Mobile Agent Based Hierarchical Intrusion Detection System in Wireless Sensor Networks

Developed by:

Surraya Khanum 353-FBAS/MSCS/F07

Supervised by:

Muneera Bano
Khalid Hussain

Department of Computer Science
Faculty of Basic and Applied Sciences
International Islamic University Islamabad
(2011)

International Islamic University Islamabad
Department of Computer Science

Date: 19th February, 2011

Final Approval

This is to certify that we have read the thesis submitted by **Surraya Khanum, 353-FBAS/MSCS/F07348.** It is our judgment that this thesis is of sufficient standard to warrant its acceptance by International Islamic University, Islamabad for the degree of **Master of Science in Computer Science.**

Committee:

External Examiner:

Dr. Abdul Sattar
Former D.G, Pakistan Computer Bureau,
House # 143, St. # 60,
I-8/3, Islamabad,
Ph: 051-4446163

Internal Examiner:

Dr. Muhammad Sher,
Professor / Chairman, DCS, FBAS, IIUI

Supervisor:

Ms. Muneera Bano,
Assistant Professor
International Islamic University Islamabad

Co-Supervisor:
Mr. Khalid Hussain,
Assistant Professor,
Riphah International University, I-14, Islamabad

22.3.11

DEDICATION

Dedicated to

My Husband, Parents and Family

A dissertation Submitted To

Department of Computer Science,

Faculty of Basic and Applied Sciences,

International Islamic University, Islamabad

As a Partial Fulfilment of the Requirement for the Award of the Degree of *Master of Science in Computer Science.*

Declaration

I hereby declare that this Thesis ***"Mobile Agent Based Hierarchical Intrusion Detection System in Wireless Sensor Networks"*** neither as a whole nor as a part has been copied out from any source. It is further declared that I have done this research with the accompanied report entirely on the basis of my personal efforts, under the proficient guidance of my teachers especially my supervisor *Miss Muneera Bano and Mr. Khalid Hussian*. If any part of the system is proved to be copied out from any source or found to be reproduction of any project from any of the training institute or educational institutions, I shall stand by the consequences.

Surraya Khanum

353-FBAS/MSCS/F07

Acknowledgement

First of all I am obliged to Allah Almighty the Merciful, the Beneficent and the source of all Knowledge, for granting me the courage and knowledge to complete this research work. I simply have no words at command to express my heart felt gratitude and immense thanks to the Allah Almighty that has helped me in completion of this research work at every stage. Then I pay special tribute to the Holy Prophet (PBUH).

The very special thanks go to my parents especially my father ***Mr. Iqbal Ahemd*** and my husband ***Mr. Muhmmad Usman*** for their heart felt prayers and moral support which is sacrificed for me so that I might be entirely free to devote myself to studies. They always encouraged me whenever I was demoralized during my academic career.

I have left no stone unturned to overcome all the important aspects of this research work. I pray to God Almighty to give success to me in this research work as well as all the other spheres of life (Aamin).

Like others, at the beginning my research work I was feeling much hesitation. I really thought that I would have to face a lot of hardship in attaining the required results and I had to face all that, but with the kind and compassionate guidance of my respected research supervisors and my husband, I was able to accomplish the task.

My special thanks and prayers are all for my teachers and my class fellows for their cooperation and healthy suggestions throughout my academic period at International Islamic University, Islamabad.

Surraya Khanum
353-FBAS/MSCS/F07

Project In Brief

Project Title:	Mobile Agent Based Hierarchical Intrusion Detection System in Wireless Sensor Networks
Undertaken By:	Surraya Khanum 353-FBAS/MSCS/F07
Supervised By:	Muneera Bano and Khalid Hussain
Start Date:	1st of January, 2010
Completion Date:	19th of February, 2011
Tools & Technologies	Omnet ++
Documentation Tools	Microsoft Word Microsoft Visio Microsoft Excel
Operating System:	Windows Vista Home Edition
System Used:	Pentium 4 Intel Core Duo CPU Memory 2.00 GB 32-bit Operating System

Abstract

Wireless Sensor Network (WSN) is usually deployed in a hostile and uncontrollable environment. The WSN is vulnerable to security threats due to its hostile nature. There are several security techniques in order to make WSN secure. These techniques are authentication, encryption keys, firewalls etc. All these techniques are static in nature and provide security from external threats. These techniques do not provide strong security mechanism because of limited energy resources of WSN. There is a need of dynamic, real time and energy efficient security mechanism for WSN. The real time security mechanisms are energy and time consuming. Furthermore, in existing literature there seems an inverse relationship between better security and efficient resource utilization of WSN i.e. if we increase security we have to compromise on efficient resource consumption and vice versa.

Our proposed idea presents a dynamic, real time and energy efficient Intrusion Detection System (IDS) for WSN which provides better security by using network resources optimally. We have presented a model that uses hierarchical IDS, Mobile Agents (MA) and Cluster Head (CH) for WSN. The MA uses two levels of IDS for WSN. Our proposed methodology reduces the workload on CH, provides better security and eliminates the need of installation of Local Intrusion Detection System (LIDS) on every node in WSN.

Table of Contents

Chapter 7: Conclusion and Outlook

Chapter 1

INTRODUCTION

Wireless Sensor Network (WSN) is an emerging technology [1,2]. The WSN is usually deployed in a critical environment where the human labours are usually not involved. The popular applications of WSN are fire response, traffic monitoring, military command etc. [1,2,3,4]. In section 1.1 of this chapter, we have discussed the motivation and challenges which are being faced by the WSN. The background of the related technology is illustrated in section 1.2. The research / problem domain is identified in section 1.3. Section 1.4 highlights our proposed scheme. Thesis outline is described in section 1.5.

1.1. Motivations and Challenges

Wireless Sensor Networks (WSN) is gaining popularity for their potential usage in safety critical system, military defensive system, scientific and real time application [1, 2]. Our target is to protect WSN against the malicious and harmful activities so that they will be easily deployed in commercial and public areas. Without an adequate security mechanism, the network information can be damaged or stolen by an unauthenticated and/or unauthorized personnel. The major challenge in WSN is to provide an adequate security mechanism by keeping in mind the resource restricted nature of this network. The foremost challenge is "How to provide an adequate security mechanism by using WSN resources optimally".

1.2. Background

In this section, we have discussed the background of WSN. This section is organized as; the architecture of WSN is illustrated in section 1.2.1. The hardware components of sensor node are highlighted in section 1.2.2. The communication structure of WSN is discussed in section 1.2.3. Section 1.2.4 describes the topology of WSN. The security related issues and limitations are discussed in section 1.2.5 and 1.2.6 respectively.

1.2.1 Architecture of WSN

Wireless Sensor Network (WSN) is an emerging technology [1, 2]. The WSN is setup in a hostile environment where the human efforts are not taken into account. The major components of sensor networks are sensor node, sink / Cluster Head (CH), sensor field and user/task manager as shown in the Fig.1 [1]. The function of a sensor node is to extract data and send the routing information back to the sink. The sink node / CH is a special type of sensor node with the specific tasks of receiving, processing and storing data collected from the neighbour sensor nodes. Its duty is to reduce the total communication cost.

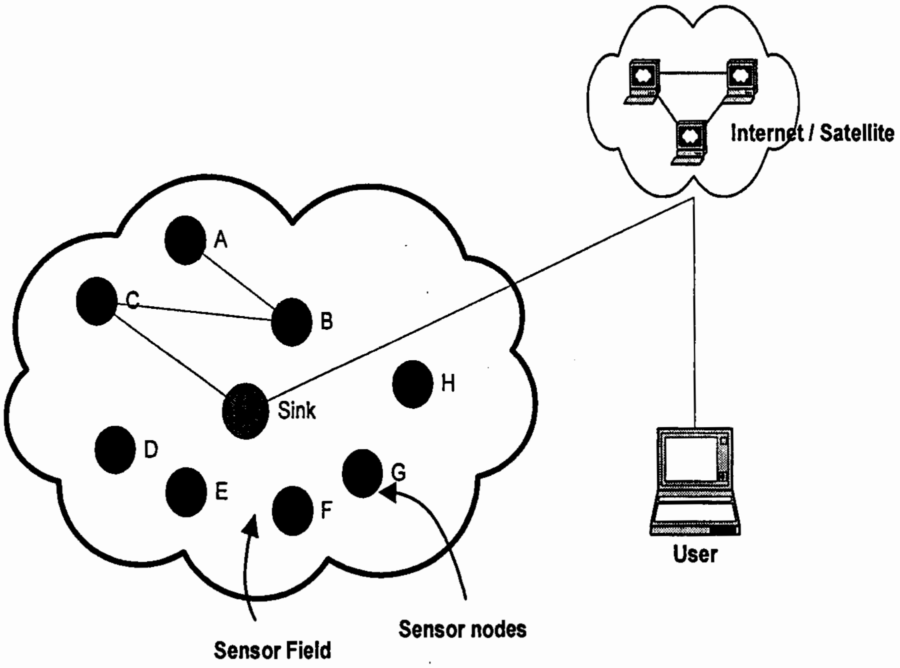


Fig 1: Architecture of Wireless Sensor Network [1]

The sensor nodes deployed over a certain geographical area that makes a sensor field [1]. The user/task manager has the centralized control over the network and can also serve as a gateway to the other networks. Their responsibilities are to gather information from the sensor nodes and transfer control information back into the network. Mainly all information is broadcast inside the network. To communicate with each other sensor nodes uses wireless media i.e. infrared, radio, optical media or Bluetooth.

1.2.2 Hardware component of WSN with their functionality

A sensor node is composed of four basic components that are sensing unit, processing unit, radio transceiver and power unit as shown in Fig.2 [5]. The power unit determines the lifetime of the sensor node therefore it is the most essential part of the sensor node. The sensors measure the analog signal and digitalize them via an Analog to Digital Converter (ADC) component. These signals are transferred to the processing unit. The processing and storage component controls the sensing functions between the sensor nodes. The transceiver acts as the communication medium and connects the nodes with the network. Three additional components are added in the hardware of sensor nodes. They are Global Positioning System (GPS), mobilizer and power generator. The GPS is a system for finding the location of sensor nodes deployed over a certain region. The mobilizer component is required to move the sensor node over a certain position related to a specific application. Power generators are the additional batteries supplied to the sensor nodes to enhance there lifetime. The battery provides source of energy to the sensor node to perform its tasks.

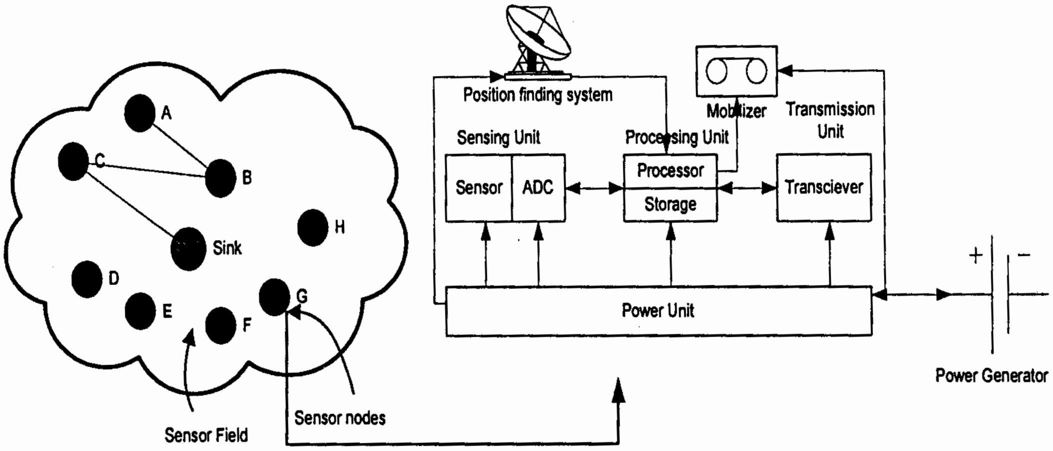


Fig 2: Sensor Node Hardware Component [5]

1.2.3 Communication Structure of WSN

In order to know about the communication structure of WSN, we have consulted F. L. LEWIS [6]. In this research article, the author has explained the architecture of WSN which is responsible for periodically sensing its environment and report to the central decision making authority as shown in Fig.3 [6]. The sensor network is divided into two networks i.e. data acquisition and data distribution networks. A data acquisition network continuously monitors its desire tasks and report to the Base Station (BS) through wireless connection. This information is forwarded to the distribution networks for analysis and decision making activities.

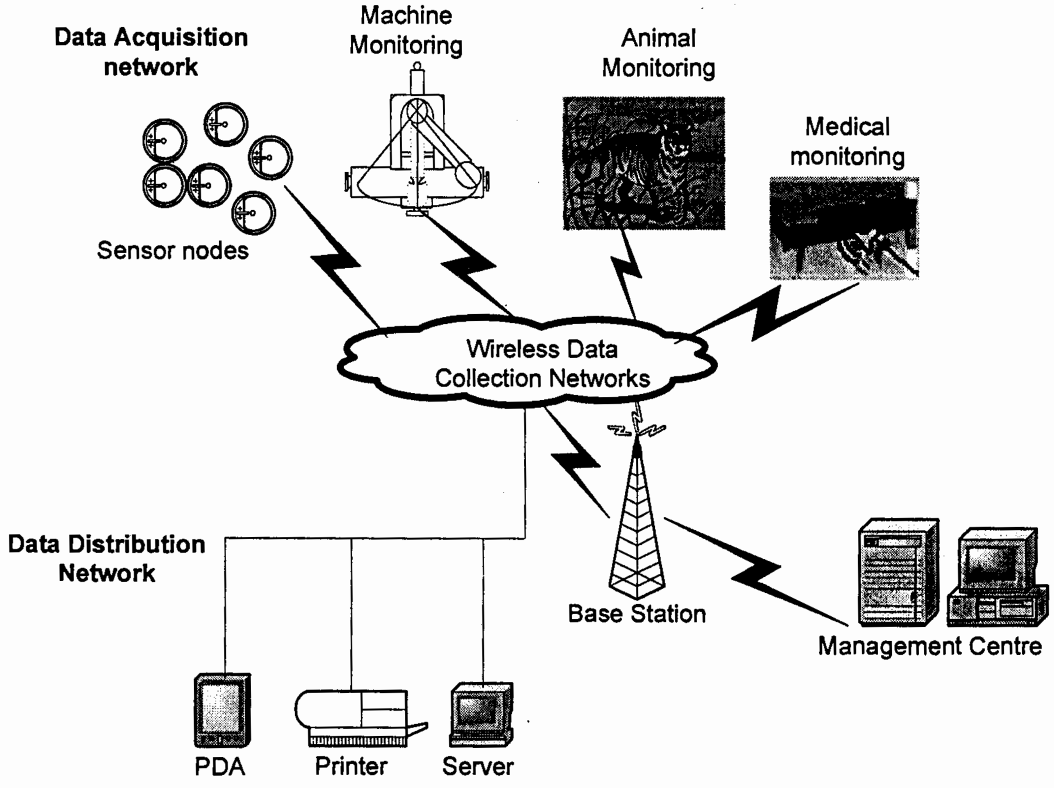


Fig 3: Communication Structure of Wireless Sensor Network [6]

Siddharth Ramesh [7] discussed that WSN is setup on critical application where regular networks are hard to deploy such as in tough terrain, climate and other environmental constraints. These networks are robust in nature because the individual node failure will not bring the whole network down. Therefore, they are more suitable for deploying in such critical areas. The sensors applications are divided into two main categories: data gathering and tracking. In data gathering, the sensor nodes measure the value periodically and send to the sink node for processing, whereas the tracking application continuously monitors the signal and identifies the presence of malicious node in its environment. The WSN have lack of common framework with no standardization in protocol used for communication. There is no interoperability mechanism that exists between two components of sensor nodes developed by different companies [7].

1.2.4 Topology of WSN

The article [8] described that WSN is an autonomous network that monitors physical and environmental situations. A gateway incorporates WSN to the other wired/wireless networks. They are usually deployed for monitoring critical applications such as structural monitoring for buildings and bridges, industrial machine monitoring, process monitoring, asset tracking etc. Three types of network topologies are used in WSN i.e. star, cluster tree and mesh network. In star topology, each sensor is directly connected to gateway. The cluster forms a tree structure and the higher node is connected to the gateway. The data flows from lower level of node to the higher level. The mesh network connects each node directly to multiple nodes in the network as shown in Fig.4 [8].

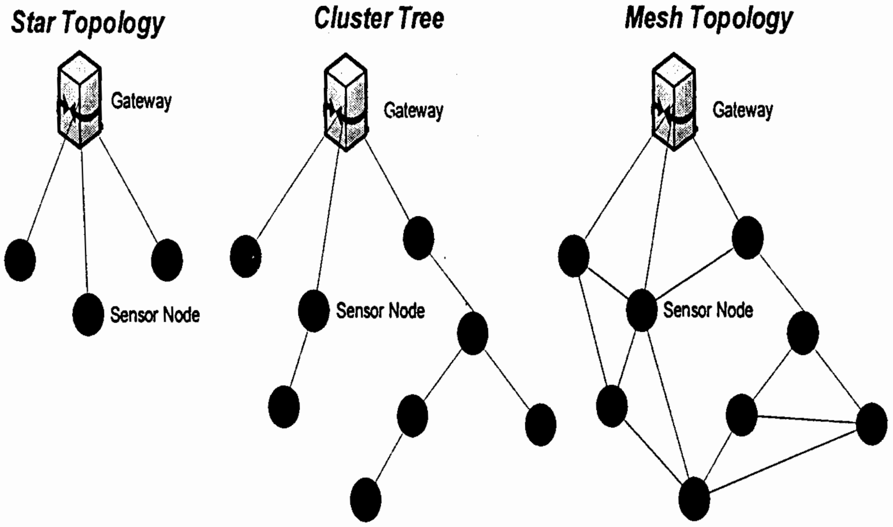
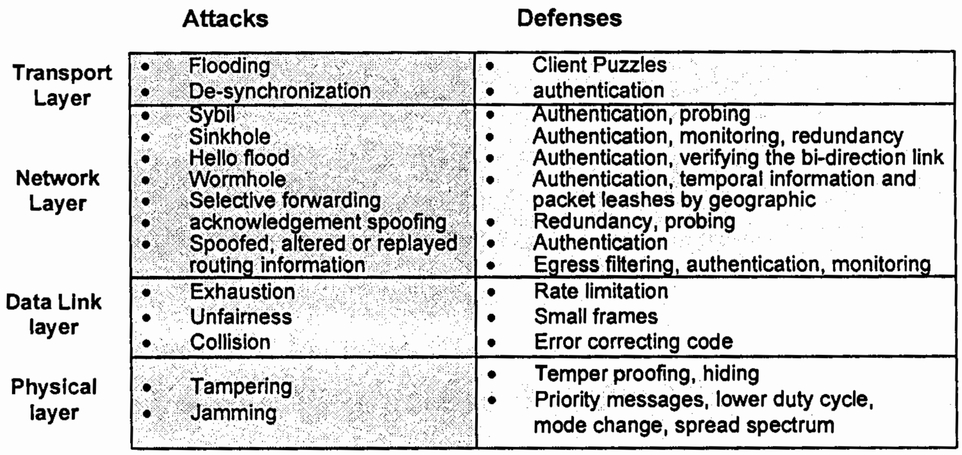


Fig 4: Topologies of Sensor Node [8]

1.2.5 Security in WSN

Sensor nodes are deployed in critical applications so they are vulnerable to various types of attacks [9]. Theses attacks can be categorized as, attacks on secrecy and authentication, stealthy attacks against service integrity and attacks on network availability. Authenticated attacks can be avoided by using cryptographic functions to avoid external attacks i.e. modification, spoofing, eavesdropping and packet replay attacks. The network accepts incorrect data value in a stealthy attack. Denial of Service (DoS) attacks makes the network service unavailable and brings the whole network down. DoS attacks may damage the real-time application i.e. health and safety that cause the serious problem. DoS vulnerabilities can may affect on each layer of sensor node architecture as shown in Table 1. [8].

Table 1: Security attacks and defences in WSN [8]



	Attacks	Defenses
Transport Layer	• Flooding • De-synchronization	• Client Puzzles • authentication
Network Layer	• Sybil • Sinkhole • Hello flood • Wormhole • Selective forwarding • acknowledgement spoofing • Spoofed, altered or replayed routing information	• Authentication, probing • Authentication, monitoring, redundancy • Authentication, verifying the bi-direction link • Authentication, temporal information and packet leashes by geographic • Redundancy, probing • Authentication • Egress filtering, authentication, monitoring
Data Link layer	• Exhaustion • Unfairness • Collision	• Rate limitation • Small frames • Error correcting code
Physical layer	• Tampering • Jamming	• Temper proofing, hiding • Priority messages, lower duty cycle, mode change, spread spectrum

The ***Physical Layer*** performs function like data encryption, frequency selection, modulation, signals detection and carrier frequency generation. General attacks on physical layers are jamming and tampering. The jamming attack deals with the radio frequencies the nodes use for communication. The temporary countermeasure is to involve variation in spread spectrum while communication or use code spreading technique. The code spreading techniques require design complexity and overhead on energy resource that makes sensor node highly vulnerable to jamming attacks. In the tampering attack, the attackers can have control over the network and replace the entire node. A solution is to provide the tamper resistant packages.

The ***Data Link Layer*** provides reliable point to multi hop and P2P delivery of messages. Major tasks are data stream multiplexing, error control and detection of data frames. Exhaustion, unfairness and collision are the major attacks on this layer. Repeated and retransmission causes the exhaustion of battery. The time division multiplexing is a better policy for this type of attack. Another defence against exhaustion attacks is to restrict the Media Access Control (MAC) layer for responding excessive requests. The loss or delayed of real time deadlines provides unfairness in the transmission. The use of small data frame lessens the effect of unfairness during transmission. When more than one sensor node tries to send messages at the same time using the shared media the collision takes' place. There is no clear and complete defence against this attack. Temporary solution is to use error correcting codes that add communication and processing overhead.

