Zhang, C. Wang and C. Wang, "A Secure Routing Protocol for Cluster-Based Wireless Sensor Networks using Group Key Management," In Proceedings of 4th IEEE International conference on Wireless Communications, Networking and Mobile Computing (WiCOM'08), pp. 1-5, October 2008.

[34] N. Asokan and P. Ginzboorg, "Key Agreement in Ad Hoc Networks, Computer Communications, Vol. 23, No. 17, pp. 1627-1637, November, 2000.

[35] S. Cheung, "An Efficient Message Authentication Scheme for Link State Routing," In Proceedings of 13th Annual Computer Security Applications Conference, pp. 90, Dec. 08-12, 1997.

[36] S. Marti , T. J. Giuli , K. Lai and M. Baker, "Mitigating Routing Misbehaviour in Mobile Adhoc Networks," In Proceedings of 6th Annual International Conference on Mobile Computing and Networking, Boston, Massachusetts, USA, pp.255-265, Aug. 06-11, 2000.

[37] G. O'Shea, M. Roe, "Child-proof authentication for MIPv6 (CAM)," ACM SIGCOMM Computer Communication Review, Vol. 31, No. 2, pp. 4-8, April 2001.

[38] P. Papadimitratos and Z. J. Haas, "Secure Routing for Mobile Adhoc Networks," In Proceedings of SCS Communication Networks and Distributed Systems Modelling and Simulation Conference (CNDS 2002), Jan. 2002.

[39] B. Dahill , K. Sanzgiri , B. N. Levine, E. M. Belding-Royer and C. Shields, "A Secure Routing Protocol for Ad Hoc Networks," In Proceedings of 10th IEEE International Conference on, pp. 78-87, IEEE, 2002.

[40] B. R. Smith , S. Murthy and J. J. Garcia-Luna-Aceves, "Securing Distance-Vector Routing Protocols," In Proceedings of 1997 Symposium on Network and Distributed System Security, pp. 85, Feb. 10-11, 1997.

[41] Y. C. Hu, D. B. Johnson and Adrian Perrig, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks," In Proceedings of Fourth IEEE Workshop on Mobile Computing Systems and Applications, pp. 3, June 20-21, 2002.

[42] Y. C. Hu, A. Perrig, and D. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks," Technical Report TR01-383, Rice University, Dec. 2001.

[43] S. Kent, C. Lynn, J. Mikkelson, and K. Seo, "Secure Border Gateway Protocol (S-BGP)", In IEEE Journal on Selected Areas in Communication, Vol. 18, No. 4, pp. 582-92, 2000.

[44] M. G. Zapata, "Secure Adhoc On-demand Distance Vector (SAODV) Routing, "SIGMOBILE, Mobile Computing Communication Review, Vol. 6, No. 3, pp. 1559-1662, 2002.

[45] W. Dargie and C. Poellabauer, “Fundamentals of Wireless Sensor Networks: Theory and Practice,” John Wiley and Sons, pp. 168-183, 191-192, 2010, ISBN 978-0-470-99765-9.

[46] P. Khatri, S. Tapaswi and U. P. Verma, “Trust evaluation in wireless ad-hoc networks using fuzzy system,” Computer systems science and engineering 29, no. 1 (2014): 43-50.

[47] G. Padmavathi and D. Shanmugapriya, "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks," in International Journal of Computer Science and Information Security, Vol. 4, No. 1, 2009.

[48] S. Basagni, K. Herrin, D. Bruschi and E. Rosti, "Secure Pebblenets," In Proceedings of Mobihoc 2001, ACM, CA, USA, pp. 156-163, 2001.

[49] S. Zhu, S. Setia and S. Jajodia, "LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks," In Proceedings of the 10th ACM conference on Computer and Communications Security (CCS'03), ACM Press, Washington D.C., USA, Oct. 27-30, 2003.

[50] A. Perrig, R. Szewczyk, J. Tygar, Victorwen, and D. E. Culler, "SPINS: Security Protocols for Sensor Networks," In Seventh Annual International Conference on Mobile Computing and Networks, 2001.

[51] R. Pietro, L. Mancini, Y. Law, S. Etalle, and P. Havinga, "LKHW: A Directed Diffusion based Secure Multicast Scheme for Wireless Sensor Networks," In Proceedings of 1st International Workshop on Wireless Security and Privacy (WiSPr 03), 2003.

