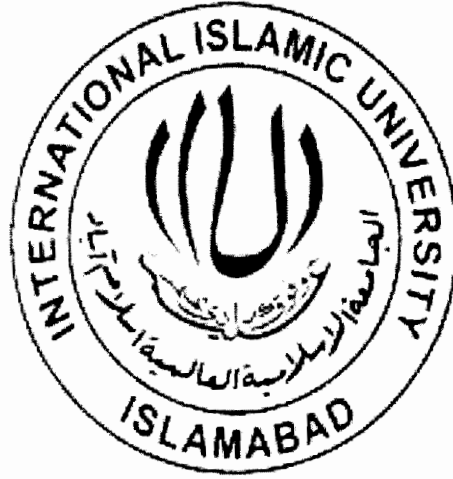


**Polynomial Subset Based Efficient Key Management for
Heterogeneous Wireless Sensor Network**



**THESIS SUBMITTED FOR PARTIAL REQUIREMENT OF MS
COMPUTER SCIENCE**

BY

ZAHID MAHMOOD

575-FBAS/MSCS/F09

SUPERVISED BY

ASSISTANT PROFESSOR DR. MUHAMMAD ZUBAIR

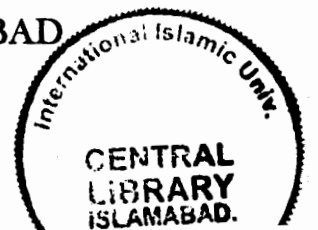
CHAIRMAN, FACULTY OF ELECTRONIC ENGINEERING

DEPARTMENT OF COMPUTER SCIENCE

FACULTY OF BASIC AND APPLIED SCIENCES

INTERNATIONAL ISLAMIC UNIVERSITY, ISLAMABAD

PAKISTAN



Accession No. TH-9318

MS
621.382
ZAP

Sensor networks
Compute. networks

DATA ENTERED

Amz
11/2/13



**Faculty of Basic & Applied Sciences, Department of Computer
Science & Software Engineering
International Islamic University, Islamabad**

FINAL APPROVAL

Dated: 14/11/2012

It is certified that we have read the thesis, entitled "*Polynomial Subset Based Efficient Key Management for Heterogeneous Wireless Sensor Network*" submitted by **Mr. Zahid Mahmood** Reg. No. **575-FBAS/MSCS/F09**. It is our judgment that this thesis is of sufficient standard to warrant its acceptance by the International Islamic University Islamabad for MS Degree in Computer Science.

THESIS EVALUATION COMMITTEE


External Examiner:

Dr. Hassan Mahmood

Assistant Professor

Department of Electronics

Quaid-i-Azam Universty, Islamabad



Internal Examiner:

Professor Dr. Muhammad Sher

Dean Faculty of Basic and Applied Science,

International Islamic University, Islamabad



Supervisor:

Dr. Muhammad Zubair

Assistant Professor

Chairman, Faculty of Engineering & Technology

International Islamic University, Islamabad



ABSTRACT

Wireless sensor networks (WSNs) are highly vulnerable to attacks because they consist of numerous resource-constrained devices and communicate via wireless links. We describe new optimized key management scheme to reduce computational complexity, communication and memory overhead and increase lifetime of network. Polynomial subset based efficient key management for heterogeneous wireless sensor network fully exploits the heterogeneity of sensor nodes to share common secret key and communicate with cluster head securely. The polynomial subset based cluster key generation process is completed by taking Exclusive-OR of randomly selected subset node identification of cluster head member instead of their product. In addition, the regeneration of keys is simple and expedient. It provides five efficient security administration mechanisms: 1) key setup, 2) node addition, 3) key renewal, 4) recovery from multiple and 5) node captures. All of these mechanisms had shown to localize the impact of attacks and considerably improve the efficiency of maintaining fresh session keys. Using simulation and mathematical analysis, we have shown that it is highly robust against node capture because the regeneration mechanism is very fast and uses lightweight key. XOR based polynomial reduces up to 65% computing cost on node and reduces the number of bits from dozen to several. Memory overheads are reduced from n -bits to m -bits where $m \ll n$. The new node addition process has 50% less communication cost and no computing is need on cluster head because base station has the authority to add new nodes.

DECLARATION

I hereby declare that neither as a whole nor a part of this work is copied from any source. It is further declaring that I have conducted this research and have accomplished this thesis entirely based on our personal efforts and under the sincere guidance of my supervisor Dr. Muhammad Zubair. If any part of this thesis, is provide to be copied out from any source or found to be reproduction of some other research, I shall stand by the consequences. No portion of the work presented in this dissertation has been submitted in support of any application for any other degree or qualification of this or any other university or institute of learning.

ZAHID MAHMOOD

575-FBAS/MSCS/F09

A Dissertation submitted to the
Department of Computer Science
International Islamic University Islamabad
As a partial fulfillment of requirements for the award of
The degree of
MS in Computer Science

DEDICATION

The dedication of my thesis is to **MOHAMMAD BIN ABDUL QADEER**, who came upon the world after long prayers of my family, but he came like a **ROSE GLOOM** in **WINTER** but **ALLAH** picked **HIM** for **HEVEN GARDEN**:

*ALLAH takes our loved ones from us^c
We know not the reasons why▷
We can only comprehend the sorrows in our hearts
From the moment their souls BLESS the sky▷*

*HE picks them like flowers from a GARDEN^c
Some prepared for his presence^c
Some without a chance to yield▷
HE will choose them and leave alone the others▷*

*It does not matter if the ones He choose
Are someone's Brothers^c Sisters^c best friends or Mothers▷
But somehow^c when reminiscing^c after all the tears are cried^c
We remember all the reasons we loved them^c
And know with all our hearts^c
Why he himself would want them by his side*

BUT

*Those we love do not go away^c
They walk beside us every day^c
Unseen^c unheard^c but always near^c
Still loved^c still missed and very dear▷*

ACKNOWLEDGEMENT

All praise to Almighty Allah who has all the names, and who needs no name the most generous, considerate, and compassionate who has blessed mankind with this verdict to think, explore, to learn and discover the hidden secrets of this universe and helped me to broaden the veils of my thought and enabling me to get through the difficulties indulged during this MS thesis. Also admiration to our beloved Prophet Muhammad (PBUH) who is always a great source of inspiration of divine devotion and dedication to me.

I would cordially pay my special appreciations and whole heartedly considerations to my reverend supervisors Dr Muhammad Zubair for his endless support, guidance and coordination while conducting this project. I owe him a great respect and honor and I am privileged to work under their supervision. It was their efforts, courage, moral support and endeavoring attitude that helped me to get through any problem or difficulty during each step of this project.

I would also like to pay my gratitude to all my respected teachers making me capable of what I am today due to their guidance and help. Thanking to Mr. Attaullah for his views, which throughout helped me to generate, improve, enhancing and implement my research work.

I also owe a special thanks and gratitude to Mr. Naizumudin for supporting me in working on this idea and accompanying me with the material for study which I needed during this research guide me at the very beginning of my research which help me regarding my research proposal. I also say special thanks to Mr. Yasir Shabir, Mr. Waqas Ahmed, Mr. Subhanullah and Mr. Rashid Abbasi on my moral support and proper gaudiness.

Finally, but the most important the role played behind my all achievements after ALMIGHTY ALLAH is my beloved uncle Col. Abdul Qadeer and the most adore aunty Assistant Professor Mrs. Kousar Abdul Qadeer who are deserve the credit more than all. Thanking them for always being there for me whenever I needed them for their help, generosity and moral support I could ever express for, being supportive to me and taught me that even the largest task can be accomplished if it is done one-step at a time. They have been a constant source of advice, love and devotion to me. From

moral to financial they have been blessing me with all the support that I needed up till now in my life. I declare myself nothing without them; I express my countless appreciation to them to help me during achieving this MS degree and hope to have the honor that they would walk along me throughout my life.

I also express my numerous appreciations to my father, who taught me that the best kind of knowledge to have is that which is learned for its own sake and my mother and sisters.

ZAHID MAHMOOD

575-FBAS/MSCS/F09

Contents

Contents

CHAPTER 1 INTRODUCTION	1
1.1 Introduction	2
1.2 Background of the Research	3
1.2.1 Classification of WSNs	4
1.2.2 Wireless Sensor Network Application	6
1.2.3 Monitoring	6
1.2.4 Tracking	7
1.3 Cryptographic Key Distribution Mechanisms for WSN	7
1.3.1 Symmetric	7
1.3.2 Asymmetric	8
1.3.3 Hybrid	8
1.4 Related Work	8
1.4.1 Self-Enforcing Techniques	8
1.4.2 Arbitrated Keying Technique	9
1.4.3 Central Key Distributed Scheme	9
1.5 Network Constraint	10
1.5.1 Resource Constraints	10
1.5.2 Sensing unit Constraints	11
1.5.3 Processing unit Constraints	11
1.5.4 Transceiver unit Constraints	11
1.5.5 Power unit Constraints	11
1.6 Network Limitations	12
1.7 Malicious Attacks	12
1.8 Security Requirements for WSN	13
1.8.1 Authenticity	13
1.8.2 Integrity	13
1.8.3 Confidentiality	13
1.8.4 Availability	14
1.9 Key management	14
1.10 Motivation of the Research	15
CHAPTER 2 LITERATURE SURVEY	18
2.1 Trusted Controller	19

Contents

2.2 Secret Master Key	19
2.3 Multiple Disjoint Path Discovery	20
2.4 Generation of Random Nonce.....	20
2.5 Probabilistic Session Key.....	21
2.6 Loop Based Key	21
2.7 Secure Large Key Pool	22
2.8 Key Chain Pool	23
2.9 Q-Composite Key Distribution	23
2.10 Generation of Key hashed from Large Key Pool.....	24
2.11 Seed – Pool Based Key Pre-Distribution	24
2.12 Generation of Polynomial by multiplying Hashed IDs of Nodes	25
CHAPTER 3 PROBLEM DEFINITION.....	26
3.1 Problem Background.....	27
3.2 Existing Solutions for Key Management	27
3.3 Problem Definition.....	27
3.4 Problem Scenarios.....	28
3.4.1 Computations Overhead.....	29
3.4.2 Memory Overhead	29
3.4.3 Communication Overhead	29
3.4.4 Addition of New L-Sensor	30
CHAPTER 4 SOLUTION & METHODOLOGY.....	32
4.1 Proposed Method	33
4.2 Polynomials.....	34
4.3 Dynamic Selection of Node IDs	35
4.4 Generation of Polynomials by using XOR Function	35
4.5 Solution Scenario	37
4.6 Key Establishment Phase	38
4.7 Addition of New Node.....	40
CHAPTER 5 SIMULATION AND RESULTS	47
5.1 Network Topology	48
5.2 Mathematical Model	49
5.3 Simulation	50
5.4 Network Deployment Simulation Scenario	52

Contents

5.5 Simulation Scenario for Group Communication.....	53
5.6 Computation Overheads.....	54
5.7 Consumption of Energy	57
5.8 Memory Overhead	59
5.9 Communication Overhead	59
5.10 Latency Time	62
5.11 Cluster Key Sharing Probability	63
CHAPTER 6 CONCLUSION & FUTURE WORK.....	65
6.1 Conclusion	66
6.2 Future Work	67
REFERENCES.....	68
References.....	69

List of Figures

LIST OF FIGURES

Figure: 1.1 WS Network Topologies [20]	5
Figure: 1.2 Application of Sensor Network [21]	6
Figure: 1.3 Component of Sensor Node [27].....	11
Figure: 1.4 Position of Key Management in Security Architecture [29]	16
Figure: 3.1 Computation of Cluster Key.....	28
Figure: 3.2 New L-Sensor Additions	30
Figure: 4.1 Wireless Sensor Network Topology [7]	34
Figure: 4.2 Cluster Key Establishment	38
Figure: 4.3 Key Distribution Flow	39
Figure: 4.4 Scenario-I.....	44
Figure: 4.5 Scenario-II	45
Figure: 5.1 Sensor Network Deployment Topology [7]	48
Figure: 5.2 Network Deployment Scenario	52
Figure: 5.3 L-Sensor Broadcasting their IDs and Cluster Communication	53
Figure: 5.4 Computing Polynomial.....	56
Figure: 5.5 Key Establishment and Energy Consumption	58
Figure: 5.7 Latency Comparisons	62
Figure: 5.8 Key Sharing Probability	64

List of Tables & Abbreviations

LIST OF TABLES

<i>Table: 4.1 Notations</i>	37
<i>Table: 5.1 Mathematical Comparisons</i>	49
<i>Table: 5.2 Simulation Parameters</i>	51
<i>Table: 5.2 Computation Cost for Polynomial Generation</i>	54
<i>Table: 5.3 Consumption of Energy During Cluster Key Establishment</i>	57
<i>Table 5.4 Energy Consumption During Addition of New L-Sensor</i>	60

LIST OF ABBREVIATIONS

Abb.	Meaning
WSN	Wireless Sensor Network
BS	Base Station
CH	Cluster Head
H-Sensor	High Power Sensor
L-Sensor	Low Power Sensor
L_i	Identification of L-Sensor
L_j	Identification of H-Sensor
KM	Master Key
H(x)	Hash Function
EK(m)	Encryption of Message m with key K
M1 M2	Concatenation of two messages
DK(m)	Decryption of Message m with K
MACK(M)	Message Authentication Code (MAC) of message M using Key K
\otimes	Exclusive-OR Operator
P_{hj}	Polynomial generated by cluster head
K_{chj}	Cluster Key
L(Ni)	New L-Sensor
MAC_ADRS	Mac Address of a Device
EKCB	Master key between base station and cluster head
NB	Nonce of base station
Ks	Session Key

CHAPTER 1 INTRODUCTION

1.1 Introduction

Due to advancement in communication technology, for several purposes wireless sensors are extensively used. Wireless Sensor Networks consist of many small, low-cost, self-governing ends called sensor nodes and having low ability to manipulate data. A standard wireless node has restricted resources for computing any inputs, lack of battery resources and memory power. There are two type of sensor network Homogeneous Network and Heterogeneous Network. If all the nodes in the network having the same competence with respect to computation, communication and storage, called Homogeneous Sensor Network. If several nodes in the network having more capable with respect to resources such as in memory, battery and computation power, called Heterogeneous Wireless Sensor Network. With the passage of time, as sizes of Wireless Sensor Network (WSN) grow it became heterogeneous instead of homogeneous sensor network. It is necessary to implement secure and efficient key management for scalable and secure WSN. In view of the fact that the information is transmitting over the vacuum, several of these function need to utilize security measures in order to prevent snoop of confidential information and the interference of the scheme by enemies. These can be achieving by the deployment of cryptographic method for assuring data privacy, integrity and authenticity fundamental services such as. As a result, security is critical for Wireless Sensor Network. Public key cryptography, RSA, ECC are well-known security methods and key sharing center but having significant overhead and need a more number of computation and data transmitting power a campier to resources. Therefore, it is an expensive to implement in WSN. It is a foundational parameter in the security to define key management methods. Before exchanging data between sensors nodes, key established among them to encrypt data. Key

establishing is an extremely important and challenging phase in Wireless Sensor Network. In the light of limited resources of Wireless Sensor Network, it is very important to employ a light key management scheme during the deployment of such network. Such that two popular sensor such that MICA2 and MICAZ Mot. These sensors accomplished with 8-bit memory, 16 Mega Hz processors [17], [18] and having a total of 4-Kilo bytes of configurable EEPROM and a programmable memory of 128K bytes. Due to the restrictions of memory space to accumulate programming function and the essential keys to ensure protection along with the limitations in processing capability, existing public-key encryption schemes available for standard networks and not feasible for sensor network. This depicts another restraint when enhancing a security method into the sensor network it causes the expensive wireless communication and computational processes. Heavy calculation reduces the battery power and it must be consider during applying the key distribution methods that every node in the network is still able to perform its necessary functions after the deployment of the network. It should be attempted such an algorithms for Wireless Network to fulfill the key management criteria which have ability to manage key with in network resources and size of essential messages being swapped between neighboring nodes and reduces the number of necessary computations.

1.2 Background of the Research

Numerous key management techniques implemented in the past for protecting the wireless communication in Wireless Sensor Network. On the other hand, mainly of these mechanism focus only on networks having all nodes same capabilities, which reduce the performance of the network. W. Du, J. Deng introduced a scheme (E-G) in [19], which

pre-loads a set of same keys deployed onto each sensor by arbitrarily choosing a number of keys from a larger secure pool of keys that have been producing before to deployment. When sensor nodes have been deploying in the targeted area and they have accomplished their bootstrapping procedure, nodes in the network are able to setup a pair wise key with their adjacent nodes if their neighbors have also elected one or more keys in ordinary from the secure pool of secret keys. However, this technique relies on the probability of two adjacent nodes having chosen at least one of the keys from the secure pool in common so moreover, a huge selection of keys must be pre-loaded on each node. The key pool size should reserve smaller to guarantee a high possibility of sensor node connectivity.

