Energy-efficient Secure Routing in Wireless Sensor Networks

A thesis submitted in partial fulfillment
of the requirements for the degree of

Master of Technology

in

Computer Science and Engineering

by

Shriram Sharma

Department of Computer Science and Engineering
National Institute of Technology Rourkela
Rourkela, Orissa, 769 008, India

May 2009

Energy-efficient Secure Routing in Wireless Sensor Networks

A thesis submitted in partial fulfillment
of the requirements for the degree of

Master of Technology

in

Computer Science and Engineering

by

Shriram Sharma

under the guidance of

Ashok Kumar Turuk

Department of Computer Science and Engineering
National Institute of Technology Rourkela
Rourkela-769 008, Orissa, India

May 2009

To my parents

&

Pandit Shambhu "DADA"

Pandit Yash Sharma

Department of Computer Science and Engineering
National Institute of Technology Rourkela
Rourkela-769 008, Orissa, India.

Certificate

This is to certify that the work in the thesis entitled ***Energy-efficient Secure Routing in Wireless Sensor Networks*** submitted by ***Mr.Shriram sharma*** in partial fulfillment of the requirements for the award of the degree of Master of Technology in Computer Science and Engineering during the session 2008–2009 in the department of Computer Science and Engineering, National Institute of Technology Rourkela is an authentic work carried out by him under my supervision and guidance.

To the best of my knowledge, the matter embodied in the thesis has not been submitted to any other University/Institute for the award of any Degree or Diploma.

Ashok Kumar Turuk
Asst. Professor
Dept. of Computer Science & Engineering
National Institute of Technology
Rourkela-769008 Orissa (India)

Place: NIT Rourkela
Date: 30 May 2009

Acknowledgment

My first thanks are to the Almighty God, without whose blessings I wouldn't have been writing this "acknowledgments".

I then would like to express my heartfelt thanks to my guide, Dr. Ashok Kumar Turuk for giving me the guidance, encouragement, counsel throughout my re-search and painstakingly reading my reports. Without his invaluable advice and assistance it would not have been possible for me to complete this thesis.

I would like to express my gratitude to Dr. Bibhudatta Sahoo, who was constant source of encouragement to me and helping me with his insightful comments on all stages of my work.

I also thank Prof. Banshidhar Majhi, Head of Computer Science and Engineering Department, Prof. Rameshwar Balihar Singh, Prof. S.K. Jena, Prof. Santanu Kumar Rath and Dr. Durga Prashad Mohapatra for serving on my Master of Technology Scrutiny Committee.

I wish to thank the Information Data base Laboratory staff and all the secretarial staff of the Computer Science and Engineering Department for their sympathetic cooperation.

I would like to thank our senior Mr. Puspendra Kumar Chandra, who was helping me on all stage of my work.

I thank my batch mates Aloka Datta, Om Prakash, Abhishek Pandey, Deepak .K, Kumar Dhiraj,Subhashish Dhal,Sunil Senapati and others who made my stay at NIT Rourkela is memorable one.

Finally, I would like to thank all of them whose names are not mentioned here but have helped me in any way to accomplish the work.

Shriram Sharma

Abstract

Wireless sensor networks can provide low cost solution to verity of real-world problems. Sensors are low cost tiny devices with limited storage, computational capability and power. They can be deployed in large scale for performing both military and civilian tasks. Security will be one of the main concerned when they will be deployed in large scale.

As sensors have limited power and computational capability, any security mechanism for sensor network must be energy efficient and should not be computational intensive.

In this thesis we propose an energy-efficient secure routing for wireless networks based on symmetric key cryptography. The proposed crypto system is session based and the session key is changed after the expire of each session. We divide the network into number of clusters and select a cluster head within each cluster. Communication between sensor and the sink takes place at the three level; sensor→ cluster-head → sink. Encryption of the sensed data is transmitted to the cluster head, which aggregated the data received from the sensor nodes of its cluster before forwarding to the next cluster head on the path or to the sink . Sensors do not participate in the routing scheme; their energy is conserved at each sensor node.

List of Acronyms

WSNs	: Wireless Sensor Networks
LEACH	: Low-Energy Adaptive Clustering Hierarchy
SPIN	: Secure Positioning for Sensor Networks
PEGA-SIS	: Power-Efficient Gathering in Sensor Information Systems
WSNSF	: Wireless Sensor Networks Security Framework
NS-2	: Network Simulator Version -2
MEMS	: Micro Electromechanical Systems
DSPs	: Digital Signal Processors
RF	: Radio Frequency
QOS	: Quality of Service
RAM	: Random Access Memory
EEPROM	: Electrically Erasable Programmable Read-Only Memory
MANETs	: Mo-bile Adhoc Networks
DSN	: Distributed Sensor Networks
SenIT	: Sensor Information Technology
DARPA	: Defense Advanced Research Project Agency
CH	: Cluster Head
TAG	: Tiny Aggregation Approach
SQL	: Database Query Language
BS	: Base Station
PDDD	: Pseudo-Distance Data Dissemination
POG	: Partial Ordered Graph
TOG	: Totally Ordered Graph
E-Span	: Energy-aware Spanning Tree Algorithm
MLDA	: Maximum Lifetime Data Aggregation
TPC	: Two-Phase Clustering
MAC	: Message Authentication Code
DES	: Data Encryption Standard
3DES	: Triple DES
RC6	: Rivest Cipher Version -6
AES	: Advanced Encryption Standard

LEAP	: Lightweight Extensible Authentication Protocol
PIKE	: Peer Intermediaries for Key Establishment in Sensor Networks
μ **TESLA**	: Micro version of the timed, Efficient, Streaming, Loss-tolerant Authentication
TRANS	: Trust Routing for Location Aware Sensor Networks
DoS	: Denial of Service
SSKS	: Secure symmetric-session based key scheme
ESDRA	: Energy-efficient Data Routing Algorithm
EECST	: Energy-efficient Cluster-head Selection Technique
SN	: Sensor Nodes
GN	: Gateway Nodes
WSGNs	: Wireless Sensor gateway Networks
ESDRP	: Energy-efficient Secure Data Routing Protocol
CBC	: Constant Bit Rate
ROM	: Read Only Memory
AMRP	: Average Minimum Reach-ability Power of sensors
MATLAB	: Matrix Laboratory
CPU	: Central Processing Unit
ASO	: Average number of Symmetric Operation
AODV	: Ad hoc On-Demand Distance Vector Routing
UDP	: User Datagram Protocol

Contents

Certificate **i**

Acknowledgement **ii**

Abstract **iii**

List of Figures **ix**

List of Tables **x**

1 Introduction **2**

1.1 Wireless Sensor Network 4

1.1.1 Sensor Network Challenges 5

1.1.2 System Architecture and Design Issues 6

1.1.3 Wireless Sensor Networks vs.Traditional Wireless Networks 11

1.1.4 Applications of Sensors 12

1.1.5 Clustering in WSN 13

1.2 Motivation of the Work 14

1.3 Objective of the Work 15

1.4 Thesis Organization 16

2 Secure Data Routing in WSN **18**

2.1 In-Network Aggregation 19

2.2 Grid-Based Data Aggregation 21

2.3 Tree-Based Approach 22

2.4 Cluster-Based Approach 26

2.5 Obstacles of Sensor Security 27

2.6 Security Requirements 28

2.7 Attacks on WSNs 30

2.8 Defensive Measures 31
2.8.1 Key Establishment 31
2.8.2 Defending Against Attacks on Routing Protocols 32
2.8.3 Defending Against DoS Attacks 33
2.8.4 A Wormhole Attack 33
2.8.5 Defending Against the Sybil Attack 34
2.8.6 Detecting Node Replication Attacks 34
2.8.7 Defending Against Attacks on Sensor Privacy 35
2.8.8 Secure Data Aggregation 35

3 Wireless Sensor Network Security Framework (WSNSF) Architecture 38

3.1 Systems Model 38
3.1.1 Function of Different Nodes 41
3.2 A Symmetric-Session based Key Scheme(SSKS) 42
3.2.1 Blowfish Algorithm 43
3.2.2 Secure Communication 44
3.2.3 Key Freshness 44
3.2.4 Integrity and Origination of the Data 44
3.3 Energy-efficient Secure Data Routing Protocol (EESDRP) 45
3.3.1 Security Algorithm 47
3.3.2 Data Routing in ESDRP 48
3.3.3 Data Redundancy Elimination Model 49
3.3.4 Energy Consumption Model 50
3.3.5 Single-hop Communication 51
3.4 An energy-efficient Cluster Head Selection - Technique (EECST) . . 52
3.4.1 Cluster Head Selection Algorithm 53
3.4.2 Energy -efficient Parameters of Cluster Algorithm 54
3.5 Error Detection Mechanism 55
3.6 Conclusion 55

4 Performance analysis of Wireless Sensor Network Secure Framework (WSNSF) 57

4.1 Simulation Platform 57

4.2 Performance Analysis of EESDR Security Protocol 59

4.3 Experimental Setup 59

4.3.1 Simulation Results 60

4.3.2 Computational and storage cost analysis of security protocol 62

4.4 Analysis of Energy efficiency of data routing protocol 65

4.4.1 Radio Communication Model 66

4.4.2 Cluster-head Election Phase 66

4.4.3 Data Transfer Phase 67

4.4.4 Start Energy for One Round 68

4.4.5 Simulation of Energy Model 68

5 Conclusion and Future Work 73

5.1 Future work 74

Bibliography 75

Dissemination of Work 80

List of Figures

2.1 In-network Architecture 20
2.2 Grid-base data aggregation Architecture 21
2.3 Tree-base data Routing Architecture 23
2.4 E-span protocol Architecture 25
2.5 Illustration of Two Phase Clustering 27
2.6 Data transmission using ESPDA 28

3.1 Three level WSNGs Architecture 39
3.2 Encrypted packet and session key transmission in WSNGs 42

4.1 Time consumption of encryption algorithms (base 64 encoding) . . 61
4.2 Time consumption of decryption algorithms (base 64 encoding) . . 62
4.3 Throughput of each encryption algorithm (Megabyte/Sec) 63
4.4 Throughput of each decryption algorithm (Megabyte/Sec) 64
4.5 Sensor node scenario with 8 sensor nodes, 2 gateway nodes and 1 sink node 70
4.6 Shows energy consumption during data communication with in a cluster 71
4.7 Residual energy of source as a function of time 71

List of Tables

1.1 Basic configuration of a simple sensor node 7

3.1 Prototype of generic-sensor nodes (Mica Mote) 39
3.2 Prototype of special-purpose sensor nodes (Spec 2003) 40
3.3 Prototype of high-bandwidth sensing nodes(RSC Wins-Hidra Nodes) 40
3.4 Notation uses in ESRA 48

4.1 Comparative execution times (in milliseconds) and throughput (Mb/sec) of encryption algorithms with different packet size 60
4.2 Comparative execution times (in milliseconds) and throughput (Mb/sec) of decryption algorithms with different packet size 60
4.3 Estimated success of brute force attacks 65
4.4 Memory space consumption (in bytes) 65
4.5 Ns2 commands for energy model 69
4.6 Ns2 Parameters for energy model 69

Chapter 1

Introduction

Wireless Sensor Network

Motivation of Work

Objective of Work

Thesis Organization

Chapter 1

Introduction

Wireless Sensor Networks have emerged as an important new area in wireless technology. In the near future, the wireless sensor networks are expected to consist of thousands of inexpensive nodes, each having sensing capability with limited computational and communication power [1] , [2] and [3] which enable us to deploy a large-scale sensor network.

A wireless network consisting of tiny devices which monitor physical or environmental conditions such as temperature, pressure, motion or pollutants etc. at different areas. Such sensor networks are expected to be widely deployed in a vast variety of environments for commercial, civil, and military applications such as surveillance, vehicle tracking, climate and habitat monitoring, intelligence, medical, and acoustic data gathering. The key limitations of wireless sensor networks are the storage, power and processing. These limitations and the specific architecture of sensor nodes call for energy efficient and secure communication protocols. The feasibility of these inexpensive sensor networks is accelerated by the advances in MEMS (Micro Electromechanical Systems) technology, combined with low power, low cost digital signal processors (DSPs) and radio frequency (RF) circuits [3], [4].They consists of a radio transceiver, microcontroller, power supply, and the actual sensor. The sensing circuitry measures ambient condition related to the environment surrounding the sensor and transforms them into an electric signal. Processing such a signal reveals some properties about objects located and/or events happening in the vicinity of the sensor. The sensor sends such collected data, usually via radio transmitter, to a command center (sink) either

directly or through a data concentration center (a gateway).

Normally sensor nodes are spatially distributed throughout the region which has to be monitored; they self-organize in to a network through wireless communication, and collaborate with each other to accomplish the common task.Basic features of sensor networks are self-organizing capabilities, dynamic network topology, limited power, node failures and mobility of nodes, short-range broadcast communication and multi-hop routing, and large scale of deployment [5]. The strength of wireless sensor network lies in their flexibility and scalability. The capability of self-organize and wireless communication made them to be deployed in an ad-hoc fashion in remote or hazardous location without the need of any existing infrastructure. Through multi-hop communication a sensor node can communicate a far away node in the network. This allows the addition of sensor nodes in the network to expand the monitored area and hence proves its scalability and flexibility property.

The key challenge in sensor networks is to maximize the lifetime of sensor nodes due to the fact that it is not feasible to replace the batteries of thousands of sensor nodes. Therefore, computational operations of nodes and communication protocols must be made as energy efficient as possible. Among these protocols data transmission protocols have much more importance in terms of energy, Since the energy required for data transmission takes 70 % of the total energy consumption of a wireless sensor network [2]. Area coverage and data aggregation [6] techniques can greatly help conserve the scarce energy resources by eliminating data redundancy and minimizing the number of data transmissions. Therefore, data aggregation methods in sensor networks are extensively investigated in the literature [6], [7], [8] and [9].

Security in data communication is another important issue to be considered while designing wireless sensor networks, as wireless sensor networks may be deployed in hostile areas such as battlefields [2], [10] and [11]. Therefore, data aggregation protocols should work with the data communication security protocols, as any conflict between these protocols might create loopholes in network security.

Presently there are different types of commercially available sensor nodes. University of California at Berkeley has developed Mica mote which is a special purpose sensor node. Other special purpose sensor nodes available are Spec, Rene, Mica 2, Telos etc. Some high bandwidth sensor nodes available are BTNode, Imote 1.0, Stargate, Inryonc Cerfeube etc. [12].

1.1 Wireless Sensor Network

Wireless sensor networks are potentially one of the most important technologies of this century. Recent advancement in wireless communications and electronics has enabled the development of low-cost, low-power, multifunctional miniature devices for use in remote sensing applications. The combination of these factors has improved the viability of utilizing a sensor network consisting of a large number of intelligent sensors, enabling the collection, processing analysis and dissemination of valuable information gathered in a variety of environments. A sensor network is composed of a large number of sensor nodes which consist of sensing, data processing and communication capabilities.

Sensor network protocols and algorithms must possess self-organizing capabilities. Another unique feature of sensor networks is the cooperative effort of sensor nodes. Sensor nodes are suitable with an onboard processor. Instead of sending the raw data to the nodes responsible for the fusion, they use their processing abilities to locally carry out simple computations and transmit only the required and partially processed data.

Sensor networks are predominantly data-centric rather than address-centric.so sensed data are directed to an area containing a cluster of sensors rather than particular sensor addresses. Given the similarity in the data obtained by sensors in a dense cluster, aggregation of the data is performed locally. That is, a summary or analysis of the local data is prepared by an aggregator node within the cluster, thus reducing the communication bandwidth requirements. Aggregation of data increases the level of accuracy and reduces data redundancy. A network hierarchy and clustering of sensor nodes allows for network scalability, robustness, efficient

resource utilization and lower power consumption.

The fundamental objectives for sensor networks are reliability, accuracy, flexibility, cost effectiveness and ease of deployment.

1.1.1 Sensor Network Challenges

Wireless sensor network uses a wide variety of application and to impact these applications in real world environments, we need more efficient protocols and algorithms. Designing a new protocol or algorithm address some challenges which are need to be clearly understood [3]. These challenges are summarized below:

- **Physical Resource Constraints:** The most important constraint imposed on sensor network is the limited battery power of sensor nodes. The effective lifetime of a sensor node is directly determined by its power supply. Hence lifetime of a sensor network is also determined by the power supply. Hence the energy consumption is main design issue of a protocol. Limited computational power and memory size is another constraint that affects the amount of data that can be stored in individual sensor nodes. So the protocol should be simple and light-weighted. Communication delay in sensor network can be high due to limited communication channel shared by all nodes within each other's transmission range.

- **Ad-hoc Deployment:** Many applications are requires the ad-hoc deployment of sensor nodes in the specific area. Sensor nodes are randomly deployed over the region without any infrastructure and prior knowledge of topology. In such a situation, it is up to the nodes to identify its connectivity and distribution between the nodes. As an example, for event detection in a battle field the nodes typically would be dropped in to the enemy area from a plane.

- **Fault-Tolerance:** In a hostile environment, a sensor node may fail due to physical damage or lack of energy (power). If some nodes fail, the protocols that are working upon must accommodate these changes in the network.