[52] H. Chan and A. Perrig, "PIKE: Peer Intermediaries for Key Establishment in Sensor Networks," In Proceedings of 24th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM '05), Miami, FL, USA, pp. 524-35. IEEE, 2005.

[53] A. W. H. E. N. Gura, A. Patel and S. Shantz, "Comparing elliptic curve cryptography and RSA on 8-bit CPUs," In Workshop on Cryptographic Hardware and Embedded Systems, (2004).

[54] G. Gaubatz, J.P. Kaps, and B. Sunar, "Public Key Cryptography in Sensor Networks - Revisited," In 1st European Workshop Security on Ad-Hoc and Sensor Networks (ESAS 2004), Lecture Notes in Computer Science, Vol. 3313, pp. 2-18, Springer Berlin Heidelberg, 2004.

[55] R. Watro, D. Kong, S. F. Cuti, C. Gardiner, C. Lynn, and P. Kruus, "TinyPK: Securing Sensor Networks with Public Key Technology," In Proceedings of the 2nd ACM workshop on Security of Adhoc and Sensor Networks (SASN '04) , pp. 59-64, ACM, New York, NY, USA, 2004.

[56] W. Diffie and M.E. Hellman, “New Directions in Cryptography,” in IEEE Transactions on Information Theory, Vol. 22, No. 6, pp. 644-654, 1976.

[57] E.-O. Blab and M. Zitterbart, "Towards AccepTable Public-Key Encryption in Sensor Networks," In Proceedings of ACM 2nd International Workshop on Ubiquitous Computing, pp. 88-93, INSTICC Press, Miami, USA, May 2005.

[58] W. Du and R. Wang, "An efficient Scheme for Authenticating Public Keys in Sensor Networks," In Proceedings of MobiHoc'05, Urbana-Champaign, Illinois, USA, May 25-27, 2005.

[59] R. Merkle, "Protocols for Public key Cryptosystems," In Proceedings of the IEEE Symposium on Research in Security and Privacy, April 1980.

[60] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," In Proceedings of the 9th ACM Conference on Computer and Communications Security (CCS'02), pp. 41-47, ACM Press, Washington, DC, USA, November 2002.

[61] H. Chan, A. Perrig and D. Song, "Random Key Pre-Distribution Schemes for Sensor Networks," In Proceedings of IEEE Symposium on Research in Security and Privacy, pp. 197, May 11-14, 2003.

[62] B. Lai, S. Kim and I. Verbauwhede, "Scalable Session Key Construction Protocol for Wireless Sensor Networks," In Proceedings of IEEE Workshop on Large Scale Real Time and Embedded Systems (LARTES), pp. 7, 2002.

[63] B. Dutertre, S. Cheung and J. Levy, "Lightweight Key Management in Wireless Sensor Networks by Leveraging Initial Trust," Technical Report, SRI-SDL-04-02, System Design Laboratory, 2004.

[64] W. Du, J. Deng, Y. S. Han, S. Chen and P. K. Varshney, "A Key Management Scheme for Wireless Sensor Networks Using Deployment Knowledge," in Proceedings of IEEE INFOCOM, 2004, Twenty-third Annual Joint Conference of the IEEE Computer and Communications Societies, IEEE, 2004.

[65] D. Liu and P. Ning, "Establishing Pair-wise Keys in Distributed Sensor Networks," In Proceedings of 10th ACM Conference on Computer and Communications Security (CCS'03), ACM Press, pp. 52-61, 2003.

[66] W. Zhang, M. Tran, S. Zhu, and G. Cao, "A Random Perturbation-Based Scheme for Pairwise Key Establishment in Sensor Networks," In Proceedings of MobiHoc'07, Montréal, Québec, Canada, pp. 90-99, ACM, 2007.

[67] R. Blom, "An Optimal Class of Symmetric Key Generation Systems," In Proceedings of Workshop on Advances in Cryptology: Theory and Application of Cryptographic Techniques (EUROCRYPT 84), Paris, France, pp. 335-338, Springer-Verlag New York, USA, 1984.