The ***Network Link Layer*** selects the efficient path from source to destination. The attacks in the network layer include Sybil, Sinkhole, Hello flood, Wormhole, Selective forwarding, Acknowledgement spoofing and spoofed altered or replayed routing information. In Sybil attack a node shows more than one identity misleading the network. Authentication and probing is a temporary defence against this attack but an algorithm is needed to conclude the redundancy identities. In sinkhole attack a compromised node aims to forge the routing information and mislead the routing tables. Authentication, monitoring and redundancy may provide temporary defence against this attack as research is still being conducted in this area. In the Hello flood the sender sends a packet in its radio range and assumes to communicate with its neighbour node. The attacker use high power transmitter to become the legitimate neighbour of the targeting node. Authentication and verifying the bi-directional link helps in defending this attack. The traffic flows between some portions of the network closely related to sinkhole attack. Two types of leashes were presented for defending wormhole attack: temporal and geographic for detecting and defending wormhole attack. The attackers in selective forwarding simply forward certain packets and drop others. Multiple paths will be chosen to route a packet from sender to destination. Another solution is to detect the malicious node and find an alternative path to route a packet. In acknowledgement spoofing the attacker spoof the acknowledgement of the packets and provides bogus information to the sender node. The attacker disturbs the network traffic by altering, replayed or spoofing the routing packets. The defence against these types is to attack is to append Message Authentication Code (MAC) or counter/timestamps with the data packets.

The ***Transport Layer*** offers functionalities i.e. error control, performance of initial and collision avoidance back-off, link level acknowledgement, time stamping, power management and retransmission. Flooding and de-synchronization are the attacks considered in this layer. The flooding attack the attacker sends many requests for connection establishment they just want to acquire the resources of the system. The counter measure against this type of attack is to use client puzzle game. In de-synchronization attack the sequence number of messages and control flags are usually modified. Authentication of control fields and packets is used to prevent this type of attack.

The security requirement includes authentication, authorization, confidentiality, integrity, availability, non-repudiation and freshness. In order to minimize the potential attacks on WSN, there are two types of defensive approaches: static and dynamic [9]. The static defensive approach provides security from external threats only and called as the first line of defence. The key establishment and management protocols are common examples of static technique. A key is established and exchange between all sensor nodes for secure communication. These protocols are trusted-server therefore it is not feasible for deployment in critical and hostile environment. One popular example of key establishment is a public key cryptography. This approach becomes too expensive in terms of memory and computation power as the size of the key increases. A single key cryptography is unsuitable, as the compromise of one node will compromise the whole network. A Pair wise key cryptography is another defensive counter measure against the security threat. However, establishing pair wise keys between each pair of nodes are impractical. This scheme requires storing (n-1) keys for each node in which most of the keys are unusable for communication. The addition/ deletion or re-keying of keys between each pair of sensor node are complex in nature. In addition, an eavesdropper performs traffic analysis to decrypt the encryption keys and stole the sensitive information. The Fig.5 [9] shows the division of security techniques among protection.

The key establishment and management are prevention based approaches. Encryption, firewalls, authentication and biometrics protect the system against the external threats only [9]. If an authenticated node inside the network is compromised, the whole security of the system is compromised. These protected based scheme doesn't helps in identifying the intruder activities and therefore insufficient to secure a system.

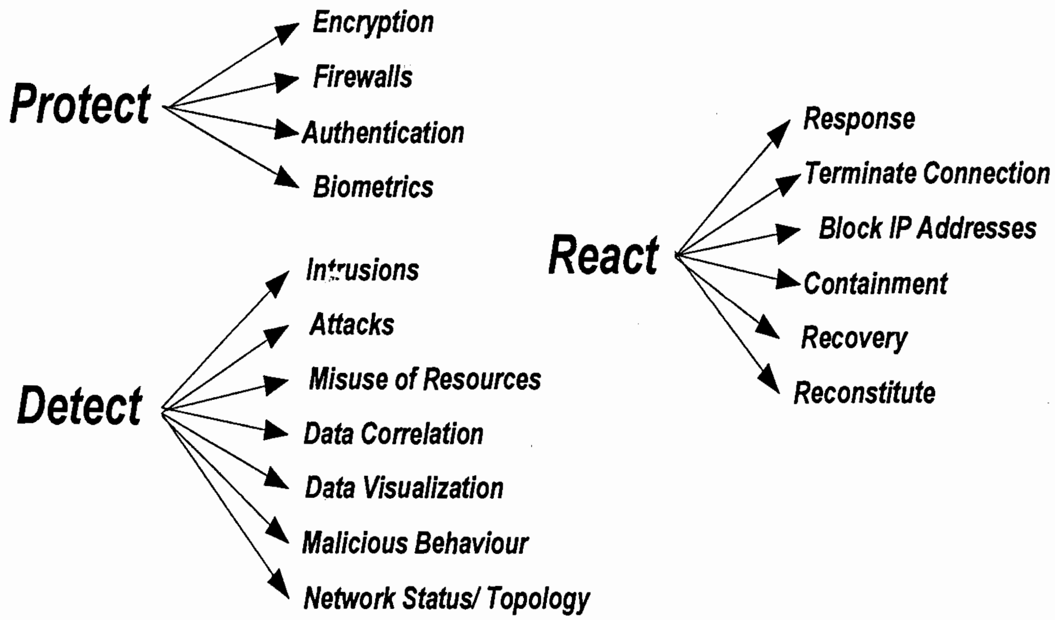


Fig 5: Division of security techniques among protection [9]

To protect the system against internal and external threats, there exist some detection and reaction schemes. These schemes are dynamic defensive in nature and called as the second line of defence. They not only help in identifying the intrusion and malicious activities but also take appropriate actions on those intrusions. The detection techniques discover intrusion, attacks, misuse of resources, data correlation, data visualization, malicious behaviour and network status/ topology to identify the intruder activity. The reaction schemes take appropriate action i.e. response, terminate connection, block IP addresses, containment, recovery and reconstitute on those intrusion activities.

1.2.6 Limitation

Existing TCP/UDP protocols may not be the best solution for sensor networks [10]. The TCP/IP protocol does not contain the property of power management and battery dissipation issues. Therefore resource aware protocol architecture is needed for efficient communication. The sensor node usually communicate though broadcast medium that increases the risk of network congestion. The error rates in wireless network are usually high that creates reliability problems during transmission. The energy of the sensor node dissipates quickly as the communication distance between sensor node increases. Therefore, we need a sophisticated security mechanism which not only provides defence against various types of attack but also uses resources of network efficiently.

1.3. Research /Problem Domain

As discussed earlier, in order to minimize the potential attacks on WSN like any other network, there are two types of defensive approaches i.e. static and dynamic [9]. As our problem area is closely associated with these approaches so in this section we will discuss them in detail. Firewalls and encryption are common examples of static technique. They provide security from external threats only. If a node inside the network is compromised then the whole security of the system will be compromised. Therefore, there is a need for a better security mechanism that prevents the network from both internal & external threats. An Intrusion Detection System (IDS) is a dynamic monitoring system used to discover malicious and harmful activities in the network. This activity takes place both at the network and host level [1]. An IDS is usually a combination of both hardware and software.

1.3.1 Intrusion detection & Intrusion Detection System

Intrusion detection is the process of identifying, examining and observing violated activities. It discovers breach and illegal access to confidentiality, unavailability, authorization, authentication, integrity and network resources [9]. Intrusion detection performs analysis on the information stored by the resource. Therefore experience personnel are required which interpret the network traffic into valuable information. An Intrusion Detection System (IDS) is a dynamic monitoring system used to discover malicious and harmful activities in the network. This activity takes place at the Network/Host level or combination of both [1].

The network based IDS monitors the network traffic for detecting misuse pattern, whereas the host based IDS monitors the node processes for detecting malicious activities as a sign of misuse. The hybrid IDS examines both the network traffic as well as the host processes. Intrusion detection concept comprises of anomaly detection, misuse detection, burglar alarms, honey pots and hybrids. The anomaly and misuse IDS are the major intrusion detection techniques. The anomaly detection technique generates a profile that contains the nodes normal activities. The deviation from the norm profile consider as a malicious activity. The major drawback of this technique is that all anomalies are treated as an attack and alarm is generated frequently. Misuse detection technique stores signature of known attack patterns and examines the behaviour with these stored attack patterns. The attack patterns include activity diagram, scenarios, events and states. This technique cannot detect unusual or novel types of intrusion which is not stored in the attack patterns. Further, an update is required to renew the attacks signature constantly.

The major components of intrusion detection model are subjects, objects, audit records, profiles, anomaly records and activity rules. Subject related to the initiator of the activity mainly its users. Objects are the resources and devices managed by the nodes. Audit records are generated in response to the action performed. Profiles are created on the behaviour of subject. Anomaly records the abnormal behaviour of nodes. Action rules are the type of activities that are taken when some conditions are satisfied i.e. update the profiles, generate network status, produce anomalies report and discover malicious nodes.

We surveyed the existing literature of WSN. Ian F.Akildiz et al. [11] reported a survey and highlighted communication architecture and design factors such as hardware constraints, scalability, fault tolerance, production costs, network topology and power consumption. They discussed that existing security schemes are not well protected against threats activities. Therefore there is a need for a strong security mechanism that best fit in WSN environment. Similarly I.F. Akyildiz et al. [12] conducted a survey that illustrates the sensor networks characteristics, critical applications and challenges WSN facing. They outline communication architecture and factors of WSN that influence the performance of sensor nodes.

Another concise survey is reported by Mona Sharifnejad et al. [13] in which the authors outlined that the WSN is usually setup in critical places so research must be focused on how to secure these networks before deployment. The authors argued that traditional security schemes like encryption and firewalls are not suitable for these types of networks. Researchers had tried to build a trust model for making WSN more secure. The authors further discussed various security requirements i.e. data authentication, confidentiality, integrity, freshness, self organization, availability, time synchronization, secure localization, scalability, availability, accessibility and flexibility. They also examined different types of security attacks such as Sybil, DoS, physical, node replication, privacy, volition and traffic analysis. The authors provided basic guidelines and defensive measures against these types of attacks.

1.4. Proposed Approach

In existing literature, there exist several mechanisms in which IDS are deployed on WSN. However, there seems a trade-off among strong security mechanism and efficient resource utilization of sensor networks. That is, if we increase network security we have to compromise on efficient resource consumption and vice versa. Therefore, we need a more sophisticated security mechanism in WSN, which provides strong network security by utilizing minimum resources of sensor network. In order to tackle this issue, we have proposed a Mobile Agent Based Hierarchical Intrusion Detection System (MABHIDS).

In our proposed scheme, the IDS work both as Network Intrusion Detection System (NIDS) and Local Intrusion Detection System (LIDS). The initial intrusion detection is performed by NIDS which detects the normal rate of packet arrival and departure. In case of deviation the Cluster Head (CH) triggers the mobile Analyzer Agent (AA) over the link where deviation has occurred. Then AA will visit the suspicious node and act as a Local Intrusion Detector (LID) over there. Then AA will use the resources of suspicious node to investigate its behaviour further. If suspicious node is found as a victim then AA will update CH. Then CH inform its sub agents i.e. Coordinating Agent (CA) and Management Agent (MA) which will take appropriate action to prevent rest of the network from intrusion either by minimizing the communication with the victim node, reducing the trust value on the victim node or by cutting its communication from rest of the network. Otherwise, the AA informs the CH that the suspicious node is not the victim; it is a safe node and unusual but harmless activity has taken place. Our proposed scheme performs two levels of intrusion detection by utilizing minimum possible network resources. The proposed scheme eliminates the cost of installing IDS module on each sensor node as we simply send a copy to the victim node for detecting malicious activity. That enhances network lifetime by reducing the work load on Cluster Head (CH) and provides enhanced security in WSN.

1.5. Thesis Outline

In chapter 2, we have discussed the related work in detail. We have also discussed the limitations of the existing literature in that chapter. In chapter 3, we have performed a requirement analysis of the proposed solution. We have also explored in depth detail of the problem domain. In Chapter 4, the proposed scheme is discussed in detail. Implementation detail is given in chapter 5. Chapter 6 includes testing and performance evaluation and chapter 7 concludes the overall outlook of our research work.

Chapter 2

LITERATURE SURVEY

In this chapter, we have discussed the survey of existing literature related to the security of WSN. We have performed a broad, in-depth and a critical survey in order to identify the problem in existing literature. This chapter is comprises of three sections. In section 2.1, we have discussed related research / technologies, in section 2.2 we have discussed the limitations of existing technologies / schemes. In section 2.3, the concluding remarks are given in the form of summary.

2.1 Related Research/Technologies

We have divided this section into three subsections i.e. security issues in WSN, different security mechanisms in WSN and applying IDS to WSN. In these subsections, we have critically reviewed the existing literature and highlighted the problems that exist in the available literature.

2.1.1 Security issues in WSN

During literature survey, primarily we reviewed the research articles in which security related issues of WSN are discussed. WSN application and its challenges are highlighted by A. Alemdar et al [14]. The authors have discussed an overview of WSN architecture, its popular applications and major hurdles faced by WSN. In this research article, various node limitation issues i.e. battery, integrated circuits, wireless communication, routing and distributed signals processing are also discussed. There are several guidelines related to security are also discussed in this article such as, the lightweight IDS provide helps in detecting DoS attacks, consumption of low energy must be keep in mind when designing the sensor nodes which enhances the network lifetime.

Tanveer Zia et al. [15] presented basic issues regarding WSN security. The authors have underlined the characteristics, architectural, network and physical limitation, confidentiality, integrity, authentication, availability, resource constraints and layer wise security issues in WSN. They classified the security attacks into classes i.e. interruption, interception, modification, fabrication. The article notifies that more research is required to make the sensor network trustful before communication.

Rodrigo Roman et al. [16] divided network infrastructure into two parts for security implementation. The two infrastructural parts of WSN are data acquisition network and data dissemination network. The data acquisition network measures the physical data from its environment and sends it to the control system. The data dissemination network is a combination of wire or wireless interface that is used for interaction. In this research paper author have discussed the security primitives, global key infrastructure, local key infrastructure, routing, data aggregation and auditory. The security primitives include Symmetric Key Encryption (SKE), Message Authentication Codes (MAC) and Public Key Cryptography (PKC) related issues. Sensor nodes are resource restricted in nature therefore efficient implementation of these primitives is needed. Global key and pair wise keys are not feasible in real time application and suffer from scalability and memory constraint issues. The key infrastructure is not enough to protect the nodes from routing attacks.

The Denial of Service (DoS) and layer wise security related problems are discussed by Anthony D. Wood et al [17]. The article describes that limited resources make encryption keys and digital signature impractical in securing WSN. Therefore, developer must take security into consideration at the design time.

The research article written by Yee Wei Law et al. [18] provides a basic guideline to protect the network from security related problems. The article notifies that WSN is an emerging technology therefore no comprehensive architecture for security is still emerged. The WSN suffer from security related problem i.e. energy efficiency, no public key cryptography, no tamper resistance and multiple layer of defence issues. To handle these challenges there must be some defensive mechanisms for host and network based perspectives.

2.1.2 Different security mechanisms in WSN

We have further surveyed different existing security mechanisms in WSN. Adrian Perrig et al. [19] presented an idea of Security Protocol for Sensor Networks (SPINS). In

SPINS, the authors have assumed that the base station is capable of storing all cryptography keys having sufficient memory and battery power. The SPINS protocol is divided into two categories: SNEP (Secure Network Encryption Protocol) and μTESLA ('micro' version of TESLA). The SNEP is used for data confidentiality, two party data authentication, integrity and freshness. μTESLA offers data broadcast for authentication. The drawback of the approach is that the overhead of energy and computation time is increases as number of messages increases during communication. Along with this drawback the authors have also not considered several issues such as information leakage or when the node is completely compromised.

Stefan Schmidt et al. [20] proposed security architecture for Mobile Wireless Sensor Nodes (MWSN) by using a cryptographic algorithm. The proposed architecture is divided into three phases. In first phase, initial key is exchanged between sensor nodes for authentication that is called as pair wise key agreement. In second phase, the key is forwarded to the cluster for broadcast. The encrypted and authenticated communication takes place in the third phase between the sensor nodes. The authors have used a Blundo-et-al-scheme, which is a pre-distribution scheme. In this scheme, every node has to maintain a shared key for all of its neighbours. Marinating all the keys are not suitable in WSN environment as the nodes are constantly joining or removing the network due to energy dissipation.

The BROSK (BROadcast Session Key) negotiation protocol for WSN is proposed by Bocheng Lai et al. [21]. It is used for broadcasting key negotiation massage to provide link dependent keys to the sensor nodes for communication. They assumed that all nodes in the network have a shared master key that should not be captured by an adversary or malicious node in the network. It is a very big assumption. If master key is compromised then WSN security will be compromised. The proposed scheme also creates a trust relationship among nodes. Initially all the nodes in the network have equal low level of trust. The authentication communication increases the trust level among nodes. Maintaining and storing all link dependent key for each node are expensive in term of memory. This scheme uses simultaneous transmission for communication that increases the rate of collision. As the node density increases the ratio of collision become high and the energy dissipate quickly. The system will become security vulnerable when a compromised node captured the master key.

The key distribution scheme using tree based approach is proposed by ErikOliver Blab et al. [22] for WSN. A scenario of sharing a key is also discussed in this research article when a new sensor node joins the network. The sink node collects data either from the sensor nodes directly or from the aggregated nodes to accomplish its task. They used aggregated node to form a tree based approach for key distribution. These nodes form a binary tree and assuming no loss of generality. When a new node joins a network, the master device or user allocates pair wise shared keys to communicate with distinct node. The proposed scheme is complex in nature and needs extra computation resources. It uses 4 symmetric encryption and 4 communication steps inside the aggregation nodes that is not feasible in WSN environment. The depth of binary tree also increases the burden on network resources.

Yang Xiao et al. [23] conducted a survey on key management schemes in WSN. The efficient key establishment technique is still a debatable issue in WSN having multiple trades off between computation, memory, resource and security. They divided key management scheme into seven categories i.e. single network wide key, pairwise key establishment, trusted base station, public key schemes, key pre-distribution scheme, dynamic key management and hierarchical key managements. The article concluded that encryptions techniques provide defensive measurement against the external threats only. The additional network resources are required as the size of the key increases. There exists no feasible key distribution technique that fits in the WSN resource constraint environment.

Rabia Riaz et al. [24] provided a framework for security with three key management schemes i.e. SACK (Symmetric Cryptography Key), SACK-P ((Symmetric Cryptography Key- Public)) and SACK-H (Symmetric Cryptography Key-Hybrid) for WSN. They evaluated these schemes on specific factors i.e. memory constraints, efficient energy utilization, communication patterns, scalability, connectivity and communication patterns. The authors have assumed that all of these schemes used hierarchical networked based model for communication. The evaluation results of the scheme shows that all three key management schemes are either secure or efficient in term of resources utilization but not both at a time.

Until now, we have discussed the static security schemes for WSN. In [19,20,21,22,23,24] we have surveyed different research papers. In these research articles, the authors have applied static defensive measures against the security attacks. All these static techniques suffer from problems i.e. computation overhead, issues related to internal threats and compromised node. The static techniques do not completely cure the system against the threat and above mentioned security problems. Therefore a dynamic approach for WSN is required which not only provides security against the internal and external threats but also discovers the compromised node and take appropriate action against it.

2.1.3 Applying IDS to WSN

In previous section, we have concluded that WSN needs a dynamic security mechanism. Intrusion Detection System (IDS) provides the dynamic security mechanism to WSN. We have surveyed several research papers in which different types of IDS architectures are installed on WSN. Let us a look at some of these techniques.

The available security models for internetworking are differentiated by Joseph G. Tront et al. [25]. Currently two types of models are used for internet security: Intrusion Prevention (IP) and Intrusion detection (ID). The IP uses authentication and firewalls for securing the boundaries of the network that are easy to penetrate. Recently attacking tools and techniques are much more sophisticated that are available for attackers, which increases the risk of threat to the Internet infrastructure. The ID uses some detection mechanism for identifying the intrusion in the network and counter measures are taken against that specific intrusion.

John McHug et al. [26] discussed the role of IIDS in organizations and offer the basic structure for IDS deployment, operation and maintenance applied to WSN. This article explained that IDS provides security to computer systems and networks from both internal and external threats.

Rodrigo Roman Jianying et al. [27] proposed a technique that observes the neighbourhood sensor node for communication that is called as spontaneous watchdog.

They assumed that the sensors are stationary and used MICA2 radio stack for energy consumption. The proposed scheme relies on broadcast communication. The nodes receive the packets and forward the packets to next-hop in order to activate the global agents for observing those packets. Only one global agent is activated per packet flowing in the network. The decision for the selection of spontaneous watchdog imposed energy overhead for activating global agent which is a major drawback of this technique. In addition, the nodes are independent which do not assure that only one global agent is activated per packet in the network.

A statistical model of intrusion detection is proposed by Ilker Onat et al. [28]. This model specifies the normal activity of each sensor node in the network. The nodes take collective actions by gathering attacks information from all its neighbouring nodes. An algorithm is used to monitor the packet power level and arrival rates for detecting the intruder activity. If the packets are consistent with the statistical of neighbour node it is assume to be a normal packet otherwise anomalous. They assumed that there exist many-to-one relationships among sensor nodes. There is no irregular node deployment; no mobility and stable path are considered. The transmission power level will not be changed during analysis. This scheme creates a trust relationship on neighbouring node which is not realistic in critical and hostile environment. The security of the system is compromised if the neighbouring node is captured and sends bogus information in the network. The sharing of intrusion information with the neighbouring nodes is security vulnerable.

Anomaly intrusion detection for Wireless Sensor Network (WSN) is presented by Vijay Bhuse et al. [29]. To detect the intrusion at physical level they use masquerade and RSSI (Received Signal Strength Indicator) values of neighbour nodes. The TDMA (Time Division Multiple Access) schedule based and sleep/wake-up based protocols are suggested at MAC layer. The IASN (Information Authentication for Sensor Networks) and ADT (Anomaly Detection Table) protocol is used at routing layer. They assumed that the adversary does not interfere at initial level and comes into play after the sensors nodes are deployed. The uses of RSSI values give large number of false positives alarms at physical layer. Keeping the track of TDMA and sleep/wake schedule at MAC layer increases the overhead on memory storage. Constructing ADTS and updating previous hop for each packet at routing layer is not energy efficient. Using masquerade at physical layer increases large number of false positives alarms. All these techniques give tight bound on the probability of false positives, false negatives and are not energy efficient for WSN.

Krontiris Ioannis et al. [30] proposed a distributed intrusion detection scheme for WSN. The IDS client is installed on each node in the network and performs three major functions i.e. network monitoring, decision making and action against the intrusion occurrence. In network monitoring each node monitor packets by collecting audit data from its neighbour. All nodes decide the threat level using their own client IDS on neighbour audit data. The threat level finding will be broadcast for making collective decision. Action responds to the threat situation carried out by each node in the network. They assume that the adversary cannot capture or introduce new nodes inside the network. The problem with this scheme is that, trusting on neighbouring node information is not realistic. Publishing each intrusion report on the link is also not energy efficient.