As an example, for routing or aggregation protocol, they must find suitable paths or aggregation point in case of these kinds of failures.

- **Scalability:** Most of the applications are needed; the number of sensor nodes deployed must be in order of hundreds, thousands or more. The protocols must scalable enough to respond and operate with such large number of sensor nodes.

- **Quality of Service:** Some real time sensor application are very time critical which means the data should be delivered within a certain period of time from the moment it is sensed, otherwise the data will be unusable .So this must be a QOS parameter for some applications.

- **Unattended operation:** In many application sensor networks is deployed once, and after deployment have no human intervention. Hence the nodes themselves are responsible for reconfiguration in case of any changes.

- **Untethered:** The sensor nodes are not connected to any energy source. They have only a finite source of energy, which must be optimally used for processing and communication. To make optimal use of energy, communication should be minimized as much as possible.

- **Security:** Security is very critical parameter in sensor networks, given some of the proposed applications. An effective compromise must be obtained, between the low bandwidth requirements of sensor network applications and security demands for secure data communication in the sensor networks (which traditionally place considerable strain on resources)Thus, unlike traditional networks, where the focus is on maximizing channel throughput with secure transmission.

1.1.2 System Architecture and Design Issues

The performance of a secure routing protocol [12] is closely depended on the architectural model and design of the sensor networks, base on the application

CPU	8-bit, 4 MHz
Storage	8K Instruction flash 512 bytes RAM 512 bytes EEPROM
Communication	916 MHz radio
Bandwidth	10 Kilobits per second
Operating System	TinyOS
OS code space	3500 bytes
Available code space	4500 bytes

Table 1.1: Basic configuration of a simple sensor node

requirements different architectures and design goals/constraints have been considered for sensor networks. In this section we attempt to capture architectural issues and highlight their implications. Table 1.1 describe basic configuration of a simple sensor node, its depends on the application requirement.

- **Security Implementation:** Security is data communication is main concerning parameter for providing secure communication in sensor networks, whiled designing wireless networks, as wireless sensor networks may be deployed in hostile areas such as battlefields .therefore, design of protocol should work with the data communication security protocols, as any conflict between these protocols might create challenge in network security.

- **Energy Considerations:** Energy is very important parameter during the creation of an infrastructure, and the process of selecting the routes for transmission. Since the transmission power of a wireless radio is proportional to distance squared or even higher order in the presence of obstacles, multihop routing will consume less energy than direct communication. However, multihop routing introduces significant overhead for topology management and medium access control. Direct routing would perform well enough if all the nodes were very close to the sink.

- **Data Aggregation/Fusion:** In the sensor network, sensor nodes might generate redundant data; similar packets from multiple nodes can be aggregated so that the number of transmissions would be reduced. Data aggregation is the combination of data from different sources by using functions

such as suppression (eliminating duplicates), min, max and average. Some of these functions can be performed by the aggregator sensor node, by allowing sensor nodes to conduct in-network data reduction. Recognizing that computation would be less energy consuming than communication, substantial energy savings can be obtained through data aggregation.

- **Network Dynamics:** There are three basic components, sensor nodes, sink and user which is monitored the events in a sensor network. Most of the network architectures assume that sensor nodes are stationary. Some application are required the mobility of sinks or cluster-heads (gateways). Routing messages from or to moving nodes is more challenging since route stability becomes an important optimization factor, in addition to energy, bandwidth etc. The sensed event can be either dynamic or static depending on the application.

- **Node Deployment:** It is an important issue to deployment of sensor nodes in topological manner. This is application dependent and affects the performance of the routing protocol. The deployment is either deterministic or self-organizing.In deterministic situations, the sensors are manually placed or data is routed through pre-determined paths. However in self-organizing systems, the sensor nodes are scattered randomly creating an infrastructure in an ad hoc manner.

- **Data Delivery Models:** Base on the application requirements of the sensor network, the data delivery model to the sink can be continuous, event-driven, query-driven and hybrid. In the continuous delivery model, each sensor sends data periodically. In event-driven and query driven models, the transmission of data is triggered when an event occurs or a query is generated by the sink. Some networks apply a hybrid model using a combination of continuous, event- driven and query-driven data delivery.

- **Node Capabilities:** Depending on the sort of work a node can be dedicated to a particular special function such as relaying, sensing and aggre-

gation since engaging the three functionalities at the same time on a node might quickly drain the energy of that node. Inclusion of heterogeneous set of sensors raises multiple technical issues making data routing more challenging.

- **Security Implementation:** Security is data communication is main concerning parameter for providing secure communication in sensor networks, whiled designing wireless networks, as wireless sensor networks may be deployed in hostile areas such as battlefields .therefore, design of protocol should work with the data communication security protocols, as any conflict between these protocols might create challenge in network security.

- **Energy Considerations:** Energy is very important parameter during the creation of an infrastructure, and the process of selecting the routes for transmission. Since the transmission power of a wireless radio is proportional to distance squared or even higher order in the presence of obstacles, multihop routing will consume less energy than direct communication. However, multihop routing introduces significant overhead for topology management and medium access control. Direct routing would perform well enough if all the nodes were very close to the sink.

- **Data Aggregation/Fusion:** In the sensor network, sensor nodes might generate redundant data; similar packets from multiple nodes can be aggregated so that the number of transmissions would be reduced. Data aggregation is the combination of data from different sources by using functions such as suppression (eliminating duplicates), min, max and average. Some of these functions can be performed by the aggregator sensor node, by allowing sensor nodes to conduct in-network data reduction. Recognizing that computation would be less energy consuming than communication, substantial energy savings can be obtained through data aggregation.

- **Network Dynamics:** There are three basic components, sensor nodes, sink and user which is monitored the events in a sensor network. Most of

the network architectures assume that sensor nodes are stationary. Some application are required the mobility of sinks or cluster-heads (gateways). Routing messages from or to moving nodes is more challenging since route stability becomes an important optimization factor, in addition to energy, bandwidth etc. The sensed event can be either dynamic or static depending on the application.

- **Node Deployment:** It is an important issue to deployment of sensor nodes in topological manner. This is application dependent and affects the performance of the routing protocol. The deployment is either deterministic or self-organizing.In deterministic situations, the sensors are manually placed or data is routed through pre-determined paths. However in self-organizing systems, the sensor nodes are scattered randomly creating an infrastructure in an ad hoc manner.

- **Data Delivery Models:** Base on the application requirements of the sensor network, the data delivery model to the sink can be continuous, event-driven, query-driven and hybrid. In the continuous delivery model, each sensor sends data periodically. In event-driven and query driven models, the transmission of data is triggered when an event occurs or a query is generated by the sink. Some networks apply a hybrid model using a combination of continuous, event- driven and query-driven data delivery.

- **Node Capabilities:** Depending on the sort of work a node can be dedicated to a particular special function such as relaying, sensing and aggregation since engaging the three functionalities at the same time on a node might quickly drain the energy of that node. Inclusion of heterogeneous set of sensors raises multiple technical issues making data routing more challenging.

1.1.3 Wireless Sensor Networks vs.Traditional Wireless Networks

There are many existing protocol, techniques and concepts from traditional wireless network, such as cellular network, mobile ad-hoc network, wireless local area network and Bluetooth, are applicable and still used in wireless sensor network, but there are also many fundamental differences which lead to the need of new protocols and techniques [13]. Some of the most important characteristic differences are summarized below:

There are many existing protocol, techniques and concepts from traditional wireless network, such as cellular network, mobile ad-hoc network, wireless local area network and Bluetooth, are applicable and still used in wireless sensor network, but there are also many fundamental differences which lead to the need of new protocols and techniques. Some of the most important characteristic differences are summarized below:

- Number of nodes in wireless sensor network is much higher than any traditional wireless network. Possibly a sensor network has to scale number of nodes to thousands. Moreover a sensor network might need to extend the monitored area and has to increase number of nodes from time to time. This needs a highly scalable solution to ensure sensor network operations without any problem.

- Due to large number of sensor nodes, addresses are not assigned to the sensor nodes. Sensor networks are not address-centric; instead they are data-centric network. Operations in sensor networks are centered on data instead of individual sensor node. As a result sensor nodes require collaborative efforts.

- Sensor nodes mainly use a broadcast communication paradigm, whereas most ad hoc networks are on point-to-point communications.

- Sensor nodes are much cheaper than nodes in ad hoc networks.

- Wireless sensor networks are environment-driven. While data is generated by humans in traditional networks, the sensor network generate data when environment changes. As a result the traffic pattern changes dramatically from time to time. Sensor networks are mainly used to collect information while MANETs (Mo-bile Adhoc Networks) are designed for distributed computing rather than information gathering.

- A unique characteristic of wireless sensor network is the correlated data problem. Data collected by neighboring sensor nodes are often quite similar which makes possible to the development of routing and aggregation techniques that can reduce redundancy and improve energy efficiency. It also been observed that the environmental quantities changes very slow and some consecutive readings sense temporally correlated data. This advantageous feature can be exploited to develop an energy efficient data gathering and aggregation techniques.

  Thus, unlike traditional networks, where the focus is on maximizing channel throughput or minimizing node deployment, the major consideration in a sensor network is to extend the system lifetime as well as the system security.

1.1.4 Applications of Sensors

- **Military Applications :** Sensor networks are applied very successfully in the military sensing. [4] Now wireless sensor networks can be an integral part of military command, control, communications, computing, intelligence, surveillance, reconnaissance and targeting systems. There are two example important programs the Distributed Sensor Networks (DSN) and the Sensor Information Technology (SenIT) form the Defense Advanced Research Project Agency (DARPA) [14], are applied very successfully in the military sensing.

- **Environmental Monitoring :** Nowadays sensor networks are also widely applied in habitat monitoring, agriculture research, fire detection [3].

- **Medical Application :** Sensor networks are also widely used in health care area. In some modern hospital sensor networks are constructed to monitor patient physiological data, to control the drug administration track and monitor patients and doctors and inside a hospital.

- **Home Application :** Many concepts are already designed by researcher and architects, like "Smart Environment: Residential Laboratory" [10] and "Smart Kindergarten" [11] some are even realized.

- **Traffic Monitoring :** The sensor node has a built-in magneto-resistive sensor that measures changes in the Earth's magnetic field caused by the presence or passage of a vehicle in the proximity of the node. A low-power radio relays the detection data to the AP at user-selectable periodic reporting intervals or on an event driven basis. By placing two nodes a few feet apart in the direction of traffic, accurate individual vehicle speeds can be measured and reported.

- **Robotics Control :** Robotics has matured as a system integration engineering field defined as "the intelligent connection of the perception to action". Programmable robot manipulators provide the "action" component. A variety of sensors and sensing techniques are available to provide the "perception".

- **Habitat Monitoring :**The intimate connection with its immediate physical environment allows each sensor to provide localized measurements and detailed information that is hard to obtain through traditional instrumentation.

1.1.5 Clustering in WSN

It is widely accepted that the energy consumed in one bit of data transfer can be used to perform a large number of arithmetic operations in the sensor processor [12]. Moreover in a densely deployed sensor network the physical environment would produce very similar data in near-by sensor nodes and transmitting such

data is more or less redundant. Therefore, all these facts encourage using some kind of grouping of nodes such that data from sensor nodes of a group can be combined or compressed together in an intelligent way and transmit only compact data. This can not only reduce the global data to be transmitted and localized most traffic to within each individual group, but reduces the traffic and hence contention in a wireless sensor network. This process of grouping of sensor nodes in a densely deployed large-scale sensor network is known as clustering. The intelligent way to combined and compress the data belonging to a single cluster is known as data aggregation [15].

There are some issues involved with the process of clustering in a wireless sensor network. First issue is, how many clusters should be formed that could optimize some performance parameter. Second could be how many nodes should be taken in to a single cluster. Third important issue is the selection procedure of cluster-head in a cluster. Another issue that has been focused in many research papers is to introduce heterogeneity in the network. It means that user can put some more powerful nodes, in terms of energy, in the network which can act as a cluster-head and other simple node work as cluster-member only. Considering the above issues, many protocols have been proposed which deals with each individual issue.

1.2 Motivation of the Work

Wireless Sensor Networks represent a new generation of real-time embedded systems with significantly different communication constraints. As these devices are deployed in large numbers, they will need the ability to assist each other to communicate data back to a centralized collection point. The integration of the sensor, coupled with unceasing electronic miniaturization, will make it possible to produce extremely inexpensive sensing device. Sensor nodes are tiny devices which are composed of a sensing unit, a radio, a processor and a limited battery power. These devices will be able to monitor a wide variety of ambient condition: Temperature, pressure, humidity, soil makeup, vehicular movement, noise levels, lighting

conditions, so on.

In wireless sensor network, there are so many challenges. The main challenges are how to provide maximum lifetime to network and how to provide secure communication to network. As sensor network totally rely on battery power, the main aim for maximizing lifetime of network is to conserve battery power or energy with some security considerations.

In sensor network, the energy is mainly consumed for three purposes: data transmission, signal processing, and hardware operation. It is said in [4]that 70 percent of energy consumption is due to data transmission. So for maximizing the network lifetime, the process of data transmission should be optimized. The data transmission can be optimized by using efficient routing protocols and effective ways of data aggregation.

Routing protocols providing an optimal data transmission route from sensor nodes to sink to save energy of nodes in the network. Data aggregation plays an important role in energy conservation of sensor network. Data aggregation methods are used not only for finding an optimal path from source to destination but also to eliminate the redundancy of data, since transmitting huge volume of raw data is an energy intensive operation, and thus minimizing the number of data transmission. Also multiple sensors may sense the same phenomenon, although from different view and if this data can be reconciled into a more meaningful form as it passes through the network, it becomes more useful to an application. Moreover when data aggregation is performing data is compress as it is passed through the network, thus occupying less bandwidth. This also reduces the amount of transmission power expended by nodes. Hence secure data aggregation can be considered as a very challenging problem in wireless sensor network.

1.3 Objective of the Work

Propose a Framework to establish seure energy-efficient data routing from source to sink. So that data can be transmit as a secure manner and consuming lesser energy. This concept provides secure data communication and increases the lifetime

of the sensor network as a whole.

Data routing protocols aims at eliminating redundant data transmission and thus improve the lifetime of energy constrained wireless sensor network. In wireless sensor network, data transmission took place in multi-hop fashion where each node forwards its data to the neighbor node which is nearer to sink. That neighbor node performs aggregation function and again forwards it on. But performing data forwarding and aggregation in this fashion from various sources to sink causes significant energy waste as each node in the network is involved in operation.so above approach cannot be considered as energy efficient. An improvement over the above approach would be clustering where each node sends data to cluster-head (CH) and then cluster-head perform routing on the received raw data and then send it to sink. In case of homogeneous sensor network cluster-head will soon die out and again re-clustering has to be done which again cause energy consumption.

We proposed a secure energy-efficient algorithm that performs secure data routing using clustering and a cryptographic algorithm, with resource rich static cluster head. Consequently reducing the communication over head by routing at cluster-head and also reduce load of the re-clustering to provide energy efficiency for maximizing network lifetime.

1.4 Thesis Organization

The thesis is organized in the following way: **Chapter 1** starts with a brief introduction of sensor network, system architecture and design issues, difference between sensor network vs traditional networks, challenges of sensor network, clustering in WSN and application of sensors followed by the motivation of this work. In **Chapter 2**, gives a detailed overview of data routing. This chapter also presents the literature survey that is related to the work. **Chapter 3** introduces and describes the new proposed protocol for data routing in cluster-based wireless sensor networks. **Chapter 4** will present the performance analysis of the proposed protocol. It will also provide the comparison results.Finally, Conclusion is given in the **Chapter 5** and scope of future enhancements is also incorporated.

Chapter 2

Secure Data Routing in WSN

In-Network Aggregation

Grid-Based Data Aggregation

Tree-Based Approach

Cluster-Based Approach

Obstacles of Sensor Security

Security Requirements

Attacks on WSNs

Defensive Measures

Chapter 2

Secure Data Routing in WSN

Advancement in sensor technology has led to the production of wireless sensors to capable of sensing and reporting of various real-word phenomena in a time sensitive manner. However these systems suffer from bandwidth, energy and throughput constraints which bound the amount of information transmission from end-to-end. Data routing is known technique considered to alleviate these problems but there is some limitation due to lack of adaption to dynamic network topologies and unpredictable traffic patterns.

The main constrains of WSNs are the power, storage and processing these limitation and the specific architecture of sensors nodes call for energy efficient and secure communication protocols. The key challenge in WSNs is to maximize the lifetime of sensor nodes because of, practically it is not possible to replace the batteries of large number of deployed sensor in the environment.

Wireless sensor networks consist of sensor nodes with sensing and communication capabilities. We focus on data-routing problems in energy constrained sensor networks. The main goal of data-routing algorithms is to gather and aggregate data in an energy efficient manner so that network lifetime is enhanced. in our framework we have also consider some security issues to establish secured data routing in wireless sensor networks with negligible over head. Data routing techniques can significantly help to conserve the limited energy resource by eliminating data redundancy and minimizing the number of data transmission .for that reason, data routing techniques in WSNs are broadly investigated in the literature. In this chapter we present a survey of data-routing algorithms and some security

related parameters in wireless sensor networks.