[68] D. Huang, M. Mehta, D. Medhi and L. Harn, "Location-aware Key Management Scheme for Wireless Sensor Networks," In Proceedings of ACM workshop on Security of Ad hoc and Sensor Networks (SASN04), pp. 29-42, ACM Washington, DC, USA, 2004.

[69] Z. Yu and Y. Guan, "A Robust Group-Based Key Management Scheme for Wireless Sensor Networks," In Proceedings of IEEE Wireless Communications and Networking Conference (WCNC 2005), New Orleans, LA USA, pp. 13-17, IEEE Press, 2005.

[70] W. Du, J. Deng, Y. S. Han, P. Varshney, J. Katz, and A. Khalili, "A Pairwise key Pre-distribution Scheme for Wireless Sensor Networks," In ACM Transactions on Information and System Security (TISSEC), Vol. 8, No. 2, pp. 228-58, ACM Press, 2005.

[71] C. Yu, C. Lu, and S. Kuo, "A Simple Non-Interactive Pairwise Key Establishment Scheme in Sensor Networks," In Proceedings of 6th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON'09), pp. 1-9, IEEE, 2009.

[72] J. Lee and D. R. Stinson, "Deterministic Key Pre-distribution Schemes for Distributed Sensor Networks," In Proceedings of ACM symposium on Applied Computing 2004, Waterloo, Canada, Lecture note in computer science, Vol. 3357, pp. 294-307, 2004.

[73] S. Camtepe and B. Yener, "Combinatorial Design of Key Distribution Mechanisms for Wireless Sensor Networks," In IEEE/ACM Transactions on Networking, Vol. 15, No. 2, pp. 346-358, 2007.

[74] M. Eltoweissy, M. Moharrum and R. Mukkamala, "Dynamic Key Management in Sensor Networks," In IEEE Communications Magazine, Vol. 44, No. 4, pp. 122-130, IEEE Press, 2006.

[75] M. F. Younis, K. Ghumman and M. Eltoweissy, "Location-Aware Combinatorial Key Management Scheme for Clustered Sensor Network," In IEEE Transactions on Parallel and Distributed Systems, Vol. 17, No. 8, pp. 865-882, IEEE Press, 2006.

[76] D. Liu, and P. Ning, "Location-Based Pair-wise Key Establishment for Static Sensor Networks," In Proceedings of 1st ACM Workshop on Security of Ad Hoc and Sensor Networks, 2003a.

[77] D. Liu, P. Ning, R. Li, "Establishing Pairwise Keys in Distributed Sensor Networks," In ACM Transactions on Information and System Security, ACM Press, Vol. 8, No. 1, pp. 41-77, 2005.

[78] D. Liu and P. Ning, "Improving Key Pre-distribution with Deployment Knowledge in Static Sensor Networks," In ACM Transactions on Sensor Networks, ACM, Vol. 1, No. 2, pp. 204-39, 2005.

[79] Z. Yu and Y. Guan, "A Key Management Scheme Using Deployment Knowledge for Wireless Sensor Networks," in IEEE Transactions on Parallel and Distributed Systems, Vol. 19, No. 10, pp. 1411-1425, October 2008.

[80] J. Lee and T. Kwon, "GENDEP: Location-Aware Key Management for General Deployment of Wireless Sensor Networks," International Journal of Distributed Sensor Networks, Vol. 2014, pp. 17, 2014.

[81] D. Du, H. Xiong and Hailiang Wang, "An Efficient Key management Scheme for Wireless Sensor Networks," In International Journal of Distributed Sensor Networks, Vol. 2012.

[82] Q. Jing, J. Hu, and Z. Chen, "C4W: an energy efficient public key cryptosystem for large-scale wireless sensor networks," In Proceedings of the IEEE International Conference on Mobile Ad Hoc and Sensor Systems (MASS), pp. 827-832, IEEE, October 2006.

[83] P. Szczechowiak and M. Collier, "Practical identity-based key agreement for secure communication in sensor networks," in Proceedings of the 18th International Conference on Computer Communications and Networks (ICCCN '09), pp. 1-6, August 2009.

[84] P. Traynor, H. Choi, G. Cao, S. Zhu and T. L. Porta, "Establishing Pair wise Keys in Heterogeneous Sensor Networks," In Proceedings of 25th IEEE International Conference on Computer Communications," pp.1-12, April 2006.

