Malicious Cluster Head Detection Mechanism in Wireless Ad-hoc Sensor Networks

MS Research Dissertation

By:

Asima Ismail

(431-FBAS/MSCS/S08)

Supervised By:

Prof. Dr. Muhammad Sher

Co-Supervised By:

Dr. Khalid Hussain

Department of Computer Science & Software Engineering

Faculty of Basic and Applied Sciences,

International Islamic University, Islamabad.

2012

1. Software Engineering

2. Software Patterns

Department of Computer Science & Software Engineering

International Islamic University Islamabad

Dated: 16-3-12

Final Approval

This is to certify that we have read the thesis submitted by **Asima Ismail, Registaration # 431-FBAS/MSCS/S08**. It is our judgment that this project is of standard to warrant its acceptance by the International Islamic University, Islamabad, for the Degree of **MS in Computer Science**.

Project Evaluation Committee

External Examiner:
Dr. Sadaf Tanvir,
Assistant Professor
Department of Computer Science
COMSATS Institute of Information Technology
Park Road, Chak Shahzad, Islamabad

Internal Examiners:
Ms. Fareeha Anwar
Lecturer,
DCS & SE

Supervisor:
Prof. Dr. Muhammad Sher
Department of Computer Science
Faculty of Basic and Applied Sciences
International Islamic University, Islamabad.

16-3-12

Co-Supervisor:
Dr. Khalid Hussain
Assistant Professor,
University Institute of Information Technology
PMAS-UAAR University
Rawalpindi.

Dedication

I dedicate this research project to my beloved PARENTS and Cooperative Friends

A Dissertation Submitted To

Department of Computer Science & Software Engineering,

Faculty of Basic and Applied Sciences,

International Islamic University, Islamabad

As a partial Fulfillment of Requirements for the Award of the

Degree of

MS in Computer Science

Declaration

I hereby declare that this Thesis "Malicious Cluster Head Detection Mechanism in Wireless Ad-hoc Sensor Networks" neither as a whole nor as a part 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 supervisors **Prof. Dr. Muhammad Sher** and **Dr. Khalid Hussain**. If any of the system proved copied out of 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.

Asima Ismail
Reg # 431-FBAS/MSCS/S08

Acknowledgement

I like to express my gratitude to Allah Almighty the Merciful, the Beneficent and the creator of this universe, for providing me the abilities and knowledge to complete this dissertation. I am heartily thankful to my supervisors **Prof. Dr. Muhammad Sher** and **Dr. Khalid Hussaisn** whose encouragement, proficient guidance and altruistic supported me alot during this dissertation. Their support also enables me to develop eloquent understanding of topic for the evolution of idea to commence this dissertation in the first instance.

Foremost, my special thanks go to **Dr. Faraz Ahsan** from Comsats, Islamabad for his expert guidance, great ideas, vision and timely inputs throughout the course of my thesis. I would also like to thank him for his constant motivation. I am also glad to have worked under him for over a year, during which he helped me identify key research areas in network security, eventually culminating in my thesis.

I am indebted to Saleem Iqbal for his support in the implementation of this project, he guided from scratch to the final level. I am also grateful to him for his understanding and gestures towards me and my project. He consistently helped me to overcome those problems, which I really faced during the idea and thesis implementation.

All of my true friends supported me a lot especially, I would like to express my admiration to Ch. Sarfraz Ahmed for his extra ordinary support, without his persistent help, this dissertation would not have been possible.

I would like to mention my family support, morally and financially during whole my academic career which enabled me to work dedicatedly especially my uncle always encouraged me that I remain persistent with my studies.