1.2.1 Classification of WSNs

On the bases of architecture, Wireless Sensor Network classified into two groups: homogeneous networks and heterogeneous networks. Here, we are considering two modules of wireless sensor nodes organized in the wireless sensor network (WSN) to make a heterogeneous sensor network (HSN) depict in Figure 1-b. Sensor nodes having high computation and communication power and temper resistant are High power sensor node (H-Sensor) and nodes having comparatively low resources are Low power sensor node (L-sensor). In past most of the researcher focused L-sensor nodes for the key management in Homogeneous Network. In a Homogeneous Wireless Sensor Network, since each node has to be capable of aggregating and forwarding data, it is necessary for each node to have complex hardware. In addition, Homogeneous Wireless Sensor Networks are not practical in many applications where strict ranks exist, such as in the military. In contrast, Heterogeneous Wireless Sensor Networks take advantage of node diversity and have better

scalability. Therefore, Heterogeneous Wireless Sensor Networks are more applicable in some practical scenarios. The survival of homogeneous network for large degree faced battery, memory and lifetime constraint. Ever since taken as a whole the cost of a large scale WSN is typically considered we focus on heterogeneous wireless sensor networks (HWSN) consisting of a large

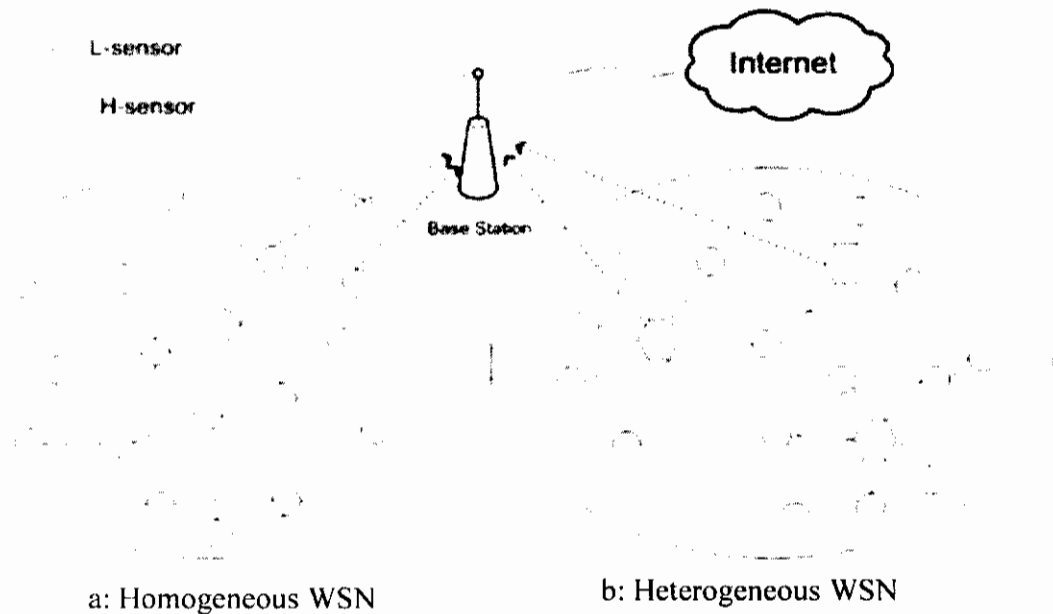


Figure: 1.1 WS Network Topologies [20]

quantity of low power sensors and radically fewer high power sensors which will be used as the heads of clusters in the wireless network. The benefit of H-Sensor is to provide secret key establish between all L-Sensor node after the deployment of network. The other advantage of H-Sensor is that it has broad transmission power and range so they can send message directly to L-Sensor in their cluster in one hope this save time and power of network having wireless node and increase the lifetime of the network.

1.2.2 Wireless Sensor Network Application

WSNs are event-driven networks broadly used for military and civilian operations. One of the secret key compensation of WSNs is that, they are potentially inexpensive resolutions to a diversity of real-world disputes. Sensors network can be organized for continuously reporting environmental data for a long period. This is a very significant enhancement with respect to existing operating circumstances where human hands had to move to the fields and take physical measurements occasionally, resulting in less data, higher mistakes, higher overheads and non-negligible obstruction with life situations of the experimental types. According to the application of WSN have categories into two types:-

1.2.3 Monitoring

Monitoring function of sensor nodes include enclosed/open environmental observing, health and fitness monitoring, electric power monitoring, catalog location monitoring,

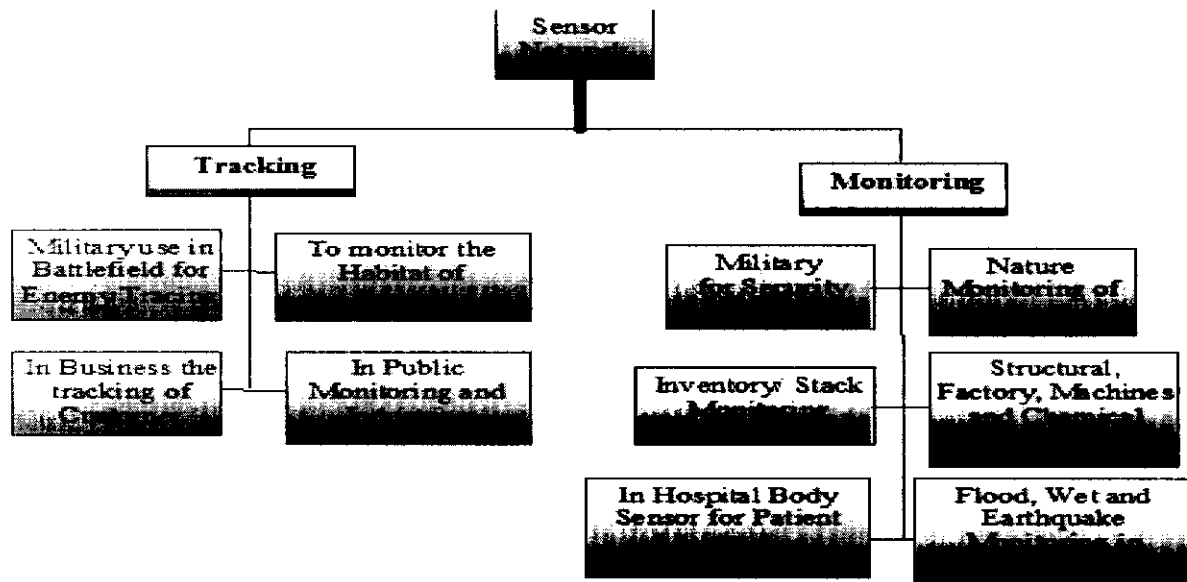


Figure: 1.2 Application of Sensor Network [21]

industrial unit and process automation, and seismic and structural supervision.

1.2.4 Tracking

Sensor nodes also use in tracking devices, such as to trace the animals behavior, humans activities, and vehicles engine and other function. Although there are numerous different purpose, underneath we illustrate a few applications example those deployed in different scenario and tested in the real atmosphere.

1.3 Cryptographic Key Distribution Mechanisms for WSN

In the wireless sensor network, the sensing nodes having limited resources such as memory, energy, computation and temper resistant so secure communication in WSN is important. To establish secure connectivity many primary security technique has been implement in WSN. Many secret key establishing schemes have introduced in recent year and generally in three main categories' based on encryption mechanisms.

1.3.1 Symmetric

In wireless sensor networks, symmetric key schemes used because these scheme consumed low energy and memory overhead. The communication and computation of symmetric key have low time when compare to other schemes and establish share secrete key efficiently in wireless sensor network. Based on secret key sharing, key establishment and common key discovery, these schemes have several categories such as; Entity based techniques, pure probabilistic base mechanisms, matrix based key distribution schemes, tree based secure key pre-distribution schemes, EBS based key allocation schemes and polynomial based pre key distribution schemes [22].

1.3.2 Asymmetric

In asymmetric schemes, such as Elliptic Curve Cryptography and RSA are well known key management schemes but these are heavyweight for wireless sensor network. The implementation of these schemes is mostly in internet realms because there is not resources constraint. But in near past several of researchers have successfully used these schemes for key management for wireless sensor network [23].

1.3.3 Hybrid

Hung et al. 2003 and Zahang et al. 2008 proposed new key management schemes for hybrid network. In cluster based network base station of power full. Motivated in a research that the key computation and distribution burden should be on base station or the any other power full node such as cluster head node. Therefore, the placing of hybrid key management schemes on base station reduced computation, communication [24].

1.4 Related Work

Depending on the characteristics, a secure key organization solution has classified in one of three common groups [D. Carman]: Arbitrated Keying Schemes, self-enforcing Schemes, and pre-deployment schemes.

1.4.1 Self-Enforcing Techniques

Asymmetric cryptography technique is using in self-enforcing scheme in order to set up keys after node deployment. The major negative aspect of this approach refers to the performance of mainly asymmetric defined algorithms at present available. Even though a substantial attempt has been devoted to the adaptation of public key cryptography to highly

constrained devices with certificates [23] and elliptic-curve - cryptography (ECC) [25], the number of resources required for achievement of these techniques is far more than the available resources in WSN.

1.4.2 Arbitrated Keying Technique

These schemes work on a trusted central node (i.e. a sink node) for key generation and management. A problem with this technique is that the trusted point becomes a favored target for attackers that, if attack succeed, than can interrupt the whole network. However, when such a central trusted point is accessible (which is frequently the case in heterogeneous hierarchical network) [16] and can be measured secure, these methods become very striking.

1.4.3 Central Key Distributed Scheme

In this scheme, Key Management Center (KDC) is especial entity, which is responsible for distributing the secret keys into the memory of sensor nodes before to deployment. this process can be accomplish through physical or logical way [26]. The interpretation at the back this technique is to keep away from the overhead, that could be instigate from dynamic secure key generation procedure. In addition, these method consequences in a network with small or no reliance on a central point after the nodes are organized. For these motives, this technique [26] frequently considered more adoptable for wireless sensor network.

1.5 Network Constraint

Sensor nodes are low-cost and have very limited resources. These sensors has typically deployed randomly in designated areas and self-organized into a network after the deployment. Sensors are usually closely scattered in unattended and even harsh situation and the scale of WSNs varies from dozens to thousands of sensor entities. The topology of WSNs may frequently change due to the mobility of nodes in some applications. Wireless channels are open and unreliable and may suffer from many kinds of attacks. Such as transmission of data, information's may be delay or they may not reach their destination at all. Indeed, security challenges in WSNs stem from these constraints.

Here we examine a number of constraints, which make the plan for security mechanisms for wireless sensor networks more complicated and difficult. In order to facilitate understanding, we categorize the constraints in to device constraints, communication constraints, and deployment constraints. Key management in wireless work is become challenge due to following unique features.

1.5.1 Resource Constraints

Sensor network having small sensor nodes, which are battery-power having only limited energy. Due to smallness and cheap they have low computation and communication capabilities so; it is not possible to implement expensive key mechanisms on these small nodes. In traditional network, having much more powerful nodes and the key management mechanisms design for them is not directly implemented on wireless sensor network.

1.5.2 Sensing unit Constraints

Sensing node is usually composed of two sub-entities: sensor and an analog signal to digital signal converter called ADC. The sensor produces analog signals of the observed physical phenomenon and the ADC converts the measurements into digital signals and these signals further process by the processing unit.

1.5.3 Processing unit Constraints

As a part of its processing unit, it has processor, memory, and I/O components. The main function of this unit is to analyze and process sensor data.

1.5.4 Transceiver unit Constraints

A transceiver unit transmits and receives data. It connects a sensor node to a network.

1.5.5 Power unit Constraints

The basis power unit of sensor node is usually a battery or could be maintained by power scavenging units such as solar chargeable cells.

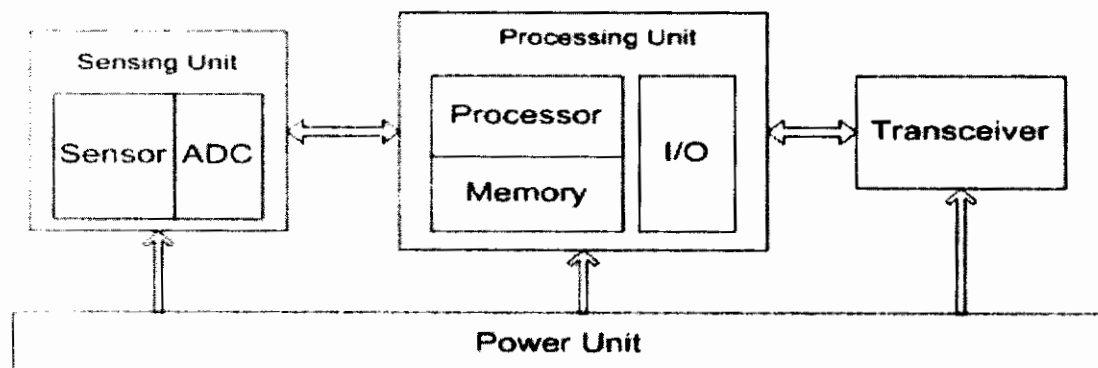


Figure: 1.3 Component of Sensor Node [27]

In some cases sensor network having more less memory so it further narrow down the key management schemes having low memory overhead. Due to above mentioned resource constraint there should be a key distribution mechanism having lightweight and work efficiently in such environment.

1.6 Network Limitations

An adversary can easily inject an arbitrary data as well as eavesdrop on all the network communications because wireless sensor network use wireless open channel. In above mentioned both active and passive attacks are possible on WSN, therefore it is necessary to impose centralized cryptosystem solution on WSN. With the passage of time, the sensor network is gain large scale so the requirement of security scalability of network should also design.

1.7 Malicious Attacks

In large-scale wireless sensor network, it is not possible to monitor each node individually and sensors are not temper resistant due to lack of resources. Therefore it has chance that adversary may capture certain sensor node from network with the knowledge of monitoring cell and stolen all secret data from those compromised node. Therefore, adversary is able to do so, than it is possible to insert malicious attack by using stolen information. In front of these challenges, some refined techniques are required to maintain a balance between security threat and sensor network within limited resources.

1.8 Security Requirements for WSN

Current sensor nodes are tiny devices with very limited resources and un rechargeable battery. Therefore, the complicated and resource-consuming security algorithms used in other networks cannot be used to protect WSNs. Therefore, during the design of security mechanism, limited memory, limited computational power and limited energy should be under consideration. A sensor network should have following abilities during the transmission of data or share in formations.

1.8.1 Authenticity

Authenticity means to enables a sensor node to clear the identities of its conversation entities so that no opponent could impersonate another entity, and distribute faked messages.

1.8.2 Integrity

Integrity means to provide guarantee that a data being transferred is never malicious or modified by a middle entity without being noticed.

1.8.3 Confidentiality

Confidentiality ensures that the content of the message being transferred is never revealed to illegal entities. The transformation on network of secret data, such as military operation information those need to be confidential.

1.8.4 Availability

Availability makes sure that the survivability of the desired sensor network services in spite of denial of service, such as DOS attacks. It is possible to start DOS attack at any level of sensor networks and could be of various forms.

1.9 Key management

Key establishment is one of the significant security features of WSNs as it is critical for providing data substantiation, privacy and truthfulness and almost all WSN security mechanisms rely on solid encryption. Even though key management has been intensively deliberated in, broadcast communication and is not an exclusive issue to wireless sensor networks, conventional key management techniques cannot be used for WSNs directly or even with minor amendment due to the limitations of sensor and their application environments. Symmetric secret key cryptography based methods are attractive for WSN application because they are energy-efficient. Symmetric secret keys are pre-allotted to sensors before network operation. After deployment, sensors execute operations of neighbors' discovery and shared key establishment to found secure communications between them. However, due to the restricted memory of sensor nodes, these Symmetric Key Cryptography based systems are not capable to attain both ideal connectivity and perfect flexibility for large-scale WSNs. Instead, the use of Public Key Cryptography (PKC) would get rid of the above problem. Due to their asymmetric characteristic, nodes do not require to hold the pre-distributed keys. Completely the network any adjacent sensors can found a secure communication path between themselves. Because of the key independence of each other's public key, detain of some nodes will not influence the

security of others node lies in the network. However, it is generally recognized that the popular cryptographic primitives for wireless sensor network are Symmetric Key Cryptography techniques such as RC6, RC5, Message Authentication Code (MAC), AES and Public Key Cryptography has long been considered infeasible in WSNs due to lack of resources in sensor nodes. To the best of our knowledge, the first challenge on common perception is the literature [28], which planned a hybrid authentication key management technique, lies on Elliptic Curve security.