A decentralized IDS for detecting various kinds of attacks is introduced by Ana Paula R. da Silva et al. [31]. The proposed algorithm is divided into three phases: Data acquisition, Rule application and Intrusion detection. The filtration of messages for analysis is the responsibility of data acquisition. The processing on stored data is done by the rule application. When the raised failures increase with the expected amount of occasional failure intrusion detection is raised. The authors have considered three types of network failure and eight types of intruder attacks over the data messages. They assumed that the network topology is fixed during analysis and don't have any kind of aggregation node. The node must forward the data message with no payload alteration. They use an array to store the message captured by the data acquisition. The length of an array shows the amount of message associated to find the intruder activity. Therefore, there exists a trade-off relation between the detection efficiency and storage space. The level of intrusion detection has also an impact on buffer size. There are no aggregated nodes inside the network so every node has to send its data towards the base station which is the major drawback of this technique. That increases the overall communication cost and is not energy efficient according to the WSN environment.

Similarly, another decentralized scheme of intrusion detection is introduced by Ioannis Chatzigiannakis et al. [32] for WSN. This scheme uses four steps and additional one more request when an anomaly is detected. The neighbour node exchanges their neighbour nodes list and calculates the local maximum cluster in the first step. Nodes exchange their local cluster with each other to adjust maximum cluster in the second step. Nodes exchange updated cluster with their neighbour and draws a final cluster in the third step. In fourth step, final cluster are formed by exchange of keys with neighbour nodes. Each node executes conformity when an inconsistency is detected in the cluster. The IDS modules are places on all nodes belong to cut set. The IDS system uses network-based approach to monitor the messages between sensor nodes. These messages are analyzed by a rule-based detection method. They have assumed that the node use energy efficient path to the base station. When a malicious activity is identified all sensor nodes in the network restart from one step which is major drawback of this technique. The hierarchical routing does not use the best energy path to the base station. There is a trade off between energy efficiency and security. They do not provide any simulation result for validation.

Debao Xiao et al [33] presented self-organizing security architecture for Mobile Wireless Sensor Network (MWSN). The objective of the proposed scheme is to discover existing attack using intrusion detection and take appropriate countermeasures against them. They discussed the attacks on two layers i.e. Data Link layer and Network layer. The current attacks on data link layer are mainly on the channel access which is divided into three main groups: integration, collision and exhaustion attacks. They proposed an intrusion detection module which is composed of collision check, power check and integration check to conclude these attacks. To protect the network from external attacks the routing protocols in Network layer is categorized as sinkhole, Sybil, wormhole, selective forwarding and HELLO flood attacks. They use routing based intrusion detection architecture that is based on two parts: check artificial links and neighbourhood information for detecting these attacks. They assumed that whole network is a grid and has a fixed number of sensor nodes. The sensor node use neighbourhood node information for detecting intrusion in the network. The security of the system becomes vulnerable when the neighbourhood node will become compromised or captured by an attacker. It is also not feasible to install each of these IDS modules on each sensor node.

An energy efficient IDS for WSN is presented by Piya Techateerawat et al [34]. This article compares different approaches of intrusion detection of WSN. They investigated three strategies for the selection of intrusion detection. They are core defence, boundary defence and distributed defence. The core defence selects IDS nodes at the centre point. The boundary defence selects nodes at the boundary of the cluster. Voting algorithm is used in the distributed defence for selection of IDS node. It consists of 4 steps: vote preparation, voting, vote counting and activate IDS. Two parameters are used in this algorithm, the number of hop count and the number of hops between candidate node and itself. A simulation is also performed in order to analyze these three strategies. The distributed defence scheme become energy exhaustive as the cluster grows in size. The core defence scheme is susceptible to attacks inside the cluster. The boundary defence scheme produce large number of false negative when the cluster size increases in size. There exists a trade off between energy consumption and efficient intrusion detection system.

An agent based IDS have been proposed by Bin Dong et al. [35]. The agents used State Transition Analysis Tool (STAT) to analyze the intruder activities and update the system architecture. The intrusion detection framework is composed of five agents: pre-processing agent, reasoning agent, decision agent, update agent and communication agent. The pre-processing agent collects require data from audition record system. The reasoning agent judge the intrusion activity. If there is an occurrence of an intrusion activity the reasoning agent updates the security officer for decision. The security officer commands the update agent. Beside these agents, the framework uses additional components i.e. file base and rule base for refreshing the knowledge-base system to analyze and record the data. The communication agent provides cooperation between hosts and agents for inspecting the intrusion activity. It is not feasible to install five agents on each sensor node in the network. The knowledge base system increase load on the memory storage, energy and communication cost. There exits an inverse relationship between the memory storage and energy efficiency.

Wang Huai-bin et al. [36] proposed multi agent IDS for WSN. The IDS agents are installed on each node which comprises of four agents: sentry agent, analysis agent, response agent and management agent. The sentry agent is responsible for monitoring all activities on the node. The analysis agent is responsible to judge whether intrusion is happened or not. The response agent prevents WSN from intrusion by making decisions such as reducing level of trust of suspicious node, cutting off the communication and re-authentication. The management agent maintains and co-ordinates the sentry agent, analysis agent and response agent. In case of addition of a new node in WSN or failure of an existing node management agent will get copy of that particular agent from neighbour nodes. Obtaining copy of failure agent from neighbour node leads towards a security breach. If the neighbouring node is compromised the management agent receives the false/bogus data. It is also not feasible to install four agents on each node due to severe resource restriction of WSN.

The design and implementation of agent based IDS for WSN is presented by Dmitriy Martynov et al [37]. They discussed an assortment of security issues related to DoS attacks and designed agent-based IDS and non agent-based IDS for sensor nodes. The purpose of agent-based IDS is to cut down the communication with the suspicious node while continuing to communicate with non suspicious node. The non agent-based is responsible for detecting and viewing network status throughout the event of DoS attack. They consider IDS as firewalls where in all outgoing and incoming traffic has to pass thorough it. The receiving node blink colour light when it receives message from any node in the network. Each node sends data using three data rates slow, medium and DoS-level fast. The blinking rate of colour light shows the ratio of receiving data packets. The light blinks quickly if a sensor node is suspected for initiating the DoS attack. This information is forwarded to the processing unit for further examination. The installation of agent based and non agent based IDS on each sensor node is not resource effective.

The hybrid and cluster based IDS agents are proposed by Tran Hoang Hai et al [38]. It is used to detect both anomaly and misuse intrusion detection technique. The local and global agents are used that are installed on each sensor node in the network The local monitoring is carried out by monitor node in which pre-defined rules are stored. The monitor node captures the data packet in its radio range and stores in an intrusion buffer for analysis. The time stamp is attached with each entry stored in buffer. When an intermediate sensor node receives data packet it checks it signature list for detecting malicious node. The global agent communicates with other global agent in order to identify the anomalies and malicious node from the network. The installation of local and global IDS agents on each sensor node is not a feasible solution. The lifetime of the network reduces quickly as the workload on the intrusion detection system increased.

The selection and activation of IDS module is presented by Tran Hoang Hai et al [39]. An algorithm is used to activate the ID module on particular sensor nodes. The sensor node sends information to its neighbouring node in order to find a node that covers all nodes in the network. They assume that the adversary cannot compromise the node during deployment phase and the neighbourhood information is always trustful. That is a very big assumption. What If? When the authenticated node becomes compromised and sends bogus information inside the network. The ID module activates for specific interval of time only and conserve large amount of energy of sensor node. At the time of rotation the selection and activation of ID module again takes place.

Zhenwei Yu et al. [40] introduced framework of machine learning based IDS for WSN. They used SLIPPER algorithm to build the detection model for training data automatically. This detection agent is installed on each sensor node in the network to monitor local and packet data. It helps in identifying the malicious node. When a false alert/alarm is generated the system can tune automatically by using the SLIPPER algorithm. They assume that there exists no trusted relationship among sensor nodes so every sensor node will be equipped with an Intrusion Detection Agent (IDA). The SLIPPER algorithm learns the confidence value from its training dataset. That might not provide very highly accurate prediction on novel type of data. It is not feasible to install the intrusion detection agent on each sensor node for its severe resource constraint functionality. The article does not provide any experimental, simulation or attack model for the verification of proposed scheme.

A distributed and cluster based IDS is proposed by Gu Hsin Lai et al. [41] to defend the network against the DoS attacks. Two types of DoS attacks are considered i.e. greedy attacks and neglected attacks. The special type of node is introduced called the security guard Node (gNode).The cluster is composed of common sensor nodes and gNodes. The gNode monitors the statistical data of cluster head and Dos attack activities. When gNode detects an abnormal event it sends a warning ticket to the cluster head. The cluster head on receiving a certain rate of warning tickets from the gNode performs an action. If the compromised node is a common sensor node it ignores all the warning tickets. If the compromised node is a cluster head, then sink node sends a re-cluster command to the cluster. There is no guarantee related to the confidentiality and integrity of warning tickets generated by the gNodes. What if the cluster contains no gNodes? This method works only when there are some amounts of gNodes in the cluster.

Rung-Ching Chen et al. [42] proposed an Isolation Table for the Detection (ITID) in hierarchical WSN. They analyzed different attacks behaviour and evaluate the performance. Two CH's are used for the detection of intrusion in the proposed scheme: Primary Cluster Header (PCH) and Secondary Cluster Header (SCH). The PCH gather sensing data and isolation table from SCH and divide the duty cycle of SCH. The SCH monitor malicious node in Monitor Groups (MGs) and monitor PCH. They conduct an experiment and compare the proposed scheme with the Collaboration-based Intrusion Detection System (CIDS) and Routing Tables Intrusion Detection (RTID). To save the energy consumption they assume that the nodes are one hop to cluster header (CH). The intruder attacks the sensor node to depose CH and alter the routing information. The intruder can attack WSN easily when the number of nodes in WSN is less alive. In this case the alarm threshold will be lower and intruder capture sensor node to depose this proposed scheme. Also the whole communication will be compromised if the PCH is under attack. That is the major drawback of this scheme.

All the above cited research articles [25,26,27,28,29,30,31,32,33,34,35,36,37,38, 39,40,41,42] propose IDS techniques for WSN. These schemes provide better security as compared with the static approach and much more efficient in terms of resource. The static mechanisms provide defensive measures against the external threats only and suffering from scalability, computations overhead problem as the key size increases.

2.2 Limitations

All above cited research papers [14, 15, 16, 17, 18] have revealed that WSN need a special security mechanism due to its severe resource restricted nature. The lack of communication structure imposes additional challenges in designing a sophisticated and adequate network security mechanism for WSN. The efficient security technique is still a debatable issue in WSN having multiple trades off between computation, memory, resource and security.

The static defensive measures [19,20,21,22,23,24] do not completely cure the system against the internal and external threats. These techniques are inadequate because of different problems i.e. computation overhead, time required to decrypt the encryption keys, information leakage when a node become compromised, maintaining and storing all link dependent key for each node, simultaneous transmission of communication effect on the collision rate, stolen the master key, issues related to internal threats and compromised node. Therefore there is a need for dynamic security technique. In [25,26,27,28,29,30,31,32,33,34,35,36,37,38,39,40,41,42] research articles the authors applied different IDS techniques to prevent the system against the malicious activities. The dynamic approaches is still suffering from trust relationship issues, selection and activation of global agent one at a time, sharing of secret information with the neighbouring nodes, emphasis only on the intrusion detection schemes only not to handle those intrusions, selection of statistical techniques increases the probability of false alarm rates and issues related to the publication of intrusion report on the shared link. Moreover, these schemes require additional network resources and time consuming in nature.

2.3 Summary

We have performed wide survey in order to identify the problem in existing literature regarding efficient security mechanism in WSN. Over the years, several security schemes have been proposed in order to secure WSN. Some of them are static and others are dynamic. Static techniques are less secure as they provide protection only form external threats. The dynamic security techniques are more secure as compared to the static techniques but they require additional network resources and are time consuming in nature. Therefore, we need a strong security mechanism which not only provides enhanced level of security but also uses network resources optimally.

Chapter 3

REQUIREMENT ANALYSIS

The Wireless Sensor Networks (WSN) is usually deployed in a sensitive environment where security is a major concern. With the increase in the popularity and usage of WSN, security breaches and vulnerabilities has been identified. To protect the system against these threats and malicious activities, different types of security techniques have been proposed in existing literature. But these techniques are not much secure and energy efficient in nature at a time.

3.1 Introduction

In this chapter, we have focused on the requirement analysis of our research work. We have discussed the different critical scenarios in section 3.2. The focus of the research is highlighted in section 3.3. Section 3.4 includes the closing remarks in the form of a summary.

3.2 Problem Scenarios

In this section, we discuss the critical scenarios such as WSN setup problems, security problems in existing approaches, issues related to IDS deployment, efficiency versus security trade-offs and attack scenarios.

3.2.1 WSN setup problems

The WSN is composed of large number of tiny size sensor nodes deployed on uncertain geographical area i.e. terrain, climate and battle field. These networks are setup on those tentative areas where individual labours participation is typically not involved. The node uses battery power and antenna to communicate with other sensor nodes in the network. As the communication between nodes increases the energy of the sensor node dissipates rapidly. In [31] there are no aggregated nodes inside the network and every node has to send its data towards the base station. That increases the overall communication cost of the network and as a result the energy of sensor node dissipates quickly. The node use irreplaceable battery therefore the topology of the WSN is constantly changing. For that reason the structure and topology of networks ought to take into concern next to the setup time.

The communication distance is another problem that needs to be addressed at deployment time. The energy level of the sensor nodes reduces as the distance between the node increases. In [33] the author uses distributed defence scheme to propose an energy efficient IDS for WSN. But this scheme becomes energy exhaustive as the cluster grows in size. Therefore the number of sensor nodes and size of the cluster also affect the performance of WSN.

3.2.2 Security issues in existing approaches

To protect the system against the threats and malicious activities, there are two major types of defensive approaches named as static and dynamic. Authentication, firewall and encryption are the examples of static technique. In these research articles [19,20,21,22,23,24] the authors applied static defensive measures against the security attacks. These schemes are suffering from problems i.e. computation overhead, time required to decrypt the encryption keys, information leakage when a node become compromised, maintaining and storing all link dependent key for each node, simultaneous transmission of communication effect on the collision rate, stolen the master key, issues related to internal threats and compromised node. They do not completely cure the system against the threats and above mentioned security problems. Therefore there is a need for another defensive approach which not only provides security against the internal and external threats but also discovers the compromised node and takes appropriate action against it.

An Intrusion Detection System (IDS) is an example of dynamic approach. In [25,26,27,28,29,30,31,32,33,34,35,36,37,38,39,40,41,42] the authors applied the IDS techniques against the security threats. The IDS protect the system both from the internal and externals threats and reduces the computation cost of decryption keys. It provides better security as compare to static technique but it require additional network resources and time consuming in nature. The dynamic approaches is still suffering from trust relationship issues, selection and activation of global agent one at a time, sharing of secret information with the neighbouring nodes, emphasis only on the intrusion detection schemes only not to handle those intrusions, selection of statistical techniques increases the probability of false alarm rates and issues related to the publication of intrusion report on the shared link.

3.2.3 Issues related to IDS deployment

There are two ways to deploy IDS either at a host level or network level. First we will discuss issues related to host level IDS then highlight on going issues in network level IDS.

In the host level, the IDS is installed on every sensor node in the network. In [35] the authors have presented an idea of host level IDS using State Transition Analysis Tool (STAT). The IDS is composed of five agents along with file base and rule base knowledge base system. The installation of five agents on each sensor node increases overhead on memory space. Similarly in [40] the authors equipped each sensor node with an Intrusion Detection Agent (IDA) to detect intrusion at the node level. They use a SLIPPER algorithm to monitor the local and packet data flowing into the node and out from the node. This algorithm might not provide high prediction accuracy on the novel type of data. The installation of IDS agent on each sensor node increases the cost of ownership and detects only the system based attacks. The WSN is a special type of network having limited amount of memory space and battery time. Therefore installing IDS or IDA on each node is not efficient in terms of resources.

In network level, the IDS is used to monitor and analyze network traffic that travel across the network. It lowers the cost of ownership, more difficult to remove the evidence of attacks, helps in real time detection and independent of operating system. In [37] the authors have proposed an idea of isolation table for the detection of intrusion at the network level. The cluster based approach is used to monitor the network traffic. Two CH's are used for this purpose named as Primary Cluster Head (PCH) and Secondary Cluster Head (SCH). The intruder can attack easily when the number of sensor nodes in

WSN is less alive. In that case the frequency of alarm will be low and intruder can capture the node easily. The whole scheme will fail if the PCH is under attack. Therefore, the selection of appropriate communication structure must be taken into account before the communication start up. Another network level IDS is proposed in [39]. The IDS module is activated for the specific interval of time only. That affects the serious problem to the security of the system. Consequently the network level IDS only monitors specific system activities and require additional hardware resources. That is not best fit to the WSN environment.

The host level and network level IDS have their own benefits and limitation which complements each other. Another solution is to use hybrid approach that combine the functionalities of both host level and network level IDS. This would reduce the installation cost, provide real time detection and identify both system and network level malicious activity. In [38] the authors have present at the hybrid and cluster based IDS agents to detect both misuse and anomaly based intrusion techniques. The local and global agents are used to discover host and network based intrusions. But the installation of local and global agents on each sensor node is not feasible solution. Therefore there is a need for resource and energy efficient IDS that best fit in the WSN environment.

3.2.4 Efficiency vs. Security trade-offs

The related work shows that there exist several techniques in order to secure WSN. Rodrigo Roman et al. [16] highlights that sensor nodes are resource restricted in nature therefore efficient implementation of security primitives is needed. Adrian Perrig et al. [19] presented an idea of Security Protocol for Sensor Networks (SPINS). The overhead on energy level and computation time rises as number of messages increases during communication. Bocheng Lai et al. proposed BROadcast Session Key (BROSK) negotiation protocol for WSN. It is used for broadcasting key negotiation massage to provide link dependent keys to the sensor nodes for communication. They assume that master key should not be captured by adversary. That causes a breach towards the system security. If master key is compromised then WSN security will be compromised. The proposed scheme also creates a trust relationship among nodes. Maintaining and storing all link dependent key for each node are expensive in term of memory. It also uses simultaneous transmission for communication that increases the rate of collision. As the node density increases the ratio of collision become high and the energy dissipate quickly. Blab et al. [22] proposed another scheme for securing WSN. The absence of aggregated node poses an additional communication step that increases the burden on the network resources.

The lack of architecture and communication structure imposes additional research challenges in designing a sophisticated and adequate network security mechanism for WSN [14, 15, 16, 17, 18]. The existing literature shows that there seems an inverse relationship between strong security mechanism and efficient network resource utilization [19, 20,21,22,23,24,25, 26,27,28,29,30,31,32,33,34,35,36,37,38,39,40,41,42]. That is, if we enhance the security of WSN then we have to compromise on network resources and vice versa.

3.2.5 Attacks Scenarios

We have divided the attack scenarios into two parts passive attacks and active attacks. The description of each attack is given below.

3.2.5.1 Passive attacks on WSN

In passive attacks, the eavesdropper quietly listen the traffic in its environment. It does not alter the contents of message therefore it is very hard to locate these types of attacks. The target of these attacks is to break the privacy and confidentiality of the system. The sensor networks are specially set up in such critical environment where extra safety measures must be taken into consideration. For example in a military environment the sensor node is used to sense the movement of its enemy and commands it's solider to take appropriate action on its opponent. The passive attacker in the military command environment listen the confidential messages that causes significant loss to the defence system.

Another technique used by the attacker is that, they uses a host somewhere else from the internet and sends traffic to the sensor nodes in the network. The attacker acts as a valid member and start listen the traffic flowing inside the network.

3.2.5.1 Active attacks on WSN

In the active attacks, the target of attacker is to alter the content of the message that is flowing inside the network. The sensor nodes broadcast its massages to communicate with each other. The contents of the message are compared whenever malicious activity takes place. Therefore it is easier to locate these types of attacks as compared to the passive attacks. If the attacker gains control over the sensor nodes it will generate false and bogus message and destruct the security policy of the system. Therefore the active attacks are more harmful in real time system.

3.3 Focus of Research

Related works shows that there seems an inverse relationship among strong security mechanisms and efficient utilization of network resources. That is if we enhance network security we have to compromise on network resources. We have also come to know through existing literature that the IDS module is activated all the time whether the intrusion happens or not. The activation of IDS module all the time quickly consumes network and its resources. To overcome these problems we need an efficient security mechanism that provide enhance level of security along with minimum network utilization. So our focus of the research is to find out a solution which best fit in resource restricted nature of WSN by providing strong enough security. Instead of activating IDS module all the time, we have proposed an idea of Mobile Agent Based Hierarchical Intrusion Detection System (MABHIDS) for WSN. In our proposed idea the IDS module is activated only when the malicious activity takes place. It uses the hybrid IDS approach with efficient utilization of IDS modules that enhance the network lifetime and performs two level of security by using resources of WSN optimally.

3.4 Summary

In this chapter, we have discussed the existing problems in WSN. Traditionally there are two types of defensive approaches static and dynamic. The static approach is called the first line of defence and provides security only from the external threats. Whereas the dynamic approach that is called as the second line of defence and provides security from both internal and external threats. Each one of these approaches has its own benefits and

shortcomings which complements each other. The study of existing literature shows that there seems an inverse relationship between strong security mechanisms and efficient resource unitization. If we increase the network security we have to compromise on resource utilization and vice versa. Therefore there is a need for better security mechanisms for WSN that best fit in the WSN resource restriction environment.

Chapter 4

SYSTEM DESIGN

The design phase creates architecture of the system. In this phase, we build a blue print of the system, which is used as a lay-out plan to build the system. It helps in the software implementation. The major objective of the design phase is to discover the appropriate design within the boundaries and limitation imposed by the environment in which the system operates.

4.1 Introduction

The basic need of the proposed scheme is identified in this chapter. This is useful in system building. The design requirement and reference architecture of our proposed scheme is highlighted in section 4.2 and 4.3 respectively. We have discussed about the methodology / algorithm in section 4.4. Section 4.5 concludes the closing remark of this chapter in the form of a summary.

4.2 Design Requirements

Intrusion Detection system (IDS) is used for identifying and handling malicious, unauthorized and harmful activities in WSN. In this section, we have discussed the IDS, its popular applications, log files and thresholds which are the fundamental requirements of our proposed architecture.