2.1 In-Network Aggregation

In-network aggregation deals with this distributed processing of data within the network. In this scheme,the sensor networks is divided into pre-defined set of regions .each region is responsible for sensing and reporting events that occurs inside the region to the sink node .In a typical sensor network scenario, different node collect data from the environment and then send it to some central node or sink which analyze and process the data and then send it to the application. But in-Network data aggregation s, data produced by different node can be jointly processed while being forwarded to the sink node. Elena Fosolo et al in [8] defines the in-network aggregation process as follows: "In-network aggregation is the global process of gathering and routing information through a multi-hop network, processing data at intermediate nodes with the objective of reducing resource consumption (in particular energy), thereby increasing network lifetime." In in-network aggregation, the sensor with the most critical information aggregates the data packets and sends the fused data to the sink. Each sensor transmits its signal strength to its neighbors. If the neighbor has higher signal strength, the sender stops transmitting packets. After receiving packets from all the neighbors, the node that has the highest signal strength becomes the data aggregator. The in-network aggregation scheme is best suited for environments where events are highly localized.

There are two approaches for in-network aggregation: with size reduction and without size reduction. In-network aggregation with size reduction refers to the process of combining and compressing the data packets received by a node from its neighbors in order to reduce the packet length to be transmitted or forwarded towards sink. As an example, consider the situation when a node receives two packets which have a spatial correlated data. In this case it is worthless to send both packets. Instead of that one should apply any function like AVG, MAX, and MIN and then send a single packet. This approach considerably reduces the

amount of bits transmitted in the network and thus saving a lot of energy but on the other hand, it also reduces the precision of value of data received. In-network aggregation without size reduction refers to the process merging data packets received from different neighbors in to a single data packet but without processing the value of data. As an example, two packets may contain different physical quantities (like temperature and humidity) and they can be merged in to a single packet by keeping both values intact but keeping a single header. This approach preserves the value of data and thus transmit more bits in the network but still reduce the overhead by keeping single header.

This of the two approaches to use depends on many factors like the type of application, data rate, network characteristics and so on. There is also a trade-off between energy consumption and precision of data for the two approaches. Figure 2.1 . An in-network data aggregation scheme ,the numbers indicate the signal

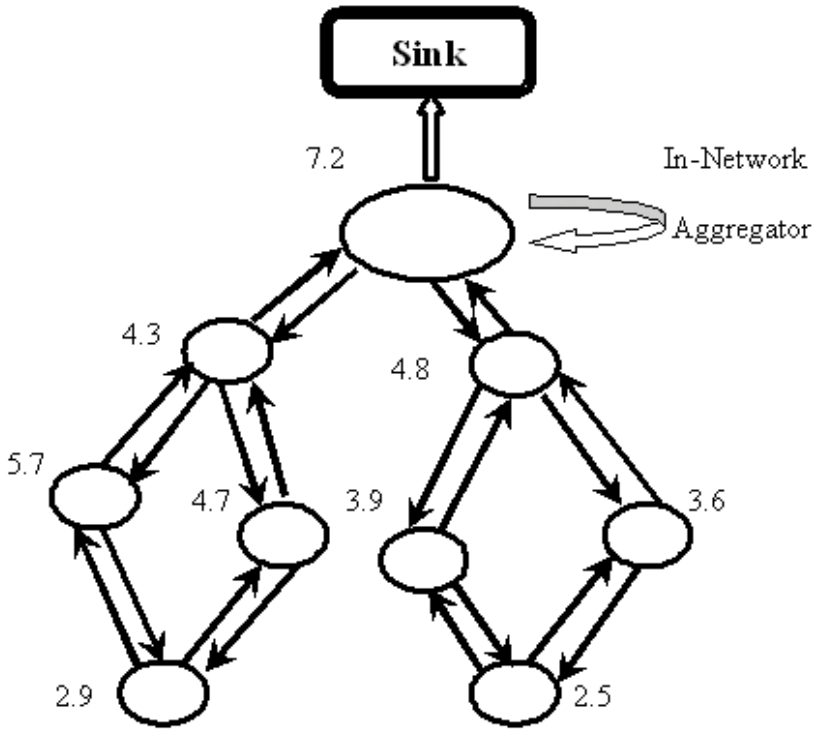

Figure 2.1: In-network Architecture

strengths detected by the sensors. The arrows indicate the exchange of signal strengths between neighboring nodes.

2.2 Grid-Based Data Aggregation

Vaidhyanathan et al. [14] have proposed grid base data-aggregation schemes which are based on dividing the region monitored by a sensor network into several grids. In grid-based data aggregation, a set of sensors is assigned as data aggregators in fixed regions of the sensor network. The sensors in a particular grid transmit the data directly to the data aggregator of that grid. Hence, the sensors within a grid do not communicate with each other.

In grid-based data aggregation, the data aggregator is fixed in each grid and it aggregates the data from all the sensors within the grid. This is similar to cluster-based data aggregation in which the cluster heads are fixed. Grid based data aggregation is suitable for mobile environments such as military surveillance and weather forecasting and adapts to dynamic changes in the network and event mobility. Figure 2.2 An grid base data aggregation scheme.

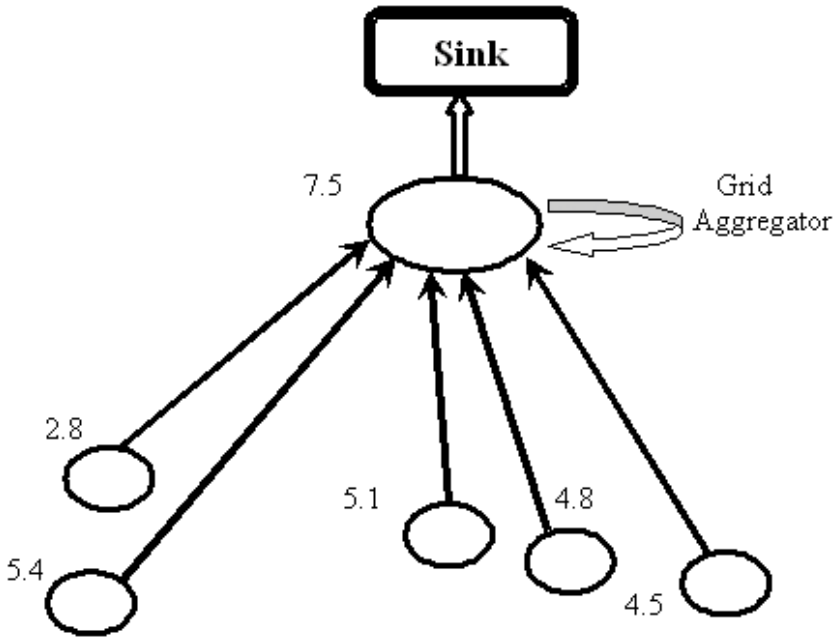

Figure 2.2: Grid-base data aggregation Architecture

The arrows indicate the transmission of data from sensors to the grid aggre-

gator.

A typical Grid-base data aggregation scheme is Fig2.2 shows that in grid-based data aggregation, all sensors directly transmit data to a predetermined grid aggregator. After collecting all data from other sensors, then aggregator sends only the critical information to the sink nodes. Thus grid-base scheme reduce the traffic in mobile environment and make sure the critical is transmitted to the sink. However grid-base scheme not perform well where events are highly localized and mostly immobile in nature.

2.3 Tree-Based Approach

The simplest way to routing data is to organize the nodes in a hierarchical manner and then select some nodes as the aggregation point or aggregators. The tree-based approach perform aggregation by constructing an aggregation tree [16], which could be a minimum spanning tree, rooted at sink and source nodes are considered as leaves. Each node has a parent node to forward its data. Flow of data starts from leaves nodes up to the sink and therein the aggregation done by parent nodes. The way this approach operates has some drawbacks. As we know like any wireless network the wireless sensor networks are also not free from failures. In case of packet loss at any level of tree, the data will be lost not only for a single level but for whole related sub-tree as well. In spite of high cost for maintaining tree structure in dynamic networks and scarce robustness of the system, this approach is very much suitable for designing optimal aggregation technique and energy-efficient techniques.

S. Madden et al. in [17] proposed a data-centric protocol which is based on aggregation tress, known as Tiny Aggregation (TAG) approach [17]. TAG works in two phases: distribution phase and collection phase. In distribution phase, TAG organizes nodes in to a routing tree rooted at sink. The tree formation starts with broadcasting a message from sink specify level or distance from root. When a node receive this message it sets its own level to be the level of message plus one and elect parent as node from which it receives the message. After that, node rebroadcast

this message with its own level. This process continues until all nodes elect their parent. After tree formation, sink send queries along structure to all nodes in the network. TAG uses database query language (SQL) for selection and aggregation functions. In collection phase, data is forwarded and aggregated from leaves nodes to root. A parent node has to wait for data from all its child node before it can send its aggregate up the tree. Apart from the simple aggregation function provided by SQL (eg: COUNT, MIN, MAX, SUM, and AVG), TAG also partitions aggregates according to the duplicate sensitivity, exemplary and summary, and monotonic properties. Though TAG periodically refresh tree structure of network but as most of the tree-based schemes are inefficient for dynamic network, so TAG may be.

C. Intanagonwiwat et al. in [3] proposed a reactive data-centric protocol for applications where sink ask some specific information by flooding, known as directed diffusion paradigm. The main idea behind directed diffusion paradigm is to combine data coming from different source and en-route them by eliminating redundancy, minimizing the number of data transmission; thus maximizing network lifetime. Directed diffusion consists of several elements: interests, data messages, gradients, and reinforcements. Figure 2.3 An tree-base data routing scheme.

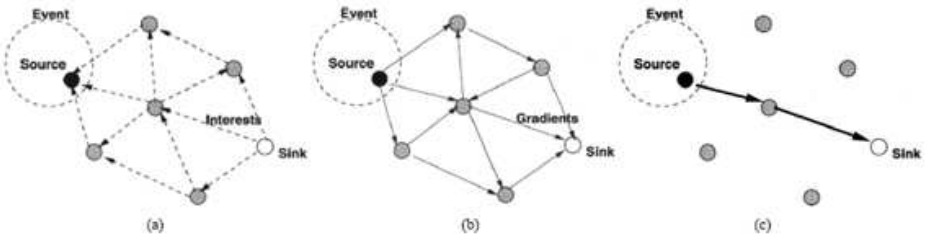

Figure 2.3: Tree-base data Routing Architecture

Figure 2.3 Simplified schematic for directed diffusion. (a) Interest propagation. (b) Initial gradients setup. (c) Data delivery along reinforced path [3].

The base station (BS) requests data by broadcasting an interest message which contains a description of a sensing task. This interest message propagates through the network hop-by-hop and each node also broadcast interest message to its neighbor. As interest message propagates throughout the network, gradients are setup by every node within the network. The gradient direction is set toward the neighboring node from which the interest is received. This process continues until gradients are setup from source node to base station. Loops are not checked at this stage but removed at later stage. After this path of information flow are formed and then best path are reinforced to prevent further flooding according to a local rule. Data aggregation took place on the way of different paths from different sources to base station or sink. The base station periodically refresh and resend the interest message as soon as it start to receives data from sources to provide reliability. The problem with directed diffusion is that it may not be applied to applications (e.g. environmental monitoring) that require continuous data delivery to base station. This is because query driven on demand data model may not help in this regard. Also matching data to queries might require some extra overhead at the sensor nodes. Mobility of sink nodes can also degrade the performance as path from sources to sinks cannot be updated until next interest message is flooded throughout the network. To cope up with above issue if introduce frequent flooding then also too much overhead of bandwidth and battery power will be introduced. Furthermore, exploratory data follow all possible paths in the network following gradients which lead to unnecessary communications overhead.

M. Lee et al. in [2] proposed a new low-control-overhead data dissemination scheme, which they called as pseudo-distance data dissemination (PDDD), for efficiently disseminating data from all sensor nodes to mobile sink. Some assumption have been made, they are: (1) all source nodes maintain routes to mobile sink node, (2) no periodically messaging for topological changes due to mobile sink node, (3) all link are bi-directional and no control messages are lost, (4) mobile sink nodes have unlimited battery power, so no need to care about battery efficiency of sink node, and (5) network partitioning is not considered. Data dissemination process

is influenced by directed diffusion [3]. Though mobile sink periodically broadcast interest message, sensor nodes do not send exploratory data and do not wait reinforcement message because each sensor node already has routes to the sink node. After getting interest message, adjacent nodes set a parent-child relationship using pseudo-distance of each node and finally a partial ordered graph (POG) has been build. Optimal data dissemination is achieved in terms of path length by forwarding packets to a parent node until topology is unchanged. Then each sensor node is assigned a level for a corresponding sink node with pseudo-distance. In order to overcome the shortcoming of POG, author used totally ordered graph (TOG) in place of POG. The problem identified in this approach is that due to mobility of sink node all sensor nodes have to maintain routes and for any change in topology nodes have to again change route accordingly which led to energy waste.

Marc Lee et al. in proposed an energy-aware spanning tree algorithm for data aggregation, referred as E-Span. E-Span is a distributed protocol in which source node that has highest residual energy is chosen as root. Other source nodes choose their parent based on residual energy and distance to the root. The protocol uses configuration message to exchange information of node i.e., residual energy and distance to the root.Each node performs single-hop broadcast operation to send packets. Single-hop broadcast refers to the operation of sending a packet to all single-hop neighbors [9].

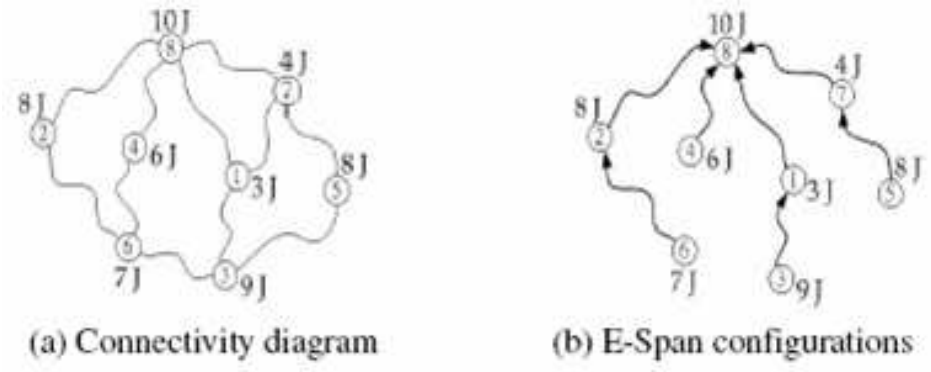

Figure 2.4: E-span protocol Architecture

2.4 Cluster-Based Approach

We talked about hierarchical organization of the network in tree-based approach. Another scheme to organize the network in hierarchical manner is cluster-based approach. In cluster-based approach, whole network is divided in to several clusters. Each cluster has a cluster-head which is selected among cluster members. Cluster-heads do the role of aggregator which aggregate data received from cluster members locally and then transmit the result to sink. The advantages and disadvantages of the cluster-based approaches is very much similar to tree-based approaches.

K. Dasgupta et al. in [14] proposed a maximum lifetime data aggregation (MLDA) algorithm which finds data gathering schedule provided location of sensors and base-station, data packet size, and energy of each sensor. A data gathering schedule specifies how data packet are collected from sensors and transmitted to base station for each round. A schedule can be thought of as a collection of aggregation trees. In , they proposed heuristic-greedy clustering-based MLDA based on MLDA algorithm. In this they partitioned the network in to cluster and referred each cluster as super-sensor. They then compute maximum lifetime schedule for the super-sensors and then use this schedule to construct aggregation trees for the sensors.

W. Choi et al. in present a two-phase clustering (TPC) scheme [15]. Phase I of this scheme creates clusters with a cluster-head and each node within that cluster form a direct link with cluster-head. Phase I of this scheme is similar to various scheme used for clustering but differ in one way that the cluster-head rotation is localized and is done based on the remaining energy level of the sensor nodes which minimize time variance of sensors and this lead to energy saving from unnecessary cluster-head rotation. In phase II, each node within the cluster searches for a neighbor closer than cluster-head which is called data relay point and setup up a data relay link. Now the sensor nodes within a cluster either use direct link or data relay link to send their data to cluster head which is an energy efficient scheme. The data relay point aggregates data at forwarding time to another data

relay point or cluster-head. In case of high network density, TPC phase II will setup unnecessary data relay link between neighbors as closely deployed sensor will sense same data and this lead to a waste of energy.