1.10 Motivation of the Research

It is not easy to put into practice security defenses in wireless sensor network. the main barriers in positioning security on WSNs is that the current network has inadequate communication and computation potentials and it is not possible to replace the battery by hand due to the unattended nature and dangerous sensing of environments. The restraints make the stipulation of adequate security countermeasures even more difficult. Key management is the stipulation made in a cryptography system design that is linked to key generation, key updating, key distribution, and key revocation [29]. Key management is the essential building block for most cryptographic solutions. The proper management of cryptographic keys decides the successful use of cryptography for security. Key management is put up on several cryptosystems and cryptographic primitives, such as MAC and PKC, and provides support to other security mechanisms, such as authentication and secure routing. The position of key management in a security architecture is displayed in **Figure 3**, part of which has been shown in [29]. However, the exclusive characteristics provide the key distribution schemes of physical media connected and common wireless

networks unsuccessful for WSNs. On the basis of these parameter, some investigators have begun to preserve WSNs with lightweight key management mechanisms. Compared with general key management schemes, lightweight. Key management systems provide security support with reduced overhead and thus are more suitable for WSNs. even though substantial developments have been made in general key management, the research on lightweight key management is still in its early years. Most of the available literature follows a routine whereby they firstly discover the potential attacks and then counteract the security problems with corresponding countermeasures. None of these solutions takes into consideration the specificities of WSNs in practical application terms.

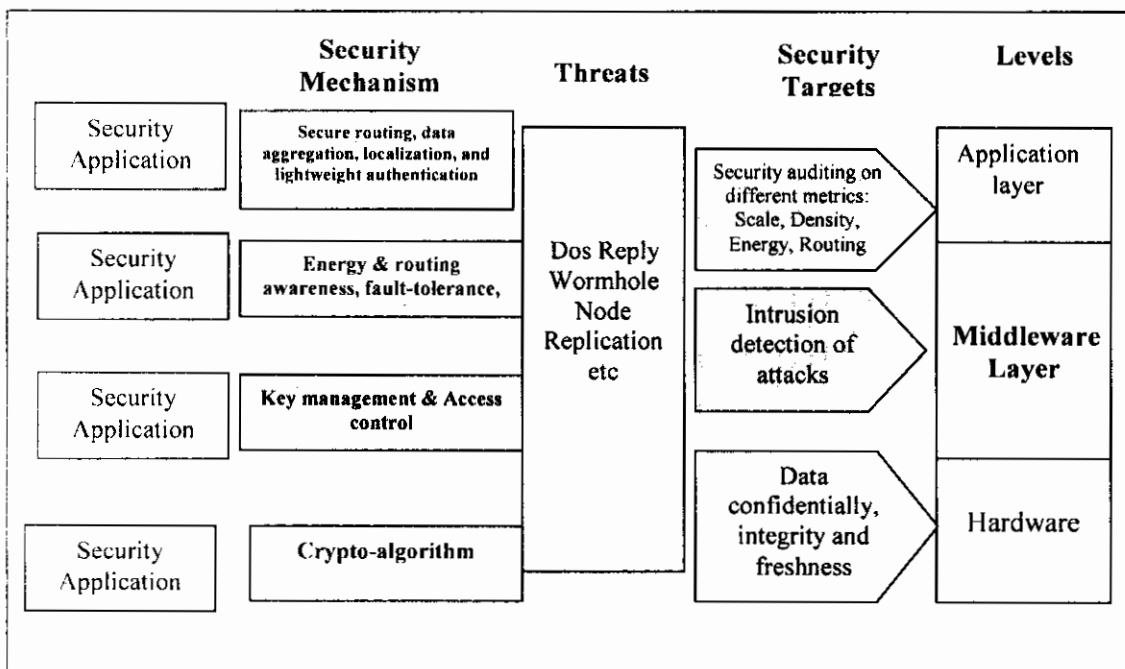


Figure: 1.4 Position of Key Management in Security Architecture [29]

WSNs are application-specific networks. Except for some familiar features, a sensor node based network for a explicit application has some different features and correspondingly

has some unique security requirements. The solution proposed for one particular application is unlikely to be readily applicable for another environment. Suppose a sensor network is deployed in the military surveillance environment and another in an agricultural base; the requirements of security should be different based on the resource that nodes possess and the risks they face. It is impossible to reach a one-fits-all key management solution. A key management mechanism would lose its practical value in applications when it is separated from the considerations of network-related issues [31]. Our designs have driven by some definite applications and in the light of their security necessities. This rule makes the designed method more reasonable. In this paper, authors integrate preceding research outcome and examine the open issues from the subsequent sub-categories such as management of different secret keys types, inherent or lightweight verification method, self-healing [32] secret key distribution method and PKC based or distributor key man secure agreement for wireless Sensor Networks.

CHAPTER 2 LITERATURE SURVEY

We organize our literature work according to key management techniques proposed for heterogeneous wireless sensor network. We have discussed different type of issues in existing techniques with respect to limited resources available in wireless sensor network. There is a contradictory concentration between minimization of resource utilization and maximization of protection altitude. A better solution actually gives a good compromise between these two.

2.1 Trusted Controller

Laurant et al [1] proposed key-Management Scheme for Distributed Sensor Network. The proposed scheme is motivation of the limitation of symmetric key pre-distribution, which focused only on group and broadcast communication and impractical for large scale DSNs. Proposed scheme is consist on three stages such as Key Pre-Distribution, Path Key Establishment and Shared Key Discovery. Shared key between nodes distributed on the bases of node id. This scheme is scalable and flexible scheme, trade off make between memory cost and connectivity. Key generation controller used, so not need to change key ring for sensor node during key pre-distribution. Key id and node id store on trusted controller node. The disadvantage of this strategy is the high processing and communication overheads, it initiates, in the path-key distribution phase.

2.2 Secret Master Key

B.Lai et al [2] proposed scalable session secure key structure protocol which enhance the security of wireless sensor networks. In this solution 'K' known as master key is used by pair of nodes M and N for establishing session key with random nonce N_A and N_B , such as $K_{MN} = \text{PRF}(K||N_N||N_M)$ and PRF is a function base on Pseudo-Random. Its need to chose

clusters size very carefully. Any sensor network with bigger clusters needs their sensor nodes to store up a larger number of secret keys.

2.3 Multiple Disjoint Path Discovery

H. Chan [3] proposed the multipath secret key re-enforcement is to make stronger the security of connected links. Update the link keys for nodes A and B after the Shared-key Discovery phase. This update is performed through multiple disjoint paths. Nodes A and B need to establish an initial link key additionally. Node X discovers all disjoint paths to Y that involve at most hops. Node X then generates m random values, which are encrypt with shared key and sent to Y through some disjoint paths. Finally, after receiving all key updates, Y generates the reinforced link key. Larger the number of hops, the better the probability that the enemy can snoop the key updates, single compromised connection in the path will make the entire connection insecure. Data transmission overhead is relative to the number of hops.

2.4 Generation of Random Nonce

B. Dutertre et al [4] improve single master key by using additional master key and proposed a Light weight key management in wireless sensor networks. In this technique, the sensor nodes of a same generation share a confirmation and generate a key and each node also keep in their memory a random nonce, as well as a secure key for each possible new generation. Than a session key is computed between two nodes. Both nodes are exchange nonce of each other. The third node recognizes itself with older node after receiving nonce function by computing secret key than generate pair the pair wise key. so, it is significant not to miscalculate the number of outlook creations with which a sensor

node have to correspond, on the other hand it may influence the network connectivity during different generations. A weakness of this technique is that an enemy need only to concession a few secret keys in order to destroy whole infrastructure of generations.

2.5 Probabilistic Session Key

P. Traynor et al [5], The effects of probabilistic key management on secure routing in sensor networks. Each node receives a group of keys, having lower size than network itself. This scheme provides better connectivity as well as low memory overhead. Probabilistic key management scheme has three sequential phases: Key pre-distribution, path-key establishment and shared key discovery. Many key pre-distribution are introduces such as basic key pre-distribution scheme, cluster key grouping, hashed random key, the Q-composite technique, session key, multipath key reinforcement and random pair wise schemes. These schemes bear scalability problems. The larger network size for a given stage increases the computation and communication overheads. The secret key sharing is limited by the memory existing on the sensor nodes, since the chance that adjacent node share a key is given by k/n , for example, the memory overhead is $O(n)$. In addition, they reduce the number of nodes addition those can be added in the network after the preliminary deployment. Finally, for fixed key chain size, the key connectivity achieved is lower than in the basic scheme.

2.6 Loop Based Key

Y. Zeng, et al [6] proposed A loop-based key management scheme (LBKMS) for wireless sensor. LBKMS think about a loop-based topology where each node such as "A" receives a unique ID, a private key K_A , and a master key K . After deployment, sensor nodes encrypt

their IDs with the global key broadcast this message. By using this information, a loop is constructing that certain number of node set S . If sensor A was responsible for the creation of loop L containing the set S , then A computes a loop-key $K_L = \text{Hash}(\text{timestamp} || KA || IDA || \{ID\})$ belongs to S . The global key was used to protect the distribution of the loop-key inside the loop. Although there are, numerous advantages of the network-wide key come up to reduce the serious security vulnerabilities. The capture of a single node would release the common key, compromising all the nodes in the network and their data transmission process. Moreover, an enemy with access to the master key possibly will without difficulty place in malicious nodes into the network. Revocation of such intruders would be very complicated or even not possible, since it would need all left over nodes to be assigning new secret key without using the older master key.

2.7 Secure Large Key Pool

Kousar et al [7] proposed Key Management and Secure Routing in Heterogeneous Sensor Network. According to the proposed methodology, a secret keys pool that have a number of symmetric secret keys is established and loaded to H-Sensor, assume that high capability node know as H-Sensors are more powerful and consist of low end L-Sensor. Every small sensor nodes are randomly pick up unique secret key from large key pool and produce a new secret key by applying one-way hash function. H-sensor makes a cluster by broadcasting a message in its communication range. After cluster formation L-Sensor discover their neighbor and discover cluster key on the cluster head based shared key. This scheme is completely connected, resilience against sensor node capturing and routing

attack but on the other hand it use and key pool that loaded on H-Sensor. In case of capturing a single H-node whole the network may compromised.

2.8 Key Chain Pool

Sajid et al [8] proposed “An Efficient Key Distribution Scheme” for heterogeneous sensor network lies on random key pre - distribution for heterogeneous sensor networks. The flow of this scheme is Key Pool \rightarrow Key Chain \rightarrow Key Ring. The achievements of this technique are equivalent probability of key sharing among nodes and store small number of key generation on node but it will reduce the memory overhead if to find the ring parameter is fixed. but for maximum key sharing it need the larger the pool size.

2.9 Q-Composite Key Distribution

Quang Yang et al [9] proposed An Efficient Key Management Scheme for Heterogeneous Sensor Network. It is challenge to establish key between homogeneous sensor node due to resource constraints so author adopt heterogeneous sensor network proposed for key establishment to attain better performance, resilience and security so author proposed symmetric secure key before deployment distribution and publicly known key cryptography for heterogeneous wireless sensor network. Three symmetric key are established. I- sink node to sink node II- Key sink node to low power nodes III-sensor key low sensor to low sensor key. Random key distribution has large key pool. In q-Composite, key two neighbor node share at least q-common key. This scheme reduces memory overhead, reduce computation overhead, provide security by high resilience against node capture and pair wise key pre distribution

2.10 Generation of Key hashed from Large Key Pool

Beming Tain [10] proposed “A Key Management Scheme for Heterogeneous Sensor Network Using Keyed-Hash Chain”. In existing technique some weakness were such as single key used that not satisfy whole communication, low probability to share key between sensor nodes and some neighbor node may not able to find a familiar key. The achievement of author are to support the establishment and renewal of five key, overcome the drawback of single key, sensor node store on commitments instead of generation key and new cluster mechanism is use that improves the key. The main problem is how to determine the length of key chain, if the key chain is longer than smaller the number of key chain. When size of key chain increase than memory is overhead increase but decreasing the size compromising on security.

2.11 Seed – Pool Based Key Pre-Distribution

Saber Banihashemian [11] A new Key Management Scheme in Heterogeneous Wireless Sensor Network based on random key pre-distribution. Connectivity and resiliency are two important criteria in key management in connectivity is increase than decrease resiliency and vice versa so author proposed random key pre-distribution scheme. Author proposed seed based scheme that reduced the storage requirement, increase connectivity and resiliency. Different seeds are to node by base station to drive a new key that is providing satisfactory security and seed use resiliency against node capture. Although different seeds are used according to distance of node but need additional computation and use of key pool face same memory overhead as in existing techniques.

2.12 Generation of Polynomial by multiplying Hashed IDs of Nodes

Mini Li et al [12] proposed scheme is based on dynamic generation of polynomial for Heterogeneous Sensor Network. This scheme motivated to enhance the life span of wireless sensor network by decreasing the computational and memory overheads and it distribute share keys without any large key pool. In this scheme the nodes are pre-loaded with master key K , to use encrypt message before the establishment of cluster key and it share among sensor node including base station. Some H-sensor id " λ_{hj} " that is a random number. To calculate some values, which are hashes of corresponding L- sensor node ids' hash function $h(x)$ is also pre-loaded on H-Sensor. Other side L-Sensor also pre-loaded " λ_{li} " their id's and a master key. The H-Sensor generate a polynomial as $(x - h(id_1))(x - h(id_2)) \dots (x - h(id_n)) K_{chj}$, where the value of id starts from 1 to n . by using all restored hash values those were decrypted by using " K " and get " λ_{li} ". This encrypted polynomial broadcast to corresponding L-Sensor ids to form a cluster key. The mechanism to generate a polynomial by the cluster head is complicated and resource consuming. Although this scheme remove the large key pool but increase the memory and computation overhead on the cluster head.

CHAPTER 3 PROBLEM DEFINITION

3.1 Problem Background

Because of vital progress in enveloping computing power and wireless data transmission technology, WSNs have expanded wide functions. On the other hand, some exclusive utilization of sensor network make them more exposed to security attacks than their wired complements. Security countermeasures should have taken to oppose analogous attacks. Key management facilitates as the foundation stone of other security methods as approximately all of security methods rely on, or are associated to, encryption. We have found that, regardless of important contributions completed over the decades, very few practical approaches, particularly in terms of key management solutions for HWSN has been proposed in the literature.

3.2 Existing Solutions for Key Management

Existing method for key management based on generation of n-degree polynomial. After deployment of sensor network, cluster head broadcast hello message with its id in encrypted form. There are large numbers of low power sensor (L-sensors) nodes surrounding the cluster head. L-sensors in the communication range of Header will receive and reply with their encrypted form id. Head nodes receive all L-sensor ids, calculate hash of all ids, and restore them. A polynomial is to be calculated on header node by as: $(x - h(id_1))(x - h(id_2)) \dots (x - h(id_n)) + K_{chj}$ and broad coast to all nodes corresponding nodes ids.

3.3 Problem Definition

Generation of cluster key in existing technique has high memory consumption, computation cost and communication overhead because H-Sensor nodes generates

polynomials by taking product of all hash values, those are calculated against the id of each L-Sensor node. The major issue with the polynomial multiplier is that especially combinatorial multipliers become very large and slow for longer factors.

When new L-Sensor Join the Cluster then H-sensors generate new polynomials to change the cluster keys according to the new received hash of (id_{new}) of L-Sensor. Then, H-Sensor broadcast novel generated polynomial to further presented L-sensors lies in the communication range of H-sensor which is decrease the life time of network.

3.4 Problem Scenarios

Key management in hierarchical wireless sensor network faced computation constrains due to low battery power of sensor nodes. Below figure demonstrates the initial phase of key management after deployment of network.