4.2.1 Intrusion Detection System

Security mechanism is a fundamental requirement of wireless networks in general and Wireless Sensor Network (WSN) in particular. Therefore, it is necessary that this security concern must be articulated right from the beginning of the network design and deployment. The WSN needs strong security mechanism as it is usually deployed in a critical and sensitive environment i.e. terrain, climate and battlefield where human effort is not concerned. Two types of security techniques are used to protect the system from invaders. One is static technique and also called as the first line of defence. Encryption, authentication and firewalls are the types of static techniques that cannot be directly applied to WSN as that provides defence only against the external threats. The other technique is the dynamic technique and also called as the second line of defence. Intrusion Detection System (IDS) is an example of a dynamic technique.

Intrusion detection is the process of identifying, examining and observing violated activities. It discovers breach and illegal access to confidentiality, unavailability, authorization, authentication, integrity and network resources [9]. Intrusion Detection System (IDS) is a dynamic monitoring system that is used to detect intrusions in real time. It also protects the system against the internal and foreign invaders. Intrusion detection performs analysis on the information stored by the computed resources. Therefore experience personnel are required that interpret the network traffic into valuable information. This activity takes place at the Network / Host level or combination of both [1].

In the network level, the IDS monitor network traffic for detecting misuse pattern, whereas in the host based IDS it monitors the node processes for detecting malicious activities as a sign of misuse. In hybrid, the IDS examine both the network traffic as well as the host processes. The sensor node has limited amount of memory and computation resources therefore efficient security mechanism is needed for WSN. The nodes in the sensor environment usually use broadcast medium to communicate each other. When the node gets captured it routes the bogus, false information and misleading its neighbour node. If the attacker attains full control over the sensor node it may destruct the whole system. Therefore, the selection of appropriate IDS scheme is the basic requirement for securing WSN against the inside and outside attacks.

4.2.2 Applications

The IDS is an important security mechanism in the world of network security. Popular examples of WSN applications are pattern recognition, machine learning approaches, faults and anomaly detection, fire response, traffic monitoring, military commands, health and monitoring heart beats etc.

4.2.3 Log files

Special type of tasks and responsibilities are assigned to each sensor node in a network. The information collected from these sensor nodes are transferred to the centralized authority called Base Station (BS) after a specific interval of time. The objective of the sensor node is to perform the assigned tasks and it is called as normal activity of that sensor node. Each sensor node maintains a separate log file for its normal activity.

4.2.4 Thresholds

The threshold shows the level of network traffic flowing inside the host and network. The deviation in the network traffic assumes to be a malicious activity which is investigated further. In our proposed architecture, we have used two thresholds frequencies. The threshold 1 is set by the CH for traffic normal activity whereas threshold 2 is set for each sensor node for its system normal activity.

4.3 Reference Architecture

In this section, we have discussed the reference architecture. In section 4.3.1, we have discussed about the topology of sensor node used in our approach. The proposed architecture and its working paradigm are discussed in section 4.3.2 and 4.3.3 respectively. Communication structure of agents with Cluster Head (CH) is reported in section 4.3.4. The section 4.3.5 highlights the communication structure of CH with Base Station (BS). The rotation of new Cluster Head (CH) described in section 4.3.6.

4.3.1 Cluster topology

Different types of network topologies such as star, tree, mesh etc are used for communication in WSN as we discussed in chapter 1. In a cluster based hierarchical approach, concentration of sensor nodes forms a cluster and one node among them acts as a Cluster Head (CH) / aggregated node. The CH assumes to have a larger battery and acts as a supervisor node for communication between other nodes. All CH in the network are connected to a Base Station (BS) which is a single decision making authority. The CH is a special sensor node with the specific tasks of receiving, processing, storing and forwarding data collected from the member nodes of that specific cluster [1].

Each CH must be connected with Regional Head (RH) or BS, depending on the deployment scheme of the WSN. The RH works very much like CH, but unlike CH, the RH connects different CH together. All the RH in the network is connected to BS which is a central governing and decision making authority. In a typical deployment of wireless sensor network, there are three tiers. At the top tier BS is deployed, RH and CH comes at middle tier, whereas the sensor node comes at lower most tiers. The sensor nodes collect data from its environment and send to the Base Station (BS) for analysis. These nodes have low cost processor and limited amount of battery time therefore energy efficient protocol is needed for communication. The lessening in communication messages make easier to save the battery time of sensor nodes. The concept of cluster is used to reduce the overall messages between the sensor nodes and BS as shown in Fig.6 for this purpose we will use the cluster tree in our proposed architecture.

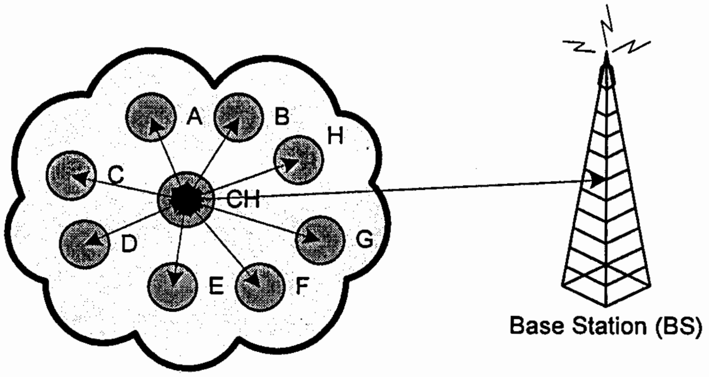


Fig 6: Cluster topology in a proposed approach

4.3.2 Proposed Architecture

We have proposed a Mobile Agent Based Hierarchical Intrusion Detection System (MABHIDS), which provides two tiers of security in WSN. In order to provide two tiers of security we have installed Musk architecture [43] on each Cluster Head (CH). We have modified the MUSK architecture in order to use of its agent behave as mobile agent. The following Fig.7 [43] shows the basic architecture of our proposed scheme. Three agents are used in this architecture named as Analyzer Agent (AA), Coordinating Agent (CA) and Management Agent (MA).

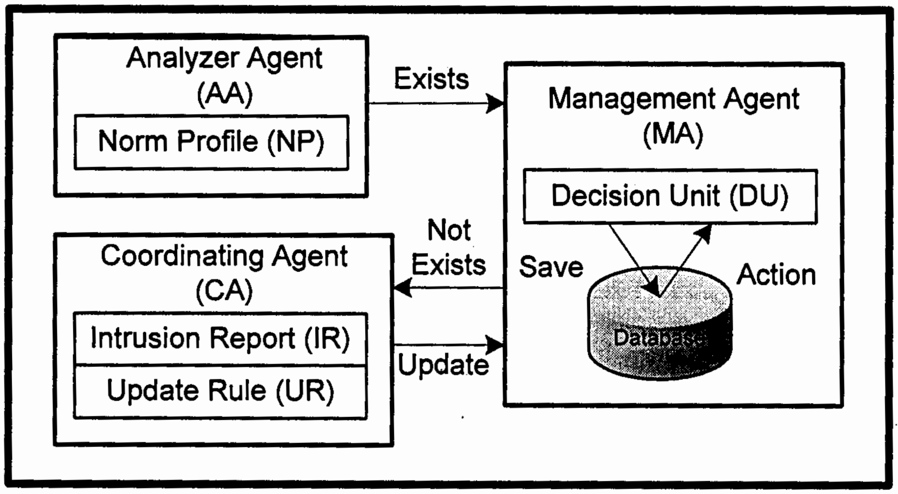


Fig 7: Modified form of MUSK Architecture [43]

4.3.3 Working Paradigm

The proposed architecture works as Network Intrusion detection System (NIDS) and Local Intrusion Detection System (LIDS). The working paradigm of NIDS and LIDS are reported in section 4.3.3.1 and 4.3.3.2 respectively. The working deployment of NIDS and LIDS is discussed in 4.3.3.3

4.3.3.1 Network Intrusion Detection system (NIDS)

The different agents of Musk architecture [43] work as NIDS which is installed on each CH within a network. The Management Agent (MA) and Coordinating Agent (CA) are stationary agents whereas the AA is a mobile agent. The NIDS capture the data packets along the path to identify an intrusion activity. Whenever NIDS on CH detects an intrusion it sends a copy of Analyzer Agent (AA) to the victim node. Here we have used two threshold frequencies. The threshold 1 is set on each CH for the traffic normal activity of the network and threshold 2 is set on each sensor node for its system normal activity. The detail information of each agent is given below.

4.3.3.1.1 Analyzer Agent (AA):

The Analyzer Agent (AA) is used to monitor node activity. It is a mobile agent and installed on each CH in the network. When CH discovers an intrusion it sends a copy of AA to the suspicious node. Then AA uses victim resources in order to verify the occurrences of intrusion. Then AA generates a Norm Profile (NP) and checks the threshold 2. If there is a deviation from the threshold frequency the AA generates an alarm and notifies the CH. The CH calls the Management Agent (MA) for local analysis.

4.3.3.1.2 Management Agent (MA):

The Management Agent (MA) contains a sub unit called as Decision Unit (DU) for the analysis of intrusion. The DU maintains the database of already occurred intrusions. When an intrusion occurs the CH calls the MA for analysis. The MA activates its DU that searches in its database whether this intrusion happened in the past or not. The database contains the predefined stored intrusions along with the decisions. If the match occurs against the pre stored intrusions then DU performs action according to already stored decision and informs to the CH. If there is no such entry in the database then MA informs the coordinating Agent (CA) regarding the occurrence of an unusual activity.

4.3.3.1.3 Coordinating Agent (CA):

The Coordinating Agent (CA) performs two basic functions i.e. generate Intrusion Report (IR) and Update Rule (UR). When CA receives a novel intrusion message from MA it sends to IR. The IR forwards this report to the Base Station (BS) regarding the occurrence of an unusual activity. The BS is a centralized decision making authority against the intrusion. It makes a decision on novel intrusion and sends it to the Update Rule (UR). The UR generates new rule against that intrusion and sends it to MA. The MA saves the intrusion in the database for future use. If the same intrusion happens again the DU searches its database and performs the already stored action.

4.3.3.2 Local Intrusion Detection System (LIDS)

The Analyzer Agent (AA) is a mobile agent and works both as NIDS and LIDS. When NIDS in CH deviates from its threshold 1 it generates an alarm informing the occurrence of intrusion. The CH makes analysis and identifies the sensor node that is generating abnormal traffic. The CH activates its mobile AA and sends it to the victim node. The AA works as LIDS and uses resources of the suspicious node for identifying the malicious activities. The AA informs the CH either the suspicious node is victim or safe.

If the node is victim the CH that takes appropriate action upon that activity. The copy of AA is only sent to the suspicious node instead of installing LIDS on each sensor node.

4.3.3.3 Working deployment of NIDS and LIDS

The Fig.8 represents a working deployment of NIDS & LIDS. It is important to mention that the NIDS is deployed on each CH whereas the actual deployment of LIDS is also at CH. On each intrusion alarm, the LIDS (which are a mobile agent) are triggered by CH for further inspection of the behaviour of suspicious node. The LIDS uses resources of suspicious node to report it either as a victim or a safe node.

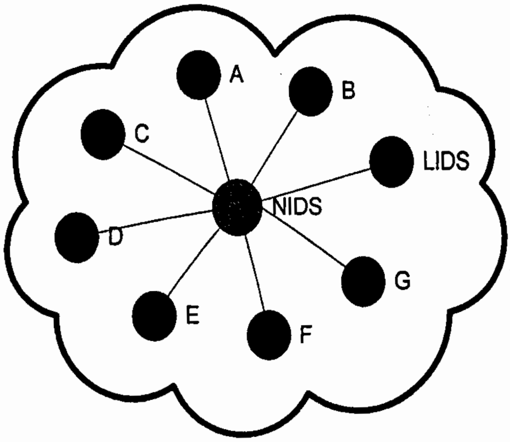


Fig 8: Working deployment of NIDS and LIDS

4.3.4 Communication Structure of agents with Cluster Head (CH)

We set two threshold levels for intrusion detection, one for Network Intrusion Detection System (NIDS) and other for Local Intrusion Detection System (LIDS). Threshold 1 is set on each CH over the network and works as the NIDS, whereas the threshold 2 is set on each sensor node and works as LIDS. The initial intrusion detection is performed by NIDS which detects the normal rate of packet arrival and departure. In case of deviation the CH triggers the mobile Analyzer Agent (AA) over the link where deviation has occurred.

The AA will visit the suspicious node and acts as Local Intrusion Detector (LID) over there. The AA will use the resources of suspicious node to investigate its behaviour further. This investigation is based on threshold 2. If suspicious node is found as victim then AA will update CH. The CH informs its sub agents i.e. Coordinating Agent (CA) and Management Agent (MA) that will take appropriate action to prevent rest of the network from intrusion either by minimizing the communication with the victim node, reducing the trust value on the victim node or by cutting its communication from rest of the network. Otherwise, the AA informs the CH that the suspicious node is not the victim; it is a safe node and unusual but harmless activity has taken place.

4.3.5 Communication Structure of Cluster Head (CH) with Base Station (BS)

The communication structure of CH with BS is discussed in this section. When CH detects an intrusion it sends an Intrusion Report (IR) message to BS. The BS takes a novel intrusion into account processes it and sends the action in the form of report to the CH. The CH generates a new rule depending on the action report and save this intrusion into its database for further use as shown in Fig.9.

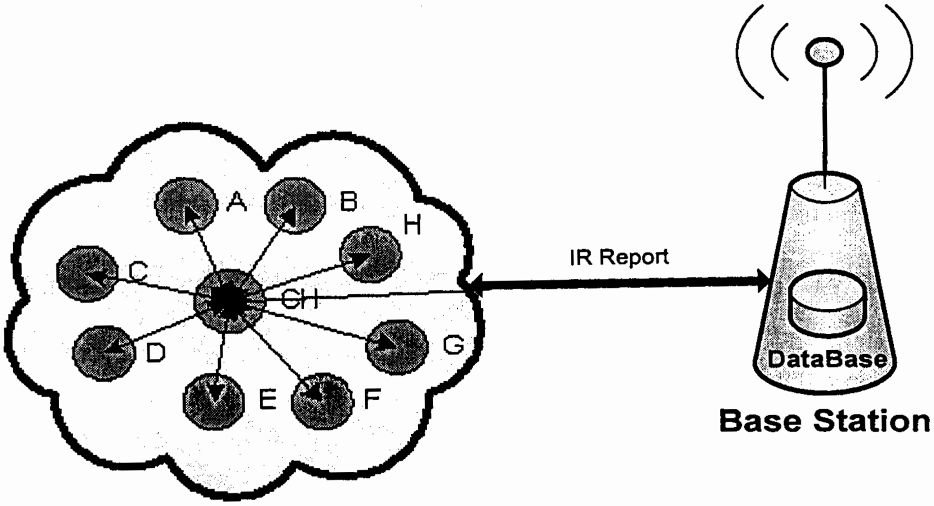


Fig 9: Communication Structure of CH with BS

If this intrusion happens again in the future the CH takes the action and saves the time and resources of BS without informing the occurrence of intrusion again. The CH transferred this IR report to other CH in the network. The proposed scheme will also update the whole network with just a single IR report to any CH. This framework eliminates the duplication of intrusion request to BS, minimizes the security control messages, reduces the network load on BS and saves the sensor node resources. The reduction of communication load over the network enhances the network lifetime which makes the whole network energy efficient.

4.3.6 Rotation of new Cluster Head (CH)

The Collaboration–based Intrusion Detection (CID) and Routing Tables Intrusion Detection (RTID) are the major types of technologies used to detect attacks [42]. The CID is an intrusion detection system which continuously monitors the intrusions during the cluster duty cycle. A Cluster Header (CH) is chosen from a cluster, assuming to be have large battery time as compared to other nodes in the cluster. The cluster duty cycle is performed after a specified interval of time for the selection of new CH. When there is a rotation of new CH, the base station (BS) takes all IR messages form all CH's in the network and saved in its database. After the selection of new CH, the BS sends the previously saved IR reports to the newly elected CH as shown in Fig.10. So that previously intrusions would not be lost during the election of new CH. which is a major advantage of our proposed scheme.

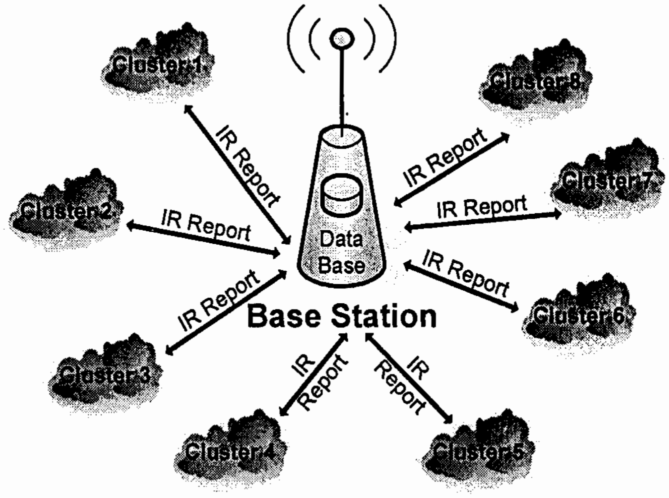


Fig 10: Rotation of new Cluster Head (CH)

4.4 Methodology / Algorithm

Methodology helps in building the structure of a proposed solution. Our intrusion detection framework builds on two important phases. They are named as initial phase and detection phase. The description of initial and detection phase is given in section 4.4.1 and 4.4.2 respectively.

4.4.1 Initial Phase

In the initial phase, the rules are embedded into the database in the form of records. During this phase the system is assumed to be in a safe state therefore no malicious activity has taken into account. Two threshold frequencies are set in this phase. The threshold 1 is set for CH and threshold 2 for sensor nodes. The threshold 1 is used for the network normal activity and set on each CH in the network. The threshold 2 is set on each sensor node for its usual activity. The job of the CH is to sense the data packet flowing inside the cluster, number of incoming and outgoing messages from each node.

4.4.1 Detection Phase

An attack is launched in this phase to check whether the system is able to detect and tackle the malicious and harmful activity or not. The CH continuously monitors the network traffic. The intrusion activity is initiated either by the network level or the node level. If there is a deviation against the network threshold frequency which is set on CH an alarm will be generated. The CH locates the node and takes the victim node into consideration. Then it sends its mobile AA agent to that particular node to inspect it further.

4.5 Summary

In this chapter, we have proposed a Mobile Agent Based Hierarchical Intrusion Detection System (MABHIDS) for WSN. The proposed scheme provides strong security by utilizing minimum network resources, reducing the security control messages in the network and eliminates the need to update the signatures manually in the database. The proposed solution is based on two tier security called as Network Intrusion Detection System (NIDS) and Local Intrusion Detection System (LIDS). The NIDS is installed over each Cluster Head (CH). The Local Intrusion Detection System (LIDS) is triggered by CH when a node is suspected to be a malicious one.

Chapter 5

IMPLEMENTATION

The objective of the implementation phase is to implement the proposed system that reflects the desired goals. There are certain measurements that help to determine how well the objective is being met. In order to obtain the desired goals and objectives it doesn't means that we should maximize every measure. However, in many cases there exists inverse relationship among measurements attributes. Our foremost objective is to create a balance relationship among these sorts of measurement attributes.

5.1 Introduction

In this chapter, in section 5.2 we have discussed working environment of our proposed scheme. The flow charts of the proposed approach are highlighted in section 5.3. Then we have discussed the pseudocodes in section 5.4. At the end of this chapter, section 5.5 concludes the closing remarks in the form of a brief summary.

5.2 Working Environment

The environment plays an important role in examining and understanding the behaviour of architecture in a given scenario. We have simulated our proposed architecture in network simulator called as OMNeT++. We have discussed the overview of OMNeT++ in section 5.2.1. The network simulation's support is highlighted in section 5.2.2. In section 5.2.3, we have discussed the basic idea of building and running simulation in OMNeT++.

5.2.1 OMNeT++

There are many simulation environments such as NS/2, J-Sim, SSFNet, Opnet, TOSSIM and TinyOS etc [44]. None of these simulation environments perfectly meets the demands of sensor networks. The intention of the OMNeT++ is to provide a simulation platform for researcher to launch their own frameworks over it. The NS-2 lacks some important modules of the simulator i.e. graphical editor, hierarchical model supports, graphical analysis tools, GUI-based execution and parallel simulation support which OMNeT++ offers. J-Sim (JavaSim) supports hierarchical model but it doesn't support graphical user interface. Therefore, it is difficult to use this simulator. SSFNet (Scalable Simulation Framework) simulation environment is not free of cost and doesn't support large model by using reusable component as that of OMNeT++ provides. Opnet simulator is used commercially but it is difficult to program as it uses Opnet API files with C programs whereas OMNeT++ uses simple C++ files. TOSSIM and TinyOS support simulation of sensor network but they are not freely available. We have opted OMNeT++, as it is versatile in features and free for use for educational purposes.

The OMNeT++ is an object-oriented and discrete event network simulator developed by Andras Varga [45]. The OMNeT++ provides friendly user interface for debugging, demonstration and batch execution. The model of the network is visible to the user allowing to control the simulation and intervene by changing variables inside the network model. That is helpful in debugging and development phase of the project. The interface tools provided by OMNeT++ are portable that facilitate to easily build a network model. It also successfully works on several UNIX flavour and Windows by using different C++ compilers. OMNeT++ assists parallel distributed simulation and provides framework for communication between parallel distribution simulations. OMNeT++ is available commercially and it is free to use for academic and research purposes.

The OMNeT++ model composed of variety of hierarchically nested modules. The nesting of module depth is not limited that allow the user to understand the logical format of actual system easily. The modules communicate by passing a message parameter with each other. The parameters are used to modify the behaviour of module and its topology. Each module in the model has its own parameters for communication. The message can composed of complex data structures and network traffic data between communicating modules. The modules send message parameter through gates and connections directly to the destination or along the predefined route. The module encapsulates the behaviour and it is lowest level of module hierarchy. These modules are called as the simple modules and they are programmed in C++.

5.2.2 Network simulation support

The OMNeT++ provides a GUI interface for modelling, running the simulation and analysis of result [44]. The simulation output can be printed on data files for analysis and testing. OMNeT++ offers a tool for plotting the content of output data files. It is not important that the output data files must be in OMNeT++ alone it may use mathematics based package like Matlab or spreadsheets like MS Excel for processing the result. The involvement of external programs gives opulent functionality to the user for statistical analysis and visualization of network. The purpose of GUI interface is to make the internal model clear to the user for controlling the simulation execution. This would also allow us to examine the inside model by changing the objects and variable of the system. That is the fundamental requirement in development and debugging phase of the simulation phase. Several independent models are stored in simulation executable which is comprises of various simple module. One can specify the name of file model from the set of simple module which is to be run. That allows us to build a large network model which comprises of several simulation models acting as a one standalone system model.