[85] F. Kausar, S. Hussain, L. T. Yang and A. Masood, "Scalable and Efficient Key Management for Heterogeneous Sensor Network," In Journal of Supercomputing, Vol. 45, pp. 44-65, 2008.

[86] F. Anjum, “Location dependent key management using random key pre distribution in sensor networks,” In Proceedings of 5th ACM workshop on Wireless security, pp, 21-30, ACM, 2006.

[87] V. Bulusu, A. Durresi, V. Paruchuri, M. Durresi, R. Jain, "Key Distribution in Mobile Heterogeneous Sensor Networks," In Proceedings of IEEE GLOBECOM 2006, San Francisco, CA, pp. 1-5, November 27 - December 1, 2006.

[88] S. Jiang, J. Zhang, J. Miao and C. Zhou, "A Privacy Preserving Re-authentication Scheme for Mobile Wireless Sensor Networks," In International Journal of Distributed Sensor Networks, Vol. 2013.

[89] S. Jiang, X. Zhu, and L. Wang, "A Conditional Privacy Scheme based on Anonymized Batch Authentication in Vehicular ADHOC Networks," In Proceedings of Wireless Communication and Networking Conference, (WCNC'13), Shanghai, China, 2013.

[90] Y. Sun, R. Lu, X. Lin, X. Shen and J. Su, "An Efficient Pseudonymous Authentication Scheme with Strong Privacy Preservation for Vehicular Communications," In IEEE Transactions on Vehicular Technology, Vol. 59, No. 7, pp. 3589-3603, 2010.

[91] S. U. Khan, L. Lavagno, C. Pastrone, and M. Spirito, "An Effective Key Management Scheme for Mobile Heterogeneous Sensor Networks," In Proceedings of International Conference on Information Society (i-Society), pp. 98-103, Jun. 27-29, 2011.

[92] X. Du, Y. Xiao, M. Guizani, and H. H. Chen, "An Effective Key Management Scheme for Heterogeneous Sensor Networks," In Journal of Ad Hoc Network,, Elsevier, Vol. 5, No. 1, pp. 24-34, 2007.

[93] J. Zhang, Y. Sun, and L. Liu, "NPKPS: A Novel Pairwise Key Predistribution Scheme for Wireless Sensor Networks" In Proceedings of Wireless, Mobile and Sensor Networks (CCWMSN07), pp. 446-449, Dec. 12-14, 2007.

[94] A. S. Poornima and B. B. Amberkerx, "Tree-based Key Management Scheme for Heterogeneous Sensor Networks' In Proceedings of 16th IEEE International Conference on Networks (ICON 2008), pp.1-6, Dec. 12-14, 2008.

[95] C. Intanagonwiwat, R. Govindan, and D. Estrin, "Directed Diffusion: A Scalable and Robust Communication Paradigm for Sensor Networks," In Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (MobiCom '00), Boston, MA, pp. 56-67, ACM, 2000.

[96] D. Braginsky and D. Estrin, "Rumor Routing Algorithm for Sensor Networks," In Proceedings of First Workshop on Sensor Networks and Applications (WSNA), Atlanta, GA, pp. 22-31, ACM, Oct. 2002.

[97] Y. Yao and J. Gehrke, "The Cougar Approach to In-network Query Processing in Sensor Networks", In ACM SIGMOD Record, Vol. 31, No. 3, pp. 9-18, ACM, September 2002.

[98] Narayanan Sadagopan, Bhaskar Krishnamachari and Ahmed Helmy, "The ACQUIRE Mechanism for Efficient Querying in Sensor Networks", In Proceedings of First International Workshop on Sensor Network Protocol and Applications, Anchorage, Alaska, pp. 149-155, May 2003.

[99] W. R. Heinzelman, A. Chandrakasan and H. Balakrishnan, "Energy-Efficient Communication Protocol for Wireless Microsensor Networks", In Proceedings of the

33rd Annual Hawaii International Conference on System Sciences (HICSS-33'0), pp. 223, Jan. 2000.

[100] S. Lindsey and C. Raghavendra, "PEGASIS: Power-Efficient Gathering in Sensor Information Systems," In Proceedings of IEEE Aerospace Conference, Vol. 3, No. 9-16, pp. 1125-1130, IEEE, 2002.