Asima Ismail
Reg # 431-FBAS/MSCS/S08

Project in Brief

Project Title:	**Malicious Cluster Head Detection Mechanism in Wireless Ad-hoc Sensor Networks**
Undertaken By:	**Asima Ismail (Reg # 431-FBAS/MSCS/S08)**
Supervised By:	**Prof. Dr. Muhammad Sher** **Department of Computer Science** **Faculty of Basic and Applied Sciences** **International Islamic University, Islamabad**
Co-Supervised By:	**Dr. Khalid Hussain,** **Assistant Professor,** **University Institute of Information Technology** **PMAS-UAAR University** **Rawalpindi.**
Start Date:	**September-2010**
Completion Date:	**February- 2012**
Tools and technologies:	**OMNET++** **VC++** **MS Visio** **MS Office**
Operating System:	**Windows XP**
System used:	**Intel(R) Pentium(R) M Processor 2.00 GHz** **Core2**

Abstract

In adhoc network nodes are mobile having no infra structure and distributed in nature this why it is susceptible to many security threats and attacks. All nodes participate for the transmission of data within the network and responsible for designing network topology where suspicious and malicious activities can be detected by different techniques like Intrusion Detection System that is dynamic in nature. Efficient resource consumption is compromise if network security is enhanced that is why security must be achieved for getting reliable and accurate data

As in clustering environment, communication carried out through cluster heads, we are having two Secondary cluster Heads (SCH) and one primary cluster head (PCH). SCHs communicate via PCH and if one of the Secondary Cluster head compromised, the entire network affected. Malfunctioning of cluster head detected and indentified so that it disowned and all network can work smoothly and securely. To handle this issue we propose "Malicious Cluster Head Detection Mechanism in Wireless ad-hoc and Sensor Network" that provide security by minimum utilization of the resources after detection and identification the malicious Cluster Head.

Proposed mechanism based on two types of threshold, for detection and identification of malicious cluster head that is dropping packets because of blackhole attack. We used watchdog technique for initial monitoring than an agent is launch for detection and identification of the packets dropping reason. Proposed mechanism specially designed for secure UDP traffic transmission and fake report detection done by any of the malicious SCH to PCH. On the bases of thresholds, malicious SCH detected and disowned from the network.

Table of Contents

Chapter 1: Introduction

Chapter 2: Preliminaries

Chapter 3: Literature Survey

Chapter 4: Research Domain & Objectives

Chapter 5: Proposed Solution

Chapter 6: Methodology

Chapter 7: Testing and Performance Evaluation

Chapter 8: Conclusion and Future Directions

Chapter 1

INTRODUCTION

MANET is a network without any infrastructure [1]. Reduction in the prices of, laptops, cellular phones, PDAs, mobile devices, became a main cause to develop the interest in wireless networks in past decade where Pervasive & ubiquitous catering had considered a most recent development in wireless network to both nomadic and fixed users. On industrial and individual level, different standards regarding wireless used to fulfill the requirements where Wireless Local Area Network is the most common. It uses a single backbone to connect many mobile nodes in one network with short coverage are deployed by cafeterias, educational and business organizations. There was also a need to meet the requirements of other scenarios like communication of soldiers in battlefield, where messages carried out by using physical constraint of the medium whiteout deploying fixed wireless access point that is risky one. It is not convenient regarding enemy access that became one of the main reasons to promote research in the field of Mobile Adhoc Networks (MANET), without dominant infra structure for communication. MANET formed by the combination of mobile hosts without having any centralized support service like administrator, provides the availability to all hosts to connect it in WLAN environment [2]

1.1 Taxonomy of Wireless Networks

Set of nodes connected in wireless network either directly or through some access point as base station to communicate with other mobile nodes. Taxonomy of Wireless Networks is as under:

1.1.1 Wireless LANs & PANs

Different devices like palmtop, laptop, PDA, PC, in wireless local area network act as mobile nodes to communicate each other via base station or any access point shown is Figure-1.

Generally, WLAN mostly deployed in offices, universities, schools, and cafeteria in different forms.