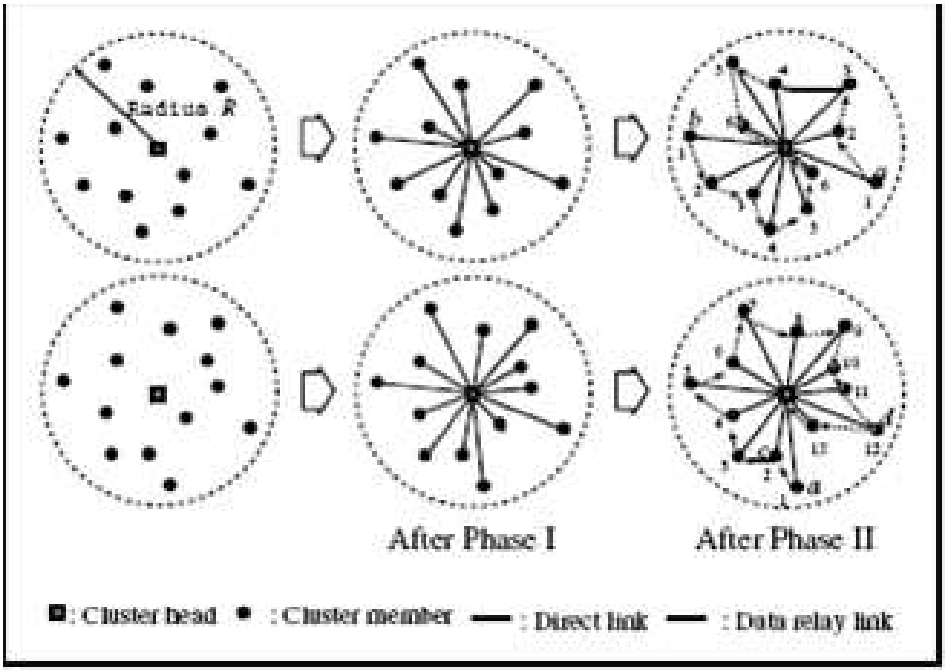

Figure 2.5: Illustration of Two Phase Clustering

H. Cam et al. in [11] present energy efficient and secure pattern based data aggregation protocol which is designed for clustered environment. In conventional method data is aggregated at cluster-head and cluster-head eliminate redundancy by checking the content of data. This protocol says that instead of sending raw data to cluster-head, the cluster members send corresponding pattern codes to cluster-head for data aggregation. If multiple nodes send the same pattern code then only one of them is finally selected for sending actual data to cluster-head. For pattern matching, authors present a pattern comparison algorithm.

2.5 Obstacles of Sensor Security

- **Limited Resources**
  - **Limited Memory and Storage Space:** A sensor is a tiny device with only a small amount of memory and storage space for the code.

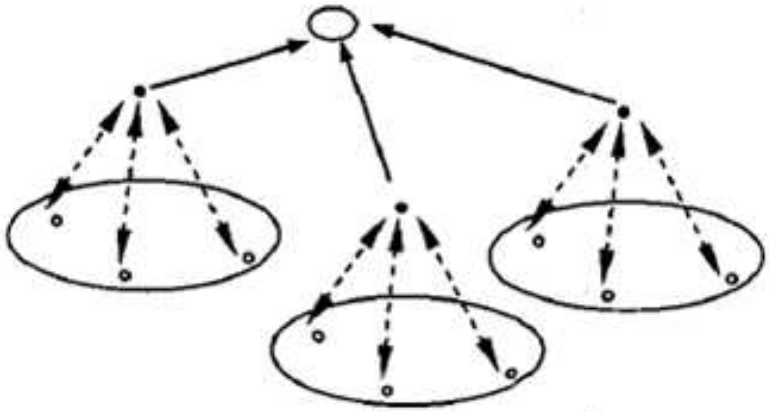

Figure 2.6: Data transmission using ESPDA

In order to build an effective security mechanism, it is necessary to limit the code size of the security algorithm. For example, one common sensor type (TelosB) has a 16-bit, 8 MHz RISC CPU With only 10K RAM, 48K program memory, and 1024K flash Storage.

- **Power Limitation:** Energy is the biggest constraint to wireless sensor capabilities. We assume that once sensor nodes are deployed in a sensor network, they cannot be easily replaced (high operating cost) or recharged (high cost of sensors).

- **Unreliable Communication:** Normally the packet-based routing of the sensor network is connectionless and thus inherently unreliable. Packets may get damaged due to channel errors or dropped at highly congested nodes. The result is lost or missing packets.

2.6 Security Requirements

A sensor network has some exclusive requirements:

- **Data Confidentiality :** In many applications nodes communicate highly sensitive data, e.g., key distribution; therefore it is extremely important to build a secure Communication channel in a wireless sensor network [10]. The adversary can change the data, so as to send the sensor network into disarray. For example, a malicious node may add some fragments or manipulate the data within a packet.

- **Data Freshness :** Data freshness suggests that the data is recent, and it ensures that no old messages have been replayed. This requirement is especially important when there are shared-key strategies employed in the design.

- **Self-Organization :** A wireless sensor network is a typically an ad hoc network, which requires every sensor node be independent and flexible enough to be self-organizing and self-healing according to different situations.

- **Time Synchronization :** sensors may wish to compute the end-to end delay of a packet as it travels between two pair wise sensors. A more collaborative sensor network may require group synchronization for tracking applications, etc.

- **Secure Localization :** A sensor network will rely on its ability to accurately and automatically locate each sensor in the network. A sensor network designed to locate faults will need accurate location information in order to pinpoint the location of a fault. For large sensor networks, the SPINE (Secure Positioning for sensor Networks) algorithm is used. It is a three phase algorithm based upon verifiable multilateration [18].

- **Authentication :** Data authentication allows a receiver to verify that the data really is sent by the claimed sender. In the case of two-party communication, data authentication can be achieved through a purely symmetric mechanism: the sender and the receiver share a secret key to compute the message authentication code (MAC) of all communicated data.

2.7 Attacks on WSNs

- **Denial of Service Attack :** "Any event that diminishes or eliminates a network's capacity to perform its expected function" [19].

- Jamming:To jam a node or set of nodes, in this case, is simply the transmission of a radio signal that interferes with the radio frequencies being used by the sensor network .

- **The Sybil Attack :** Sybil attack is defined as a "malicious device illegitimately taking on multiple identities" [20]. It was originally described as an attack able to defeat the redundancy mechanisms of distributed data storage systems in peer-to-peer networks . In addition to defeating distributed data storage systems, the Sybil attack is also effective against routing algorithms, data aggregation, voting, fair resource allocation and foiling misbehavior detection. For instance, in a sensor network voting scheme, the Sybil attack might utilize multiple identities to generate additional "votes."

- **Node Replication Attacks:** An attacker seeks to add a node to an existing sensor network by copying (replicating) the node ID of an existing sensor node [21]. A node replicated in this fashion can severely disrupt a sensor network's performance; packets can be corrupted or even misrouted. This can result in a disconnected network, false sensor readings, etc.

- **Attacks Against Privacy:** Monitor and eavesdropping: By listening to the data, the adversary could easily discover the communication contents. When the traffic conveys the control information about the sensor network configuration, which contains potentially more detailed information than accessible through the location server, the eavesdropping can act effectively against the privacy protection [22].

2.8 Defensive Measures

2.8.1 Key Establishment

Traditionally, key establishment is done using one of many public-key protocols. One of the more common is the Diffie-Hellman public key protocol, but there are incompatible in low power devices such as wireless sensor networks. This is due largely to the fact that typical key exchange techniques use asymmetric cryptography, also called public key cryptography. In this case, it is necessary to maintain two mathematically related keys, one of which is made public while the other is kept private. This allows data to be encrypted with the public key and decrypted only with the private key. The problem with asymmetric cryptography, in a wireless sensor network, is that it is typically too computationally intensive for the individual nodes in a sensor network. This is true in the general case, however, [23] , [24] , [25], [26] show that it is feasible with the right selection of algorithms.

Symmetric schemes utilize a single shared key known only between the two communicating hosts. This shared key is used for both encrypting and decrypting data. The traditional example of symmetric cryptography is DES (Data Encryption Standard). The use of DES, however, is quite limited due to the fact that it can be broken relatively easily, other symmetric cryptography systems have been proposed including 3DES (Triple DES), RC6, AES, and so on [23] , [27].

Key Establishment and Associated Protocols: - The LEAP protocol [25], [28] takes an approach that utilizes multiple keying mechanisms. Their observation is that no single security requirement accurately suites all types of communication in a wireless sensor network. Therefore, four different keys are used depending on whom the sensor node is communicating with. Sensors are preloaded with an initial key from which further keys can be established.

In PIKE [29], a mechanism for establishing a key between two sensor nodes that is based on the common trust of a third node somewhere within the sensor network. The nodes and their shared keys are spread over the network such that for any two nodes A and B,there is a node C that shares a key with both A and

B. Therefore, the key establishment protocol between A and B can be securely routed through C.

Adrian Perrig et al. propose a key-chain distribution system for their μTESLA secure broadcast protocol [30]. The basic idea of the μ TESLA system is to achieve asymmetric cryptography by delaying the disclosure of the symmetric keys. In this case a sender will broadcast a message generated with a secret key. After a certain period of time, the sender will disclose the secret key. The receiver is responsible for buffering the packet until the secret key has been disclosed. After disclosure the receiver can authenticate the packet, provided that the packet was received before the key was disclosed.

2.8.2 Defending Against Attacks on Routing Protocols

Techniques for Securing the Routing Protocol: - TRANS (Trust Routing for Location Aware Sensor Networks) [30]. The TRANS routing protocol is designed for use in data centric networks. It also makes use of a loose-time synchronization asymmetric cryptographic scheme to ensure message confidentiality. In their implementation, μTESLA is used to ensure message authentication and confidentiality.

Using μTESLA, TRANS is able to ensure that a message is sent along a path of trusted nodes while also using location aware routing. The strategy is for the base station to broadcast an encrypted message to all of its neighbors. Only those neighbors who are trusted will possess the shared key necessary to decrypt the message. The trusted neighbor(s) then adds its location (for the return trip), encrypts the new message with its own shared key and forwards the message to its neighbor closest to the destination. Once the message reaches the destination, the recipient is able to authenticate the source (base station) using the MAC that will correspond to the base station. To acknowledge or reply to the message, the destination node can forward a return message along the same trusted path from which the first message was received [30].

2.8.3 Defending Against DoS Attacks

One strategy in defending against the classic jamming attack is to identify the jammed part of the sensor network and effectively route around the unavailable portion. Wood and Stank Vic [19] describe a two phase approach where the nodes along the perimeter of the jammed region report their status to their neighbors who then collaboratively define the jammed region and simply route around it. To handle jamming at the MAC layer, nodes might utilize a MAC admission control that is rate limiting. This would allow the network to ignore those requests designed to exhaust the power reserves of a node.

2.8.4 A Wormhole Attack

A malicious node eavesdrops on a packet or series of packets, tunnels them through the sensor network to another malicious node, and then replays the packets. This can be done to misrepresent the distance between the two colluding nodes. It can also be used to more generally disrupt the routing protocol by misleading the neighbor discovery process. Additional hardware, such as a directional antenna [21] ,is used to defend against wormhole attacks.

Use a visualization approach to identifying wormholes. They first compute distance estimation between all neighbor sensors, including possible existing wormholes. Using multi-dimensional scaling, they then compute a virtual layout of the sensor network. A surface smoothing strategy is then used to adjust for round off errors in the multi-dimensional scaling. Finally, the shape of the resulting virtual network is analyzed. If a wormhole exists within the network, the shape of the virtual network will bend and curve towards the offending nodes. Using this strategy the nodes that participate in the wormhole can be identified and removed from the network. If a network does not contain a wormhole, the virtual network will appear flat [31].

2.8.5 Defending Against the Sybil Attack

The network needs some mechanism to validate that a particular identify is the only identity being held by a given physical node [20].Two methods to validate identities

Direct Validation: - In direct validation a trusted node directly tests whether the joining identity is valid. Direct validation techniques, including a radio resource test. In the radio test, a node assigns each of its neighbors a different channel on which to communicate. The node then randomly chooses a channel and listens. If the node detects a transmission on the channel it is assumed that the node transmitting on the channel is a physical node. Similarly, if the node does not detect a transmission on the specified channel, the node assumes that the identity assigned to the channel is not a physical identity.

Indirect Validation: -In indirect validation, another trusted node is allowed to vouch for (or against) the validity of a joining node [20].

2.8.6 Detecting Node Replication Attacks

In [21], Parno, et al. describes two algorithms: Randomized multicast: - deterministic multicast by randomly choosing the witnesses. In the event that a node is replicated two sets of witness nodes are chosen. Assuming a network of size n, if each node derives pn witnesses then the birthday paradox suggests that there will likely be at least one collision. In the event that a collision is detected, the offending nodes can easily be revoked by propagating a revocation throughout the network. The communication cost of the randomized multicast algorithm is still O (n2) - too high for large networks.

Line-selected Multicast:-It is based upon rumor routing [21]. The idea is that a location claim traveling from source s to destination d will also travel through several intermediate nodes. If each of these nodes records the location claim, then the path of the location claim through the network can be thought of as a line segment .In this case the destination of the location claims is one of the randomly chosen witnesses as the location claim routes through the network

towards a witness node; the intermediate sensors check the claim. If the claim results in an intersection of a line segment then the nodes originating the conflicting claims are revoked. The line selected multicast algorithm reduces the communication cost to O(npn) as long as each line segment is of length O(pn) nodes. The storage cost of the line-selected multicast algorithm is O (pn).

2.8.7 Defending Against Attacks on Sensor Privacy

Anonymity Mechanisms: Anonymity mechanisms depersonalize the data before the data is released, which present an alternative to privacy policy-based access control. Secure Communication Channel Using secure communication protocols, such as SPINS [18], the eavesdropping and active attacks can be prevented.

2.8.8 Secure Data Aggregation

An aggregator is responsible for collecting the raw data from a subset of nodes and processing/aggregating the raw data from the nodes into more usable data [31].

Aggregate-commit-prove Technique: - This technique is composed of three phases. Aggregate: The aggregator collects data from the sensors and computes the aggregation result according to a specific aggregate function. Each sensor should share a key with the aggregator. This allows the aggregator to verify that the sensor reading is authentic.

Commit Phase: The aggregator is responsible for committing to the collected data. This commitment ensures that the aggregator actually uses the data collected from the sensors. One way to perform this commitment is to use a Merkle hash-tree construction .Using this technique the aggregator computes a hash of each input value and the internal nodes are computed as the hash of their children concatenated. The commitment is the root value. The hashing is used to ensure that the aggregator cannot change any input values after having hashed them.

Proving Phase: The aggregator is charged with proving the results to the user. The aggregator first communicates the aggregation result and the commitment. The aggregator then uses an interactive proof to prove the correctness of the results. This requires two steps. (1) The user/home server checks to ensure

that the committed data is a good representation of the data values in the sensor network. (2)The user/home server decides whether the aggregator is lying. This can be done by checking whether or not the aggregation result is close to the committed result. The interactive proof differs depending on the aggregation function that is being used.

Chapter 3

WSNSF Architecture

Systems Model

A Symmetric-session based Key Scheme(SSKS)

Energy-efficient Secure Data Routing protocol (EESDRP)

An Energy-efficient Cluster Head Selection - technique (EECST)

Error Detection Mechanism

Conclusion

Chapter 3

Wireless Sensor Network Security Framework (WSNSF) Architecture

The proposed framework called Wireless Sensor Network Security Framework (WSNSF) which is consists of four interacting components that can be used to design energy-efficient security protocols that are adaptive to the environment: a symmetric-session based key (SSKS) scheme (blowfish encryption/decryption), energy-efficient secure Data routing algorithm (EESDRA), an energy-efficient cluster technique (ECT) and an Error detection mechanism. Each of these components can achieve certain level of security and energy efficient routing in the wireless sensor networks. WSNSF takes into consideration the communication and computation limitations of sensor networks. While there is always a trade off between security and performance, experimental results prove that the proposed framework can achieve energy efficient routing and high degree of security with negligible overheads.

3.1 Systems Model

We describe a three-level system model in the wireless sensor network comprising the Sensor nodes (SN), Gateway nodes (GN) and Sink as shown in Figure 3.1 We divide the whole network into certain clusters and each cluster comprises one GN that controls several SNs.The GNs of different cluster communicate with each other to exchange the collected data. The GNs forward the collected data to the

Processor	8-bit, 4 MHz
Memory	8 KB flash 512 bytes RAM 512 bytes EEPROM
Radio	916 MHz radio
Data Rate	10 Kbps

Table 3.1: Prototype of generic-sensor nodes (Mica Mote)

nearby Sink and finally to the user or the controlling authority, which is located somewhere, far away from the monitoring region that accesses the sensed data and monitors the network via the Sinks. The three different level of the WSNs may be planned as given below.

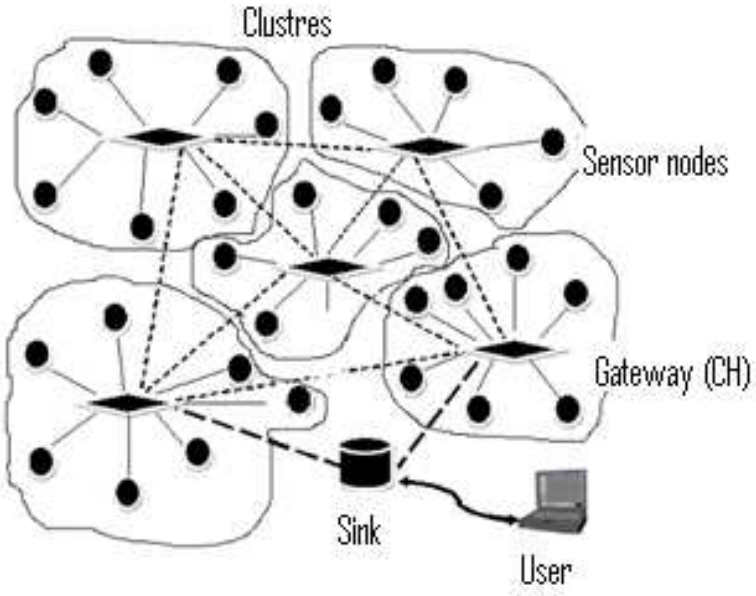

Figure 3.1: Three level WSNGs Architecture

Based on different hardware constraints and the applications of WSNs, we have classified the sensor nodes into three categories such as the generic, special-purpose and the high-bandwidth sensors. The hardware specifications of these nodes are given in Table 3.1,3.2 and 3.3 respectively.