[101] Ossama Younis and Sonia Fahmy, "HEED: A Hybrid, Energy-Efficient, Distributed Clustering Approach for Ad-hoc Sensor Networks," In IEEE Transactions on Mobile Computing, Vol. 3, No. 4, pp. 366-379, IEEE, Oct-Dec 2004.

[102] A. Manjeshwar and D. P. Agarwal, "TEEN: A Routing Protocol for Enhanced Efficiency in Wireless Sensor Networks," In Proceedings of 1st International Workshop on Parallel and Distributed Computing Issues in Wireless Networks and Mobile Computing, IEEE Computer Society, April 2001.

[103] W.R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "An Application-Specific Protocol Architecture for Wireless Microsensor Networks" In IEEE Transactions on Wireless Communications, Vol. 1, No. 4, pp. 660-670, October 2002.

[104] A. Manjeshwar and D. P. Agarwal, "APTEEN: A Hybrid Protocol for Efficient Routing and Comprehensive Information Retrieval in Wireless Sensor Networks," In Proceedings of International Parallel and Distributed Processing Symposium (IPDPS), pp. 195-202, IEEE Computer Society, 2002.

[105] J. N. Al-Karaki, R. U. Mustafa and A. E. Kamal, "Data Aggregation in Wireless Sensor Networks - Exact and Approximate Algorithms," In the Proceedings of IEEE Workshop on High Performance Switching and Routing (HPSR 2004), Phoenix, Arizona, USA, pp. 945-60, April 18-21, 2004.

[106] J. N. Al-Karaki, A.E. Kamal, "On the Correlated Data Gathering Problem in Wireless Sensor Networks," In Proceedings of Ninth IEEE Symposium on Computers and Communications, Alexandria, Egypt, IEEE, July 2004.

[107] Q. Li, J. Aslam and D. Rus, "Hierarchical Power aware Routing in Sensor Networks," In Proceedings of DIMACS Workshop on Pervasive Networking, May, 2001.

[108] F. Ye, H. Luo, J. Cheng, S. Lu and L. Zhang, "A Two-tier Data Dissemination Model for Large-Scale Wireless Sensor Networks," In Proceedings of 8th Annual International Conference on Mobile Computing and Networking, ACM/IEEE MOBICOM, 2002, pp. 148-59, ACM NY, USA, 2002.

[109] R. N. Enam, R. Q. and S. Misbahuddin, "A Uniform Clustering Mechanism for Wireless Sensor Networks," in International Journal of Distributed Sensor Networks, Vol. 2014, pp. 14, 2014.

[110] H. Rong-hua, D. Xiao-mei and W. Da-ling, "Mutual Defense Scheme for Secure Data Aggregation in Wireless Sensor Networks," in International Journal of Distributed Sensor Networks, Vol. 2014, pp. 14, 2014.

[111] H. Lee, M. Jang and J. W. Chang, "A New Energy-Efficient Cluster-Based Routing Protocol Using a Representative Path in Wireless Sensor Networks," in International Journal of Distributed Sensor Networks, Vol. 2014, pp. 12, 2014.

[112] Y. Xu, J. Heidemann and D. Estrin, "Geography-informed Energy Conservation for Ad-hoc Routing," In Proceedings of Seventh Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom'01), pp. 70-84, ACM/IEEE, 2001.

[113] Y. Yu, D. Estrin, and R. Govindan, "Geographical and Energy-Aware Routing: A Recursive Data Dissemination Protocol for Wireless Sensor Networks," UCLA Computer Science Department, Technical Report, UCLA-CSD TR-010023, May 2001.

[114] I. Stojmenovic and X. Lin, "GEDIR: Loop-Free Location Based Routing in Wireless Networks," In Proceedings of International Conference on Parallel and Distributed Computing and Systems, Boston, MA, pp. 1025-28, Nov. 3-6, 1999, IASTED 1999.

[115] L. Li and J. Y. Halpern, "Minimum-Energy Mobile Wireless Networks Revisited," In Proceedings of IEEE International Conference on Communications (ICC'01), Helsinki, Finland, pp. 278-283, IEEE 2001.

[116] V. Rodoplu and T. H. Meng, "Small Minimum Energy Mobile Wireless Networks," In IEEE Journal on Selected Areas in Communications, Vol. 17, No. 8, pp. 1333-1344, Aug. 1999.