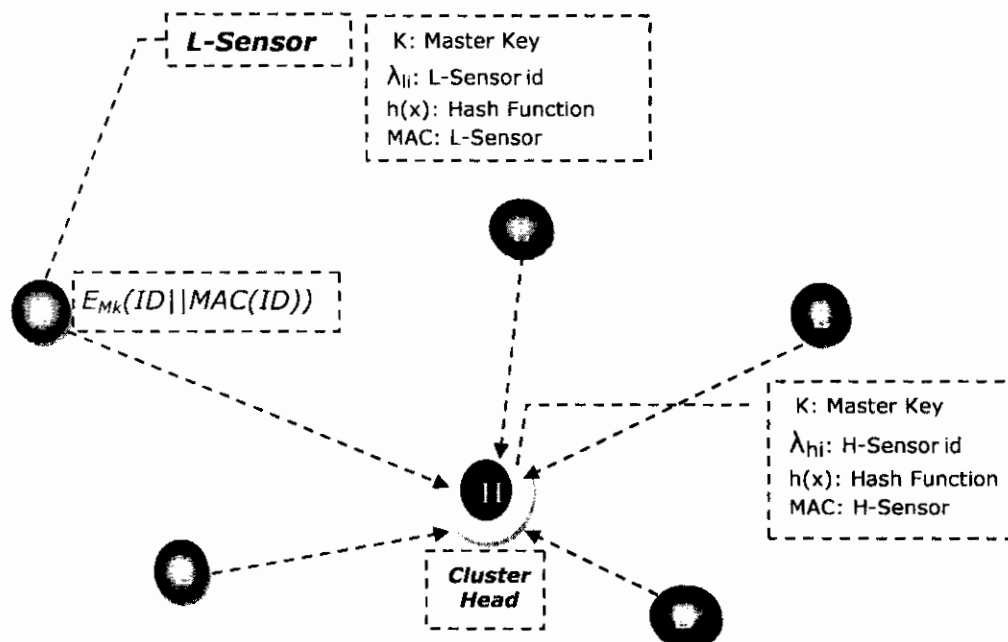


Figure: 3.1 Computation of Cluster Key

- 1: $L_1: L_1 \Rightarrow * E_k(\lambda_{li} | MAC_k(\lambda_{li}))$.
- 2: $H_1: L_1 \Rightarrow H: E_k(\lambda_{li} | MAC_k(\lambda_{li})), i = 1, 2, 3 \dots n; \lambda_{l1}, \lambda_{l12}, \lambda_{l13} \dots \lambda_{ln}$
 $D_K(E_K(\lambda_{li} | MAC_K(\lambda_{li}))), i = 1, 2, 3 \dots n;$
 $(h(\lambda_{l1}), (h(\lambda_{l2}) \dots (h(\lambda_{ln}))) : h(x), x = \lambda_{li}, i = 1, 2, 3 \dots n;$
 $P_{hj}: (x - h(\lambda_{l1}))(x - h(\lambda_{l2}) \dots (h(x - \lambda_{ln}))) + K_{chj}, j = 1, \dots n$
 $H_j \Rightarrow * E_K(P_{hj} | MAC_K(P_{hj}))$.
- 3: $L_i: H_j = L_i: D_K(E_K(P_{hj} | MAC_K(P_{hj}))), j = 1, 2, \dots m;$
 $K_{chj}: (x - h(\lambda_{l1}))(x - h(\lambda_{l2}) \dots (h(x - \lambda_{ln}))) + K_{chj}, x = h(\lambda_{li})$

3.1 Protocol for Computing Secret Key

3.4.1 Computations Overhead

During the key establishment phase in existing technique clusters' member node broadcast their ids and the cluster head in the communication range receive those ids and restore them by taking their hash. Polynomial generated on cluster head by multiplying "n" time of receiving ids; it is energy-consuming process.

3.4.2 Memory Overhead

Although it has assumed, that H-Sensor has enough memory to store cluster key but when number of L-Sensor increases so, the number of id also increases. It becomes memory overheads with the scalability of network.

3.4.3 Communication Overhead

Radio infrastructure consumes much more battery power than the cluster key computation in wireless sensor networks. To save the energy utilization, proposed security schemes

should have low communication overhead. Those schemes based on secure key pre-distribution, the communication overhead mostly occurs in the network initialization stage, since its need to exchange secure key information's with cluster nodes having low memory bit.

3.4.4 Addition of New L-Sensor

When a new L-sensor adds to a network, it broadcasts a hello message in order to join the clusters Head in its communication range. The Cluster head which receives a hello message replies with a message containing its own id and polynomial which is encrypted with Master key "K". The L-sensor computes the H-sensor's hash value $h(id_{hj})$ and then derives the cluster key K_{hj} through the polynomial.

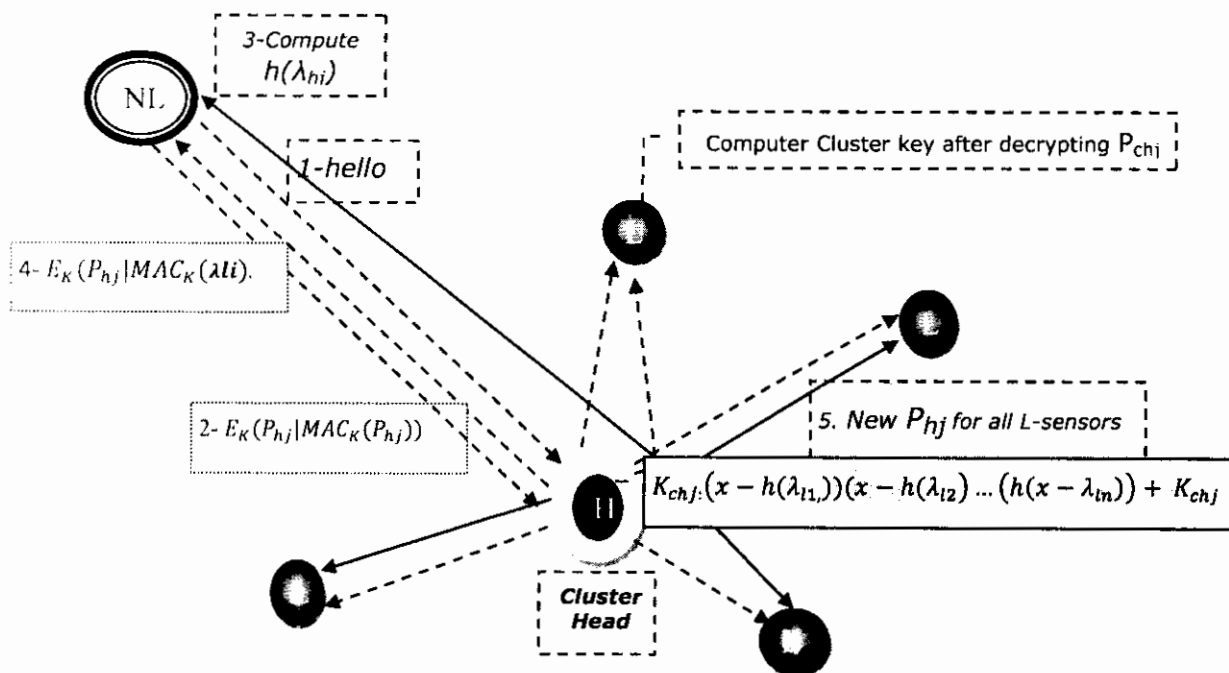


Figure: 3.2 New L-Sensor Additions

After this the L-sensor sends a message containing its own hash values $h(id_i)$ which is encrypted by K_{ch} to the corresponding H-sensors. These

H-sensors generate new polynomials to change the cluster keys according to the new received $h(\lambda_i)$. Then, they broadcast new polynomial to other existing L-sensors in their communication range. When new L-sensor add into the cluster the cluster head again broadcast the polynomial which increase communication cost and reduce the sensor network lifetime.

CHAPTER 4 SOLUTION & METHODOLOGY

4.1 Proposed Method

The model defined by Kausar et al [7] is adopted for our proposed scheme, that is a heterogeneous sensor network based model. In this model, nodes are divided into two groups for Heterogeneous Sensor Network. The high-end sensor node called as H-Sensors are the clusters head and the nodes with less resource with respect to their communication, computation and memory called L-Sensors. To increase lifetime of network the clustering based technique is used for network deployment in which nodes are divided according to their workload. The heterogeneous model used to propose our mechanism is described below:

- **Base Station:** It is assumed that base station is highly protected, not flat for malfunction. Base station is also powerful with respect to resources such as energy, bandwidth, processing, and storage capacity.
- **H-Sensors:** High power sensors (H-sensors) have more storage power and computation potential. The additional capability of cluster heads is that they can directly communicate with base station and are equipped with tamper resistant hardware. Cluster head node has well-off resources, but these are still inadequate as compared to the base station. In heterogeneous model, crossbow's nodes were used as cluster heads.
- **L-Sensors:** These are normal sensor nodes and have limited memory and processing power. The L-sensors obtain data from the surrounding atmosphere and send the composed data to the H-sensor.

Initially when sensor network is deployed there are large number of low power sensor nodes and limited quantity of cluster heads. Future, easy continuation and scalability both

H-sensors and L-sensors are added according to need. It is also assumed that H-Sensor and L-sensors are deployed uniformly and randomly.

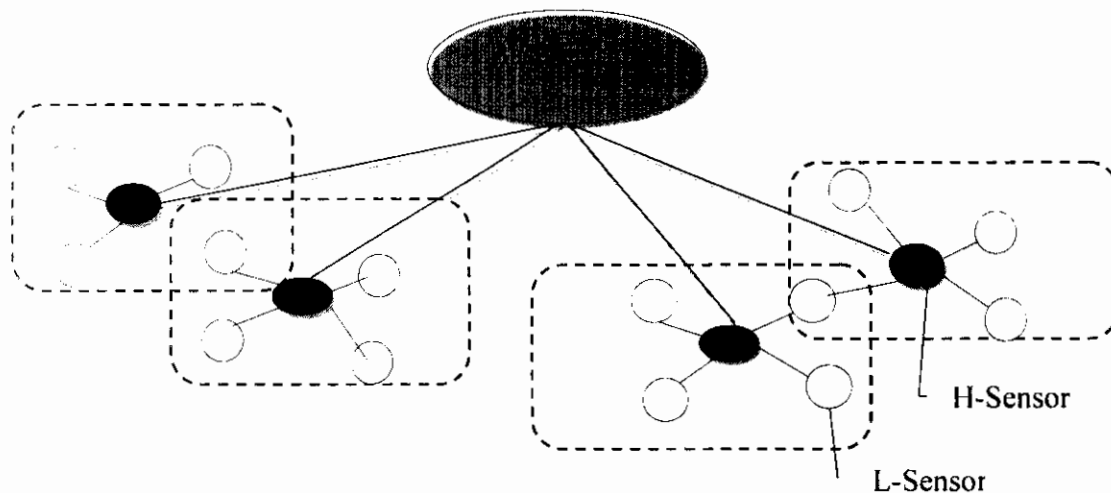


Figure: 4.1 Wireless Sensor Network Topology [7]

In cluster base network, processing is enabling on local processing which reduce communication overhead on network. HSN is consisting of distributed organization where nodes divided into clusters and each cluster managed by a cluster head, as depicted in Fig. 4.1. In hierarchical structure H-nodes acts as cluster head, connected to base station and all L-sensors. L-sensors can securely share information with their neighbor node and cluster head.

4.2 Polynomials

A polynomial made up a term that is only, added, subtracted and multiplied. It can be simply stated as, polynomial terms are functions in which x perform as an input variable. The polynomial computation process is made up of two factors, the first factor is the

coefficient of x and the second factor is being x power to some positive integers as $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$. In polynomial, the values of x should be positive, whole number and equal to zero. Coefficient of the equation as $a_n, a_{n-1}, \dots, a_1, a_0$ and all are real numbers. The upper limit of the polynomial calculating function is the uppermost value for its degree shown by n where the value of n should not be zero.

4.3 Dynamic Selection of Node IDs

After network deployment, broadcasting hello message by L-Sensor appending with its id (λ_{i_i}) the cluster key establishment phase will start. To ensure maximum probability that L-Sensor is identified, L-Sensor broadcasts its id several times by encrypting with key K that is preloaded. To restore original ids of L-Sensor, H-Sensor decrypts all received ids of L-Sensor by using K , and computes hash of L-Sensors id(s) and restores them in the high end power nodes. H-Sensor chooses hash of L-Sensor ids subset to generate polynomials.

4.4 Generation of Polynomials by using XOR Function

Polynomials are generated by multiplying all hash values that are restored on H-Sensor, i.e. $(x - h(id_1)) (x - h(id_2)) \dots (x - h(id_n)) + K_{chj}$, where id starts from 1 to n , and K_{chj} is the cluster key that is generated by H-Sensor using " K ". Proposed methodology is based on randomly chosen hash values that are restored on H-Sensor instead of multiplying up to " n ". Polynomials are generated by taking XOR of randomly selected $h(\lambda_{i_i})$ and broadcast them to corresponding L-Sensors. The exclusive-OR based polynomial is $P_{HJ} = (x - h(id_1)) \text{ XOR } (x - h(id_2)) \dots \text{ XOR } (x - h(id_n))$. This will reduce computation overhead and reduce

memory utilization. An XOR function is a function of the form $g(x, y)$. Where, $g(x, y)$ is equal to $f(x \otimes y)$. It is for from some of Boolean functions, which is f lies on some n bits.

1. Generate N Polynomial;
2. For $i = 1; N$
3. Convert into Binary Polynomial [N]
4. END
5. For $i = 1: N$
6. Polynomial $[i] \otimes$ Polynomial $[i+1]$
7. END

4.1: Pseudo code for \otimes Based Polynomial [21]

After network deployment of pre-loaded information of sensor node, the sensor node in complete the following steps to make a network.

1. Every sensor node broadcasts the directory of its generation key ids beside with its own id, MAC (message authentication code) and nonce (number used once).
2. Each neighboring node receives the message, compares the list of generation key ids with its own list.
3. If a adjacent node discovers a common secret key with the source node, it will sends message as an acknowledgement. This reply message holds a list of common generation key ids, a nonce number, node's id and equivalent MAC.
4. The nodes will complete a challenging response procedure to confirm the common generation keys. If this verification procedure gives a positive result, then the connected link between the nodes measured as secure link.

4.5 Solution Scenario

First, we are conforming that the network topology mentioned in our solution scenario is adopted proposed by Kousar et al [7] but instead of large key pool we generate dynamic polynomial based on low power sensor nodes' id. The enhanced efficient key management scenario has shown in figure 4.2, which have low computation, communication, latency and memory overhead. Our proposed scheme also gave new protocol for adding of new low power sensor node securely and efficiently. We list below notation which appear in figure 4.2.

Table: 4.1 Notations

Notation	Definition
BS	Base station
CH	Cluster head
$H-Sensor$	High Power Sensor
$L-Sensor$	Low Power Sensor
L_j	Ids of H-Sensor
L_i	Ids of L-Sensor
*	Represent any L-sensor or H-sensor
$h(x)$	Hash function to compute hash values
KM	Master key
$EK(m)$	An encryption of message m with key K
$M_1 M_2$	Concatenation of message M_1 and M_2
$E_K(M)$	Encryption of message M with K
$D_K(M)$	Decryption of message M with K
\otimes	XOR
$MAC_K(M)$	Message Authentication Code of message M using key K .
P_{bi}	Polynomial generate by cluster head on the basis of hashed L-sensor ids.
K_{chj}	Cluster key

4.6 Key Establishment Phase

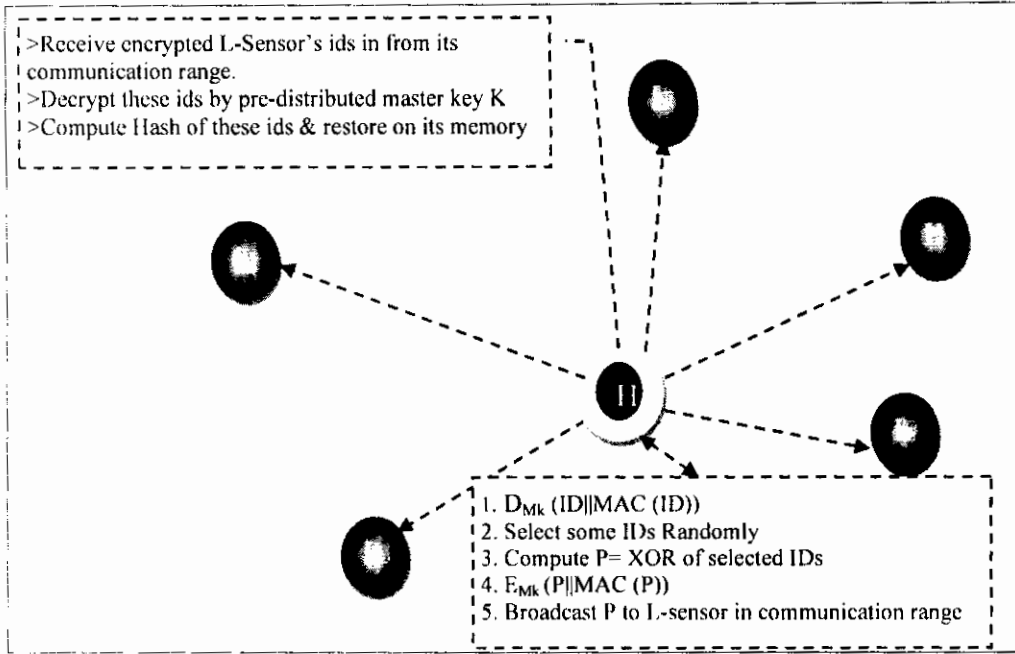


Figure: 4.2 Cluster Key Establishment

The proposed methodology based on XOR of hash function. The H-Sensor will generate Polynomial, which uses randomly selected hash values restored on it instead to multiply all hash values.