Level-1: These are the set of generic sensor nodes(SN) like Mica Motes [14]

Processor	4-8 MHz Custom 8-bit
Memory	0.1 Mb flash memory 3K-4Kb RAM
Radio	50-100Kbps
Data Rate	20 Kbps

Table 3.2: Prototype of special-purpose sensor nodes (Spec 2003)

Processor	Intel Strong ARM 1100@133 MHz 150 MIPS
Memory	4 MB Flash memory 1MB SRAM
Radio	3 wire RS-232
Data Rate	100 Kbps

Table 3.3: Prototype of high-bandwidth sensing nodes(RSC Wins-Hidra Nodes)

and are deployed hundreds of thousands in a specific monitoring area. The whole monitoring area is divided into certain clusters which can be formed based on cluster selection algorithms and based on the number and type of sensors for different applications [5] , [12] , [17]. Their functions are simple, specific and are usually operated independently. They sense the medium, collect the raw data and forward it to the second level. The hardware specifications of such nodes are shown in Table3.1.

Level-2: These are some special-purpose sensor nodes like Spec 2003 [14], limited number of which is deployed in the monitoring region. In each cluster, there exists only one cluster head and is termed as the Gateway node (GN), which can collect raw data from the SNs of its cluster. These nodes are more powerful in computation and energy than the SNs and their respective prototypes are presented in Table 3.2.

Each GN of the network has unique ID and its assignment is based on the cluster number. GNs can track events or targets using the sensors of its own cluster and prepare the final report using data fusion and aggregation techniques and forwards the fused data to the third level.

Level-3: The high-bandwidth sensing and communication nodes like RSC Wins-Hidra Nodes [14] form the third level of the network and are known as the

Sink of the WSGNs. The operating characteristics of such nodes are given in Table 3.3 These nodes have relatively powerful processing, memory and transmission capacity and are having long battery life. These Sinks and the user or the controlling center are connected via wireless such as internet and satellite.

3.1.1 Function of Different Nodes

Function of Sink

1. Decrypted the data packet and check the integrity of the packet
2. Generate new session key
3. Whenever session expire send new session key to the gateway in encrypted with current session key.

Function of Gateways (CH)

1. Append logical time stamp and its own id on Receive data packets from all single hop its cluster sensor nodes.
2. aggregate the data packets by applying redundancy factor and route it to sink.
3. Receive a new session key from Sink
4. Sends control packets (session keys) to all its cluster nodes.

Function of Sensor Node (SN)

1. Encrypted the data packet by blowfish algorithms.
2. Send data packets to the gateway (CH) nodes.
3. Receive control packets from gateway (CH) nodes.
4. Update the session key base on control packets.

3.2 A Symmetric-Session based Key Scheme(SSKS)

In our design every sensor node has a session key at a time of deployments. Initially sensor nodes encrypt the sensed data apply the Blowfish Algorithm, which makes the data transmission more secure, then send encrypted data to gateways. The advantage of this technique is that it increases communication security and requiring very less energy comparatively other cryptography algorithms. After completing a current session, sink will generate a new session key using a pseudorandom function (f) and current session key and send to the corresponding gateway. The new session key broadcast to its cluster's sensors by the gateway, for data encryption of the new session .so in this communication process session key has change dynamically for every session by the Sink.

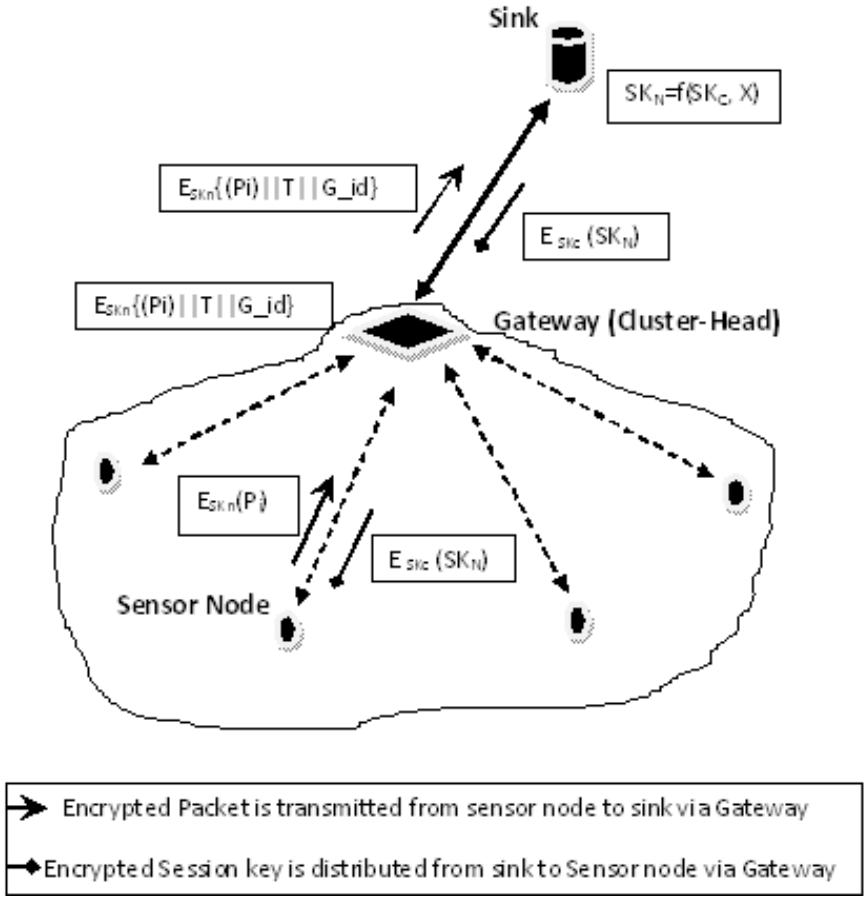

Figure 3.2: Encrypted packet and session key transmission in WSNGs

In our algorithms, CBC [32] protocol is used to provide data authentication

is granted by using periodically changing user specific session keys. These session keys are generated form the Sink and send to the gateways (CH) and then gateway broadcast the key to its cluster sensors node for using next session.

3.2.1 Blowfish Algorithm

It is a symmetric (i.e. uses the same secret key for both encryption and decryption) block cipher (encrypts data in 8-byte blocks) that uses a variable-length key, from 32 (4 bytes) bits to 448 bits (56 bytes). The algorithm consists of two parts: a key-expansion part and a data-encryption part. Key expansion converts a variable key of at least 4 and at most 56 bytes into several subkey arrays totaling 4168 bytes. Blowfish has 16 rounds. Each round consists of a key-dependent permutation, and a key and data-dependent substitution. All operations are XORs and additions on 32-bit words. The only additional operations are four indexed array data lookups per round. Blowfish uses a large number of sub-keys. These keys must be precomputed before any data encryption or decryption [33].

When we evaluate the performance of different symmetric cryptographic algorithms we find out that AES algorithm [34] is a very fast algorithm but requires at least 800-byte memory space for lookup tables ,DES also uses large lookup tables and its throughput is very less hence weaknesses of DES, which made it an insecure block cipher. RC6 [35] is a small algorithm, but it is slower than blow-fish .Finally, we decided on Blowfish [33]. Mini version of Blowfish is implementable on 8-bit processor with a minimum of 24 bytes of RAM (in addition to the RAM required to store the key) and 1 kilobyte of ROM [34] .

The amount of computational energy consumed by a security function on a given microprocessor is primarily determined by the number of clocks needed by the processor to compute the security function. The number of clocks necessary to perform the security function mainly depends on the efficiency of the cryptographic algorithm [36] , [16] , [37] , [38]. In our algorithms, CBC [35] , [38] protocol is used to provide data integrity, where as node authentication is granted by using periodically changing user specific session keys. These session keys are generated form the sink and send to the gateways (CH) and then gateway distribute the key

to its cluster sensors node for using next session.

3.2.2 Secure Communication

The communication is secure because the message encrypted by the session key, which will be different for each session. Therefore attacker cannot access the message. Thus session key dynamically change after each and every session so it is very difficult to eavesdrop attack on the network for an intruder. In order to make be sure, secure data communication in our sensor network.

3.2.3 Key Freshness

Sink used pseudorandom function for generating the new session key. As the number is random, key generation algorithm produces a different session key for the each and every session in order to ensure the freshness of the session key.

3.2.4 Integrity and Origination of the Data

Gateways append the logical time stamp and its id with the encrypted packets. When packet reached to the sink ,then sink check the logical time stamp and match this time stamp with the own time stamp,if it is match that means packet is fresh in order to ensure that message is not altered . Sink also check the gateway id which is attached to the packet by help this id, sink to know the origination of the packet for further action.

3.3 Energy-efficient Secure Data Routing Protocol (EESDRP)

Secure data Routing Algorithm: Routing

Begin

There are three types of communications in the proposed scheme:-

(a)Sensor to Gateway

(b)Gateway to Gateway

(c)Gateway to Sink

Secure communication in each of these schemes is explained blow

1. **Sensor to Gateway:-** A Sensor node S_i encrypt the packet P_i using current session key SK, which is built-in at the time of sensors deployments and send to it's a local gateway G_i.

Si $\rightarrow$ Gi

E_{SK} (P_i)

2.**Gateway to Gateway:-** Following action are performed at the gateway:

(i) Gateway concatenates the encrypted packets it received from the sensors in its own cluster and from the other gateways on the path to the sink,

(ii) Increment the value of logical time stamps T_{GS} by one and appends it to the concatenated packets,

(iii) Concatenate its own ID and send it to the next Gateway on the path to the Sink.

$G_h \rightarrow G_k$

$\{\{E_{SK}(P_l)\} ||\{E_{SK}(P_m)\}||\ldots||\{ E_{SK}(P_n)\}||T_{GS} ||G_h \}$

$\{\{(E_{S1K1}(P_d) \}||T_{GS} ||G_m)\}||\ldots.||\{\{(E_{S2K2}(P_x)\}||T_{GS} ||G_n)\}$ where E_{SK} (P_i), $E_{SK}(P_m)$,$E_{SK}(P_n)$ are encrypted packets from the sensor node l, m,n belonging to the cluster, of gateway G_h, $(E_{S1K1}(P_d)||T_{GS}||G_m)$

:-Encrypted packets received from cluster head G_m , ($E_{S2K2}(P_x)||T_{GS}$ $||G_n$):- Encrypted packet received from the cluster head G_n.

T_{GS} :- Time stamp belonging to the each cluster head .

3.**Gateway to Sink:** Sink has received concatenated Encrypted packets from the gateway

$G_k \rightarrow$ Sink

$\{\{E_{SK}(P_l)\}$ $||\{E_{SK}(P_m)\}||\ldots||\{$ $E_{SK}(P_n)\}||T_{GS}$ $||G_h$ $\}$

$\{\{E_{S1K1}(P_d)$ $\}||T_{GS}$ $||G_m\}||\ldots.||\{\{(E_{S2K2}(P_x)\}||T_{GS}$ $||G_n$ $)\}$

Gateway to sink communication is same as the gateway to gateway communication. Unlike gateway, sink process the received packet, rather then forwarding it.

4. The following actions are performed by the sink on receiving packet from the gateway:

(i)For a credible time stamp sink decrypts the encrypted packets using the current session key, D_{SK} $\{\{E_{SK}(P_l)\}$ $||\{E_{SK}(P_m)\}||\ldots||\{$ $E_{SK}(P_n)\}||T_{GS}$ $||G_h$ $\}$

$\{\{(E_{S1K1}(P_d)$ $\}||T_{GS}$ $||G_m)\}||\ldots.||\{\{(E_{S2K2}(P_x)\}||T_{GS}$ $||G_n$ $)\}$

if ($T_{GS} \geq T_{SG}$),the time stamp is credible and data is authentic (to obtain the original message Px). That is DSK E_{SK} $(P_x) \rightarrow P_x$,

if ($T_{GS} \leq T_{SG}$),then the sink either discard the packet or send a retransmission request to the gateway.

(ii) Checks the timestamp credibility by first, sink extracts gateway ID from packet. For a valid gateway ID, it checks the timestamp credibility comparing the sequence number T_{GS} appended by the gateway with the latest value of its logical time stamp T_{SG},

(iii) Verify gateways IDs in the packets.

5. On expiry of current session, sink increments the value of T_SG by 1, and generate the new session key using the pseudorandom function (f) and current session key. The new session key is a function of current session and x.

New Session SK_n = f(SK_c ,x) where x is random number .

6. Session key is updated for the next session. Session key is updated as follows.

(i)Sink encrypt the new session key (SK_n) using the current session key(SK_c) and send to the corresponding gateways,

(ii) Gateway broadcast the new session key in its own cluster,

(iii) Sensor nodes update its session keys, with the new session key.

7. End

Data routing in wireless sensor networks eliminates redundancy to improve bandwidth utilization and energy-efficiency of sensor nodes. We present a secure energy-efficient data routing protocol called ESDRP which provides both security and energy efficiency together in cluster-based wireless sensor networks.ESDRP prevents the redundant data transmission from sensor nodes to sink.

Gateways implement data routing based on event occurrence take place and only distinct data in encrypted form is transmitted from sensor nodes to the sink via gateways. for avoiding redundant data communication, gateway check the content of every message which is received from its cluster's sensor nodes and if sensor node sense same data, then gateway eliminate the redundant data and only necessary information has been send to the base station.

3.3.1 Security Algorithm

The EESDRP employs session base symmetric key encryption technique to provide authenticity, confidentiality and data integrity in WSGNs.

In each session, sink send a new session key SK_n, which is encrypted using the current session key SK_c .Gateway nodes broadcast the new session key to its cluster. Sensor nodes received broadcasted new session key SK_n and update their secret session key. Our propose algorithm is provide data confidentiality by using SK_n for all the subsequent data encryption and decryption during the session, and each sensor node encrypting data with SK_n also provide authentication .

Notations	Description
P_i	Packet
E ( )	Encryption function
SK	Session key
G_l, G_m, G_n	Gateways ID
D ( )	Decryption function
f ( )	Pseudorandom function
T_GS	Logical time stamp(sequence- numbers)of the gateways
T_SG	Logical time stamp (sequence - numbers) of the Sink
SK_n	New session key
SK_c	Current session key
X	Random number
||	Concatenation operator

Table 3.4: Notation uses in ESRA

Changing encryption key in each session is help to ensure data freshness in the WSGNs; in addition, it also provides the confidentiality of the transmitted data by preventing the use of same key in every session. Ensuring data freshness avoid the replay attack in the nerwork.During the data communication each gateway node appends its GID and logical time stamp to the packet to ensure data freshness and integrity. During receiving a packet, sink decrypt the data using SKn and find out time stamp with associates GID on the message, and verify the data authentication, then obtain the original message P_i.if the is altered or replayed ,then sink discard the data or send a retransmission request to the corresponding gateway node. During aggregation of data gateway node appends its GID before forwarding data to sink to help the sink in locating the origin of the data and reduce the search time required to find the originating cluster node .proposed security algorithm use Blowfish for encrypt and decrypt the data.

3.3.2 Data Routing in ESDRP

Our design based on hierarchical structure where data is routed from sensor nodes to the Sink through Gateways. Sinks are assumed to have sufficient power and memory to communicate securely with all the sensor nodes and gateways. Sensor nodes are deployed randomly over an area to be monitored and organize themselves into clusters after the initial deployment. A cluster-head (gateway) is chosen

from each cluster to handle the communication between the clusters nodes and the Sink. Cluster-heads (gateways) are resource rich like as they have more computational and communication power comparatively other sensors nodes. Here we are assuming static gateway (CH) concept. That means gateways (CH) choose once at the time of network deployment using energy-efficient cluster head selection algorithm, based on its resource rich characteristic of the gateway, in order to saved power consumption among all sensor nodes, unlike other conventional algorithms the cluster head has change dynamically, due to this communication over head will be more, so these algorithms consume more energy. Since data transmission is a major cause of energy consumption, ESDRP first reduces transmission of data from sensor nodes to cluster-heads with the help of static cluster-head concept. Then, data aggregation is used to eliminate redundancy and to minimize the number of transmissions for saving energy. In our data aggregation methods, gateway receives all the data from sensor nodes and then eliminates the redundancy by checking the contents of the sensor data. In security protocol, sensor data, which is identified as non-redundant by the gateways, is transmitted to the Sink in encrypted form.

3.3.3 Data Redundancy Elimination Model

When all sensor nodes select the gateway to which it can forward the data packet. The cluster selection procedure is based on our propose energy efficient cluster selection algorithm. After selecting the gateway node, each sensor node now forwards its data to its gateway. When a gateway node receives multiple data packets from its cluster's nodes, it performs aggregation operation by eliminating redundancy in the data. Each gateway node checks the equation below:

$$VN_i - VN_j < K$$

Where, VN_i is data value of node i, VN_j is data value of node j and K is redundancy factor.