[117] M. Zorzi and R. R. Rao, "Geographic Random Forwarding (GeRaF) for Ad hoc and Sensor Networks: Mutlihop Performance," In IEEE Transactions on mobile Computing, Vol. 2, No. 4, pp. 337-348, Oct.-Dec. 2003.

[118] B. Nath and D. Niculescu, "Routing on a curve", In ACM SIGCOMM Computer Communication Review, Vol. 33, No.1, pp. 155-160, Jan. 2003.

[119] G. Xing, C. Lu, R. Pless, and Q. Huang, "On Greedy Geographic Routing Algorithms in Sensing-Covered Networks," In Proceedings ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc'04), Tokyo, Japan, pp. 31-42, ACM, May 2004.

[120] X. Mao, S. Tang, X. Xu, X. Y. Li, and H. Ma, " Energy-Efficient Opportunistic Routing in Wireless Sensor Networks", In IEEE Transactions on Parallel And Distributed Systems, Vol. 22, No. 11, pp. 1934-1942, Nov. 2011.

[121] T. He, J. A. Stankovic, C. Lu, and T. AbdelZaher, "SPEED: A Stateless Protocol for Real-time Communication in Sensor Networks," In Proceedings of International Conference on Distributed Computing Systems, Providence, RI, pp. 46-55, May 2003.

[122] C. Perkins et al., "Ad hoc On-Demand Distance Vector (AODV) Routing," Internet Draft draftietfmanet-aodv-11.txt, June 2002.

[123] D. B Johnson et al., "Dynamic Source Routing in Ad Hoc Wireless Networks", in Mobile Computing, edited by Tomas Imielinski and Hank Korth, Kluwer Academic Publishers, ISBN: 0792396979, 1996, Chapter 5, pp. 153-181, 1996.

[124] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless Sensor Networks: A Survey," Computer Networks (Elsevier) Journal, Vol. 38, No. 4, pp. 393-422, Mar. 2002.

[125] K. Akkaya and M. Younis, "An Energy-Aware QoS Routing Protocol for Wireless Sensor Networks," In Proceedings of IEEE Workshop on Mobile and Wireless Networks (MWN 2003), Providence, Rhode Island, May 2003.

[126] H. Shin, S. Moh and I. Chung, "Clustering with One Time Setup for Reduced Energy Consumption and Prolonged Lifetime in Wireless Sensor Networks," In International Journal of Distributed Sensor Network, Vol. 2013.

[127] M. Tubaishat, J. Yin, B. Panja and S. Madria, "A Secure Hierarchical Model for Sensor Network," In ACM SIGMOD Record, Vol. 33, No. 1, pp. 7-13, March 2004.

[128] J. Chen, H. Zhang and J. Hu, "An Efficiency Security Model of Routing Protocol in Wireless Sensor Networks," In Proceedings of 2008 Second Asia International Conference on Modelling and Simulation, pp. 59-64, Washington, DC, USA, IEEE Computer Society, 2008.

[129] J. Zhang, X. Li, J. Ma, and W. Wang, "Secure and Efficient Authentication Scheme for Mobile Sink in WSNs Based on Bilinear Pairings," in International Journal of Distributed Sensor Networks, Vol. 2014, pp. 11 pages, 2014.

[130] H. L. Chen, T. Chen and S. H. Hu, "A Convergent Algorithm for Energy-Balanced Cluster-Heads Selection in Wireless Sensor Networks," in International Journal of Distributed Sensor Networks, Vol. 2014, pp. 8, pages, 2014.

[131] E. K. Wang, Y. Ye and X. Xu, "Lightweight Secure Directed Diffusion for Wireless Sensor Networks," in International Journal of Distributed Sensor Networks, Vol. 2014, pp. 12, 2014.

[132] F. Kausar, S. Hussain, T. Y. Laurence and A. Masood, "Scalable and Efficient Key Management for Heterogeneous Sensor Network," In Journal of Super Computing, Vol. 45, pp. 44-65, 2008.

[133] Y. Cheng, D. P. Aggarwal, "An Improved Key Mechanism for Large Scale Hierarchical Wireless Sensor Networks," In Proceedings of Security Issues in Sensor and Adhoc Networks, Elsevier, Vol. 5, No. 1, p.p. 35-48, 2007.