According to IEEE 802.11 standard, WLAN having

(a) Transmission range (1 Mbps to 45 Mbps)

(b) Frequency bands (2.4 GHz to 5 GHz)

(c) Bandwidth (Upto 54 Mbps) according to new standard IEEE 802.11g

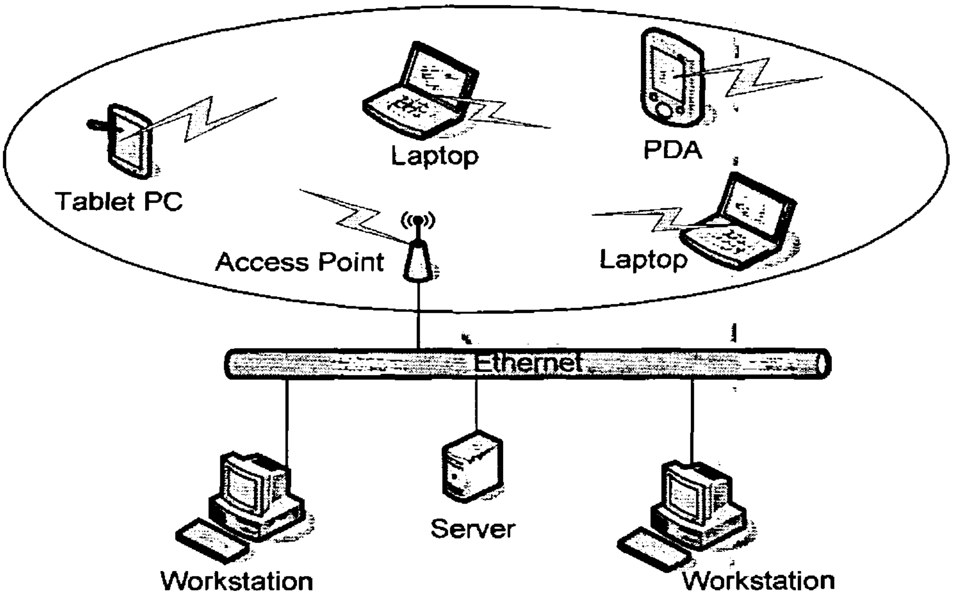

Figure-1: Wireless LAN [2]

WPAN is a network of Personal devices like digital camera, PDAs, laptops etc having

(a) No fix infra structure

(b) Short range

(c) WPAN follows IEEE 802.15.1 standard for Bluetooth devices

1.1.2 Wireless WANs and MANs

Wireless internet is an emerging technology having no backbone to connect to the internet by using mobile nodes. By covering large area, network divided into cells having several mobile terminals (MT) with fixed base station used for communication by following cellular architecture shown below:

In the structural design of cellular networks, first, second and third generation systems are used that follow handoff procedure for communication between two cells via base station. Second generation (2G) having TDMA, GSM, PDC, and GSM having old technology CDPD overlay on AMPS [4] are mostly being used as second and third generation cellular network support data/voice transmission fully with increased transmission speed.

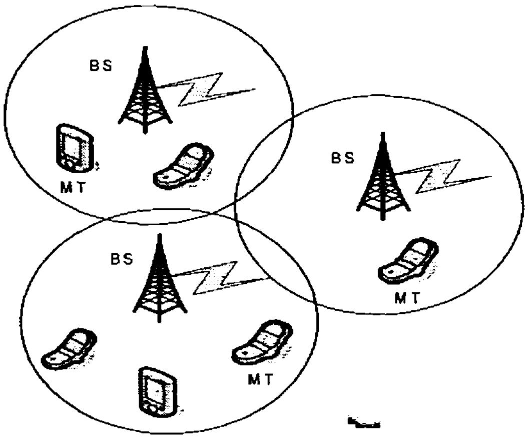

Figure-2 wireless Internet [2]

If large part of city and number of kilo-meters are covered for communication then it is called wireless Metropolitan Area Network (WMAN) that rely on OSI model following IEEE 802.16 standard that often being used for multimedia applications including telephony and digital video and real time data as well.

WWAN covers large area network than WLAN with additional supporting features like radio signals over analog, microwaves and electromagnetic waves, digital cellular or PCS networks are also part of WWAN.