If this equation satisfies, the gateway node perform aggregation by applying any aggregation functions like MIN, MAX, and AVG on the values of data packet

and send only one packet while discarding other packets. But if this equation do not satisfies, the gateway performs aggregation by simply concatenating two data packet in to one keeping value of both packets intact.

The selection of value for redundancy factor (K) has a trade-off between precision and energy consumption. If the application wants more precision, it should select a low value for redundancy factor otherwise a high value. Selecting high value for K means sending only one value thus less number of bits needs to be transmitted and hence low energy consumption.

3.3.4 Energy Consumption Model

In simple radio model presented in [15], radio dissipates E_{ele} = 50 nJ/bit at the sender and receiver sides. Let us assume the d is the distance between the sources and destination, then, the energy loss is d^2. The transmit amplifier at the sender consumes E_{amp} d^2, where E_{amp} =100 pJ/bit/m^2. Therefore, from the sender side, to send one bit at distance d, the required power is E_{ele} + E_{amp} *d^2, whereas at the receiver will need is Eele only. Normalizing both by dividing by E_{amp}:Pt = E + d^2 and Pr = E, where Pt and Pr are the normalized transmission and reception power respectively, and E = E_{ele} / E_{amp} = 500m^2.the power needed for transmission and reception at distance d is: transmission u(d) = Pt + Pr = 2E + d^2

In reception u(d) =2E , Where 2E = 1,000. For example conventional data aggregation models which are use multi-hop communication (sensor send data to nearby neighbor node then it will send to the sink) for the sensors are based on the first order radio model described in [15]. A sensor consumes E_{elec} = 50nJ/bit to run the transmitter or receiver circuitry and E_{amp} = 100pJ/bit/m^2 for the transmitter amplifier and distance between two nodes is 10 meter. Thus, the energy consumed by a sensor j in receiving a l-bit data packet is given by,

$$ERx, j = E_{elec} * l \tag{3.1}$$

While the energy consumed in transmitting a data packet to sensor i is given by,

$$ETxj, i = E_{elec} * l + E_{amp} * d_i, i^2 * l \tag{3.2}$$

Suppose then j send packet to the cluster head so again energy consumption by node j is given by

$$ETxj, g = E_{elec} * 1 + E_{amp} * d_i, g * 1 \tag{3.3}$$

While the energy consumed in receiving a data packet from node j to gateway is given by

$$ERx, g = E_{elec} * 1 \tag{3.4}$$

So total energy consumption by equation 3.1,3.2,3.3,3.4
will be 50+1050+1050+50=2200 pJ/bit/m2.

But in our algorithm all nodes is adjusted in such a way that they can perform single hop broadcast. In single hop communication sensors directly send the packet to its cluster heads. Suppose here distance between sensor to cluster head is double di=20 meter, so energy consumption in transmitting a data packet from the sensor node i to cluster head G is given by

$$ETxi, g = E_{elec} * 1 + E_{amp} * d_i, g * 1 \tag{3.5}$$

While the energy consumed in receiving a data packet by the gateway is given by

$$ERx, g = E_{elec} * 1 \tag{3.6}$$

Where d_i,j is the distance between nodes i and j . So total energy consumed in our algorithm by equation 3.5,3.6 will be 2000+50=2050 pJ/bit/m^2. Thus in our algorithm we can save 150 pJ/bit/m^2 energy from one communication (transmission /receiving).

3.3.5 Single-hop Communication

ESDR significantly reduces the energy consumption of all nodes in the cluster by reducing the transmission power of all nodes. The important beneficial issue in our designed protocol is that after the formation of cluster and selection of cluster-head, all sensor nodes have to reduce their transmission power in such a way that they could only reach their single-hop distance neighbors. This operation requires some kind of synchronization among all nodes. The nodes have to

calculate AMRP before to perform the single-hop communication. For this, we are using our propose algorithm. Now when cluster-head received all data packets and aggregated them, it has to now increase its transmission power so that it can transmit the final aggregated data up in the cluster-head hierarchy towards the sink.

Though EESDR requires all nodes to adjust their transmission power after the deployment and requires energy efficient cluster selection algorithm and secure energy efficient encryption/decryption algorithm before, it conserves a significant amount of energy. So in the presence of the above issue, ESDR outperforms when we try to maximize the network lifetime.

3.4 An energy-efficient Cluster Head Selection - Technique (EECST)

The nature of wireless sensors networks depends on batteries consumption. A limited energy capacity may be the most significant performance constraint. Therefore, radio resource and power management is an important issue of any wireless network. In wireless sensor networks, cluster-based architecture is one of the most important approaches for many applications. Cluster-base architecture divides the network into several zones. Each Zone consists of a cluster head and others node associated with it. Cluster heads are elected based on upon agreed rule (AMRP, energy leveletc). Cluster-based protocols organize the network into a hierarchical structure to manage the network in an efficient way.

Consider a homogeneous network of number of sensor nodes, some gateways nodes and a sink node distributed over a region. The location of the sensors and the are fixed and known priori. Each sensor produces some information as it monitors its vicinity. We assume that the whole network is divided in to several clusters; each cluster has a cluster-head(CH). The clustering and the selection of gateways are based on the EECT. We also assume that after the formation of cluster the transmission power of all nodes is adjusted in such a way that they can perform single hop broadcast. Single hop broadcast refers to the operation of

sending a packet to all single-hop neighbors in single hop communication sensors directly send the packet to the its cluster heads, in order to save the energy by the single hop communication.

3.4.1 Cluster Head Selection Algorithm

At the time of deployment of wireless sensor networks. Cluster head is selected once based on the 2 parameters.

1. Weight of the gateways
2. Average minimum reach ability power of sensors

Weight of the gateways: It is the sum of (i) Average of the distance from gateway to neighbor gateway and distance between gateway to sink, and (ii) battery power of the gateways. Weight of gateways = Power + average distance

$$W_v = P_v + D_v$$

Here Power of gateways is measured based on the range of the broad cast message in particular area.

$$P_{rx} = P_{tx} * (\lambda/4\pi d)^2$$

Equation 3.1 (used for estimating distance) is developed for a free space scenario and does not take into account any interference. Initial distance calculations using Equation (3.1). In this equation, Prx represents the remaining power of the signal at the receiving node (signal strength). Ptx is the transmission power of the sending node. λ is the wave length of the signal, and d corresponds to the transmission distance.

Average distance calculate based on the strength of the broadcast messages which is broad cast by the gateways and sink at the time of deployment of the networks.

$$WD_{v2} = (P_{tx}/P_{rx})((\lambda/4\pi))^2$$

The correlation between signal strength and distance used to calculate the weight of the each gateway. Those gateways has maximum weight will be selected

as CH and they broad cast the selection message. We assume desire CH should be static base on the sort of the work.

Average Minimum Reach Ability Power: AMRP is the average of all the minimum power levels required for each sensor node within a cluster range(r) to communicate effectively with the CH .Sensor nodes calculate average minimum reach ability power based on strength of the CH selection message which is broadcast by the gateways, and based on the AMRP each sensor node self choose its cluster-head. Each sensor node looks in to the weight of all its possible gateways. The gateway node which has single hop or least hop distance, and it has closest to sink, is selected as cluster-head. In case when two gateway nodes have the least but equal hop distance, the node checks the weight of two neighbor gateway nodes. The gateway node that has greater weight is now selected as cluster-head.

Here W_V average weight of the gateway, D_V average distance, P_V power and AMRP Average minimum reach-ability power.

3.4.2 Energy -efficient Parameters of Cluster Algorithm

1. **Static Gateways (CH) Selection:**in other conventional algorithms cluster head has been changed dynamically, so every time communication over head will be increase for selection a new cluster head but in our algorithm we have some resource rich (based on battery power and computational power) nodes which are permanently select as a cluster head based on the our algorithm .so using static cluster head concept we can reduce the energy consumption.

2. **Single-hop Communication:** Based on the AMRP the transmission power of all sensor nodes are adjusted in such a way that they can perform single hop broadcast. Single hop broadcast refers to the operation of sending a packet to all single-hop neighbors in single hop communication sensors directly send the packet to the its cluster heads, in order to save the energy by the single hop communication.

3.5 Error Detection Mechanism

In our model, whenever packet has reached to the sink, then sink try to decrypt the packet using session key and check the contents of the packet like logical time stamp and corresponding gateway id, if packet altered or loss any content of the packet in the communication way, sink will discard the packet or re-send the retransmission request to the corresponding gateway, thus we can detect the that sort of errors.

3.6 Conclusion

This chapter, a new framework for secure energy efficient data aggregation is proposed. The proposed framework uses a new approach of encryption and aggregation on the based on secure energy efficient algorithms for large-scale and low energy wireless sensor and gateway networks (WSGN).The entire framework is based on the a three level architecture for energy constrained sensor node at lower level, a sizeable numbers of energy rich gateways at the middle level ,and a sink which monitored the activity of sensor field at the upper level. The propose scheme conserve the sensor nodes energy as they are not involved in routing, unlike in WSNs. Communication between sensor nodes and the sink is secured as the sensor data is encrypted using symmetric key cryptography. In the propose scheme the session key is generated after the expiring of every session.

Chapter 4

Performance Analysis of WSNSF

Simulation Platform

Performance Analysis of EESDR Security Protocol

Analysis of Energy efficiency of EESDR Protocol

Chapter 4

Performance analysis of Wireless Sensor Network Secure Framework (WSNSF)

The proposed Wireless Sensor Network Secure Framework (WSNSF) framework Provide a secure data routing environment for three-level wireless sensor gateway networks (WSGNs).It is consists of four interacting components that can be used to design energy-efficient security protocols that are adaptive to the environment.

We have already discussed about proposed algorithms which considering energy-efficient security and hardware constraints of sensor nodes. Performance analysis of our framework shows that it is satisfies the energy and hardware limitations of the WSNs and maintains the secure communication of the network.

4.1 Simulation Platform

We have chosen Network Simualtor-2 (NS-2) [39], in particular NS-2.33, as our tool to simulate the proposed protocol. NS-2 is an object-oriented discrete time event simulator written in C++, with an OTcl interpreter .and its modular design made it to be extensible. C++ is the predominant programming language in ns-2. It is the language used for all the small programs that make up the ns-2 hierarchy. C++, being one of the most common programming languages and specially designed for object- oriented coding, was therefore a logical choice what language to be used. This helps when the user wants to either understand the code or do some alterations to the code.

Object Tcl (OTcl) is object-oriented version of the command and syntax driven programming language Tool Command Language (Tcl). The front-end interpreter in NS-2 is OTcl which link the script type language of Tcl to the C++ backbone of NS-2. Together these two different languages create a script controlled C++ environment. This helps when creating a simulation, simply writing a script that will be carried out when running the simulation.

NS uses two languages because simulator has required two different kinds of issues. First, detailed simulation of protocols requires a systems programming language which can efficiently manipulate bytes, packet headers, and implement algorithms that run over large data sets. For these tasks run-time speed is important and turn-around time (run simulation, find bug, fix bug, recompile, re-run) is less important. On the other hand, a large part of network research involves slightly varying parameters or confgurations, or quickly explore a number of scenarios. In these cases, iteration time (change the model and re-run) is more important. Since configuration runs once (at the beginning of the simulation), run-time of this part of the task is less important. ns meets both of these requirements with two languages, C++ and OTcl. C++ is fast to run but slower to change, making it suitable for detailed protocol implementation. OTcl runs much slower but can be changed very quickly (and interactively), making it ideal for simulation configuration. ns (via tclcl) provides glue to make objects and variables appear on both languages.

The Network Animator NAM is a graphic tool to use with ns-2. It requires a nam-tracefile recorded during the 0simulation and will then show a visual representation of the simulation. This will give the user the possibility to view the traffic packet by packet as they move along the different links in the network. NAM offers the possibility of tracing a single packet during its travel and the possibility to move the nodes around for a user to draw up his network topology according to his requirement. The existence of an X-server allows NAM to be able to open a graphical window.

MATLAB is also used for simulating performance of security protocol issues

4.2 Performance Analysis of EESDR Security Protocol

In our proposed framework, we have uses symmetric key cryptographic Blowfish algorithm which is applicable to all three level of the network.we simulate several cryptographic algorithms which are widely used for encryption and decryption in wireless sensor environment.

4.3 Experimental Setup

In our simulation, we use an Intel P-IV 1.60 GHz CPU, 512 Mb RAM in which performance result is collected. In the simulation, we have input a different file size ranges from 25 K byte to 2.139Mega Byte. In this analysis process consider of measuring the performances of encryption process at the C programming language's script. This is followed by conducting tests simulation in order to obtain the best encryption algorithm.

Several performance metrics are collected:

1. Encryption time
2. CPU process time
3. CPU clock cycles and battery power

An encryption algorithm takes the time to produce a cipher text from a plaintext called encryption time. Encryption time is used to calculate the throughput of an encryption algorithm. It indicates the rate of encryption. The throughput of the encryption scheme is calculated as the total encrypted plaintext in bytes divided by the encryption time.

The CPU process time is the time that is required to a CPU is dedicated only to the particular process of calculations. It reflects the load of the CPU.

The CPU clock cycles are a metric, reflecting the energy consumption of the CPU while performing on encryption operations. Each cycle of CPU will consume a minute amount of energy.

Data input size in(Kb)	DES	AES	RC6	Blofish
25	17.00	27.31	19.78	19.03
60	34.72	39.21	28.13	36.92
100	48.67	92.00	62.29	38.81
250	49.32	113.16	79.32	47.00
1000	266.11	209.97	129.87	67.38
2187.6	676.54	607.04	361.07	61.89
Average Execution Time	179.739	173.115	113.511	45.171
Throughput(MB/sec)	3.330	3.478	5.305	13.333

Table 4.1: Comparative execution times (in milliseconds) and throughput (Mb/sec) of encryption algorithms with different packet size

Data input size in(Kb)	DES	AES	RC6	Blofish
25	26.07	31.12	17.14	18.37
60	43.18	59.23	28.71	27.12
100	58.30	60.10	59.21	54.00
250	74.00	78.03	69.30	69.07
1000	161.19	167.00	118.35	83.74
2187.6	392.57	326.83	343.42	78.81
Average Execution Time	125.885	120.341	106.021	55.185
Throughput(MB/sec)	4.784	5.00	5.680	10.913

Table 4.2: Comparative execution times (in milliseconds) and throughput (Mb/sec) of decryption algorithms with different packet size

4.3.1 Simulation Results

Simulation results of encryption and decryption (Base 64):

Average data input Size=602.266

Simulation results are given in Fig. 4.1 and Fig. 4.2 for the selected four symmetric encryption algorithms at base 64 encoding method. Fig. 4.1 shows the results of time consumption of encryption algorithms at base 64 encoding.

Execution time is indicates the required time to encrypted a given data. It is consider as a speed of encryption technique. The throughput of the encryption algorithm is calculated by dividing the total plaintext in Megabytes encrypted on the total execution time for each algorithm. When the throughput value is increased, the power consumption of this encryption technique is decreased.

Simulation results for this compassion point are shown Fig. 4.3 and Table 4.1

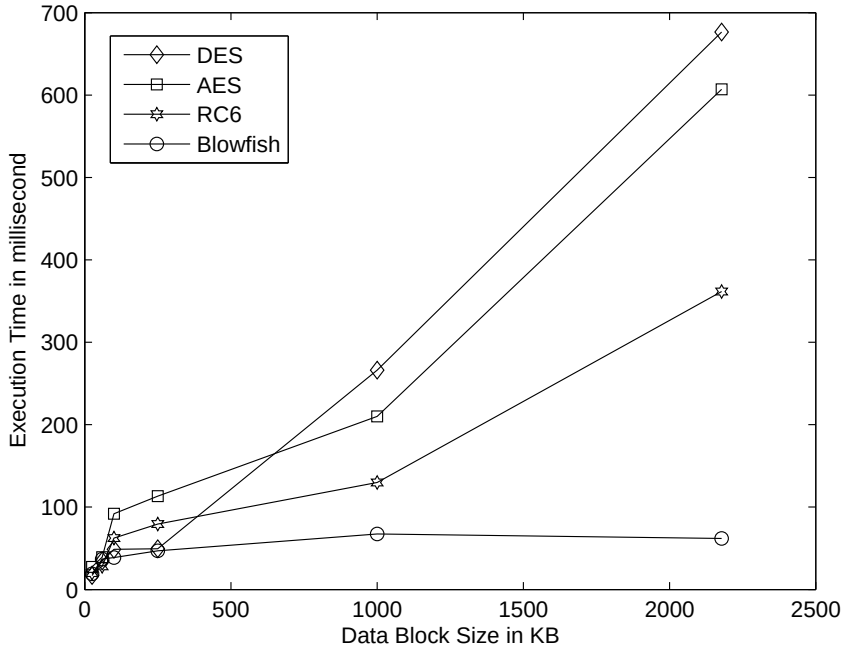

Figure 4.1: Time consumption of encryption algorithms (base 64 encoding)

at encryption phase. The results show the supremacy of Blowfish algorithm over other algorithms in terms of the execution time and throughput. RC6 requires less time than all algorithms except Blowfish. AES has an advantage over DES in terms of time consumption and throughput. Finally, it is found that Blowfish has high performance and high throughput when compared with other three algorithms.