[134] B. Karp and H. T. Kung, "GPSR: Greedy Perimeter Stateless Routing for Wireless Networks," In Proceedings of 6th Annual International Conference on Mobile Computing and Networking (MobiCom '00), ACM, NY, USA, 243-254, ACM, 2000.

[135] W. Gu, N. Dutta, S. Chellappan and X. Bai, "Providing End-to-End Secure Communications in Wireless Sensor Networks," In IEEE Transaction on Network and Service Management, Vol. 8, No. 3, 205-218, 2011.

[136] S. Oh, S. Hur and G. Lee, "An Efficient Energy Usage of Wireless Sensor Network," In IE Interfaces, Vol. 23, No. 2, pp. 108-117, 2010.

[137] W. Bo, H. Han-Ying and F. Wen, "An Improved LEACH Protocol for Data Gathering and Aggregation in Wireless Sensor Networks," In Proceedings of International Conference on Computer and Electrical Engineering (ICCEE 2008), pp. 398-401, 2008.

[138] Shen, B., Zhang, S. and Zhong, Y. (2006), "Cluster-Based Routing Protocols for Wireless Sensor Networks," In Journal of Software, Vol. 17, No. 7, 2006.

[139] STANDARDS FOR EFFICIENT CRYPTOGRAPHY (SEC 1): Elliptic Curve Cryptography, Certicom Corporation, 2000.

[140] S. U. Khan, C. Pastrone, L. Lavagno, M. A. Spirito, "An Energy and Memory-Efficient Key Management Scheme for Mobile Heterogeneous Sensor Networks," In Proceedings of 6th International Conference on Risk and Security of Internet and Systems (CRiSIS), Vol., No., pp.1-8, Sept. 26-28, 2011.

[141] M. Bohge and W. Trappe, “An Authentication Framework for Hierarchical Ad hoc Sensor Networks,” In Proceedings of 2nd ACM Workshop on Wireless Security (WiSe ’03), New York, NY, USA, pp. 79–87, ACM, 2003.

Publications

International Journals

1. Kamal Kumar, A. K. Verma, R. B. Patel, "A Location Dependent Connectivity Guarantee Key Management Scheme for Heterogeneous Wireless Sensor Networks," Journal of advances in Information Technology (JAIT), Vol. 1, No. 3, pp. 105-115, August 2010, DOI: 10.4304/jait.1.3.105-115, ISSN 1798-2340, Academy Publisher, Finland.

2. Kamal Kumar, Anil Kumar Verma, R. B. Patel, "Variance Aware Secure Routing for Heterogeneous Wireless Sensor Networks," In Malaysian Journal of Computer Science, Vol. 26, No. 2, pp. 159-169. **(SCI indexed)**

3. Kamal Kumar, Anil Kumar Verma, R. B. Patel, "Secure Multipath Routing Scheme using Key Pre-Distribution in Wireless Sensor Networks,", in International Journal of Foundation in Computer Science & Technology, Vol. 4, No. 4, 2014. (Accepted for Publication), Australia.

4. Kamal Kumar, Anil Kumar Verma, R. B. Patel, "Evaluating Location Augmentation Key Pre-distribution Scheme in Heterogeneous Wireless Sensor Networks," in Wireless Personal Communications, Springer. **(SCI indexed) - (Under Review)**

5. Kamal Kumar, Anil Kumar Verma, R. B. Patel, " Secure Data Collection using Mobile Sensors in Statically Deployed Sensor Networks ," In Malaysian Journal of Computer Science **(SCI indexed) -** (**Under Review**).

International Conference

6. Kamal Kumar, Verma Anil Kumar, Patel R.B., "Promising Key Management Schemes in Wireless Sensor Networks: A Review", in Proceedings of IEEE International Advance Computing Conference (IACC'09) on March 6-7, 2009 , pp. 1061 - 1066, Thapar Institute of Engineering and Technology, Patiala, India.

7. Kamal Kumar, Anil Kumar Verma, R. B. Patel., "An Inexpensive Key Management Scheme for Heterogeneous Wireless Sensor Networks", In the proceedings of International Conference on Wireless Networks & Embedded Systems WECON 2009, pp. 302-308, 23rd – 24th October, 2009, India.