5.2.3 Building and running simulation

The OMNeT++ model consists of three basic parts: NED language topology description, message definitions and simple modules sources [45]. The NED language topology description illustrates the structure of the given module with gates, connection and parameters. The NED files can be written on GNED graphical editor or any text editor i.e. Notepad / WordPad. The NED files save with .ned extension. We define messages and data field in message definition files. The responsibility of OMNeT++ is to translate all message definitions into C++ classes. The simple module sources are C++ files with .h suffix. The simulation system uses two basic component called simulation kernel and user interface. The simulation kernel contains the C++ codes which manages the simulation and simulation classes. They compile and form a library with .lib/ .a extension. User interface helps in debugging the execution of simulation. The simulation programs constructs from these components. In the first step, the message definitions files are translated into C++ codes. In the second step all C++ files are compiled and linked with simulation kernel and user interface library. In the last step the NED files are translated into C++ using NED tool at the start of simulation.

5.3 Flowchart

The flowchart defines the working flow of a system. It helps in understanding the sequence of the proposed approach. It contains a set of activities that takes place during the process. It is the easiest way to show the functionality of overall system especially when the system is very complex in nature.

There are four basic events that are introduced in our proposed approach. They are named as NIDS, LIDS, intrusion detection using MUSK architecture and rotation of new CH. The flowchart of NIDS and LIDS are discussed in section 5.3.1 and section 5.3.2 respectively. In section 5.3.3, we have discussed the flowchart of MUSK architecture. The flowchart of rotation of new CH is shown in section 5.3.4.

5.3.1 Flowchart of Network Intrusion Detection System (NIDS)

The Network Intrusion Detection System (NIDS) is installed on each CH in the network. The NIDS in CH monitors all the sensor nodes in that cluster. It captures data packets to monitor network traffic. The AA performs analysis on the data traffic. It uses a file which contains description of an outgoing, incoming, minimum and maximum number of messages passing to and from each sensor node. The Fig.11 shows the basic flow chart of NIDS.

The deviation from the norm profile shows the occurrence of malicious activity in the cluster. If there is a deviation, then AA will locate the malicious node and send its mobile AA to that particular suspicious node. The copy of AA will be sent to the malicious node to verify it further. Else if, there is no deviation the AA continuously monitors network traffic flowing inside the cluster.

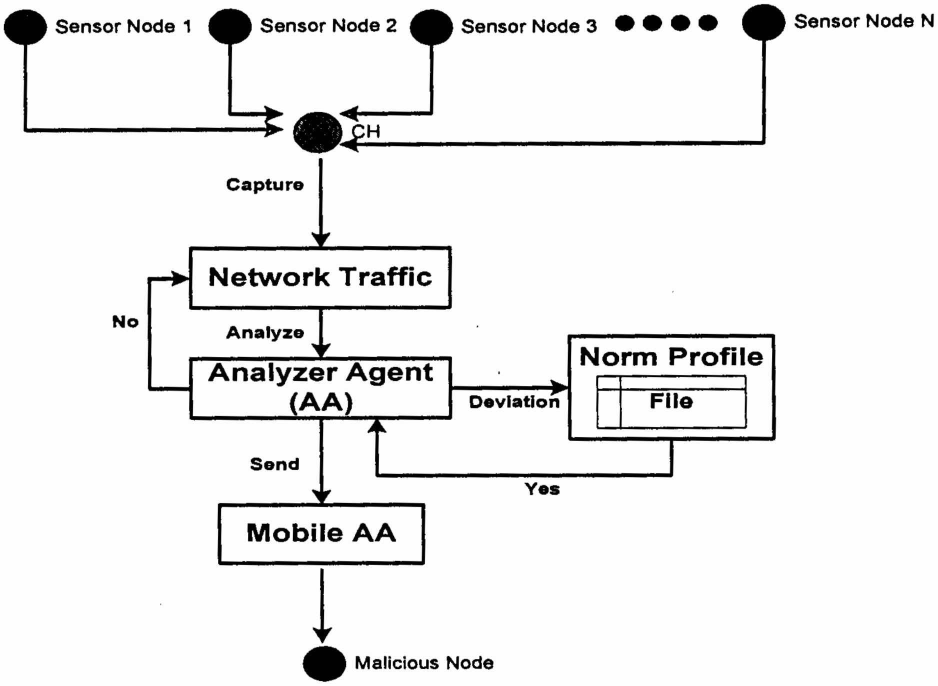


Fig 11: Flowchart of Network Intrusion Detection (NIDS)

5.3.2 Flowchart of Local Intrusion Detection System (LIDS)

The mobile AA works as LIDS on the malicious node. It uses resources of the victim node to verify the occurrence of intrusion further. The flowchart of LIDS is depicted in Fig12. The mobile AA uses resources of victim node to analyze the intrusion further. It is important to note that on each sensor node threshold value is set as 2 in its norm profile. If the mobile AA finds deviation from the node's norm profile then it will send an occurrence of malicious message to the CH else sends a normal activity message to the CH.

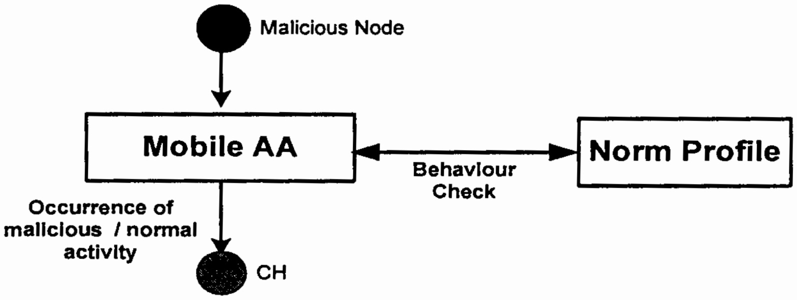


Fig 12: Flowchart of Local Intrusion Detection (LIDS)

5.3.3 Flowchart of MUSK architecture

For the detection of novel or previously known intrusions activities, we have used MUSK architecture. This architecture is composed of three agents; Analyzer agent (AA), Management Agent (MA) and Coordinating Agent (CA). In above flow charts of NIDS and LIDS, the AA is used to detect the malicious activity. When AA detects the malicious activity two cases may take place. In first case, the novel intrusion is occurred whereas in second case pre-stored intrusion is occurred. In order to locate the intrusion activity the flow chart of MUSK architecture is given in Fig.13.

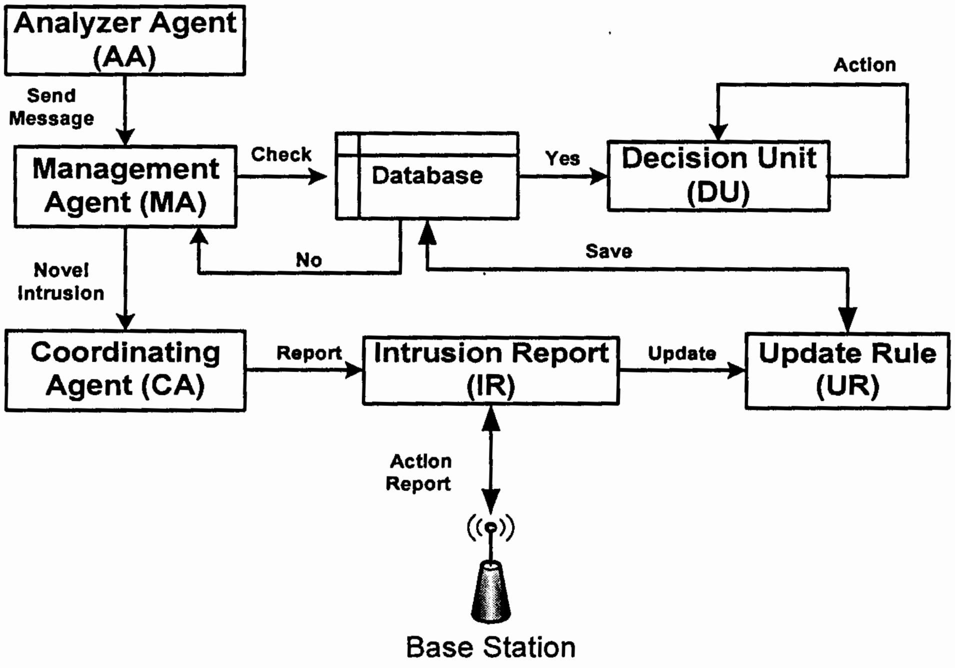


Fig 13: Flowchart of MUSK Architecture

When AA detects a malicious activity it sends an intrusion message to MA. Then MA checks its database whether this intrusion happens in the past or not. If yes, then Decision Unit (DU) takes a pre-stored action against the malicious activity, else, it sends not exist message to the MA. Then MA sends message to CA informing that novel intrusion has occurred. The CA send IR message in the form of Intrusion Report (IR) to the Base Station (BS). Then BS sends an action to IR. The IR makes a rule called Update Rule (UR) to store the action against that particular intrusion in the database. The DU then takes an action against the previously unknown intrusion.

5.3.4 Flowchart of rotation of new Cluster Head (CH)

The formation of new CH takes place after the specified interval of time. During the formation of new CH the previously Intrusion Report (IR) that are still in progress were lost. In our proposed approach, the BS sends a request for IR messages to all CH in the networks before the rotation of new CH. The BS saves all these IR messages in its database. After the formation of all new CH's in the network the entire IR messages are retrieved and sent to the new selected CH in the network as shown in Fig 14.

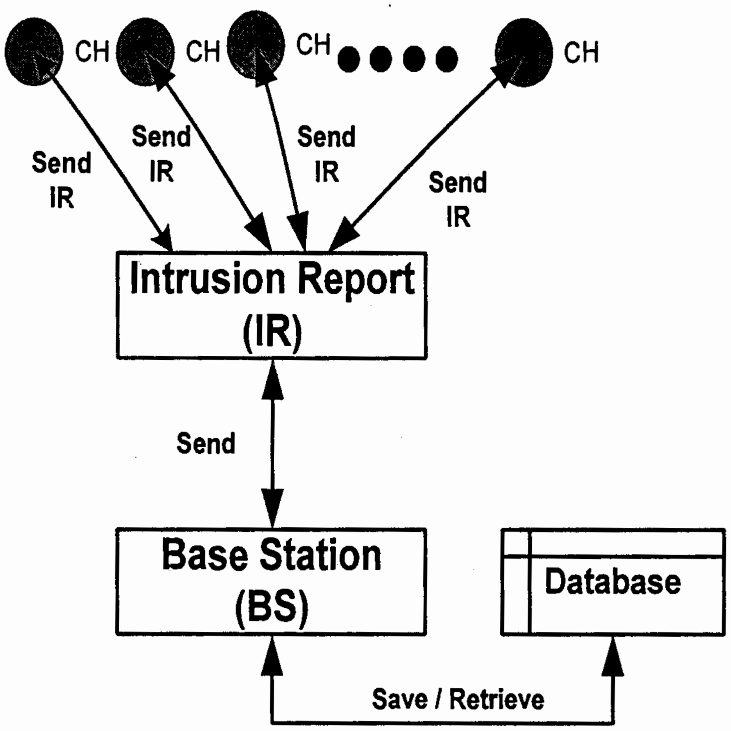


Fig 14: Flowchart of rotation of new Cluster Head (CH)

5.4 Pseudocodes

In this section, we have described the pseudo code of each flow chart. In section 5.4.1, we have discussed the pseudo code of NIDS architecture that is installed on each CH. The pseudo code of LIDS architecture is described in section 5.4.2. Section 5.4.3 elaborates the pseudo code of MUSK architecture. Finally, we have described the pseudo code of rotation of a new CH in section 5.4.4.

5.4.1 Pseudo code of Network Intrusion Detection System (NIDS)

The pseudo code of NIDS is given below. This pseudo code is written on each CH in the network.

Abbreviations:

Sensor Node in a cluster = SN

Compare =CMP

Cluster = C

Network Data Packets = NDP

Deviation = D

Mobile AA = MAA

Network Traffic Threshold on CH = TCH

Cluster Head = CH

AA of CH = AACH

Malicious Node = MN

Network Traffic Threshold on sensor node = TSN

Malicious Message = MM

Normal Activity = NA

Management Agent = MA

Database = DB

Match Occur = MO

Decision Unit = DU

Action against MM = AMM

Coordinating Agent = CA

Base Station = BS

Action Report from BS = ARBS

Update Rule = UR

New Rule = NR

Network= NW

Database of Base Station= DBBS

Time required for the Formation of all new CH = TNCH

New CH = NCH

Pseudo code:

```
BEGIN for all SN in C
        The CH capture NDP
        Forward NDP to AACH
        AACH will CMP NDP with TCH
        Check the condition (D with TCH) if it True then
          Forward MAA to MN
        Otherwise do,
          Ignore the NDP
          CH continue to capture new NDP
END
```

5.4.2 Pseudo code of Local Intrusion Detection System (LIDS)

The pseudo code of LIDS is given below. These steps are performed when CH detects that sensor node is performing a malicious activity.

Pseudo code:

```
The MAA will CMP NDP with TSN
        Check the condition (D with TSN) if it True then
          Forward MM to AACH
        Otherwise do,
          Forward NA to AACH
```

5.4.3 Pseudo code of MUSK architecture

When an intrusion occur the AACH performs following steps,

Pseudo code:

```
AACH will forward MM to MA
The MA will CMP MM with DB
Check the condition (MO == 'YES') if it True then
  The DU perform AMM
  Inform the CH about AMM
Otherwise do,
  MA will forward MM to CA
  The CA Store MM in IR
  CA will forward IR to BS
  Wait for the BS response
  Receive the ARBS
  CA will forward ARBS to UR
  The UR formulate NR from ARBS
  UR will forward NR to DB
  The DU takes AMM
  Inform the CH about AMM
```

5.4.4 Pseudo code of rotation of new Cluster Head (CH)

The formation of new CH is performed by the BS. The BS performs the following functions for selecting all new CH in the network.

Pseudo code:

```
The BS request IR from all CH's in NW
It Store IR in DBBS
Wait Until TNCH
Forward IR to NCH
```

5.5 Summary

In this chapter, we have discussed the working environment of OMNeT++. It provides GUI interfaces with the support of NED tool for simulation and plotting graphs to analysis the result of test scenarios. The depth of module is not limited; therefore it is widely used in complex environment. In our proposed scheme, there are four basic types of events that happen. They are NIDS, LIDS, intrusion detection using MUSK architecture and rotation of new CH in network. The flow charts and pseudo codes of events are also discussed in this chapter.

Chapter 6

TESTING AND PERFORMANCE EVALUTION

The testing and evaluation helps us to asses the quality and excellence of the proposed idea. In this chapter, we have evaluated the performance of our proposed scheme on different test scenario. We have also undertaken an analytical performance evaluation. In analytical evaluation, we have compared our architecture with various existing schemes. The results show that our proposed idea offers better results as compare to the existing approaches.

6.1 Introduction

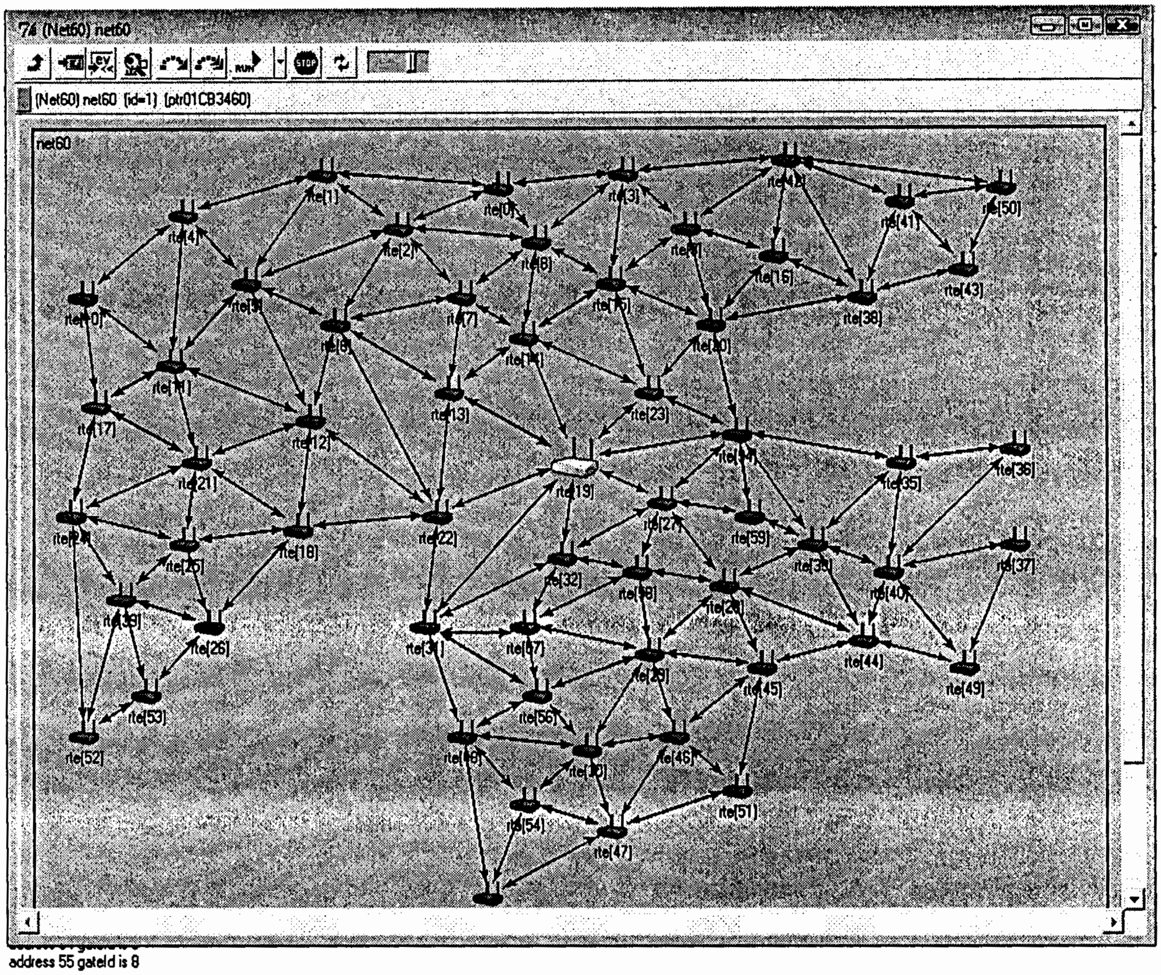
We have discussed different test scenarios in section 6.2. The performance and evaluation measurements have been examined in section 6.3. The concluding remarks of this chapter are given in section 6.4.

6.2 Test Scenarios

To evaluate the performance of the proposed scheme, we have to develop some test scenarios. Before applying test scenarios, we must to know the topology and structure of the network. Therefore we have discussed our simulation topology in section 6.2.1. The structures of simple and compound modules are highlighted in section 6.2.2. In section 6.2.3, we have discussed different test scenarios.

6.2.1 Simulation Topology

We have performed simulation in OMNeT++ simulator. The simulation topology is wireless. The topology architecture consists of 60 nodes in a cluster. All of these nodes in a network are stationary and do not change their location during communication. These nodes fall into two categories: member nodes in a cluster and CH. The member node acts as a sender node whose responsibility is to generate network traffic inside the cluster. There are 60 sensor nodes in which 3 nodes act as the destination nodes and 1 node works as CH in our simulation environment. The member nodes are connected to single CH as shown in Fig.15.



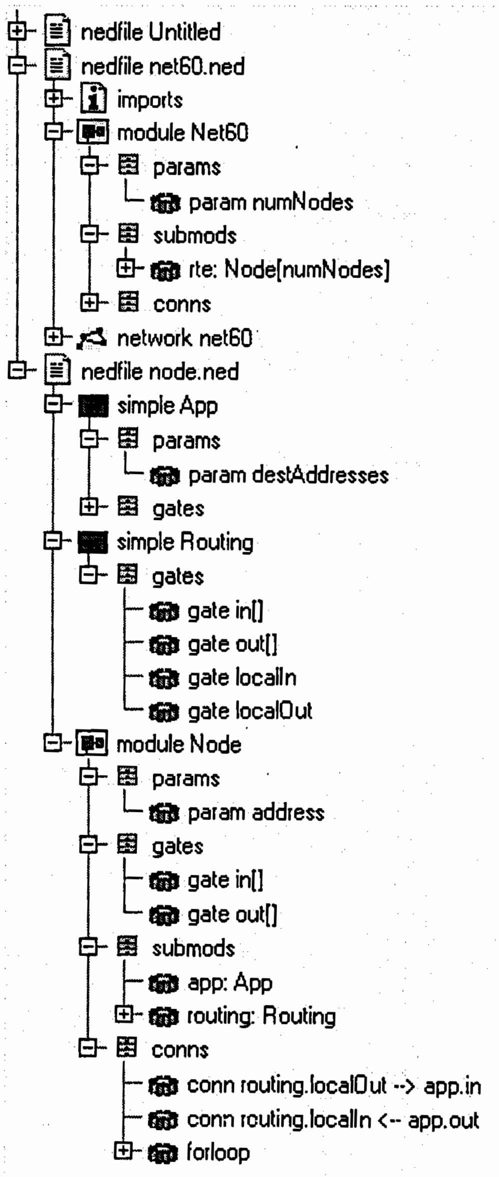
address 55 gateId is 8

Fig 15: Simulation Topology

The member nodes are named as rte[0], rte[1], rte[2], rte[3], rte[4],..... rte[59]. These member nodes usually pass network traffic through the CH to other member node in the network. The CH monitors network traffic by capturing data packets flowing inside the network. The data packets are dropped after arriving at the destination nodes to control the communication in the network.

6.2.2 Structure of simple and compound modules

We have used two compound modules named as Net60 and Node in our simulation environment. The Net60 is used to build the network nodes in a cluster. This module uses three attributes params, submods and conns. The params takes numeric number of nodes in the cluster. The submods take numeric value of params to generate network node in the cluster. The conns defined the connection between pairs of network nodes. Each node in the network is of compound type module called as Node. The following Fig.16 shows the hierarchical structure of simp!e and compound module.



```
nedfile Untitled
nedfile net60.ned
    imports
    module Net60
        params
            param numNodes
        submods
            rte: Node[numNodes]
        conns
    network net60
nedfile node.ned
    simple App
        params
            param destAddresses
        gates
    simple Routing
        gates
            gate in[]
            gate out[]
            gate localIn
            gate localOut
    module Node
        params
            param address
        gates
            gate in[]
            gate out[]
        submods
            app: App
            routing: Routing
        conns
            conn routing.localOut --> app.in
            conn routing.localIn <-- app.out
            forloop
```

Fig 16: Hierarchical structure of Simple and Compound Module

The Node consists of two simple modules named as Router and App which represent the aggregate traffic of the subnets connected to that router. The compound module Node uses four attributes params, gates, submods and conns. The params pass destination address for routing. The input and output links of module are defined in gates parameter. The submods is divided into two simple modules Router and App. The Router demonstrates routing in the network. It uses only one attribute called as gates that defines the input and output connection. The App is used to generate traffic for the network and handle incoming and outgoing messages. It also uses one attribute called as destination address as params. The conns of compound module of Node define the connection between simple modules App and Router.