Mobile Adhoc Network in one of the types of wireless networks that need no infra structure and base station an can be easily deployed in the environment where setting wired network is impossible. Every node in the MANET act as a router that form a router complex and can communicate by forwarding packets without any particular base station as shown on the figure-3

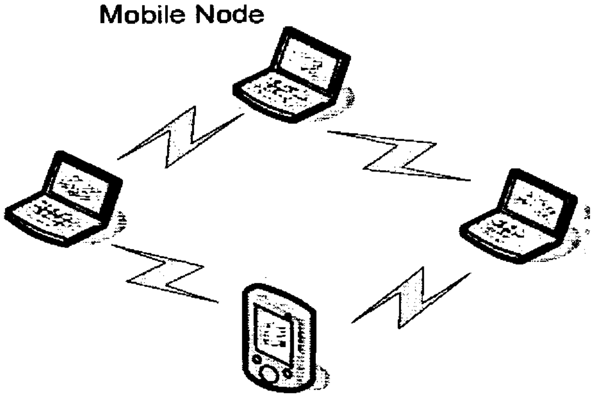

Figure-3: Adhoc Network [2]

1.2 Application of MANET

In the environment where we can not rely on central nodes we prefer to deploy Adhoc Network that is decentralized and dynamic in nature and required less configuration in the case of any emergency like war. As compared to the wired network its adoptive nature of communication protocol, dynamic topology and less time consumption make it preferable in critical environment. There are many applications where Adhoc Networks deployed while we consider some of the scenarios given below:

1.2.1 Rescue Operations & Battlefield

In the case of fire fighting we have to deploy node quickly so in that case MANET are preferable as in battlefield hand-held devices used so that soldier's troops may communicate with each other confidentially.

1.2.2 Vehicle mounted Devices

Movement of soldiers and vehicles judged by using Adhoc networks that mounted with vehicles to recharge the mobile device by using power source.

1.2.3 Event coverage

In such scenarios, multimedia traffic exchanged between different nodes that can be PCs, laptop, palmtop, PDAs etc as for example in press conference all reporters share date among themselves gradually.

1.2.4 Class rooms

For sharing data among all students within the classrooms, Adhoc Network made.

Adhoc network divided into three types on the bases of its main applications, which are:

(a) Mobile Adhoc Networks

(b) Wireless Mesh Networks

(c) Wireless Sensor Networks

1.3 Silent features of MANET

Following are silent features of MANET:

(a) Network component are not dedicated

(b) Operation are energy-constrained

(c) Limited bandwidth

(d) Physical security is limited

1.4 Advantage of MANET

Because ease of deployment, cost efficiency, convenience, mobility, scalability MANET has many advantages, [3] like Scalability: Random joining and leaving of node have no effect on network. In a wired network, if we want to add more nodes we need more equipment but not required in Adhoc case. Deployment: MANET is a network without having any infrastructure and required fewer configurations so it deployed in any environment easily. Mobility: Nodes in MANET can access internet from anywhere not only from the working place but also from any other place as its node are mobile like bluetooth, infra red that are wireless node and can provide internet connection any where any time. Cost: There is no need of cable to make a network so its cost is much less than other wired/ wireless networks. Convenience: Because of mobility MANET, users can access all the resources within their office or home equally. Productivity: Continuous connection from a particular network maintained from one to another place, as it is more productive than any other network because employees can be available to their company all time.

1.5 Disadvantage of MANET

MANET advantages mentioned above now we looked at prone & cons of MANET that make it un- feasible to deploy [3]. Reliability where mobile devices communicate each other in the form of signals that is subject to the interruption especially by microwaves that badly affect the performance, reliability and scalability of the MANET so that it is not preferable in small area networks. Bandwidth is one of the constraints of the MANET because of its low capacity links that facilitates mobile uses to interact with the wireless network easily. Range where MANET users can access it within a fixed range because of that it is used for small networks and not supportable for large infrastructure. Radio emission in wireless technology rely on the radio frequencies for the transmission of data or messages via bluetooth, infra red or any other technology, emission of such signal through the interface may cause bad effects on human health. Security regarding MANET use open medium for communication and having no fixed infra structure so strong encryption techniques demanded to meet the security aspect that is a challenging task for research.