1. $L_i: L_1 \Rightarrow *; E_k(\lambda_{i1} | MAC_k(\lambda_{i1}))$.
2. $H_i: L_i \Rightarrow H: E_k(\lambda_{i1} | MAC_k(\lambda_{i1})), i = 1, 2, 3 \dots n; \lambda_{i1}, \lambda_{i2}, \lambda_{i3} \dots \lambda_{in}$.
3. $H_j: D_K(E_K(\lambda_{i1} | MAC_K(\lambda_{i1}))) \quad i=1, 2, 3 \dots n;$
 $(h(\lambda_{i1}), (h(\lambda_{i2}) \dots (h(\lambda_{in}))) : h(x), x=\lambda_{i1}, i = 1, 2, 3 \dots n;$
4. $H_i: \text{Rand} \leftarrow \text{some of } \lambda_{i1}$
5. $H_i: P_{hj}: (x - h(\lambda_{i1})) \otimes (x - h(\lambda_{i2})) \dots \otimes (x - h(\lambda_{i1})) + K_{chj}, i = 1, \dots n$
6. $H_j \Rightarrow * E_K(P_{hj} | MAC_K(P_{hj}))$.

$$7. L_i: H_j: \Rightarrow L_i: D_K \left(E_K \left(P_{hj} \parallel MAC_K(P_{hj}) \right) \right), j = 1, 2, \dots, m;$$

$$L_i: DK(K_{chj}: (x - h(\lambda_{t1})) \otimes (x - h(\lambda_{t2})) \dots \otimes (x - h(\lambda_{ti})) \otimes (x - h(\lambda_{tj})) + K_{(chj)}) x = h(\lambda_{ti})$$

Protocol 4.2 Enhanced Protocol Cluster Key Distribution

After cluster key establishment phase the hash function $f(x)$ is delete for more security although is assumed that H-sensor are equipped with temper-resistant hardware and H-sensor also delete L-sensor node ids . Flow diagram is as follow:

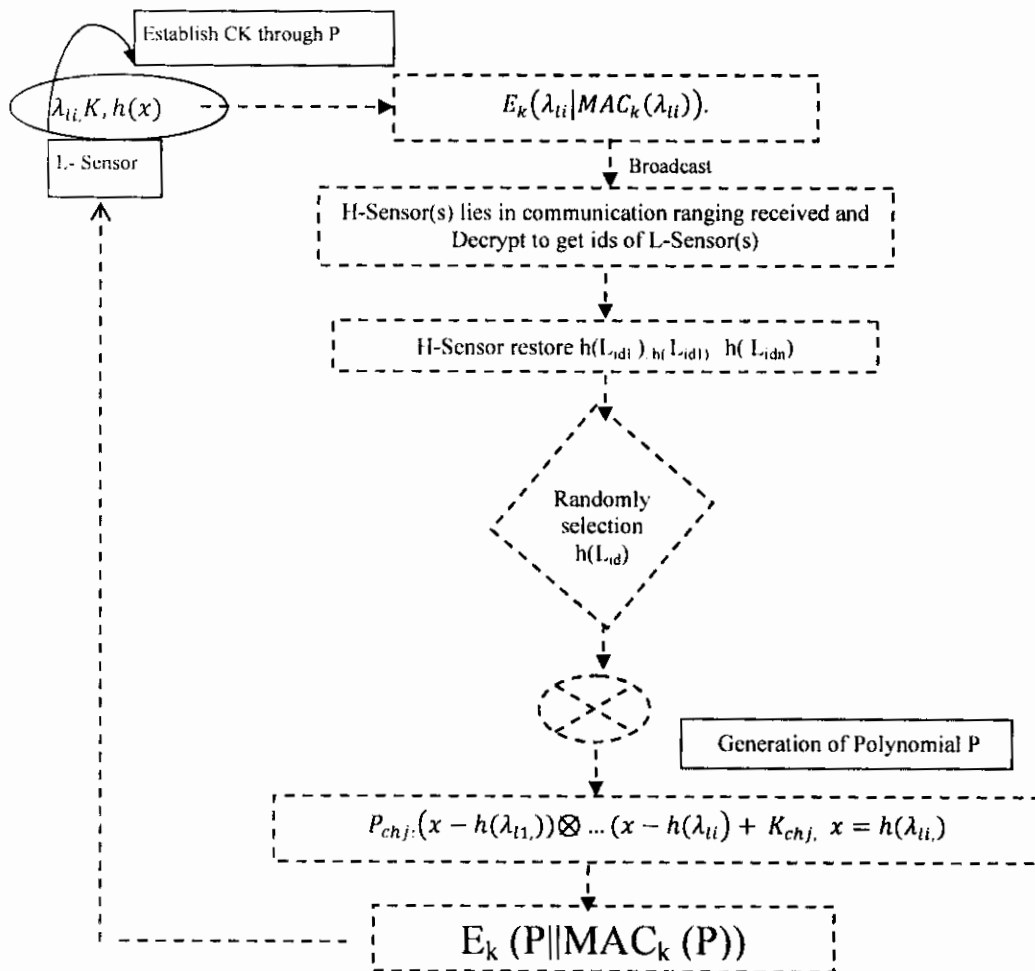


Figure: 4.3 Key Distribution Flow

4.7 Addition of New Node

An advantageous property in a scalable key management system is the capability of adding new nodes to the network. These recently deployed sensor nodes require to set up secret key with accessible nodes. On the other hand, before adding up new nodes into network, it should be guaranteed that the newly installed sensor node is not an opponent node. The proposed method is robust for adding new lawful L-sensors in the network.

Protocol: 4.1 Notations

BS: Base Station

CH: Cluster Head

L_i : Low Energy Sensor

$L_{(Ni)}$: New Added L-Sensor

MAC_ADRS: Mac Address of Device

E_{KCB} : Master key between base station and cluster head

N_B : Nonce of base station

K_s : New session key

To reduce the communication cost of CH and L-sensors in the network our scheme is robust and efficient. It is understood that in the network base station is more powerful, temper resistant and having much resources such as memory, strong communication ability and monitoring capability to all network. Therefore, it is a responsibility of base station to recognize and adding new node in the network. The process of adding new sensor node in the wireless sensor network using Mac address of sensor is the main contribution of our

scheme. New sensor authentication, recognition and addition of done by base station and cluster heads, so it is efficient and secure.

Protocol: 4.1.2 Pre Loaded Information to L_{Ni}

1. K : Master Key
2. $h(x)$: One way hash function
3. Randomly selected node id i.e. λ_{ii}

The process of addition of new node is different from exiting technique. Before the deployment of new sensor node in the network, some information's are pre-loaded to it as mentioned in protocol 4.1.2. After pre-loaded the desired information new L-sensor is deploys randomly in the exiting define sensor network area.

Protocol: 4.1.3 Adding New Node Protocol

1. $BS \rightarrow CH$: $E_{K_{CB}}(id_{(lni)}, N_B, MAC_Add_{(lni)}, List_{(lni)})$
2. $CH \rightarrow BS$: $E_{K_{CB}}(id_{(CH)}, N_B)$
3. $CH \rightarrow *$: $E_{chj}(Ks, List_{(lni)} || MAC_{(lni)})$
4. I_{ii} : Store $(List_{(lni)} \& MAC_{(lni)})$

Before the deployment of new L-sensor in the network, as shown in protocol: 4.1.3 base station broadcast a message-containing id of new L-sensor, MAC, and a list of new L-sensor node in encrypted form to all cluster head nodes. In heterogeneous sensor network $CH \ll L$ -sensors so there is no communication overhead is so far. This basic idea of this scenario is to verify the new added sensor by cluster heads and minimizing to enter a

malicious sensor node and eliminate the process of new polynomial generation for the entire network when after adding new node. Base stations entire the network receive this information from the base station and restore the MAC and id(s) of new sensor nodes to be add. Cluster heads broadcast the information of new node(s) to their communication range encrypting with cluster key to recognize the new node(s) by existing nodes. So, that L-sensor not forward any message sends by malicious node. All L-sensors in the communication range receives these in formations and make a MAC list of new nodes to add in the network, the process shown in protocol 4.1.3.1 occurs simultaneously there is no network delay occur.

Protocol: 4.1.3.1-Scenario-I: If heterogenating communication than

1. $L_{ni} \rightarrow CH: E_{Ks} (id_{(Lni)}, MAC_{(lni)}) | M_{BC}(MAC, id_{(Lni)}) \quad i=1, 2...n$
2. $CH \rightarrow L_{ni}: E_{Kc} (P_{hj}, Nc)$
3. $L_{ni} \rightarrow CH: Ek_{ChNi} (Nc, id_{(lni)})$
4. $CH \rightarrow * Add_Node(id_{(lni)})$

Completing the new sensor node deployment there may be two scenarios for establishing the cluster key for new sensor node. According to scenario-I if the communication new L-sensor is directly with cluster head without any other L-sensor mediator, then new added sensor broad cost its id and MAC. New L-sensor will encrypt this message through its pre load key K. Cluster head, which already have a list of new sensor, is recognize by comparing the received MAC with its own list. After verifying that requested is not malicious, it replies with polynomial, which is in encrypted form by K. New L-senor

decrypts this message and gets polynomial to calculate a cluster key. The communication overheads reduced during the addition of new sensor node depict in protocol 4.1.3.1-scenario-I. In proposed scheme, the most of the communication burden lays on base station.

Protocol 4.1.3.2 - Scenario-II: *If L_{Ni} indirectly communicate with CH than*

1. $L_{ni} \rightarrow * : \text{hello_msg}(id_{(Lni)} | MAC_ADRS)$
2. $* : \text{compare } MAC_ADRS_{(Lni)}, List_{(*ni)}$
3. *if $MAC_{(Lni)}$ in $MAC(List_{(Li)})$ than*
4. $L_i : \text{Hello reply } (id_{(Li)})$
5. $L_n : \text{adds the } (id_{(Li)}) \text{ into neighbor list}$
- Else*
6. *discard*

The protocol 4.1.3.2 scenario-II is adding new sensor node in the cluster if the new sensor node communicate with cluster via already member nodes. Figure 4.4 shows the proposed scheme to add a new sensor in the network. Our proposed scheme has two scenarios to add a new sensor in the network, which is secure and authentic. To reduce the communication, computation and network delay, base station handles the process of adding new node because base station is more secure and having no resource constraints. In heterogeneous network after the deployment of new node lies in such a position where it can communicate directly with cluster head as show in figure 4.1 scenario-I.

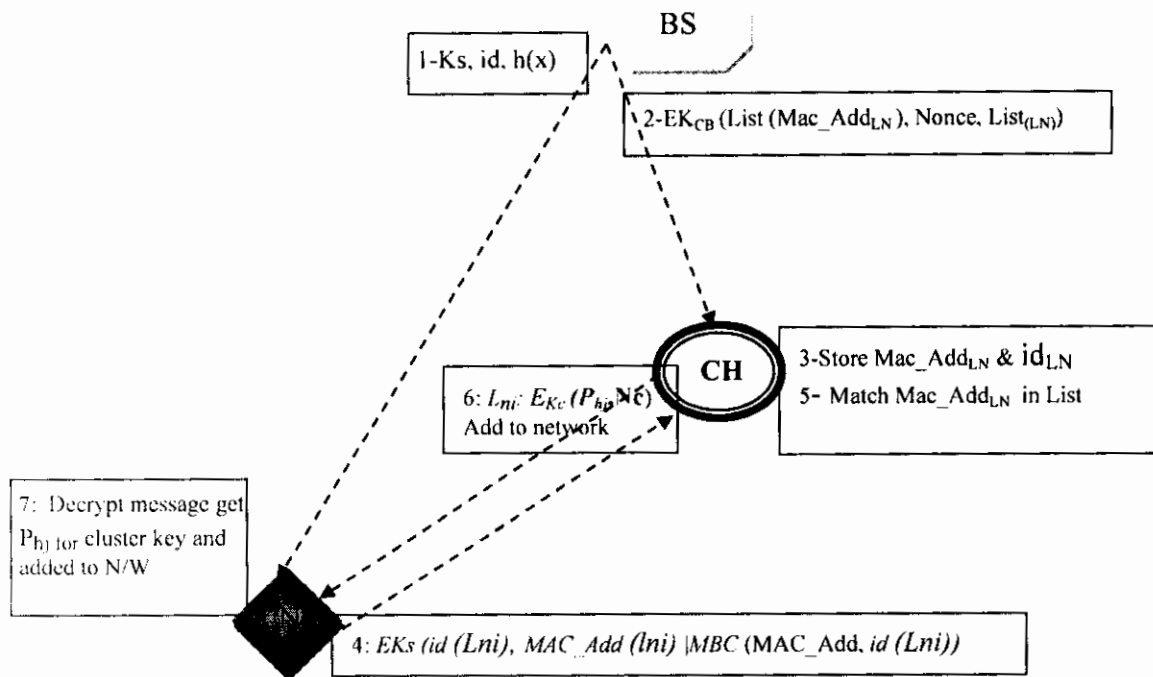


Figure: 4.4 Scenario-1

Before the deployment of new sensor in the network, base station pre-loaded some information in to the new sensor as show in protocol 4.1.2. To prevent from malicious and replay attack we proposed a new technique that before sending the information of new base station establish a new session key between itself and cluster head(s) K_{CB} as shown in protocol 4.1.3 and send $MAC_ADDRESS$ of new sensor(s) to be added and their list encrypted with K_{CB} . Our scheme reduced 50% communication, computation and network delay during the addition of new node as compare to existing scheme proposed by Mini Li et al. existing technique completed node addition after four communication steps and whenever a new node added cluster head generate a new polynomial and broadcast to all its member nodes i.e. low energy end L-Sensors. $MAC_ADDRESS$ of a device is unique and 8-bit. Instead of generating new polynomial whenever a new sensor is add and refresh

to the entire network. Base station makes a list of new L_sensor , appends their $MAC_ADDRESS$ in encrypted form, and sends to all cluster heads entire the network. After the deployment of new node in the network, when new node sends join request to cluster head(s). Cluster head recognize comparing the $MAC_ADDRESS$ of joining node within its data base and if its finds same the new node become its member otherwise in case of malicious node it sends a intrusion detection message to base station.

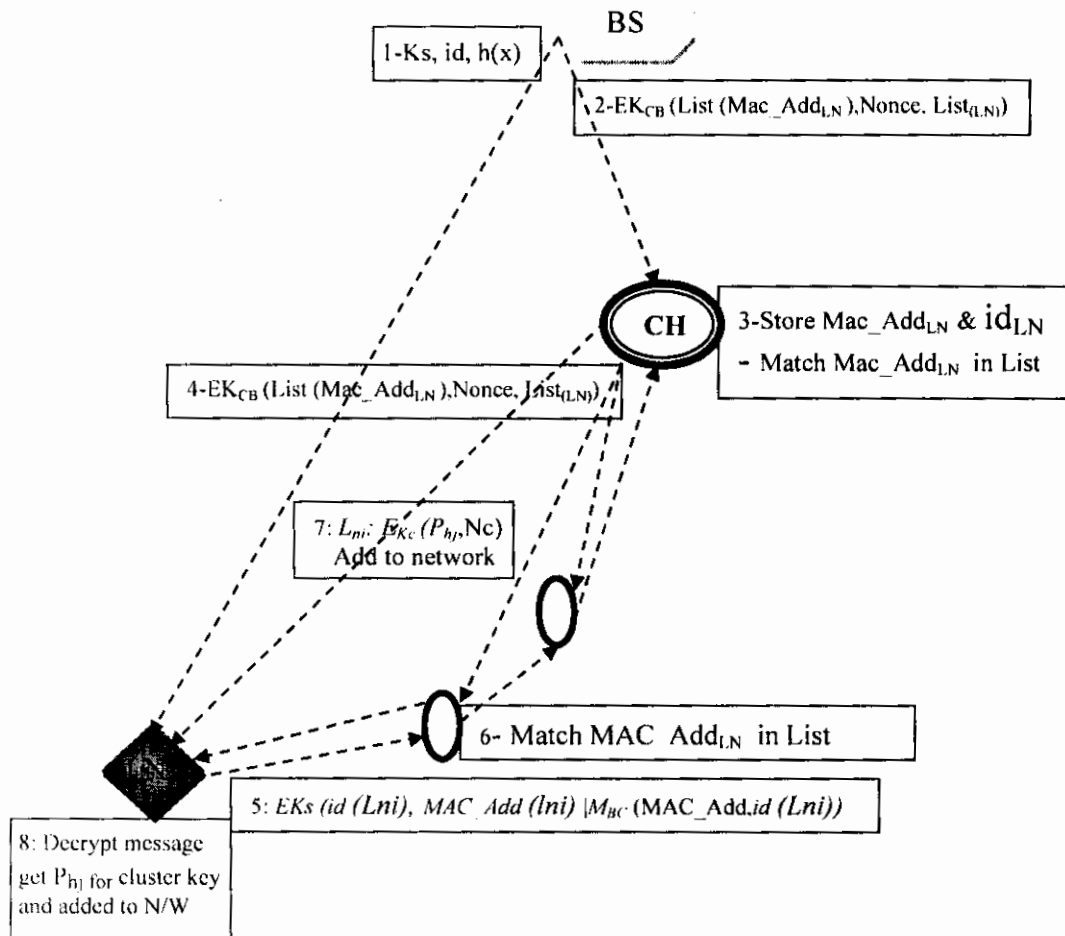


Figure: 4.5 Scenario-II

Figure 4.5 scenario-II depicts the addition of new L-sensor if the communication of new added sensor via already clusters members.