It is important to note here that App and Router are called for every sensor node in the cluster. The NED language doesn't provide any concept of global variables therefore the change in one node file does not affect the other node file. To run the project on the network configuration, we have used a network file named as net60. It uses ommetpp.ini file to run the desire project over the network.

6.3 Performance Evaluation

In this section, we have evaluated our scheme by comparing it with the existing schemes. The analytical assessment of the scheme is performed in section 6.3.1. The summarized results are given in section 6.3.2.

6.3.1 Analytical Assessment

In this section, we have discussed the analytical assessment of our proposed approach with the existing schemes. We have divided this assessment into two parts: Model based assessment and security and efficiency based assessment.

6.3.1.1 Model Base Assessment

We have compared our architecture with some of the existing schemes [35, 36, 43]. We have taken seven sensor nodes in a cluster that are connected to a single CH. In [35] the authors proposed an agent based intrusion detection system using State Transition

Analysis Tool (STAT). The agents used STAT to analyze the intruder activities and update the system architecture. This intrusion detection framework is composed of five agents: Pre-processing Agent (PA), Reasoning Agent (RA), Decision Agent (DA), Update Agent (UA) and Communication Agent (CA) as shown in Fig. 17. The PA collects required data from audition record system. The RA judge the intrusion activity. If there is an occurrence of intrusion activity it informs the security officer of DA. The security officer commands the UA. Beside these agents, the framework uses additional components File Base (FB) and Rule Base (RB) for refreshing the knowledge Base (KB) system to analyze and record the data. The CA provides cooperation between hosts and agents for inspecting the intrusion activity. This architecture requires extra storage space and additional databases to store the signature of malicious activities. Every node has to handle its own databases and takes its own action against that intruder activity. Storing and maintaining the databases with five IDS agents on each individual sensor node is not a feasible solution as they are resource restricted in nature. The KB systems also increase load on the memory storage, energy and communication cost.

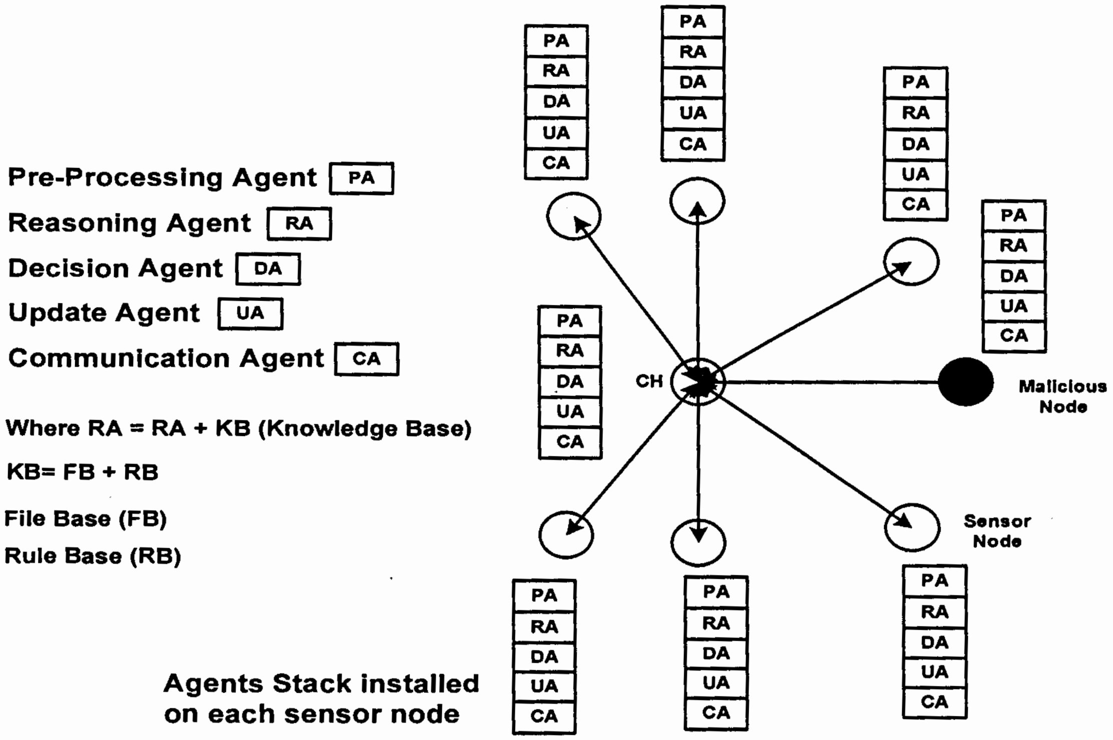


Fig 17: An Improved Intrusion Detection System based on Agents [35]

The pictorial diagram shows the architecture that is proposed by [35]. The ID agents are installed on each node of the network whether the node is malicious or not. That increases the load on memory and is not a cost effective solution in a critical environment.

Similarly in [36] the authors have divided the IDS architecture into four agents: Sentry Agent (SA), Analysis Agent (AA), Response Agent (RA) and Management Agent (MA) as shown in Fig.18. The SA is responsible for monitoring all activities on the node. It is responsible to judge whether intrusion has happened or not. The RA prevents WSN from intrusion by making decisions such as reducing level of trust of suspicious node, cutting off the communication and re-authentication. The MA maintains and co-ordinates the SA, AA and RA. In the case of addition of a new node in WSN or failure of an existing node the MA will get copy of that particular agent from the neighbour nodes. These agents stack is again installed on each sensor node even the node is malicious or not. The installation of multiple agents increases the burden on the sensor node resources. Obtaining copy of failure agent from neighbour node leads towards a security threat.

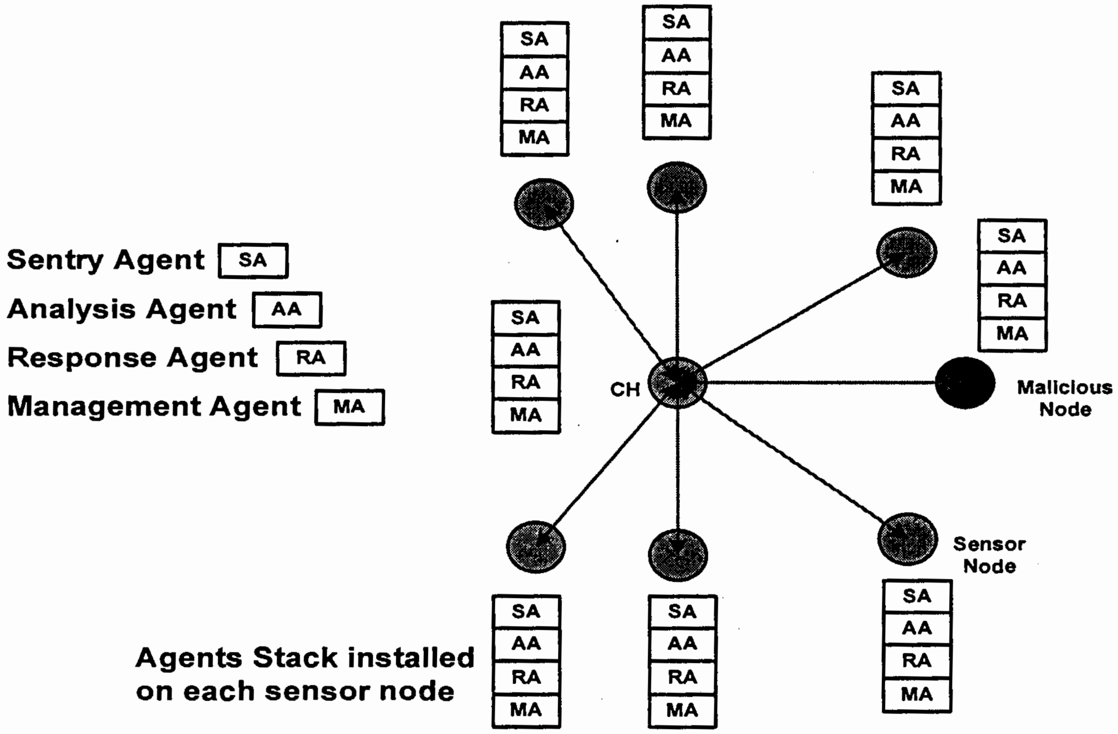


Fig 18: Intrusion Detection System for Wireless Sensor Networks Based on Multi-Agent and Refined Clustering [36]

The pictorial diagram shows the architecture proposed by [36]. The IDS is also installed on each node. When an agent fails the node obtains a copy from its neighbouring node. Obtaining a copy from neighbouring nodes leads towards the security breaches if the neighbouring node is under attack.

We have proposed IDS architecture for WSN [43]. It is divided into three basic units called as Monitoring Unit (MU), Management Unit (MGU) and Co-ordinating Unit (CU) as shown in Fig. 19. The MU is used to monitor the intruder activity. The MGU handle the novel and unknown intrusions. The CU controls the working between these units. These units are independent and failure of one unit does not affect the performance of other unit. These units are installed on each individual sensor nodes and work as LIDS only. As the installation of multiple units on each sensor nodes is not a feasible solution for detecting intruder activity. So our initially proposed solution was not that efficient.

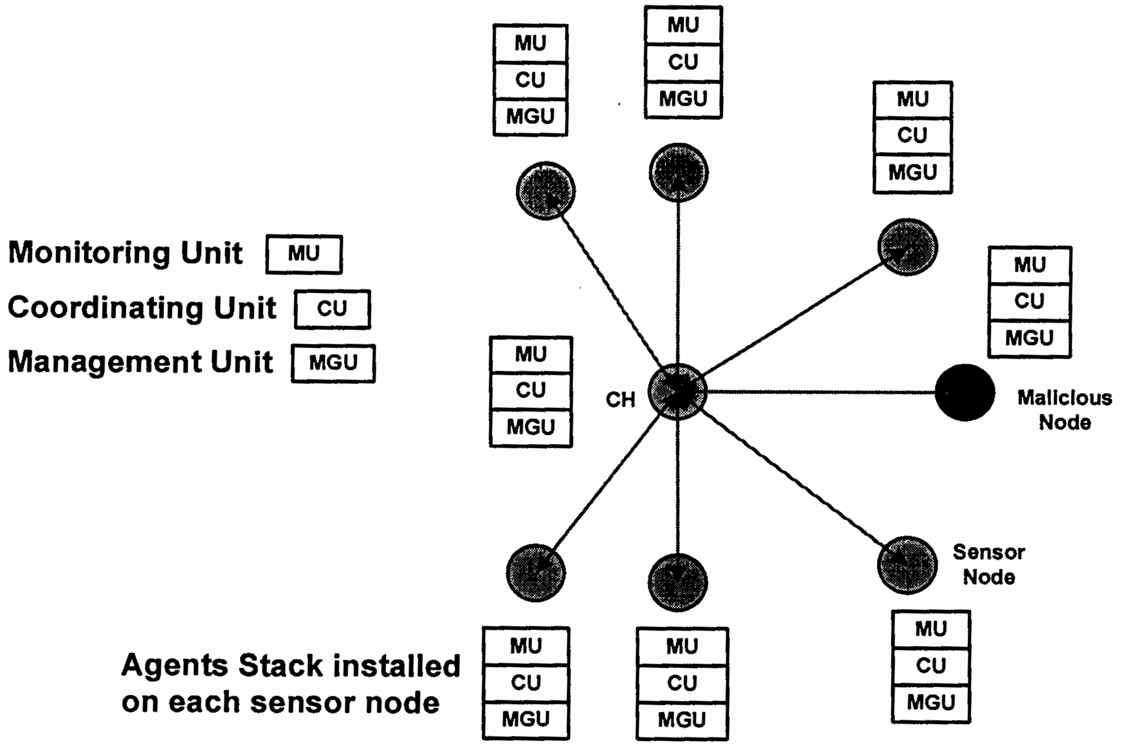


Fig 19: Energy-Efficient Intrusion Detection System for Wireless Sensor Networks Based on MUSK Architecture [43]

The pictorial diagram shows that the architecture proposed by [43] is also installed on each sensor node that is not energy efficient solution in terms of resources. We need to find a security mechanism that not only provides better security but also uses resources of WSN optimally.

We have improved our proposed model [43]. Instead of installing of each intrusion detection module on sensor nodes we have installed on supervisor node called Cluster Head (CH). It is composed of three basic agents named as Analyzer Agent (AA), Coordinating Agent (CA) and Management Agent (MA). We used two threshold frequencies for NIDS and LIDS. . By keeping the limitation of sensor nodes in mind instead of installing IDS architecture on each sensor node we have installed it on the CH only. The CH continuously monitors the network packets. Whenever the malicious activity takes place the CH sends mobile AA to the victim node that works as LIDS. We use mobile agent AA for detecting and further investigating the intruder activity as shown in the Fig 19.

The pictorial diagram shows that the IDS module is only installed on CH. Whenever the malicious activity takes place the mobile AA is transferred to the victim node that uses the resources of suspicious node. The AA sends the malicious to CH for action.

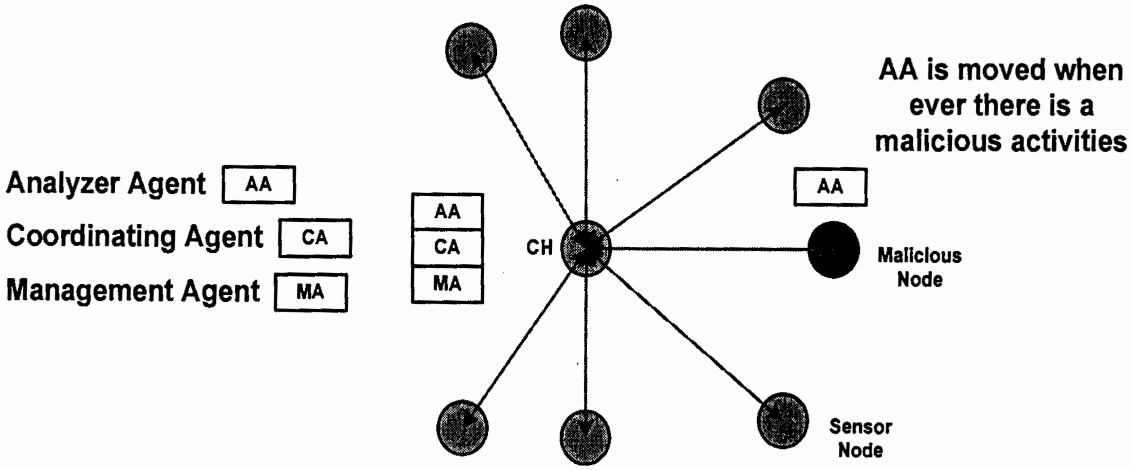


Fig 20: Mobile Agent Based Hierarchical Intrusion Detection System in WSN [44]

6.3.1.2 Security and Efficiency Assessment

We have carried out the performance comparison of our proposed scheme with the existing schemes. We have analysed their performance on two major factors i.e. Security and Efficiency [44].

The security factor is divided further into three parameters i.e. internal, external and novel threats. Internal threats are those attacks that are initiated or injected by the intruder residing inside the network. External threats are from outside attackers. Novel threats are the unusual or unrecognized form of the intrusions which have not occurred previously. Three types of possible values used by these intrusions are low, high and medium that indicates how clearly the proposed scheme identifies these intrusions. We have given a low value to all those schemes that do not provide defence against the compromised node, under attack nodes, inside attackers, master or secret key is captured or the node activity is dependent on the neighbourhood node information, trust relationship on nodes etc. A medium value to all those proposed schemes that identify the intrusion but do not provide any defensive measurement so that how to handle them, generate false negative in large amount. A high value to all those schemes that clearly identify the intrusion as well as provide the counter measure against that intrusion, compromise of one node will not make the whole security of the system vulnerable.

Table 2: Comparison table of different existing security techniques

Sr. No	Scheme Name	Security			Efficiency			
		Internal Threats	External Threats	Novel Threats	Comp. Costs	Network Band-Width	Node Resource	No. of Messages
1	Security Protocol for Sensor Networks [19]	Low	High	Low	High	High	High	8
2	A Security Architecture for Mobile WSN [20]	Low	High	Low	High	High	High	---
3	Scalable Session Key Construction Protocol for WSN [21]	Low	Low	Low	High	Medium	High	---
4	A Tree Based Approach for Secure Key Distribution in WSN [22]	---	---	---	High	Medium	High	4+4
5	A unified security framework with three key management schemes for WSN [24]	Low	High	Low	High	High	High	---
6	An IDS for WSN [28]	Medium	Medium	High	---	High	High	---
7	Anomaly Intrusion Detection in WSN [29]	Medium	Medium	---	---	---	---	---
8	Decentralized Intrusion Detection in WSN [31]	---	---	---	High	High	High	---
9	A Decentralized IDS for Increasing Security of WSN [32]	High	High	High	High	High	High	---
10	Intrusion Detection based Security Architecture for WSN [33]	Medium	Medium	High	High		High	---
11	Energy Efficiency of IDS in WSN [34]	High	High	High	High	High	High	---
12	An Improved IDS Based On Agent [35]	---	---	---	High	High	High	---
13	A Framework of Machine Learning Based Intrusion Detection for WSN [40]	---	---	Low	---	---	High	---
14	Mobile Agent Based Hierarchical IDS (Proposed Scheme)	High	High	High	Medium	Medium	Medium	---

We have divided the efficiency factor into four parameters i.e. computation costs, network bandwidth, node resource utilization and number of messages. Two types of values are used high and medium in computation cost, network bandwidth and node resource utilization. We have given high value to all those schemes that increase burden on network resource i.e. cryptographic algorithms are resource hungry in nature that require extra computation and memory overhead, communication steps between nodes increases, simultaneous transmission increases the rate of collision that affect the bandwidth issues, large amount of false negative dissipate the energy resources etc. The medium value is given to the scheme that uses victim resources in order to discover an intrusion by using minimum network resources. The number of messages which contains the integer value i.e. additional steps used by the proposed schemes in order to identify the intrusion. The above Table 2 shows that our proposed scheme is efficient in several aspects as compared to the existing schemes.

6.3.2 Summarized Results

In this section, we have summarized our results from above discussion. We have analysed different attacks graph with different number of packets flowing inside the network. We have summed up the result on the basis on three parameters. These parameters are number of monitor node for detecting intrusions, number of active IDS module on different number of packets and workload on sensor node.

6.3.2.1 Different Attack Graphs

The IDS testing techniques are divided into four categories [45]. This categorization is based on background traffic. These are testing using no background traffic, testing using real background traffic, testing using sanitized background traffic and testing by generating background traffic.

Testing using no background traffic:

In this scheme, the IDS is deployed on either at host or at network level. To detect whether or not IDS can detect malicious activities the computer attacks are launched. These attacks are based on both host and network level. The responsibility of IDS is that it should label each attack properly and has a signature for a set of attacks. This scheme can neither notify about the true or false alarms and thus easy to implement [45]. Our evaluation criteria are based on this testing technique.

Testing using real background traffic:

This scheme is used to determine the hit rate of IDS for a particular scenario. The hit rate tests the quality of IDS. In this technique, it is impossible to assure the classification of attacks naturally occurred in a given scenario. Due to the privacy concern, the real background traffic is not publicly distrusted [45].

Testing using sanitized background traffic:

In this scheme, the scenario or background traffic is prerecorded first and then sensitive data is sanitized. The attacks are then injected into the sanitization data stream. There are two ways to accomplish this task either by creating attack separately and then inject into the sanitized data or replaying the sanitized data stream and attack concurrently [45].

Testing by generating background traffic:

A simulated network or test bed is used with host or network level that can easily be attacked. The victim uses complex traffic generator that models actual network traffic statistic [45].

To analyze the security attacks in WSN Tanveer Zia [15] divide attacks into four classes named as interruption, interception, fabrication and modification. The communication link becomes lost or unavailable in interruption attacks. The adversary captures the node and gains access over it in the interception attacks. In the fabrication attack, the attackers injects false data over the communication path, whereas, the modification attack alters the contents of message.

We have used the above categorization of attacks and divided it into similar four classes. In the scenario 1 we have set maximum threshold up to 30 packets. It means that sensor node will transmit maximum 30 messages to the destination node. The battery time up to 10V and trust level is set up to 10 points. When we simulate our network on 500 packets we have found 10 malicious nodes and 50 safe nodes from a total of 60 nodes. The following table 3 shows the results obtained by running the simulation on the proposed architecture. The entry in red color in simulation environment shows that the selected node is malicious in nature and CH has taken appropriate action against it. To control the communication messages the CH and destination nodes have larger battery time and threshold level as compared to other sensor node in the network. Here it is important to note that the OMNeT++ uses first two nodes ID 0 and 1 for its own gateways for deploying the architecture over the network.