Fig.4.4 and Table 4.2 decryption phase. We can find in decryption that Blowfish is the better than other algorithms in throughput and power consumption. Thus analysis is concluded that Blowfish has better performance than other general encryption algorithms in term of the battery and time consumption.

In our algorithms, CBC protocol is used to provide data integrity, where as node authentication is granted by using periodically changing user specific session keys. These session keys are generated form the sink and send to the gateways (CH) and then gateway distribute the key to its cluster sensors node for using next session.

The cryptographic algorithm, Blowfish, require 1KB memory space and it needs 400-Byte for key setup .The total memory space cryptographic primitives

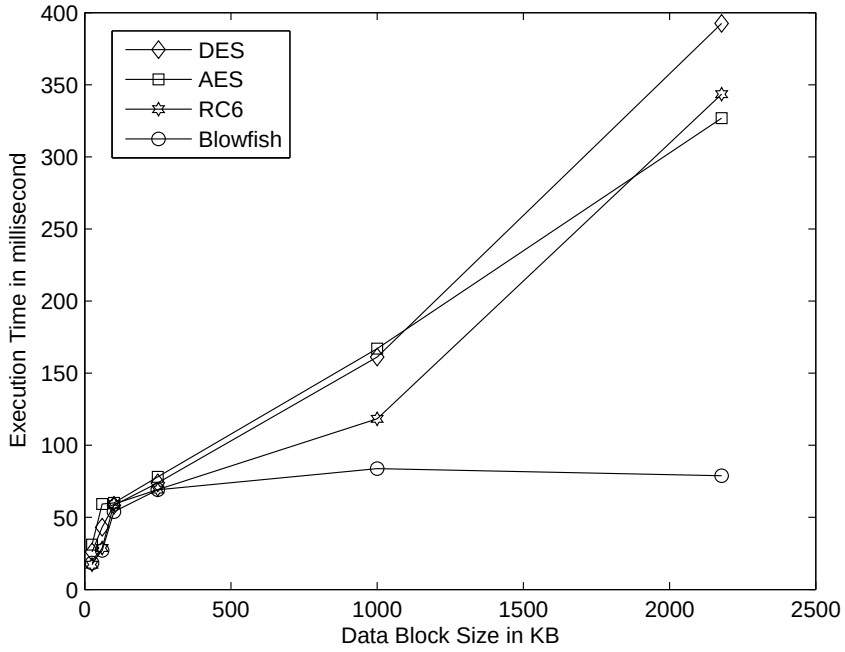

Figure 4.2: Time consumption of decryption algorithms (base 64 encoding)

is around 2KB (Table 4.2) and this amount adequate for wireless Sensor nodes.

Thus performance analysis results show that blowfish algorithms satisfied both the energy and storage limitation of wireless sensor networks.

4.3.2 Computational and storage cost analysis of security protocol

Now we analyze the computational and storage cost of our protocol because of the key updating, establishment, encryption and decryption operations during the data communication and verification. We assign a single key to all the sensors nodes including gateway and sink nodes. So in our protocol, there is no computational cost required in establishing the keying relationship among either the SN_s or GN_s or BS_s. Also, our protocols don't impose any computational burden for key updating or in establishing the keying relationship at the SN_s.Sink is responsible for key updating and gateways performs the key establishing task in the network ,as we know according our system model gateways and sink nodes are resource rich . hence key updating and establishment are manageable by resource rich node.

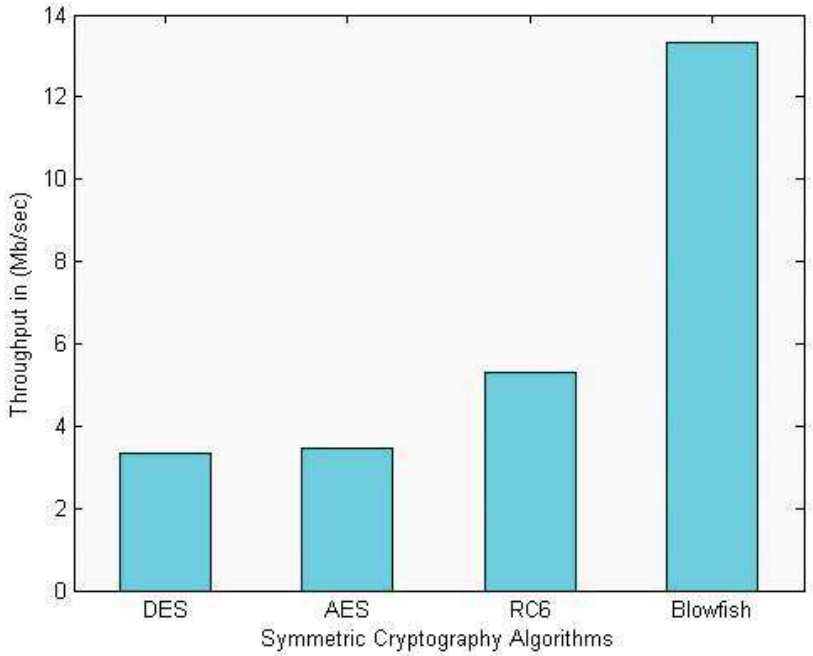

Figure 4.3: Throughput of each encryption algorithm (Megabyte/Sec)

However, the computational cost in encrypting or decrypting the message can be calculated as follows.

In case of SN_s: Suppose, in a cluster a node has n different neighbors and b_i, i=1,2,3...,n be the number of neighbors of those n nodes. So total number of required encryptions is:

$$E_T = \sum_{i=1}^{n} b_i \tag{4.1}$$

, for i= 1,2,3...,n. Similarly total number of decryption is also

$$D_T = \sum_{i=1}^{n} b_i \tag{4.2}$$

, for i= 1,2,3...,n. In a cluster, average numbers of symmetric operations are

Where ASO is Average number of symmetric operation.

$$ASO = 2\sum_{i=1}^{n} b_i/(n + \sum_{i=1}^{n} b_i + 1) \tag{4.3}$$

Where ASO is Average number of symmetric operation.

In case of GN_s: In our protocol GN_s communicate with each by unicasting the message. Suppose, the whole network has g numbers of GNs.In the worst case,

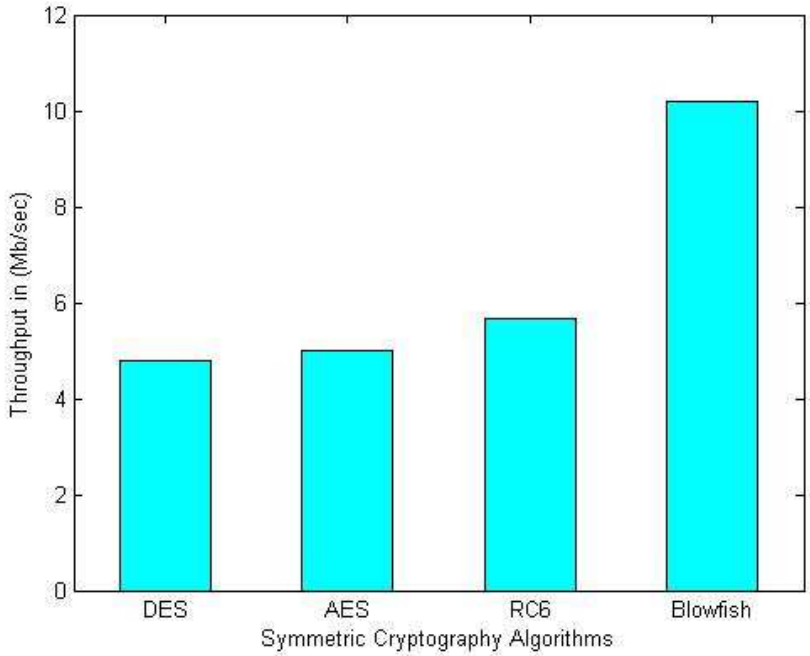

Figure 4.4: Throughput of each decryption algorithm (Megabyte/Sec)

a GN will have at most (g-1) neighbors. The average number of encryptions and decryptions in case of the GNs is:

$$ASO = 2(g-1)/g \tag{4.4}$$

In case of BS_s: Suppose, the whole network contains s number of BS_s. As the communication among the BSs is also unicasting, average number of encryptions and decryptions is

$$ASO = 2(s-1)/s \tag{4.5}$$

In our protocol, sp gm n. So the total average number of encryption and decryptions operations

$$ASO_T = 2\sum_{i=1}^{n} b_i/(n + \sum_{i=1}^{n} b_i + 1) + 2(g-1)/g + 2(s-1)/s \tag{4.6}$$

Other important issue is that, in our protocol, a node stores only a single session key e.g. . E_{SK} and session key is same for all the nodes in a particular cluster. So there is no necessitating storing the chain of keys for its neighbors. If l1 is the key length of E_{SK} then the total key length is required to store in each

Algorithm	**Key Length (bit)**	**Keys searched per second**	**key-searching technology**	**Approximate time to search all possible keys**
DES	56	100 billion	DES-cracking machine	8 days
TEA	128	1 billion billion (1 x 1018)	Large-scale Internet project in the year 2005	10,783 billion years
AES	128 to 256	1 x 1023	Special-purpose quantum computer in the year 2015	2 x 1027 years
Blowfish	32 to 448	1 x 1023	Special-purpose quantum computer in the year 2015	3.7 x 1046 years

Table 4.3: Estimated success of brute force attacks

Encryption	Key Setup	Total Memory Consumption
1000	400	1400

Table 4.4: Memory space consumption (in bytes)

SN is l = l1.while sensor nodes are memory constrains, for a reasonable key length of E_{SK}, storage is not a matter in our protocol. It is observed that the storage requirement, encryption and decryption computational costs of our protocol are better than the LEAP [9].

4.4 Analysis of Energy efficiency of data routing protocol

In this section, we describe a radio communication model that is used in the quantitative analysis of our protocol. The energy dissipation is analytically determined.

4.4.1 Radio Communication Model

We use a radio model as described in [HCB00], where for a shorter distance such as single-hop transmission, for instance direct data transfer from sensor node to cluster-head, the energy consumed by a transmit amplifier is proportional to r^2. However, for a longer distance transmission, such as multi-hop transmission from a sensor node to the sink, the energy consumed is proportional to r^4. Using the given radio model, the energy consumed to transmit an l-bit message for a longer distance, d, is given by:

$$E_T = E_e + E_m d^4 \tag{4.7}$$

in the same way, the energy consumed to transmit an l-bit message for a shorter distance is given by:

$$E_T = E_e + E_s d^2 \tag{4.8}$$

In addition, the energy consumed to receive the l-bit message is given by:

$$E_T = E_e \tag{4.9}$$

4.4.2 Cluster-head Election Phase

For a sensor network of n nodes, the optimal number of clusters is given as c. some nodes are assumed to be at the relatively high energy level at the beginning called gateway. At the start of the election phase, the base station randomly selects a given number of gateways as a cluster heads base on our proposed energy-efficient cluster- technique (EECT).

Uniformly distributed clusters, each cluster contain n/c nodes. Using Equation 4.8 and Equation 4.9, the energy consumed by a cluster head is estimated as follows:

$$E_{CH-elec} = \{E_e + E_s d^2\} + \{(n/c - 1)E_e\} \tag{4.10}$$

The first part of Equation 4.10 represents the energy consumed to transmit the advertisement message; this energy consumption is based on single-hop distance

energy dissipation model. The second part of Equation 4.10 represents the energy consumed to receive (n/c - 1) messages from the sensor nodes of the same cluster.

Using Equation 4.8 and Equation 4.9, the energy consumed by non-cluster head sensor nodes is estimated as follows:

$$E_{non-CH-elec} = \{c * E_e\} + \{E_e d^2\} \tag{4.11}$$

The first part of Equation 4.11 shows the energy consumed to receive messages from c cluster heads; it is assumed that a sensor node receives messages from all the cluster heads. The second part of Equation 4.11 shows the energy consumed to transmit the decision to the corresponding cluster head. Equation 4.11 can be simplified as follows:

$$E_{non-CH-elec} = E_e(1 + c) + E_s d^2 \tag{4.12}$$

4.4.3 Data Transfer Phase

During data transfer phase, the sensor nodes transmit messages to their gateway and gateways transmit aggregated data to the sink. The energy consumed by a cluster head is as follows:

$$E_{CH-frame} = \{(n/c - g)E_e\} + 1\{E_e + E_m d^4\} \tag{4.13}$$

The first part of Equation 4.13 shows the energy consumed to receive messages from the remaining (n/c -g) nodes which is not a part of the cluster head-set. The second part of Equation 4.13 shows the energy consumed to transmit a message to the distant sink. The energy, $E_{CH/frame}$, consumed by a non-cluster head node to transmit the sensor data to the gateway is given below:

$$E_{non-CH-frame} = \{E_e + E_s d^2\} \tag{4.14}$$

For circular clusters with a uniform distribution of sensor nodes and a network diameter of M, the average value of d^2 is, given , as: $E[d^2] = (M^2/ \Pi\ 2\ c)$ Equation 4.14 can be simplified as follows:

$$E_{non-CH-frame} = \{E_e + E_s * (M^2/(2\Pi c))\} \tag{4.15}$$

4.4.4 Start Energy for One Round

There are c clusters and n nodes. In only first iteration (in our algorithm we assume that cluster head is permanently selected once at the time of first iteration), g nodes are elected as a cluster head for each cluster. Iteration consists of an election phase and a data transfer phase. The energy consumed in one iteration of cluster is as follows:

The start energy, E_{start}, is energy of a sensor node at the initial start time. An estimation of Estart is given below:

$$E_Start = E_{CH-node} + (n + cg - 1)E_{non-CH-node} \tag{4.16}$$

Thus total Energy consume in one iteration

$$E_{Total} = \{(E_{CH-elec} + E_{non-CH-elec})/g\} + \{(E_{CH-frame} + E_{non-CH-frame})/g\} \tag{4.17}$$

Using Equation 4.17, residual energy can be given as below:

$$E_{Residual} = E_{Start} - E_{Total} \tag{4.18}$$

4.4.5 Simulation of Energy Model

Sample parameter values of the radio communication model used in our quantitative analysis. Where Energy consumed by the amplifier to transmit at a single-hop E_s =10 pJ/bit/m^2, Energy consumed by the amplifier to transmit at a multi-hop E_m =0.0013 pJ/bit/m^4, Energy consumed in the electronics circuit to transmit or receive the signal E_e=5 nJ/bit, the number of nodes n=10 the start energy E_{start}=500nj/bit distance d=5m ,number of cluster c=2 ,elected gateway g=2 and diameter M =10m.

Analysis Results: Total energy consumption in first iteration E_{Total} = 35.612 nj/bit Thus Residual energy is $E_{Resudial}$=464.39 nj/bit

Energy model is ON. Transmit power, Receive power, Idle power, Sleep power, Transition power, Initial energy, Transmission range and Receiving threshold value of antenna is set accordingly. All other parameter taken default value.

set val(energymodel)	Energy model ; # Energy model is on
set val(initial energy)	100 ; # initial energy in joules
set val (rx power)	35.28e-3 ; # receiving power
set val(tx power)	31.32e-3 ; #transmit power
set val (idelpower)	712e-6 ;# idel power
set val(sleep power)	144e-9 ;#sleep power
Phy/WirelessPhy set CSThresh_$dist	(40m)
Phy/WirelessPhy set RXThresh_ $dist	(40m)
$cbr set random	false

Table 4.5: Ns2 commands for energy model

Channel Type	Wireless channel
Propagation Model	Two Ray Ground
MAC Type	802.11
Network Interface Type	Phy/WirelessPhy
Interface Queue Type	Queue/DropTail/PriQueue
Antenna Model	Antenna/OmniAntenna
Routing Protocol	AODV
Simulation Time	80 sec
Parameters set for data transfer are:	
Transmission rate	2.0 packets / sec
Cluster-head	2 gateway nodes with UDP agent attached
Source node	8 sensor nodes with UDP agent attached
Base station	1 sink node with UDP agent attached

Table 4.6: Ns2 Parameters for energy model

ESDRP :During simulation for ESDRP we set transmission range of 40m such that a node sends its data to its single-hop gateway node and gateway is forwarded in a multi-hop fashion. Figure 4.3 shows the data energy consumption in a cluster. When data transmitted from sensor node to gateway. Node 4, 5,6 and 7 are source nodes and gateway0 is aggregator in that cluster. Since the transmission range is set to 40m, node 4,5,6 and 7 can directly send its data to gateway0 and node 0,1,2,3, can directly send data to gateway1.so in this scenario from all sensor node to gateway communication is using a single-hop communication for reducing the energy consumption .