1. To reduce the communication and computation cost of cluster head we have proposed that base station is responsible for deploying the new sensor in the network. Base station will pre-load the new sensor node L_n with session key, node id and hash function.
2. Base station will generate a list of new sensor node id, the MAC Address, and a nonce number send to its cluster heads.
3. Cluster head stores this information's of new L-Sensor to be added in the cluster.
4. Cluster head encrypts this information's adding it nonce number and broadcast a small length bit size list to its member nodes; this is only for scenario-II.
5. After deployment of new sensor node, it does encryption by using session key and broadcast. The sensor nodes in its communication range recognize by matching its information with their own list and add it in their neighbor list.
6. After verification, neighbor node forwards information is of new node to cluster head.
7. Cluster head generates cluster key for new node and send to it for further secure communication within cluster. After receiving cluster key new sensor node deletes existing data.

CHAPTER 5 SIMULATION AND RESULTS

In this chapter, we will discuss the implementation scenarios and elaborate to obtained results in detail. The implementation scenario is divided into, network model, and mathematical model, key computation cost, memory overhead, communication cost, addition of new node and probability of key sharing among the sensor nodes.

5.1 Network Topology

The network is heterogeneous sensor network consisting of three types of nodes: Base Station: It is assumed that the base station is secure, and does not have any resource limitation. H-Sensors having more processing capability memory and equipped with tamper resistant hardware and these can exchange information directly with the base station

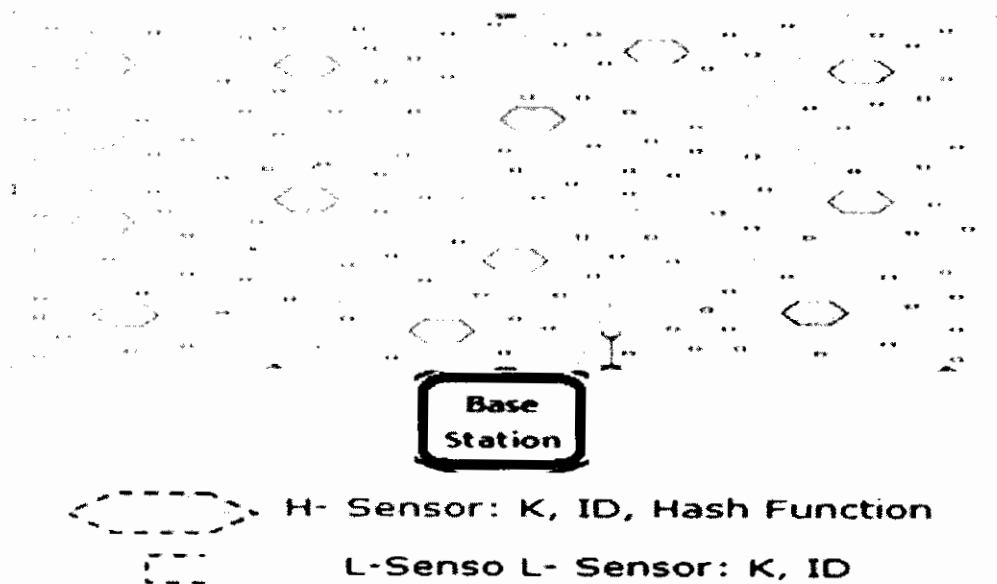


Figure: 5.1 Sensor Network Deployment Topology [7]

In heterogeneous WSN, all L-Sensor nodes directly communicate with their cluster head and cluster heads communicate with Base Station. Base station is more powerful and having high resilience against malicious attack.

5.2 Mathematical Model

Key management for sensor networks countenance many problems due to resource constraints. In table 5.1, we compared our scheme mathematically with existing technique.

Table: 5.1 Mathematical Comparisons

Schemes	Computation	Communication	Memory
Min Le et al	1) Cost of computing HASH n times 2) Cost $\prod_{i=1}^{i=L}(x_i - h_i)$ 3) Cost Enc($\prod_{i=1}^{i=L}(x_i - h_i)$) 4) Cost Dec($\prod_{i=1}^{i=L}(x_i - h_i)$) n times	$\left \text{Enc} \left(\prod_{i=1}^{i=L} (x_i - h_i) \right) \right $	Need to Store n-values where n is the ids of all L-Sensor nodes in the cluster. Multiplication results of all sensor nodes' ids.
Proposed	1) Cost of computing HASH M times where M is any random value $\ll n$ 2) Cost computing $(x_i - h_i) \oplus (x_j - h_j)$ 3) Cost Enc($(x_i - h_i) \oplus (x_j - h_j)$) 4) Cost Dec($(x_i - h_i) \oplus (x_j - h_j)$) n times	$\left \text{Enc} \left(\prod_{i=1}^{i=L} (x_i) \oplus (x_{i \ll L}) \right) \right $	Need to store M-values where M is some randomly selected values and $M \ll n$. several bits need to store and there XOR.

The comparison of existing and proposed scheme shown in table 5.1 mathematically. According to Min Le et al H-sensor generate polynomial by applying multiplication operation of all received ids and restore their hashes. It needs to encrypt n-bit data using master key K before broadcasting cluster key, which cause communication overhead and as well as memory and computation overhead on cluster head. We have enhanced existing scheme by reducing computation, communication and memory overhead on cluster head. According to our proposed scheme cluster head select L-sensor ids randomly and generate

polynomial by computing XOR of selected ids. The cost of encryption on cluster head and decryption on L-sensor node is reduces several times. It increases the key sharing probability between the cluster head and the member nodes by broadcasting more than two time the nod ids and increase the network connectivity.

5.3 Simulation

We have simulated the proposed solution on NS2.35. A simulation has been completed with the help of well-known and worldwide acceptable NS2 simulator. NS2 is a distinct event simulator targeted at networking research. It is an object-oriented, discrete event driven network simulator developed at UC Berkely written in C++ and OTcl (Tcl script language with Object-oriented extensions). It implements network protocols such as UDP and TCP, traffic source behavior such as FTP, Telnet, Web, CBR and VBR, router queue management mechanism such as Drop Tail, RED and CBQ, routing algorithms such as Dijkstra, and more. NS-2 also implements multicasting and some of the MAC layer protocols for LAN simulations. NS-2 includes a tool for viewing the simulation results, called NAM. NAM is a Tcl/TK based animation tool for viewing network simulation traces and real world packet trace data. During an NS simulation, user can produce topology configurations, layout information, and packet traces using tracing events in NS. The NS-2 simulation is a flexible tool for network engineers to explore how different protocols work with different configurations and topologies. Our simulation works on group based network where heavy sensor nodes works as a cluster heads and they directly connected with the base station. Each cluster head communicate with low power sensor nodes. The simulation parameters shown in table 5.2 and we initialize the energy, receiving

cost and data packet size and deploy our enhanced key distribution procedure for comparison with existing technique.

Table: 5.2 Simulation Parameters

SIMULATION SETUP	
Parameter	Values
Network Field	(500 x500) in meters
Node numbers	100~300
Cluster radius	r 400 m
Sensing radius	rs 120 m
Initial energy	1000 J
Data packet size	40 Bytes
Broadcast packet size	25 Bytes
E-threshold	0.01 J
Channel Type	Wireless
Propagation Model	Two Ray
Physical Type	Wireless Physical
Mac Protocol Type	Mac/802-11
Queue Type	Queue/DropTail/PriQue
Link Layer Type	Link Layer
Antenna Type	Omni Antenna
Max Packet in Queue	50
Routing Protocol	DSDV
Agent Trace	ON
Router Trace	ON
Mac Trace	ON
Movement Trace	ON

When the trace file is generated, it is ready to be animated by NaM. Upon startup, NAM will read the trace file, create topology, pop up a window, do layout if necessary, and then pause at the time of the first packet in the trace file. Through its user interface, NAM

provides control over many aspects of animation. This simulation tool has worldwide acceptability with very high acceptance of result.

5.4 Network Deployment Simulation Scenario

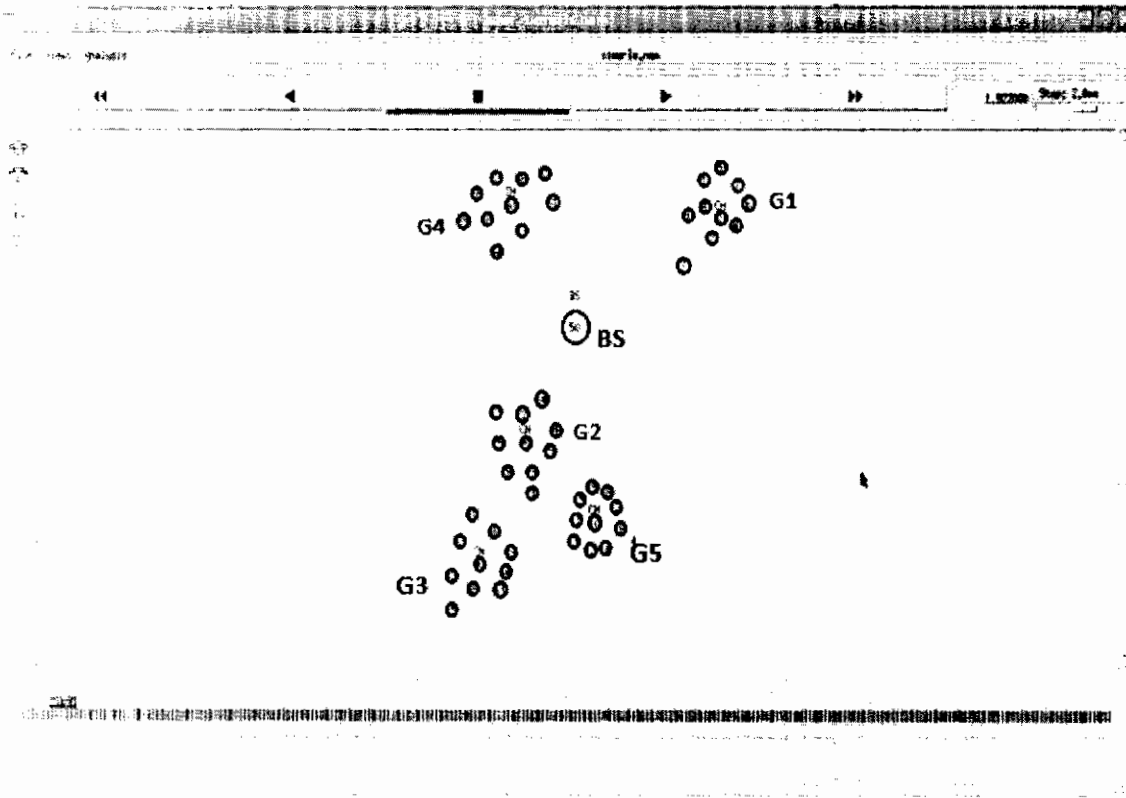


Figure: 5.2 Network Deployment Scenario

We deployed our sensor network in NS2 simulator. In figure 5.2, a Base Station (BS) communicates with Cluster Heads (CH) and after deployment of heterogeneous wireless sensor network randomly its make five groups represented by G1, G2, G3, G4, and G5.

5.5 Simulation Scenario for Group Communication

In this scenario, we have simulated initial cluster key establishment phase after the deployment of group based sensor network in which there are cluster head having more

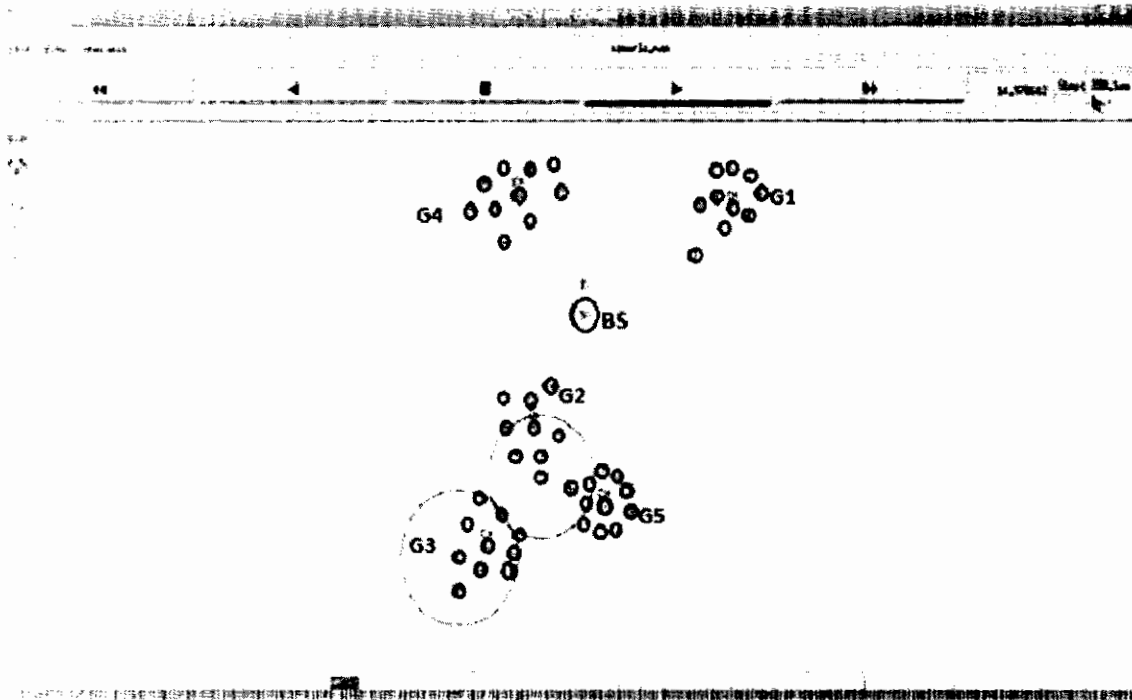


Figure: 5.3 L-Sensor Broadcasting their IDs and Cluster Communication

All L-sensor nodes are broadcasting their ids and the CH in their communication range receives these node identifications and restores them after calculating their hash. To increase the probability that CH received the node of L-sensor, each L-Sensor broadcast its id more than one time after some time delay.

Computation Overheads

Let us now analyze the number of basic operations used by long multiplication of two numbers a and b each of which has n digits. In case one is shorter than the other is, we can pad it with zeros at the front. For each digit y of b we need to do one short multiplication axy this needs $2 \times n$ basic operations. Because there are n digits in b , long multiplication needs n short multiplications which together account for $n \times (2 \times n) = 2 \times n^2$ basic operations. The results of the short multiplications are aligning under the respective digits of b . To simplify the further analysis, we put zeros in the empty positions. According to these calculations, multiplication operation takes more computing time than the XOR operation.

Table: 5.2 Computation Cost for Polynomial Generation

Node	Computation Cost of Polynomial	
	Multiplication	XOR
10	139.8	2.9
20	303.7	3.4
30	449.2	4.7
40	615	5.5
50	766.5	7.2
60	918	8.1
70	1078.7	9.4
80	1235	11.1
90	1384.7	13.2
100	1543	14.1

So to reduce computation cost on sensor nodes we have proposed XOR operation instead of multiplication to generate polynomial for generating cluster key. In our scheme, each L-sensors and H-sensors are pre load with their ids and assumed of 32-bit IP, a hash function, a master key, and the cluster head randomly select some of ids and generate a polynomial by applying XOR operation on them. This scenario simulated in network simulator and shows that our proposed scheme is efficient with respect to computation overhead on sensor node. For example, when we take XOR of two string of 5-bit binary data. It will take five essential steps. However, when we apply XOR function on two string of 100-bit binary information will acquire 100 fundamental steps. The algorithm used to apply XOR function is the same in each problem and its complexity was specified in terms of the size of the binary information or data. The size of a number n is distinct to be the numeral of binary bits required to mark n in binary.