Table 3: Summary of Results

Scenario 1
Max. Threshold = 30
Battery time = 10V
Trust Level = 10
No of Packets = 500
No of Malicious Node = 10
No of Safe Node = 50
Cluster Head (CH) = Node ID 21
Destination = Node ID 23,24,25

* 21, 23, 24 and 25 nodes have larger battery time and maximum threshold level

Node ID	Threshold Level	Remaining Battery Time	Trust Level	Node Status	Malicious Type	Action Performed
2	23	7.699993	10	Sleep	No Attack	Trusted Node
3	26	7.399993	10	Sleep	No Attack	Trusted Node
4	29	7.099994	10	Sleep	No Attack	Trusted Node
5	24	7.599993	10	Sleep	No Attack	Trusted Node
6	28	7.199994	10	Sleep	No Attack	Trusted Node
7	18	8.199993	10	Sleep	No Attack	Trusted Node
8	33	6.699994	8	AA Active	Interception Attack	Re-Authentication Required
9	21	7.899993	10	Sleep	No Attack	Trusted Node
10	11	8.899996	10	Sleep	No Attack	Trusted Node
11	7	9.299997	10	Sleep	No Attack	Trusted Node
12	8	9.199997	10	Sleep	No Attack	Trusted Node
13	58	0	0	Sleep	Interception Attack	Re-Authentication Required
14	96	0	0	Sleep	Fabrication Attack	Isolated Node
15	11	8.899996	10	Sleep	No Attack	Trusted Node
16	33	6.699994	7	AA Active	Modification Attack	Isolated Node
17	15	8.499994	10	Sleep	No Attack	Trusted Node
18	8	9.199997	10	Sleep	No Attack	Trusted Node
19	9	9.099997	10	Sleep	No Attack	Trusted Node
20	28	7.199994	10	Sleep	No Attack	Trusted Node
21*	110	89.00017	10	Sleep	No Attack	Trusted Node
22	38	6.199995	2	AA Active	Modification Attack	Isolated Node
23*	76	92.40012	10	Sleep	No Attack	Trusted Node
24*	171	82.90026	10	Sleep	No Attack	Trusted Node
25*	108	89.20017	10	Sleep	No Attack	Trusted Node
26	17	8.299994	10	Sleep	No Attack	Trusted Node
27	10	8.999996	10	Sleep	No Attack	Trusted Node

28	16	8.399994	10	Sleep	No Attack	Trusted Node
29	53	0	0	Sleep	Modification Attack	Isolated Node
30	37	6.299994	3	AA Active	Modification Attack	Isolated Node
31	9	9.099997	10	Sleep	No Attack	Trusted Node
32	24	7.599993	10	Sleep	No Attack	Trusted Node
33	57	0	0	Sleep	Modification Attack	Isolated Node
34	6	9.399998	10	Sleep	No Attack	Trusted Node
35	7	9.299997	10	Sleep	No Attack	Trusted Node
36	48	0	0	Sleep	Interception Attack	Re-Authentication Required
37	28	7.199994	10	Sleep	No Attack	Trusted Node
38	5	9.499998	10	Sleep	No Attack	Trusted Node
39	7	9.299997	10	Sleep	No Attack	Trusted Node
40	23	7.699993	10	Sleep	No Attack	Trusted Node
41	9	9.099997	10	Sleep	No Attack	Trusted Node
42	16	8.399994	10	Sleep	No Attack	Trusted Node
43	11	8.899996	10	Sleep	No Attack	Trusted Node
44	12	8.799995	10	Sleep	No Attack	Trusted Node
45	8	9.199997	10	Sleep	No Attack	Trusted Node
46	10	8.999996	10	Sleep	No Attack	Trusted Node
47	17	8.299994	10	Sleep	No Attack	Trusted Node
48	9	9.099997	10	Sleep	No Attack	Trusted Node
49	11	8.899996	10	Sleep	No Attack	Trusted Node
50	44	0	0	Sleep	Interception Attack	Re-Authentication Required
51	4	9.599998	10	Sleep	No Attack	Trusted Node
52	5	9.499998	10	Sleep	No Attack	Trusted Node
53	9	9.099997	10	Sleep	No Attack	Trusted Node
54	9	9.099997	10	Sleep	No Attack	Trusted Node
55	9	9.099997	10	Sleep	No Attack	Trusted Node
56	4	9.599998	10	Sleep	No Attack	Trusted Node
57	9	9.099997	10	Sleep	No Attack	Trusted Node
58	8	9.199997	10	Sleep	No Attack	Trusted Node
59	7	9.299997	10	Sleep	No Attack	Trusted Node
60	10	8.999996	10	Sleep	No Attack	Trusted Node
61	5	9.499998	10	Sleep	No Attack	Trusted Node

The Fig 21 shows the graph of interruption attack by simulating on above scenario 1. We have considered number of packets on x-axis and attacks on y-axis. When we generated 500 packets with threshold 30, battery time 10V and trust level up to 10 pts we have 0 interruption attacks. But when we generate simulation for 1000 packets we got 4 interruption attacks. At 1500 and 2000 packets we got 8 and 10 attacks respectively.

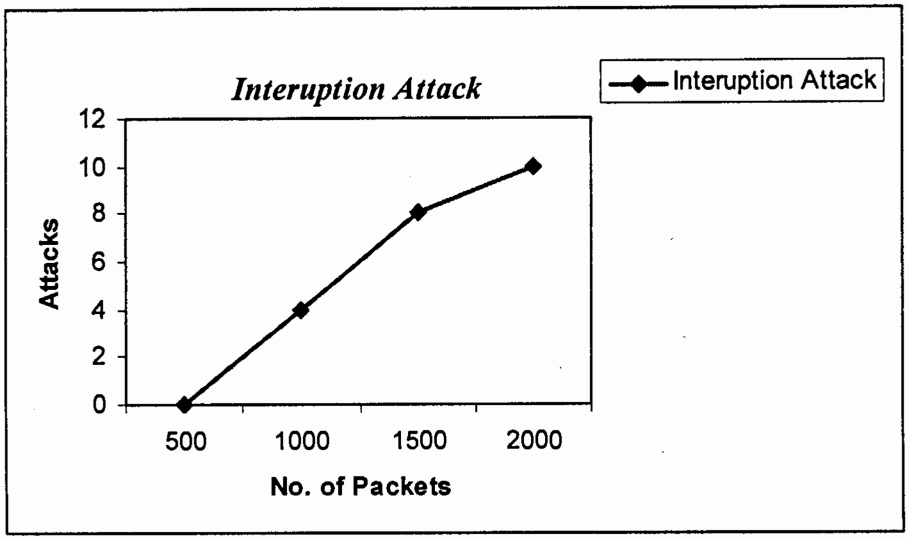


Fig 21: Interruption Attack

The Fig 22 shows the graph of interception attacks by simulating on a similar above scenario1. When we generated simulation for 500, 1000, 1500 and 2000 packets we got 4, 7, 9 and 12 interception attacks.

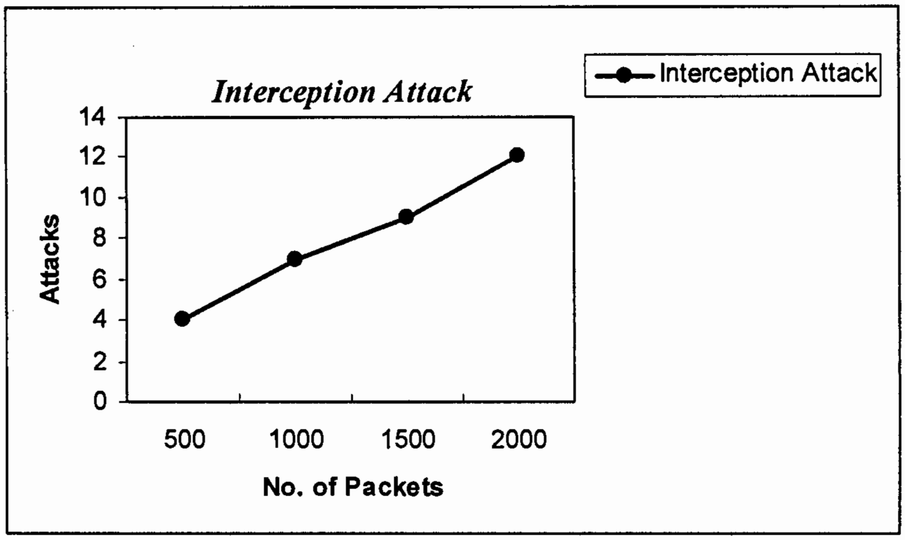


Fig 22: Interception Attack

The Fig 23 shows the graph of fabrication attack. We received 1, 5, 7 and 11 attacks by simulating on 500, 1000, 1500 and 2000 packets.

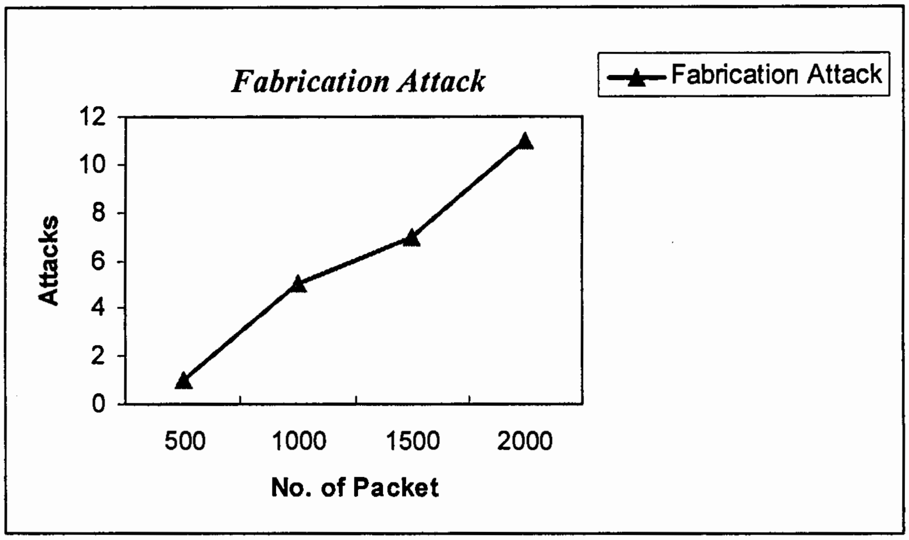


Fig 23: Fabrication Attack

The Fig 24 shows the graph of modification attacks. We received 5, 8, 8 and 13 attacks at 500, 1000, 1500 and 2000 packets.

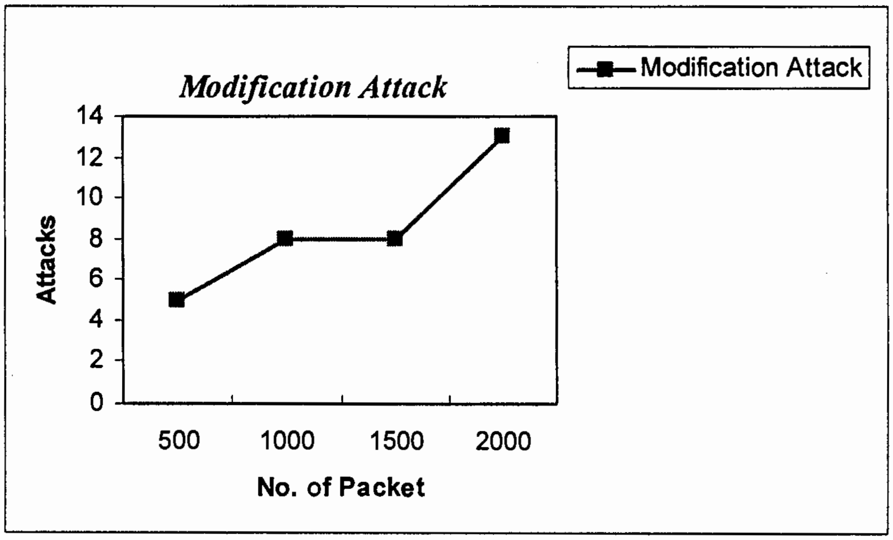


Fig 24: Modification Attack

The Fig 25 shows that accumulated graph of interruption, interception, fabrication and modification attacks by simulating on 500, 1000, 1500 and 2000 number of packets.

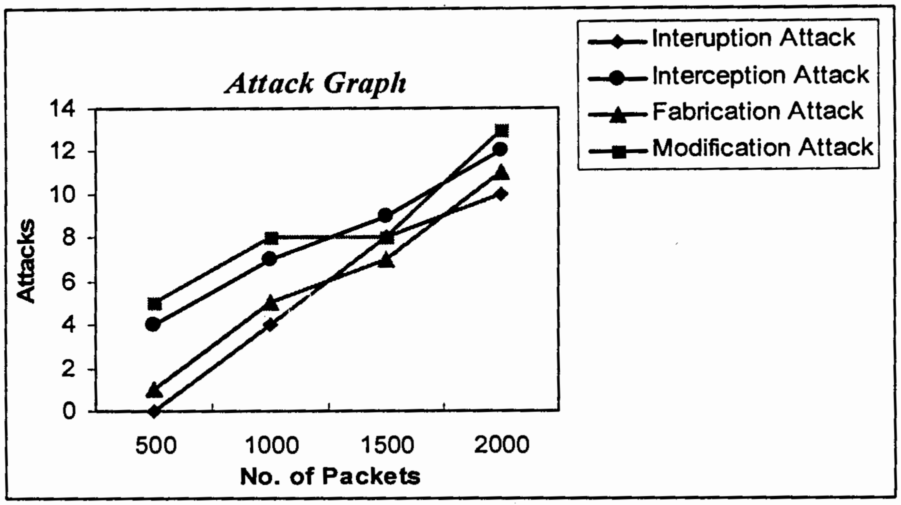


Fig 25: Attack graph (Scenario 1)

The Fig 26 shows the collective graph of interruption, interception, fabrication and modification attacks. We have simulated 500, 1000, 1500 and 2000 packets with threshold 60, battery and trust level up to 20pts (Scenario 2). We got 0, 0, 3, 6 interruption attacks 0, 4, 6, 7 interception attacks, 1, 1, 3, 4 fabrication attacks and 2, 11, 19, 12 modification attacks.

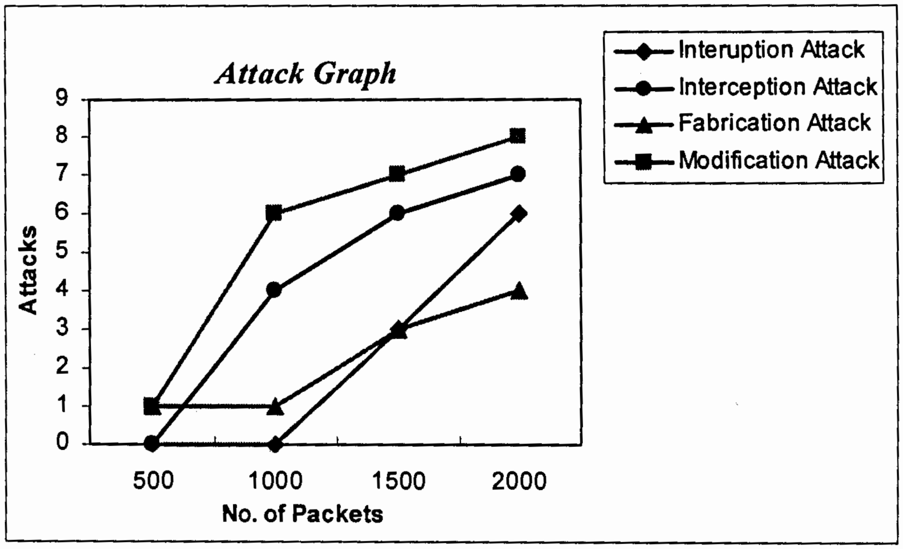


Fig 26: Attack graph (Scenario 2)

The Fig 27 shows the comparison graph of number of monitor node between minimizing intrusion detection module in wireless sensor network [46] and mobile agent based hierarchical intrusion detection system in wireless sensor network that is our proposed scheme. We have considered different number of sensor node called as network density on x-axis. The number of monitor node to detect intrusion on y-axis. The graph shows that [46] constantly uses 10 monitor node to detect intrusion with different network density. For example when there are 20 nodes in a network it uses 10 monitor nodes to detect intrusions. Similarly, in the case of 40 and 60 nodes it also uses 10 monitor nodes. Whereas, our proposed scheme uses only one supervisor node named CH to monitor intrusion with different network density.

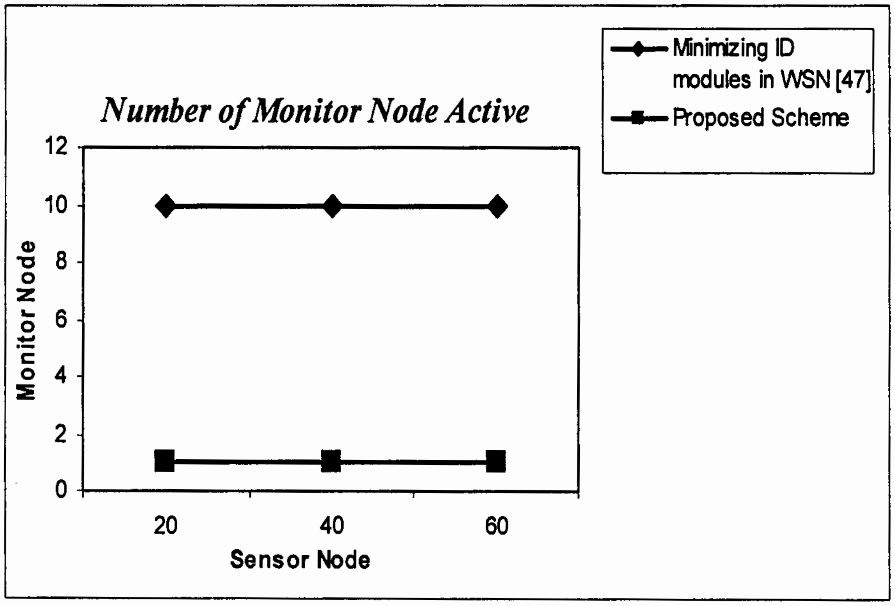


Fig 27: Comparison of monitor node with different network density

The Fig 28 shows the comparison graph of number of active IDS module between [46] and proposed scheme. We have considered different number of packets at x-axis and number of IDS module active on y-axis. When we generate 500, 1000, 1500 and 2000 packets [46] scheme have 13, 16, 15 and 21 IDS module that is monitoring intrusions. Whereas, our proposed scheme uses only 4, 7, 6 and 15 IDS module on 500, 1000, 1500 and 2000 packets respectively.

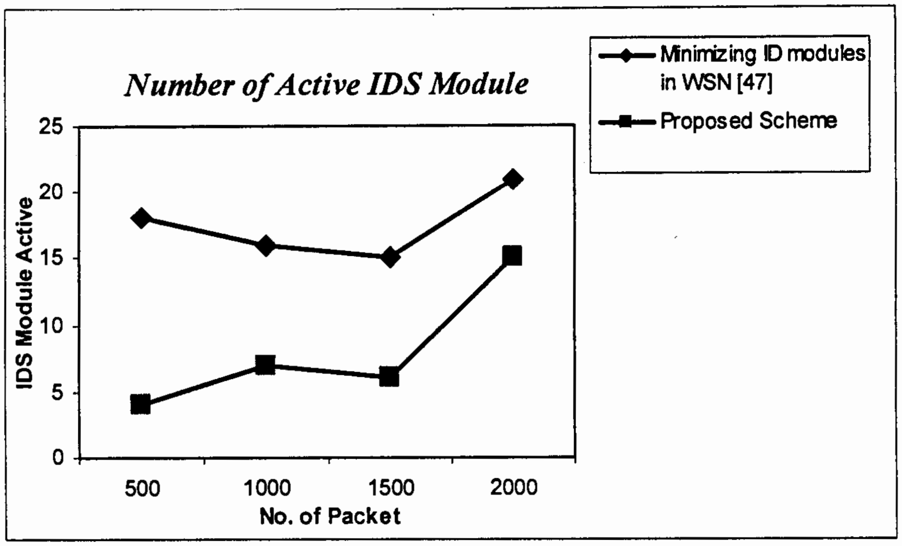


Fig 28: Number of IDS module active on different no. of packets

The Fig 29 shows the graph of comparison of number of agents installed on each CH. The paper [35] uses 5 IDS agents along with the knowledge base system that is installed on each CH. The paper [36] uses 4 IDS agents. The paper [43] and our proposed scheme use only 3 IDS agents that are installed on CH to detect the intrusion.

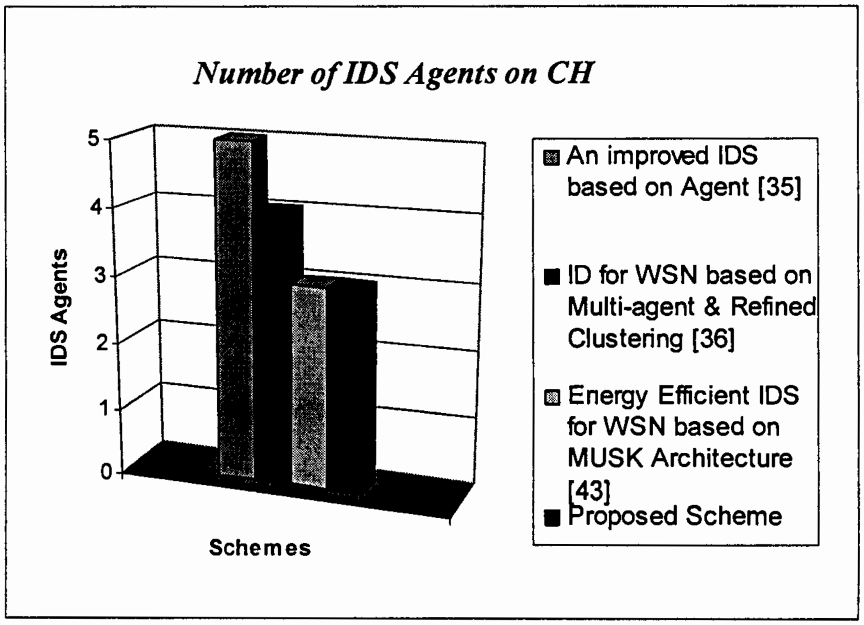


Fig 29: Number of agents installed on CH

The Fig. 30 shows the comparison graph of number of agents installed on malicious node. The paper [35] shows that each sensor is equipped with 5 IDS agents to monitor malicious activity whether it is safe node or malicious. The paper [36] and [43] uses 4 and 3 IDS agents respectively. Our proposed scheme uses only one IDS agent.

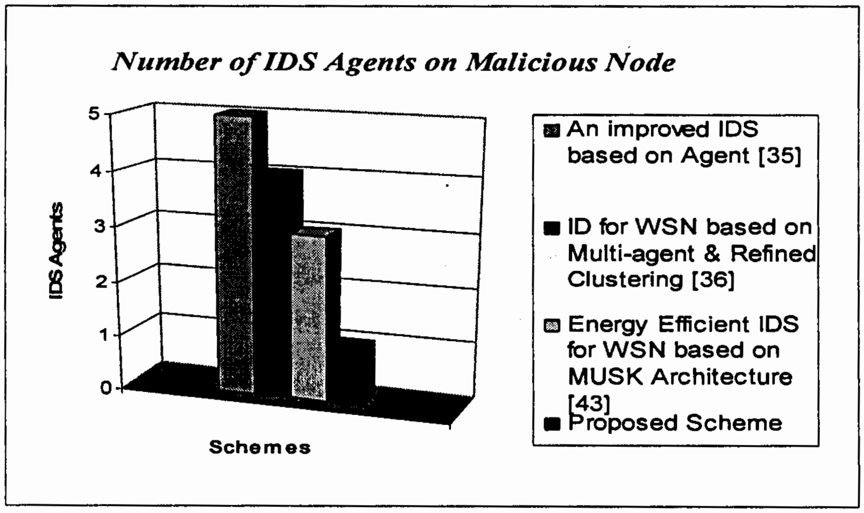


Fig 30: Number of agents installed on Malicious Node

The Fig. 31 shows the comparison graph of number of agents installed on safe node. The paper [35] uses 5 IDS agents. The paper [36] and [43] uses 4 and 3 IDS agents. Our proposed scheme eliminates the need of installing IDS agent on safe node.