Conventional Protocols: In convention protocol, sensor node in a cluster sends data to its neighbor node like that data reach to the cluster head thought multi-hop communication. Due to this multi-hop communication transmitting and receiving

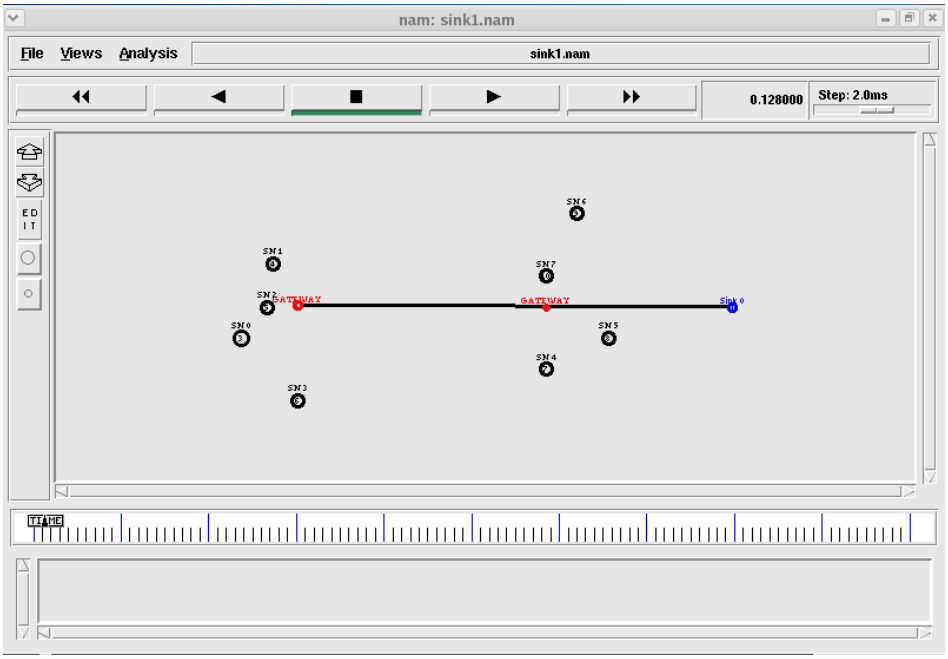

Figure 4.5: Sensor node scenario with 8 sensor nodes, 2 gateway nodes and 1 sink node

power consumption is more than 20 % increase as compare to ESDRP.

Conserving Energy: We find out residual energy of the sensor node during data communication, which is defined as the remaining energy of a node and considered that as the metric to prove energy efficiency of our proposed protocol. We used this metric to show the impact of transmission power on energy reduction. This shows the benefit of sending data in a single-hop fashion towards cluster-head. Analysis result shows that in ESDRP, after first iteration energy consumption will be decrease unlike conventional protocol; due to static cluster head (gateway) concept and single-hop communication from sensor nodes to gateway node .while gateway node is resource rich, so energy consumption at gateway is manageable. Thus no need to cluster election phase in subsequent iterations. Figure 4.6 shows the significant reduction in energy consumption by using ESDRP when compared with conventional protocol.

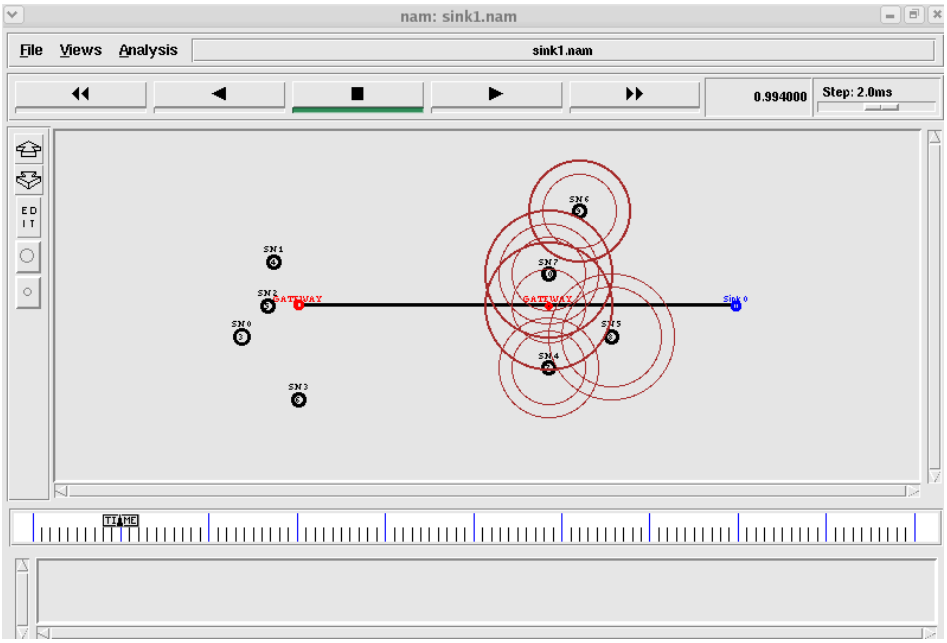

Figure 4.6: Shows energy consumption during data communication with in a cluster

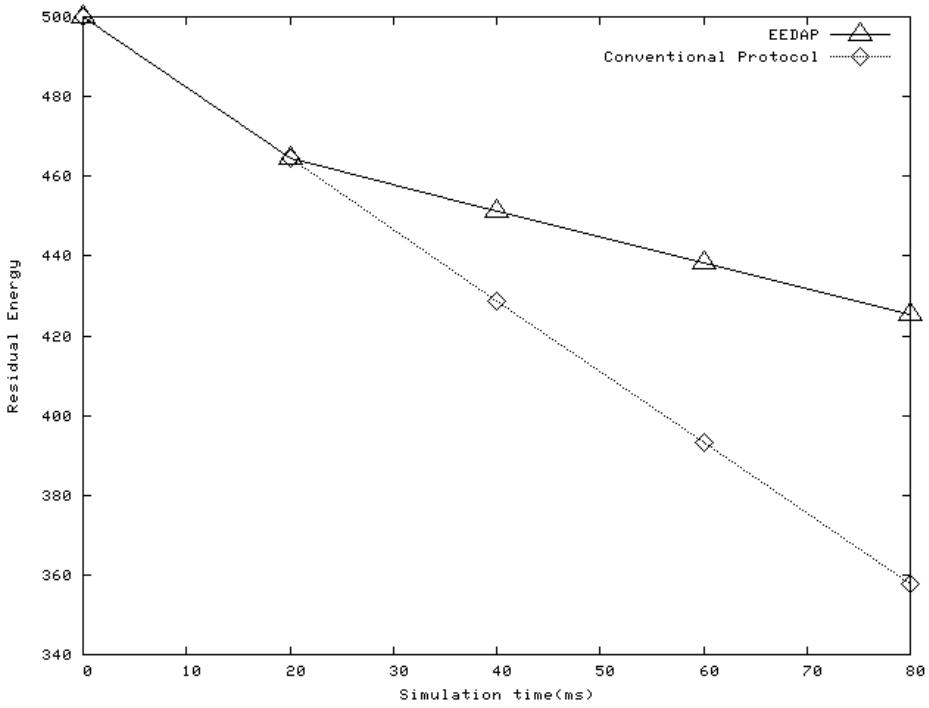

Figure 4.7: Residual energy of source as a function of time

Chapter 5

Conclusion and Future Work

Main Contributions

Future Work

Conclusion

Chapter 5

Conclusion and Future Work

In this thesis we design the energy efficient secure data Routing protocol (EESDRP) for energy constraints wireless Sensor Networks. Using cluster based topology and session based symmetric key cryptography. In our algorithm we provide security and energy efficiency in data routing. There exist several protocols for data routing which uses different approaches to provide energy efficient security in resource limited wireless sensor networks. In cluster-based approaches, nodes send their data to cluster-head and cluster-head then aggregate and forward the data towards sink. We exploited this approach and proposed a new protocol called Energy-efficient secure data routing protocol (EESDRP).

EESDRP use positive features of symmetric key cryptography and cluster-based methods. In EESDRP the wireless sensor network is divided in several clusters, each has a gateway node as a cluster head. During the data routing each cluster uses EESDRP to provide security and also reduce data redundancy. For secure routing sensor encrypted each packet using session key which is change after each session by the sink node. When a gateway node receives data from its different cluster nodes, it eliminates the redundancy in the data received from different nodes and then forward. The difference between EESDRP and other cluster-based approach lie upon secure communication and the reduction of transmission power of wireless sensor networks as in EESDRP a node send data directly to its cluster head instead of sending to neighbor node. The simulation result shows, in case of sending data directly to cluster-head in single-hop fashion the energy consumption is low as compared to that , when the data from source node is

send to cluster-head through neighbors nodes in a multi-hop fashion is increase transmission and receiving power.

In this thesis we have design EESDRP for wireless sensor network and compared the performance of our protocol with the existing conventional protocols.We have chosen two matrices to analyze the performances of our proposed protocol.The results of comparison have been presented in the form of graphs.

Our analysis of comparison results established that our proposed protocol is performing better than the conventional protocol.

5.1 Future work

The simulation result shows that when the data routed using EESDRP and send data directly from source node to cluster-head with enycrpyed from of packet, to maintain the secure communiction in wireless sensor networks.These are the major performance improvement factors of EESDRP.

Future work will focus on the implementation of EESDRP in NS-2 as a separate module so that it could be tested more accurately. As we have already tested the effect of secure communication and reduction of transmission power on the energy consumption and we got positive result. After implementing in NS-2, we will measure the whole network lifetime, packet delivery ratio and effect of network density. Also the effect of redundancy factor on energy consumption and overall security performance of our protocol will be measured. Enhancing EESDRP by introducing an effective key updating technique for protocol is also the part of future work.

Bibliography

[1] W. Su Y. Sankarasubramaniam E. Cayirci Akyildiz, I.F. A survey on sensor-networks. *IEEE Communications Magazine*, pages 102–114, 2002.

[2] Kumar.S.P. Chee-Yee Chong. Sensor networks: Evolution, opportunities, and challenges. *Proc IEEE*, August 2003.

[3] Ismail H. Kasimoglui Ian .F. Akyildiz. Wireless sensor and actor :research challenges. *(Elsevier) Journal*, 2(38):351–367, 2004.

[4] Sungha Pete Kim Bo-Cheng Charles Lai, David D. Hwang. Reducing radio energy consumption of key management protocols for wireless sensor networks. *ACM 1-58113-929-2/04/0008*, pages 9–11, August 2004.

[5] Sarika Agarwal Leszek Lilien Maleq Khan, Bharat Bhargava and Pankaj. Self-configuring node clusters, data aggregation, and security in microsensor networks. *Department of Management Information Systems Krannert Graduate School of Management Purdue University, West Lafayette*, (IN 47907), 2007. pankaj@mgmt.purdue.edu.

[6] Sundeep Karthikeyan Vaidynathan, Sayantan sur and Sinha. Data aggregation techniques in sensor networks. *Technical Report,OSU-CISRC-11/04-TR60*, 2004.

[7] D. Agrawal N. Shrivastava, C. Buragohain and S. Suri. Medians and beyond: new aggregation techniques for sensor networks. *Proceedings of the 2nd international conference on Embedded networked sensor systems*, pages 239–249, 2004. ACM Press.

[8] Xiuli Ren and Haibin Yu1. Security mechanisms for wireless sensor networks. *IJCSNS International Journal of Computer Science and Network Security*, VOL.6(No.3):100–107, March 2006.

[9] S. Setia S. Zhu and S. Jajodia. Leap: efficient security mechanisms for large scale distributed sensor networks. *Proceedings of the 10th ACM conference on Computer and communications security*, pages 62–72, 2003. ACM Press.

[10] J. Stankovic A. Perrig and D. Wagner. Security in wireless sensor networks.

[11] P.Nair H.Cam, S.Ozdemir and D. Muthuavinashiappan. Espda: Energy-efficient and secure pattern based data aggregation for wireless sensor networks. *Computer Communications IEEE Sensors*, 29:446–455, 2006.

[12] Jonathan Jen-Rong Chen Prasan Kumar Sahoo and Ping-Tai Sun. Efficient security mechanisms for the distributed wireless sensor networks. *Proceedings of the IEEE Third International Conference on Information Technology and Applications (ICITA'05)*, pages 0–7695–2316–1, 2005.

[13] Vijay Garg b M.S. Meitei c S. Raman c A. Kumar c N. Tewari R.K. Ghosh a, *. Ad hoc networks. pages 168–185, 2006.

[14] Wei Ding and et.al. Energy equivalence routing in wireless sensor networks.

[15] Sajid Hussain and Abdul W. Matin Jodrey. Energy efficient hierarchical cluster-based routing for wireless sensor networks. *Technical Report - TR-2005-011*, 2005. 073720m@acadiau.ca.

[16] M. Lee and V.W.S. Wong. An energy-aware spanning tree algorithm for data aggregation in wireless sensor networks. *IEEE PacRrim*, August 2005.

[17] A. Chandrakasan W.R. Heinzelman and H. Balakrishnan. Energy-efficient communication protocol for wireless microsensor network. *IEEE Proceedings of the Hawaii International Conference on System Sciences*, pages 1–10, January 2000.

[18] Debao Xiao Meijuan Wei Ying Zhou. Secure-spin: Secure sensor protocol for information via negotiation for wireless sensor networks. *Industrial Electronics and Applications, 2006 1ST IEEE Conference*, pages 1–4, May 2006.

[19] A. D. Wood and J. A. Stankovic. Denial of service in sensor networks. computer. 35(10):54–60, 2002.

[20] D. Song J. Newsome, E. Shi and A. Perrig. The sybil attack in sensor networks analysis and defenses. *In Proceedings of the third international symposium on Information processing in sensor networks*, pages 259–268, 2004. ACM Press.

[21] C. Karlof and D. Wagner. Secure routing in wireless sensor networks: Attacks and countermeasures. *Elsevier's AdHoc Networks Journal, Special Issue on Sensor Network Applications and Protocols*, 1(2-3):293–315, SEptember 2003.

[22] H. Chan and A. Perrig. Security and privacy in sensor networks. *IEEE Computer Magazine*, pages 103–105, 2003.

[23] Sanjay Burman. Cryptography and security - future challenges and issues. *Invited Talk, in proc. of ADCOM*, 2007.

[24] Samir Alan Price, Kristie Kosaka. A secure key management scheme for sensor networks. *Proceedings of the Tenth Americas Conference on Information Systems, New York*, 41, August 2004.

[25] Mustafa C Gaurav Jolly. A low-energy key management protocol for wireless sensor networks. *Proceedings of the Eighth IEEE International Symposium on Computers and Communication (ISCC'03)*, pages 1530–1546, 2003.

[26] Martina Zitterbart Erik-Oliver Bla. An efficient key establishment scheme for secure aggregating sensor networks. *ASIACCS'06*, pages 233–241, March 2006. ACM 1-59593-272-0/06/0003.

[27] Hatem Mohamed Abdul Kader Diaa Salama Abdul. Elminaam and Mohie Mohamed Hadhoud. Performance evaluation of symmetric encryption

algorithms. *IJCSNS International Journal of Computer Science and Network Security*, 8(12), December 2008.

[28] Devasenapathy Muthuavinashiappan Hasan am, Suat zdemir1 and Prashant Nair. Energy efficient security protocol for wireless sensor networks. *IEEE*, pages 0–7803–7954, March 2003.

[29] H. Chan and A. Perrig. Pike: Peer intermediaries for key establishment in sensor networks. *In IEEE Infocom*, 2005.

[30] D. Liu and P. Ning. Multilevel. ?tesla: Broadcast authentication for distributed sensor networks. trans. on embedded computing sys. *IEEE Concurrency*, 3(4):800–836, 2004.

[31] D. Song B. Przydatek and A. Perrig. Sia. Secure information aggregation in sensor networks. *Proceedings of the IEEE Conference on Measuring and Modeling of Computer Systems*, 2003.

[32] Matt Blaze. Cryptography policy and the information economy. *AT and T labs-Research*, DEcember 1996. mab@research.att.com.

[33] Bruce Schneier. The blowfish encryption algorithm retrieved. *http://www.schneier.com/blowfish.html*, October 2008.

[34] A.A. Tamimi. "performance analysis of data encryption algorithms. *www.cs.wustl.edu*, October 2008.

[35] N. El-Fishawy. Quality of encryption measurement of bitmap images with rc6, mrc6, and rijndael block cipher algorithms. *International Journal of Network Security*, pages 241–251, November 2007.

[36] S.Hirani. "energy consumption of encryption schemes in wireless devices thesis. *university of Pittsburgh*, October 2008. portal.acm.org/citation.cfm?id=383768.

[37] Xiaojun Cao Fei Hu. Security in wireless actor and sensor networks(wasn) :towards a hierarchical re-keying design. *Proceeding of the IEEE International Conference on Information Technology*, pages 0–7695–2315, 2005.

[38] Xiaojiang Du. Security in wireless sensor networks.

[39] The network simulator ns-2. *http://www.isi.edu/nsnam/ns/*, January 2008.

Dissemination of Work

- Shriram Sharma ,A.K.Turuk "Energy-efficient secure data aggregation mechanism for wireless sensor networks ",*International Conference on International Conference on Emerging and Futuristic System and Technologies (ICE-FST'09)*,pages 83-87, 09th April to 11th April 2009

- Shriram Sharma, A.K. Turuk "Security in wireless Sensor and Actor classifier network ", *All India Conference on Recent Innovation in Computer Science and Engineering (AICON - 09)*, 15-22, February 2009.