Here $\text{bry}(n)$ is used to signify the range of n .

$$\text{bry}(5) = \text{bry}(101_2) = 3$$

$$\text{bry}(20) = \text{bry}(10100_2) = 5$$

$$\text{bry}(2^{12}) = \text{bry}(4096) = \text{bry}(100000000000_2) = 13$$

The bry is obtain when take XOR of two binary information all of size bry then we take n steps. The resultant XOR has computational order with respect to its complexity of “*order n*” which is denoting by $O(n)$. If we take the double for computing the dimension of the problem the size of the number to be XOR will be double because the computing steps requirement will be double as well as the computing time.

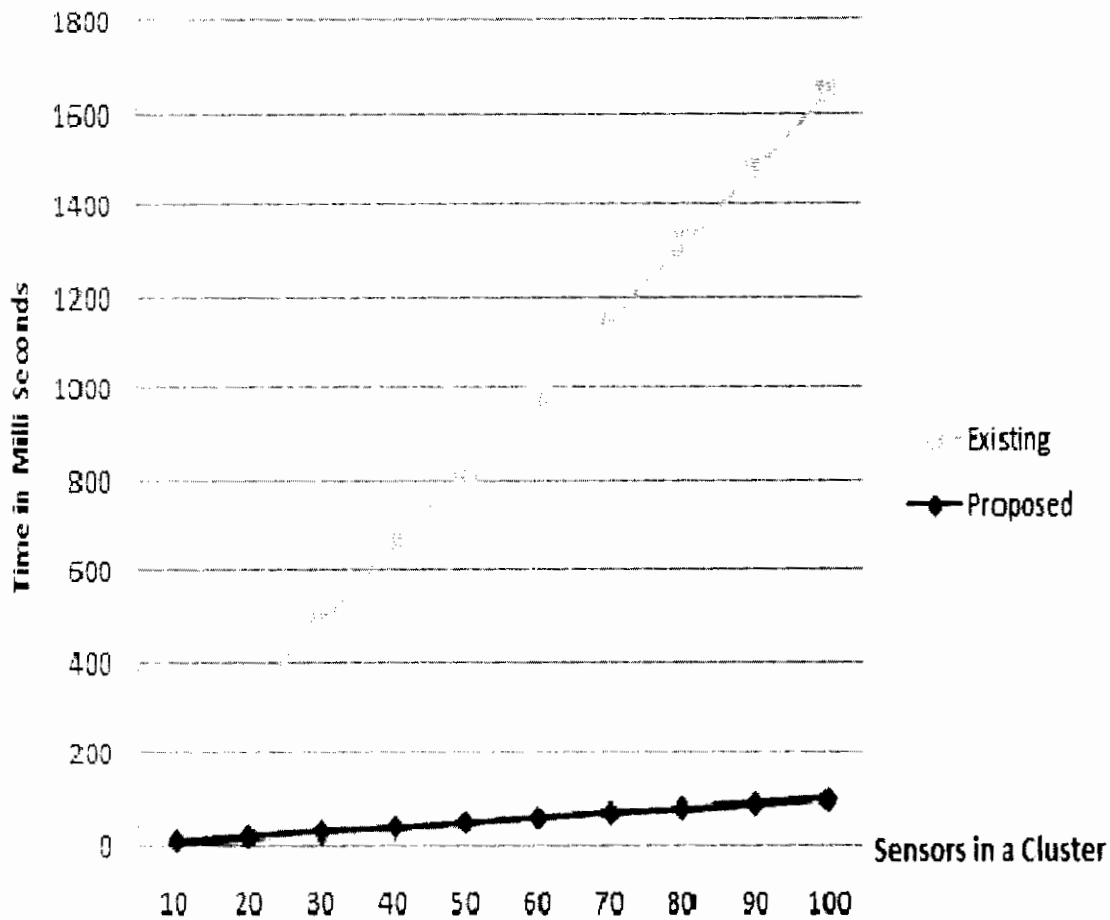


Figure: 5.4 Computing Polynomial

Computational complexity calculated separately of the operation. The amount of time that is needed to perform n basic steps will differ from node to node. The significant thing to note is that for an algorithm with complexity big $O(n)$, multiplying the size of the problem by X will have the effect of multiplying the time required by X as well. The computational complexity of adding two binary numbers is also big $O(n)$. However, the computational complexity of multiplying two numbers is big $O(n^2)$. If you double the number of bits in the numbers to be multiplied, then the time required quadruples because $(2n)^2 = 4n^2$.

5.7 Consumption of Energy

Due to battery, constraint in wireless sensor network it is very important that key distribution protocol should be efficient so energy overhead should be minimal. Proposed technique is very energy efficient and increase the lifetime of network.

Table: 5.3 Consumption of Energy During Cluster Key Establishment

S/No	Nodes	Energy $\mu\text{J}/\text{Byte}$	
		Existing Technique	Proposed Technlque
1	10	469.42	236
2	20	858.18	472
3	30	1231.30	708
4	40	1627.59	944
5	50	1966.67	1180
6	60	2420.51	1416
7	70	2823.93	1652
8	80	3213.62	1888
9	90	3759.29	2124
10	100	4696.52	2360

In existing technique, cluster head calculate polynomial after receiving all ids of L-Sensors in its communication range. To compute SHA-1 sensor node consumed 5.9 $\mu\text{J}/\text{Byte}$ [16]. To computer SHA-1 of n L-sensor the sensor node consumed bulk of energy. We enhanced existing technique for more comprehensive decision of energy consumption for generating polynomial by cluster head. To compute on SHA of L-sensor id is 5.9 $\mu\text{J}/\text{Byte}$, so when we generated polynomials through existing technique suppose the number of L-sensor are n than the consumption of energy is $n \times 5.9$ which mean it is directly proportional with the incremental of L-sensors. The simulation of our propose technique save four time than

existing technique. SHA-1 has 128-bit data to be processed which mean that 16-byte x 5.9 μ J for one hashing.

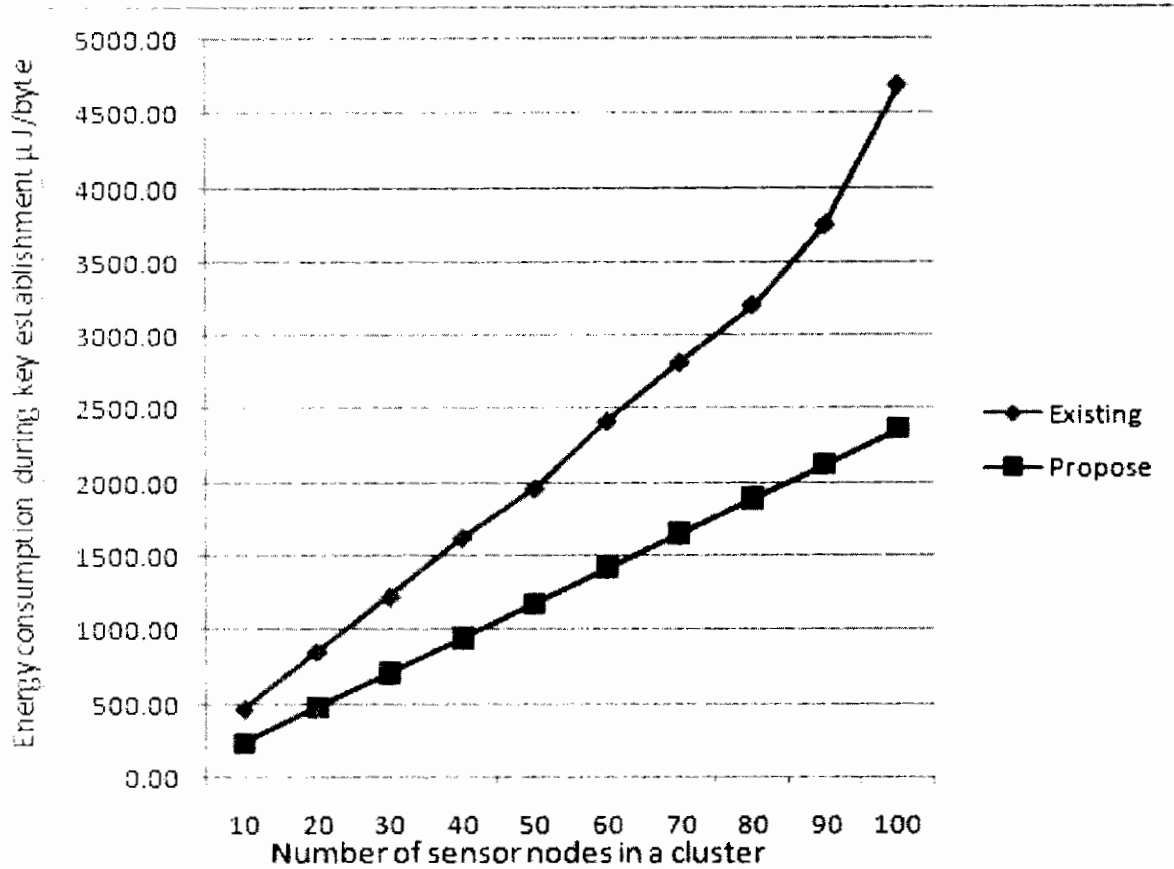


Figure: 5.5 Key Establishment and Energy Consumption

This results shows that the generation of polynomial through multiplication is energy consumption than the XOR. The number of sensor nodes varies from 10 to 100. The simulation results have shown in Figure 5.3. We can find that existing technique proposed by Min Li has cost much more energy than our proposed. This is due to the too much energy cost by point multiplication, pairing, and mapping algorithms. Each node needs to operate these algorithms many times, and the number of a sensor node neighbors determines the number of operation times.

5.8 Memory Overhead

Memory Overhead is the quantity of memory mandatory to store security resources. Represent the total number of nodes in a Heterogeneous Wireless Sensor Network, the number of H-sensors and L-sensors are represented as total number of sensor node in a network (n_T) and total high power nodes as (n_H) and low end or member nodes as (n_L) respectively, where $P = id \times n_L$ and $n_H + n_L = n_T$ [5]. Proposed scheme the $P = (id \times n_L)/4$ which is randomly selected by (n_H) and finally generate polynomial that reduced memory overhead. In our simulation, result had shown the comparison of memory overhead to existing technique.

5.9 Communication Overhead

The communication cost measured by the ratio of byte transmitted to the number of useful data byte received. The majority of energy consuming process in sensor networks in communication. Therefore, it is significant that communication be used sparingly.

$$\begin{aligned} Cost &= \frac{\text{Utilized Bandwidth}}{\text{Effective Data Through put}} \\ &= \frac{\text{Total Byte Transmitted}}{\text{Total Byte of Data Received}} \end{aligned}$$

The total numbers of bytes transmitted counted at the channel, which is including control packets as well as data packets. Min Li et al proposed that when new sensor node added in the network, each new L-sensor broadcast a message containing its id after deployment. The basic purpose of this message is to join the clusters that lie in the communication range of L-sensor. Cluster heads (H-sensor) which receives this message replies to correspondent with a reply hello message that contain the id of cluster head and encrypted

polynomial by using pre assign key K . The L-sensor generate the H-sensor's hash value as $h(\lambda_{hj})$ and then generate the cluster key which is recognize by K_{hj} through the polynomial. Then, it sends a message containing its own hash values $h(\lambda_{di})$ which is encrypted by K_{hj} to the corresponding H-sensors. These cluster heads generate fresh polynomial to modify the cluster key according to the updated $h(\lambda_{di})$. After updated polynomial broadcast by cluster head to other accessible L-sensors. Each new L-sensor deletes $h(x)$ and $h(\lambda_{hj})$. According to scenario, depict in figure 3.2 it need four communication steps to add a new node. Our proposed scheme reduces these overhead depict in figure 4.4. Our simulation results shown that proposed scheme is also efficient with respect to communication overheads during the addition of new sensor nodes.

Table 5.4 Energy Consumption During Addition of New L-Sensor

Cluster Size	New Node	Communication Cost of Adding New L-Sensor	
		Existing	Proposed
10	1	0.2152	0.0878
20	2	0.3312	0.1164
30	3	0.4872	0.145
40	4	0.6632	0.1736
50	5	0.8192	0.2022
60	6	1.1062	0.2308
70	7	1.3012	0.2594
80	8	1.5822	0.288
90	9	1.7532	0.3166
100	10	1.9492	0.3452

MAC Address based new node addition algorithm implemented results shown on table 5.4, which shows that our proposed scheme reduced communication steps and there is no

need to regenerate polynomial by H-sensor and broadcast to whole the cluster. We have proposed that, verification process of new node accomplished by base station, because it has no resource constraint. Base station broadcast an id list and MAC_Add of new nodes to be added in the network to all cluster heads. When new node is deploying in the network is pre loaded some information as shown in algorithm 4.1.3. Cluster head have recognize new node by it MAC_Add with list receive from base station.

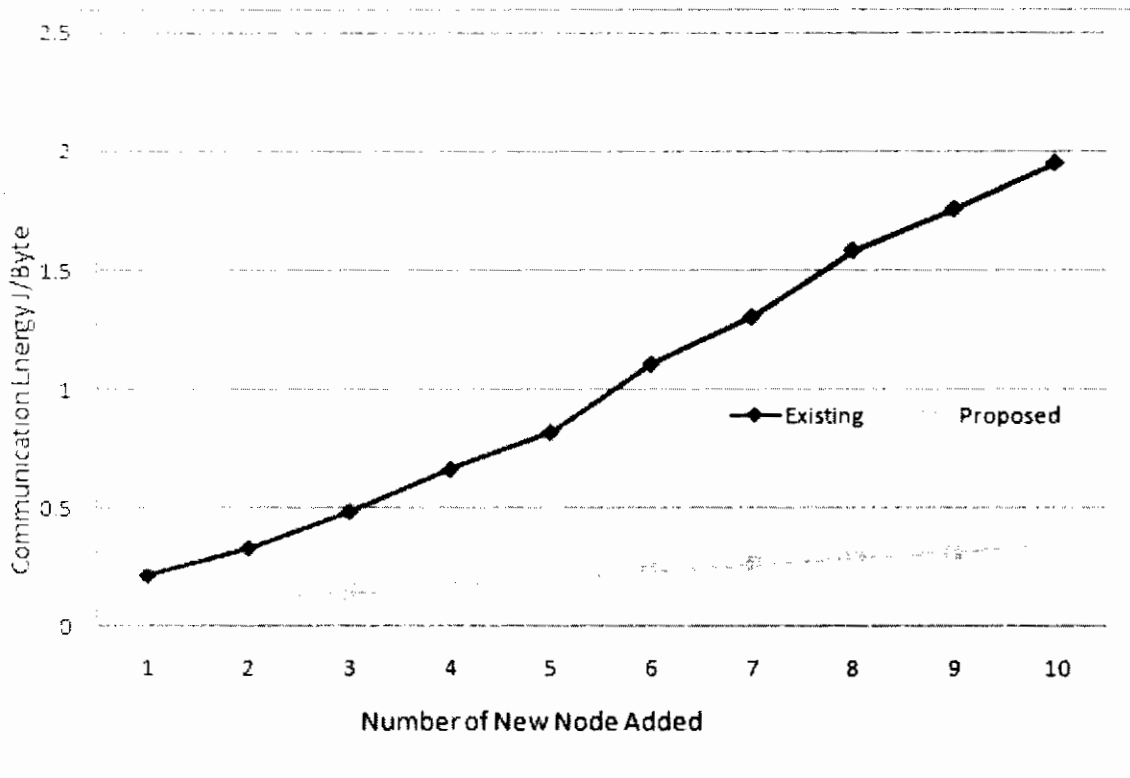


Figure: 5.6 Addition of L-Sensor

We have set 59.2μ Joule to transmit and 28.6μ Joule receiving energy consumed to one-byte data. The total consumed is $n \times T_c$. The sensor network lifetime is inversely proportional to the consumption of energy. Because that to make a network scalable it is important to save energy during adding new node.

5.10 Latency Time

Latency also measured as a significant factor manipulating key establishment protocol design. Latency in a WSN is an appearance of how much time consume for a data packet having cluster key to get from one cluster head in the sensor network to the L-Sensors or member nodes of the cluster head.