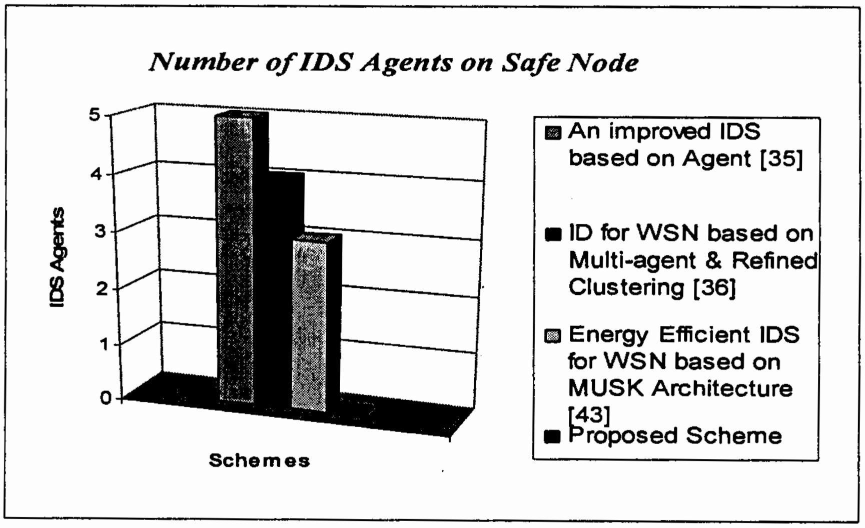


Fig 31: Number of agents installed on Safe Node

The Fig 32 shows the graph of number of IDS active with different network density. Our proposed scheme activates IDS module only on malicious node. When we generate 500 packets we found 10 malicious nodes whereas the paper [17] activates 18 IDS module.

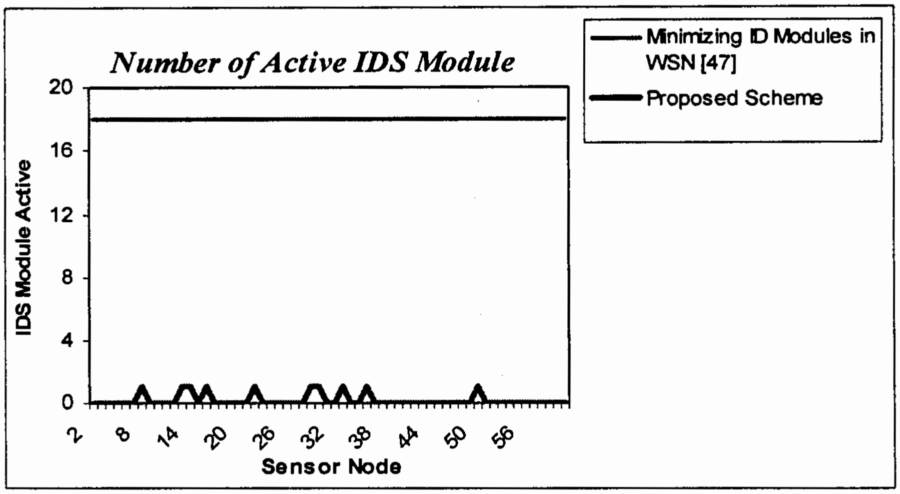


Fig 32: No. of IDS active with different network density

The Fig 33 shows the comparison graph of number of IDS module with different network density between energy-efficient intrusion detection system for wireless sensor network based on musk architecture [43] and our proposed scheme. The graph shows that [43] IDS module increases with the number of sensor nodes whereas our proposed scheme activities IDS module just on the malicious node.

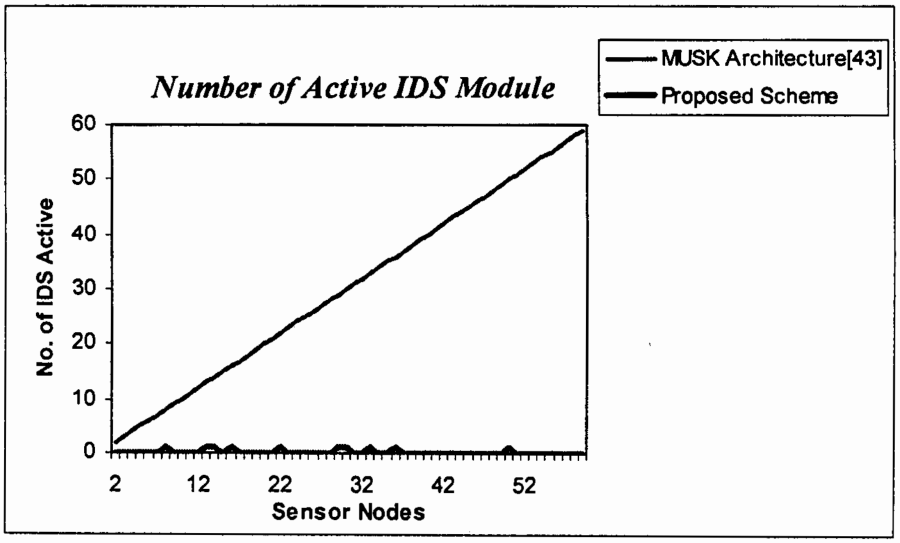


Fig 30: Comparison of no. of IDS module with different network density

6.4 Summary

We have proposed an idea of Mobile Agent Based Hierarchical Intrusion Detection System (MABHIDS) for WSN. It consists of three agents in which one is mobile in nature. The mobile agent activates only when the supervisor node detects an intrusion. Instead of installing IDS on each sensor node we just send a copy of an agent to detect the intrusion. The mobile agent uses victim resources to verify the malicious activity further.

The results show that our proposed scheme provides much better results as compared with the other existing IDS schemes. Instead of installing intrusion detection module on each sensor node we have just installed on the CH or sink node. Whenever the CH detects an intrusion it sends a copy of agent to the victim node to verify the malicious activity. We have used OMNet++ simulator to test our proposed scheme. Our framework consists of 60 nodes in which three nodes acts as a destination node and one node works as the CH to monitor the packets flowing inside the network. The result shows that only one monitor node is active with different network densities as compared to other techniques. The IDS module is active only when the malicious activity takes place. That eliminates the need to install IDS agents on each node and enhances network lifetime.

Chapter 7

CONCLUSION AND OUTLOOK

In this chapter we have discussed the concluding remarks. In section 7.1 we have highlighted our achievements. Improvements are examined in section 7.2. In section 7.3 we have discussed our future work. Brief summary is presented in section 7.4.

7.1 Achievements

A security mechanism for WSN is proposed which provides two levels of security (works both as NIDS and LIDS) by optimally utilizing network resources.

7.2 Improvements

One major advantage of our proposed approach is that it works both as NIDS and LIDS by providing two level of security. It reduces the workload on CH for detecting intrusion and malicious activities. Instead of using CH resources we transfer an agent to the victim node in order to detect malicious activity. That removes the cost of installing IDS module on each sensor node. By keeping in mind the resource restriction in WSN we activate IDS module only on malicious node that is detected by CH. Whenever the novel intrusion occurs the result of that intrusion from the BS will be saved for further use. That eliminates the duplication of intrusion request to BS. One novel request to BS makes whole network update. It also minimizes the security control messages, reduces the network load and saves the sensor node resources. The reduction of communication load over the network enhances the network lifetime which makes the whole network energy efficient. There also exists no trust relationship between each pair of sensor nodes, a sharing of intrusion report with its neighbours node is security vulnerable. In our proposed security mechanism, if one or some (not all) nodes are compromised it will not compromise the whole network. The results show that our proposed framework activates less IDS module than other IDS techniques and eliminates the need to install IDS module on each sensor node.

The CH duty cycle is performed for the specific time of interval. Whenever there is a formation of new CH the previous intrusions by old CH are lost. To tackle that problem the BS collects IR messages from all CH's and saves in its database. After the selection of new CH, the BS sends stored intrusion to the new elected CH. Therefore the previous intrusion in progress would not be lost during rotation of new CH which is the major advantage of our approach.

7.3 Future Recommendations / Outlook

We will proceed with our future works into two directions. First, we will enhance our proposed architecture to detect novel type of intrusion by communicating CH with BS (Anomaly Based Detection). Then we will deploy this architecture into a real scenario for detecting false alarm rate by taking Tanveer Zia et al. [15] into consideration.

7.4 Summary

Lack of tamper resistant packages and insecure nature of wireless channel cause WSN to suffer from security related problems. Traditional security techniques cannot be directly applied to WSN for its severe resource restriction functionality. Therefore, we need to find a security mechanism that not only provides better security but also uses WSN resources optimally. The resource restricted nature of WSN demands a more sophisticated and secure security mechanism for these sorts of networks. There seems an inverse relationship in better security and optimum resource utilization of network resources in existing security schemes of WSN.

In this research article, we have proposed a security model which not only provides good level of security but it also uses network resources optimally for the provision of better security. In our proposed approach, we have proposed a two tier security model for WSN. The NIDS and LIDS are involved in providing two tier securities. The NIDS is installed on all CH whereas LIDS is based on mobile agent. The LIDS is activated whenever CH finds any node suspicious. The CH issues LIDS for further scrutiny of malicious activities of suspicious node in order to confirm it as a compromised node. The LIDS uses resources of suspicious node to investigate it further. The proposed mechanism provides enhanced security using resources of WSN optimally.

The results show that our scheme provides better functionality when compared with other techniques. It not only reduces the IDS modules but also works as NIDS and LIDS. It efficiently utilizes the network resource by using the victim resources for detecting malicious activities. That reduces the work load on CH and enhances network lifetime. The proposed scheme will also update the whole network with just a single IR report to any CH. This framework eliminates the duplication of intrusion request to BS, minimizes the security control messages, reduces the network load on BS and saves the sensor node resources. The reduction of communication load over the network enhances the network lifetime which makes the whole network energy efficient.

References

[1]. ***"Security Models for Wireless Sensor Networks"*** by Sophia Kaplantzis March 20, 2006 Supervisors: Dr N. Mani, Prof. M. Palaniswami, Prof. G. Egan sophia.kaplantzis@eng.monash.edu.au

[2]. ***"Security in Wireless Sensor Networks"*** by Adrian, Perrig, John Stankovic *and* David Wagner, Communications of the ACM June 2004/Vol. 47, No. 6.

[3]. ***"Sensor Networks for Emergency Response: Challenges and Opportunities"*** by Konrad Lorincz, David J. Malan, Thaddeus R.F. Fulford-Jones, Alan Nawoj, Antony Clavel, Victor Shnayder, Geoffrey Mainland and Matt Welsh *and* Steve Moulton, Published by the IEEE 2004.

[4]. ***"Sensor Networks: Evolution, Opportunities, and Challenges"*** by C.Y. Chong and S. Kumar, In Proceedings of the IEEE, Vol. 39, No. 8, August 2003, pp. 1247-1256.

[5]. ***"Overview of sensor Networks"*** by David Culler University of California, Berkeley Deborah Estrin Mani Srivastava University of California, Los Angeles, published by the IEEE Computer society August 2004.

[6]. ***"Wireless Sensor Networks"*** by F. L. LEWIS Associate Director for Research (To appear in Smart Environments: Technologies, Protocols, and Applications ed. D.J. Cook and S.K. Das, John Wiley, New York, 2004).

[7]. ***"A Protocol Architecture for Wireless Sensor Networks"*** by Siddharth Ramesh, School of Computing, University of Utah.

[8]. ***"What is sensor network"*** (National Instruments. All rights reserved. LabVIEW, National Instruments, NI, ni.com) Site address: ***www.ni.com.***

[9]. ***"A Survey of Security issues in Wireless Sensor Networks"*** by Yong Wang, Garhan Attebury, and BYyrav Ramamurthy, University of Nebraska-Lincoln, published by IEEE Communications Surveys & Tutorials 2006).

[10]. ***"Intrusion Detection for Wireless Sensor Networks"*** Edith C.H. Ngai, The Chinese University of Hong Kong Department of Computer Science and Engineering Spring 2005.

[11]. ***"A Survey on Sensor Networks"*** by Ian F.Akildiz, Weilian Su, Yogesh Sankarasubramaniam and Erdal Cayirci Grogia institute of technology, published by

IEEE Communication Magazine August 2002)

[12]. ***"Wireless sensor networks: a survey"*** by I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci Published by Elsevier Science B.V. 2002.

[13]. ***"A Survey on Wireless Sensor Networks Security"*** by Mona Sharifnejad, Mohsen Sharifi, Mansoureh Ghiasabadi and Sareh Beheshti, Published in 4th International Conference: Sciences of Electronic, Technologies of Information and Telecommunications SETIT March 25-29, 2007 – TUNISIA.

[14] ***"Wireless Sensor Networks: Applications and Challenges"*** by A. Alemdar and M. Ibnkahla Electrical and Computer Engineering Department Queen's University, Kingston, Canada , Published by IEEE 2007.

[15] ***"Security Issues in Wireless Sensor Networks"*** by Tanveer Zia and Albert Zomaya, School of Information Technologies University of Sydney, Published by IEEE.

[16] ***"On the Security of Wireless Sensor Networks"*** by Rodrigo Roman, Jianying Zhou, Javier Lopez, Institute for Infocomm Research, 21 Heng Mui Keng Terrace, Singapore and Ingenieria Informatica, University of Malaga, 29071, Malaga, Spain.

[17] ***"Denial of Service in Sensor Networks"*** by Anthony D.Wood John A. Stankovic University of Virginia, published by IEEE 2002.

[18] ***"How to Secure a Wireless Sensor Network"*** by Yee Wei Law and Paul J.M. Havinga Faculty of Electrical Engineering, Mathematics and Computer Science University of Twente, Netherlands, Published by IEEE ISSNIP 2005.

[19] ***"SPINS: Security Protocols for Sensor Networks"*** by Adrian Perrig, Robert Szewczyk, J.D. Tygar, Victorwen and David E. Culler, Department of Electrical Engineering and Computer Sciences, University of California, Berkeley, Wireless Networks 2002 Kluwer Academic Publishers.

[20] ***"A Security Architecture for Mobile Wireless Sensor Networks"*** by Stefan Schmidt, Holger Krahn, Stefan Fischer and Dietmar W¨atjen, published by Springer-Verlag Berlin Heidelberg LNCS 2005.

[21] ***"Scalable Session Key Construction Protocol for Wireless Sensor Networks"*** by Bocheng Lai, Sungha Kim and Ingrid Verbauwhede Department of Electrical Engineering University of California, Los Angeles

[22] *"A TreeBased Approach for Secure Key Distribution in Wireless Sensor Networks"* by ErikOliver Blaß, Michael Conrad and Martina Zitterbart.

[23] *"A Survey of Key Management Schemes in Wireless Sensor Networks"* by Yang Xiao, Venkata Krishna Rayi, Bo Sun, Xiaojiang Du, Fei Hu, and Michael Galloway, published by computer communications, special issue on security on wireless adhoc and senor networks April 24, 2007.

[24] *"A unified security framework with three key management schemes for wireless sensor networks"* by Rabia Riaz, Ayesha Naureen, Attiya Akram, Ali Hammad Akbar, Ki-Hyung Kim, H. Farooq Ahmed, published by Elsevier 17 June 2008.

[25] *"Internet Security: Intrusion Detection & Prevention"* by Joseph G. Tront and Randy C. Marchany, published by IEEE 2004.

[26] *"Defending Yourself: The Role of Intrusion Detection Systems"* by John McHugh, Alan Christie, and Julia Allen, Software Engineering Institute, CERT Coordination Center, Published by IEEE Software September/October 2000.

[27] *"Applying Intrusion Detection Systems to Wireless Sensor Networks"* by Rodrigo Roman, Jianying Zhou and Javier Lopez, *publication in the IEEE CCNC 2006 proceeding.*

[28] *"An Intrusion Detection System for Wireless Sensor Networks"* by Ilker Onat Ali Miri, School of Information Technology and Engineering, University of Ottawa, Canada, published by IEEE 2005.

[29] *"Anomaly Intrusion Detection in Wireless Sensor Networks"* by Vijay Bhuse and Ajay Gupta, Western Michigan University, Kalamazoo, MI-49008, USA, published in 2005.

[30] *"Towards Intrusion Detection in Wireless Sensor Networks"* by Krontiris Ioannis, Tassos Dimitriou, and Felix C. Freiling, Athens Information Technology Greece and Department of Computer Science,University of Mannheim, Germany.

[31] *"Decentralized Intrusion Detection in Wireless Sensor Networks"* by Ana Paula R. da Silva, Marcelo H.T. Martins, Bruno P.S. Rocha, Antonio A.F. Loureiro, Linnyer B. Ruiz and Hao Chi Wong, published by ACM in 2005.

[32] *"A Decentralized Intrusion Detection System for Increasing Security of Wireless Sensor Networks"* by Ioannis Chatzigiannakis and Andreas Strikos, work

has been partially supported by the IST Programme.

[33] *" Intrusion Detection based Security Architecture for Wireless Sensor Networks"* by Debao Xiao , Chao Chen and Gaolin Chen, Department of Computer Science, Central China Normal University, China, Proceedings of ISCIT2005, Published by IEEE 2005.

[34] *"Energy Efficiency of Intrusion Detection Systems in Wireless Sensor Networks"* by Piya Techateerawat and Andrew Jennings, School of Electrical and Computer Engineering Proceedings of the 2006 IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology.

[35] *"An improved intrusion detection system based on agent"* by Bin Dong and Xiu-Ling Liu, Proceedings of the Sixth International Conference on Machine Learning and Cybernetics, Hong Kong, Published by IEEE in August 2007.

[36] *"Intrusion Detection for Wireless Sensor Networks Based on Multi-Agent and Refined Clustering*" by Wang Huai-bin, Yuan Zheng and Wang Chun-dong, Department of Computer Science and Technology, Tianjin University of Technology Tianjin, China, Appeared in International Conference on Communications and Mobile Computing, published by IEEE 2009.

[37] *"Design and Implementation of an Intrusion Detection System for Wireless Sensor Networks"* by Dmitriy Martynov, Jason Roman, Samir Vaidya and Huirong Fu, In Proceedings IEEE EIT 2007.

[38] *"Hybrid Intrusion Detection System for Wireless Sensor Networks"* by Tran Hoang Hai, Faraz Khan and Eui-Nam Huh, Internet Computing & Security Lab, Department of Computer Engineering, Kyung Hee University, South Korea, LNCS 4706, Part II, pp. 383–396, Springer-Verlag Berlin Heidelberg 2007.

[39] *"Optimal Selection and Activation of Intrusion Detection Agents for Wireless Sensor Networks"* by Tran Hoang Hai and Eui-Nam Huh, Internet Computing and Security Laboratory, Department of Computer Engineering, Kyung Hee.

[40] *"A Framework of Machine Learning Based Intrusion Detection for Wireless Sensor Networks"* by Zhenwei Yu and Jeffrey J.P. Tsai, Department of Computer Science, University of Illinois at Chicago, Published by IEEE 2008.

[41] *"Detecting Denial of Service Attacks in Sensor Networks"* by Gu Hsin Lai and

Chia-Mei Chen, Department of Information Management, ational Sun Yat-Sen University, Kaohsiung 804 Taiwan.

[42] ***"A New Method for Intrusion Detection on Hierarchical Wireless Sensor Networks"*** by Rung-Ching Chen, Chia-Fen Hsieh and Yung-Fa Huang, appeard in ICUIMC-09C January 15-16, 2009, Suwon, S. Korea, Published in ACM 2009.

[43] ***"Energy-Efficient Intrusion Detection System for Wireless Sensor Network Based on MUSK Architecture"*** by Surraya Khanum, Muhammad Usman, Khalid Hussain, Rehab Zafar, and Muhammad Sher, accepted in: HPCA 2009, LNCS 5938, pp. 212–217, 2010.© Springer-Verlag Berlin Heidelberg 2010 (In Press).

[44] ***"OMNeT++ Discrete Event Simulation System"***, by András Varga, Version 3.2, A user Manual Guide.

[45] ***"Intrusion detection with OMNeT++"*** by Bazara I.A.Barry, university of khartoum, faculty of mathematics sciences, published by ICST in 2009.

[46] ***"Minimizing the Intrusion Detection Modules in Wireless Sensor Networks"*** by Tran Hoang Hai and Eui-Nam Huh, internet computing and security laboratory, department of computer engineering, Kyung Hee, pulished by IEEE 2008.

Acronyms

ADC:	Analog to Digital Converter
ADT:	Anomaly Detection Table
BROSK:	BROadcast Session Key
BS:	Base Station
CH:	Cluster Head
CIDS:	Collaboration-based Intrusion Detection System
DoS:	Denial of Service
DVSIS:	Distributed virtual Shared Information Space
gNode:	guard Node
GPS:	Global Positioning System
GUI:	Graphical User Interface
IASN:	Information Authentication for Sensor Networks
IDA:	Intrusion Detection Agent
IDS:	Intrusion Detection System
IP:	Intrusion Prevention
IPS:	Intrusion Prevention System
ITID:	Isolation Table Intrusion Detection
J-Sim:	Java Simulator
LIDS:	Local Intrusion Detection System
MABHIDS:	Mobile Agent Based Hierarchical Intrusion Detection System
MAC:	Message Authentication Code
MAC:	Media Access Control
MG's:	Monitor Group's
MUSK:	Muhammad Usman Surraya Khanum
MWSN:	Mobile Wireless Sensor Nodes
NIDS:	Network Intrusion Detection System
NS/2:	Network Simulator -2
PCH:	Primary Cluster Header

PKC:	Public Key Cryptography
P2P:	Point to point
RSSI:	Received Signal Strength Indicator
RTID:	Routing Tables Intrusion Detection System
SCH:	Secondary Cluster Header
SKE:	Symmetric Key Encryption
SNEP:	Secure Network Encryption Protocol
SPINS:	Security Protocol for Sensor Networks
STAT:	State Transition Analysis Tool
TDMA:	Time Division Multiple Access
WSN:	Wireless Sensor Networks