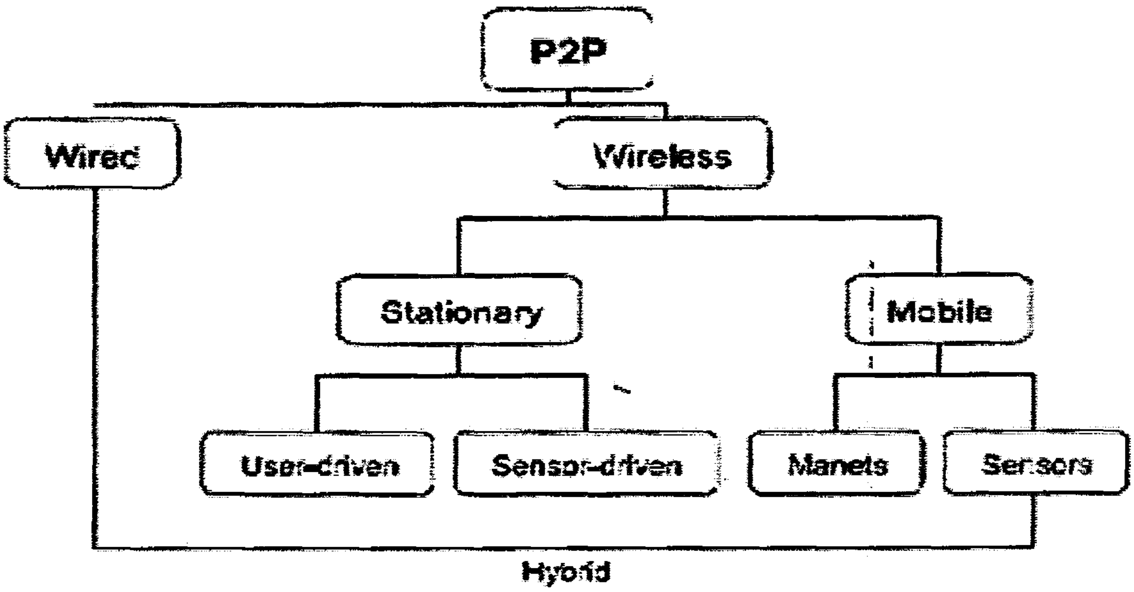

Figure-4 Hierarchy of Networks

1.6 Motivation:

Adhoc network is wireless networks that need mobile nodes acting as a router. They have no infra structure for data transmission that considered as an attractive feature but if we consider security aspects in MANET, it is still an issue even though many mechanisms like:

- Proactive as for example encryption and firewall
- Detective like Intrusion, data correlation
- Reactive like, recovery, block IP address & terminate connections etc.

regarding security are proposed but on attack handling there is still a gap for further research. Just like that in sensor networks where each node is battery depended, there must be a way that can deal proper and secure delivery of data. Achieving security and delivering data efficiently is the main task in sensor networks. Data transmission is carried out by mutual communication of all nodes so misbehave of a single node can damage the whole performance of the network so it must be detected to carry on secures communication. In the environment where sensors deployed properly and base station is not receiving measured information than we can say sensor deployment is not fruitful that is obviously because of some misbehavior that must be diagnosed.

1.7 Problem Domain

Wireless Sensor Network is an up-and-coming technology. Inadequate amount of energy, processing capability and storage capacity considered some of the restrictions of the WSN. Because of these restrictions traditionally security mechanism of the ad-hoc network are not adequate for the WSN. Self-protecting approaches in WSN are static like firewall and encryption while in the case of dynamic these called first lines of defense as it facilitates only external threats. While we need security mechanisms, related to both internal and external threats to make our system reliable and efficient because compromised cluster head not only affect the whole cluster but also degrade the network performance.

Security is an important aspect in wireless networks as it is vulnerable to many attacks. Because of distributed environment and open media, attacks can easily affect the network. Suspicious and malicious activities detected by the Intrusion Detection System that is dynamic in nature. Efficient resource consumption is compromise if network security is enhanced as the strong security and efficient resource utilization of sensor nodes have inverse relation cleared from my given literature to handle this issue we proposed "Malicious Cluster Head Detection Mechanism in Wireless ad-hoc and Sensor Networks" that provide reliable data transfer.