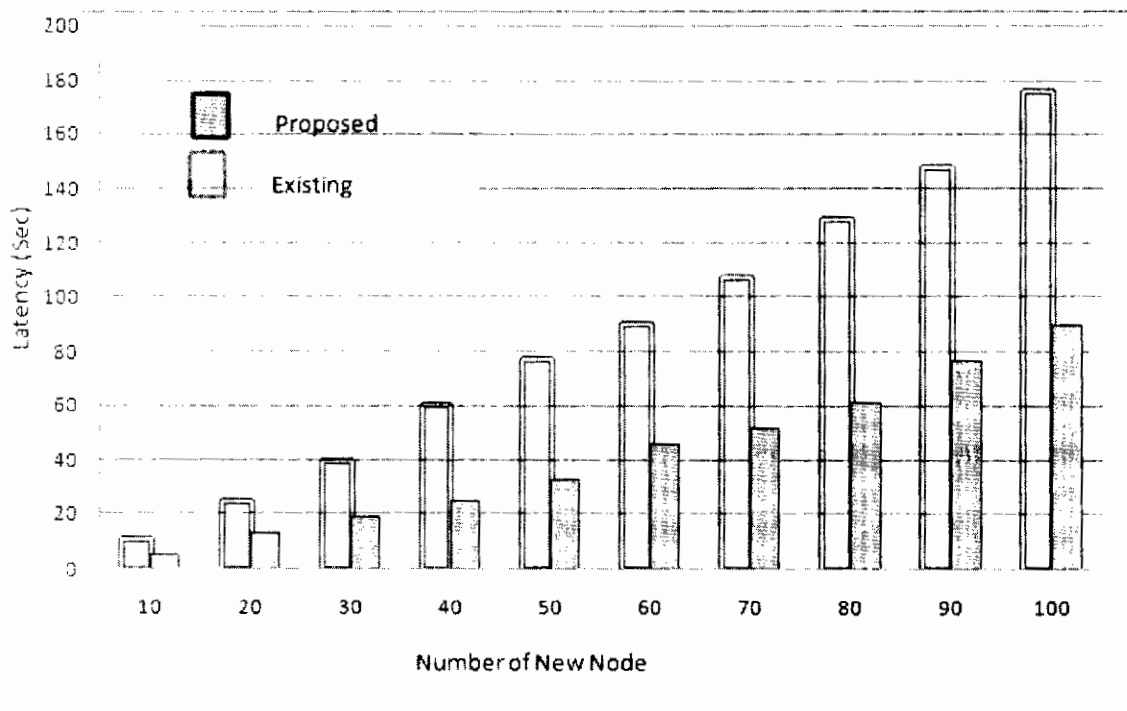


Figure: 5.7 Latency Comparisons

Whereas latency or delay in sensor base network is calculated either, the time it acquire for the source node to send a data packet to the targeted node who receive it or round-trip. For node round trip, the mean of latency occur one-way from sending node receiving. It is counting the one-way latency from the receiving node to back to the sending node. We computed the latency time between the cluster had and destination which are L-sensors. Our result shows that latency time considerably reduced when it compared with the exiting

method. Since our approach computed the cluster, key efficiently and reduced the delay on the cluster head. Our method outperforms other methods in achieving reduced latency time.

5.11 Cluster Key Sharing Probability

We have simulate our scenario in the area of 1000x1000 meter an compare the node key sharing ratio with the existing 300x300 meter simulation scenario. Let us p consider the possibility that in the whole the network small nodes who are the members of cluster head stores one cluster key to full fill its minimum requirement. If is consider that any small node was unable to store cluster key of any cluster. The resultant of no key establish between small node and cluster head it cannot discover cluster key. The responsibility of cluster head to generate the cluster key with small nodes lies in the communication radius. Apparently, the number of cluster head determines p. Figure 5.8 illustrates that value of p changes with the quantity of cluster head in the network. We have simulated our proposed scenario and in 1000\1000 meter area and find the probability of cluster key sharing by small nodes and achieve better key sharing probability with existing technique having 300x300 meter sensor node deploying area.

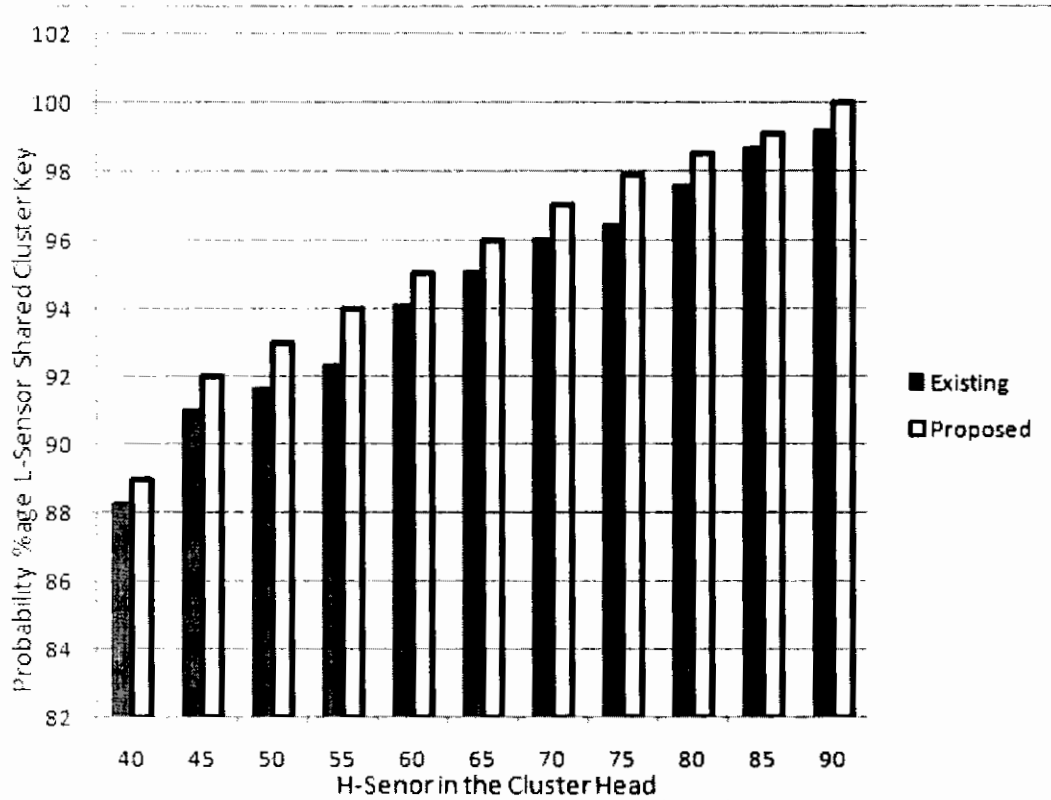


Figure: 5.8 Key Sharing Probability

Figure 5.8 shows that, cluster head should attain some amount in classify to formulate small node having maximum probability to store at least one cluster key for communication. When there are enough cluster head organized in the concerned area, p is relatively high. In figure 5.8, p is 88.3% when H-sensors' quantity is 40 and P achieves 99.2% when H-sensors' quantity is more than 89 but in our scenario shows more efficient with respect to cluster key sharing.

CHAPTER 6 CONCLUSION & FUTURE WORK

6.1 Conclusion

For cluster based wireless sensor network a secure and efficient key management scheme is need to secure and manage the large number of keys in the scheme. The main objective of proposed research an efficient key management is to apply and evaluate a new technique for key establish for Heterogeneous Wireless Sensor Network allowing secure transmission of data among nodes and reduce memory overhead and computation cost. This scheme based on generation of polynomials by applying XOR of randomly selected values, which increase the lifetime of sensor network and will hopefully reduces the communication cost, memory overheads and processing high-end sensor node for generating polynomial. We enhanced existing technique in term of adding new sensor in the cluster. Efficiently addition of new sensor node increase the life time of network as well as provide better security. We have giving new MAC_ADDRESS base node addition, which is more effective with respect to communication cost. During systematic and simulation results, we have exposed that subset based polynomial key establishing is resilient for node and key sharing while necessitating a less communication, memory and computation overhead.

6.2 Future Work

We have proposed polynomial subset based key management scheme in which cluster head is responsible to manage secure key in the cluster. The simulation results of proposed scheme have been shown to be better and efficient. Having less computation cost with respect to time and reduced communication delay in the network it is more secure and reliable. The cluster key formation process reduced from n-bit to some selected bit, which reduced memory overhead on cluster head as well as other low-end sensor nodes. In future, we want to test the performance of this scheme for different mobility scenarios of the sensor nodes. After that, it will be further tested on Mobile Ad-hoc Network (MANET).

REFERENCES

References

References

- [1]. L.Eschenauer, V.D.Gligor “A Key-Management for Distribute Sensor Networks” in Proceedings of the 9th ACM Conference on Computer and Communications security U.S Army, November, 2002, pp. 41-47.
- [2]. B.Lai, S.Kim, I.Verbauwhede, “Scalable Session Key Construction Protocol for Wireless Sensor Networks”, the fourth IEEE Workshop on Large Scale Real-Time and Embedded Systems (LARTES), Austin, Texas, December 2002, pp.134-144.
- [3]. H.Chan, A.Perrig, D.Song, “Random Key Pre-Distribution Schemes for Sensor Networks”, in Proceedings of the 2003 IEEE Symposium on Security and Privacy (SP’03), IEEE Computer Society, Washington, DC, USA, 11-14 May 2003, pp.197 - 213.
- [4]. B.Dutertre, S.Cheung, J.Levy, “Lightweight Key Management in Wireless Sensor Networks”, the International Conference on Performance, Computing and Communications, 2004, pp. 813 – 818.
- [5]. P.Traynor, C.Guohong, T.La Porta, “The Effects of Probabilistic Key Management on Secure Routing in Sensor Networks”, in Conference (WCNC’06), Wireless Communications and Networking, IEEE Computer Society, Washington, DC, USA, vol. 2, 2006, pp. 659 – 664.
- [6]. Y.Zeng, B.Zhao, J.Su, X.Yan, Z.Shao, “A Loop-Based Key Management Scheme for Wireless Sensor Networks” the International Journal of Computer, Vol.4809, October 2007, pp. 103-114.
- [7]. F.Kausar, S.Hussain, L.T.Yang, A.Masood, “Scalable and Efficient Key Management for Heterogeneous Sensor Networks”, the Journal of Supercomputing, Vol. 45, pp. 44-65, Feb 2008.

References

- [8]. S.Hussain, F.Kausar, A.Masood “An Efficient Key Distributed Scheme for Heterogeneous Sensor Network” the 7th International Conference on Wireless Communications and Mobile Computing IWCMC , 2007, pp. 388 - 392
- [9]. Q.Yang, Q.Li, S.Li “ An Efficient Key Management Scheme for Heterogeneous Sensor Networks”, the 4th International Conference on Wireless Communication, Networking & Mobile Computing, October 14, 2008, pp.1-4.
- [10]. B.Tian, T.Dillon, S.Hand “A Key Management Scheme for Heterogeneous Sensor Network Using Keyed-Hash Chain” the 5th International Conference on Mobile Ad-hoc and Sensor Network, December 16, 2009, pp. 448-456.
- [11]. S.Banihashemian, A.G.Bafghai, “A New Key Management Scheme in Heterogeneous Wireless Sensor Network”, the 12th International Conference on Advance Computation Technology, Feb 2010, pp.141-146.
- [12]. M.Li, J.Yin, J.Long, Younganwu and J. Cheng, “An Efficient Key Management Based on Dynamic Generation of Polynomials for Heterogeneous Sensor Networks”, the 2nd International Conference on Computer Engineering and Technology (ICCET), April, 2010, pp. V5-460-V5-464.
- [13]. D.Aranha, L.Oliveira, J.López, R.Dahab, “Implementing Cryptographic Pairings on an 8-bit Platform”, the Journal Wireless Sensor Network, Vol. 4913, November 2009, pp.305-320.
- [14]. A.Liu, P.Ning, “TinyECC, a configurable library for elliptic curve cryptography in wireless sensor networks”, the 3rd International Conference on Information

References

- Processing in Sensor Networks (IPSN'08), IEEE Computer Society, Washington, DC, USA, 2008.
- [15]. C.Kuo, M.Luk, R.Negi, A.Perrig, "Message-in-a-Bottle, User-friendly and Secure Key Deployment for Sensor Nodes", in Proceedings of the 5th International Conference on Embedded Networked Sensor Systems, 2007, pp 233-246.
- [16]. Gura, N.Eberle, H.Gupta, V.Shantz, "Energy Analysis of Public-Key Cryptography for Wireless Sensor Networks", the 3rd IEEE International Conference on Pervasive Computing and Communications, 2005, pp. 324 – 328.
- [17]. C.Krlof, N.Sastry, D.Wagner, "A link Layer Security Architecture Wireless Sensor Network", in Proceeding of 2nd International Conference on Embedded Networked sensor system, 2004, pp. 162-175.
- [18]. Crossbow Technology Inc. [Online]. <http://www.xbow.com>
- [19]. W.Du, J.Deng, Y.S.Han, P.K.Varshney, "A Pair-wise Key Pre-distribution Scheme for Wireless Sensor Networks," in proceedings of the 10th ACM Conference on Computer and Communications Security (CCS 2003), Washington (DC), October 2003, pp. 42-51.
- [20]. A.Alemdar, M.Ibnkahla, "Wireless Sensor Networks, Applications and Challenges", in Proceedings of the 9th International Symposium on Signal

References

- Processing and Its Applications (ISSPA 2007), IEEE Computer Society, Washington, DC, USA, 2007, pp. 1–6.
- [21]. T.Arampatzis, J.Lygeros, S.Manesis, “A Survey of Applications of Wireless Sensors and Wireless Sensor Networks, in Proceedings of the 2005 IEEE International Symposium on Intelligent Control – Mediterranean Conference on Control and Automation, IEEE Computer Society, Washington, DC, USA, 2005, pp. 719–724.
- [22]. R.Blom, “An Optimal Class of Symmetric Key Generation Systems”, in Proceedings of the EUROCRYPT 84 Workshop on Advances in Cryptology. Theory and Application of Cryptographic Techniques, Springer, New York, NY, , pp. 335–338, 1985.
- [23]. D.Carman, P.Kruus, B.Matt, “Constraints and Approaches for Distributed Sensor Network Security”, Technical Report 00-010, NAI Labs, September 2000.
- [24]. S.Çamtepe, B.Yener, “Key Distribution Mechanisms for Wireless Sensor Networks”, A survey (tr-05-07), Technical report, Rensselaer Polytechnic Institute, 2005.
- [25]. P.S.Zzechowiak, A.Kargl, M.Scott and M.Collier, “On the Application of Pairing Based Cryptography to Wireless Sensor Networks”, in proceedings of the Second

References

- ACM Conference on Wireless Network Security (WiSec'09), ACM, New York, NY, USA, 2009, pp. 1–12.
- [26]. C.Kuo, M.Luk, R.Negi, A.Perrig, “Message-in-a-bottle: User Friendly and Secure Key Deployment for Sensor Nodes”, in proceedings of the 5th International Conference on Embedded Networked Sensor Systems (SenSys'07), ACM, New York, NY, USA, 2007, pp. 233–246.
- [27]. W.Su, S.Bramaniam, Y.Cayirci, “A survey on sensor networks”, Communication Journals & Magazine, IEEE, Vol. 40, Issue 8, pp.102 – 114, Aug 2002.
- [28]. A.Liu, P.Ning, “A Configurable Library for Elliptic Curve Cryptography in Wireless Sensor Networks”, the 4th International Conference on Information Processing in Sensor Networks (IPSN'08), IEEE Computer Society, Washington, DC, USA, 2008, pp. 245–256.
- [29]. E.Biagioni, K.Bridges, “The Application of Remote Sensor Technology to Assist the Recovery of Rare and Endangered Species”, the International Journal of High Performance Computing Applications, Vol. 16, pp 315-324, August 2002.

References

- [30]. Li, Bee, "Lightweight Authentication for Recovery in Wireless Sensor Networks", 2009, the 5th International Conference on Mobile Ad-hoc and Sensor Networks, December 16, 2009, pp.465-471.
- [31]. L.Akyildiz, W.Su, Y.S.Brarnaniamn, E.Cayirci, "A Survey on Sensor Networks", IEEE Communications Magazine, August 2002, pp. 102-114.
- [32]. J.Hwan, C.Leandros, L.Tassiulas, "Maximum Lifetime Routing in Wireless Sensor Networks", the Journal IEEE/ACM Transactions on Networking (TON) archive Vol. 12, Issue 4, pp. 609-619, August 2004.