1.8 Thesis Contribution:

Misbehaving activity can results in packet drop that may be cause of any attack or link error. There are many network layer attacks like selective forwarding, sinkhole, hellow flood attack while black hole attack is considered in this research work, in cluster based environment, on cluster head.

Proposed mechanism makes the communication smooth and reliable by the detection and identification of malicious cluster head that drop packets because of black hole attack. After detection of malicious cluster head, it dis-owned from the network and new CH selected. It also provides reliable traffic within the network by detecting fake reporting of malicious CH in case of UDP traffic.

1.9 Thesis Organization

In chapter-2 we have a look on the basics of thesis topic, chapter-3 describe the background related to the malicious node / cluster head detection, Chapter-4 narrated literature survey related to problem domain. Chapter-5 elaborates the identified problem domain after that Chapter-6 explains the proposed solution regarding to sort out my problem. Chapter-7 gives us information about implementation and simulation related to problem domain. Chapter-8 has conclusion & Future work

Chapter 2

PRELIMINARIES

Everything had some background if we came to know that we can easily find out its prone & cons. MANET is an emerging technology where security aspects considered because of its distributed nature. Many issues lies in mobile adhoc networks but security and reliable transmission of data can not be neglected in any case. In this chapter, different type of attacks & threats related to security with their handling ways discussed. Attack in MANET are also considered to make background of problem domain and problem statement focused in thesis

2.1 Security threats in wireless networks

There are a lot of the possible aspects that can make changes in the wireless network performance either weather, noise, media cause or malicious node or any mal-functioning activity that effect the network and deceitful for its bandwidth as well. For effecting network performance intruder can break the link most frequently after switching from one link /channel to another link / channel as in automatic fault management (AFM) case attacker produce as many fault alarms as the actual attack can be neglected that is stiff to be find out in research area [5]. Different supposition and solution are present as in TCP case it can be declared that packets dropping can be because of congestion while on MAC layer contention is considered the cause of the same problem both having terrible effect on the transmission rate as channel conditions are going to suffer here [6]. There can be many other security threats related to reliability, packet dropping, delays etc.

Many problems may exist in wireless environment like:

- In wireless network harms like packet loss, occur because of congestion (rarely), handoffs (results in slow start or timer out problems), bit errors and reordering in some type of wireless nets.
- Packet loss simulated in TCP either for the reason of congestion having poor interaction with the network, trigger by the loss of wireless packets and reordering.

- Duration of noise and poor signal strength are also causes of packet loss in TCP Window handled if we slow down the increase of congestion window or add some congestion control.
- Even though in low bandwidth delay rate is high like RTT, quite long as in busty loss, that is why cumulative Acknowledgement Scheme is not so fair.

Many problems exist within Mobile Adhoc Network as packets forwarded by the collaboration of all nodes that act as a router. In this section, we briefly have a look on these issues:

2.1.1 Distributed Network:

Like Peer-to-peer network, MANET distributed without any fixed infrastructure, as there is no central device to manage all clients.

2.1.2 Security

Security is main issue in the MANET as all nodes are mobile and corporate each other for communication so confidentiality, authentication and integrity is hard-core to achieve in such scenario. That is an important aspect of research now a day.

2.1.3 Addressing Scheme:

In centralized system mobile IP handled by any central authority or a base station but in MANET addressing scheme that avoid any duplicate address is handled by dynamics nature of network topology.

2.1.4 Dynamic Topology:

Because of distributed nature and lack of fixed infra structure the topology used in MANET is not continuous and change time by time by using adoptive routing protocol that support the self organization factor of the mobile nodes.

2.1.5 Network Size:

Sever upper bound is applied on the network size by the protocol that is being used in MANET although it is the striking nature of the MANET as it is being used on commercial level for delivering data in meeting, class rooms etc.

2.1.6 Power Awareness: Mostly, MANET deployed in an unfriendly environment. Functionality of mobile nodes relies on the power consumption or battery timings so the protocol that used must have power awareness.

2.2 Network security

A platform where the entire users interact and communicate to share information & data, a network shaped that have some protected resources that must be secure and demand of network security. Valued accessible network resources and protect the network from the unfair and unauthorized access by monitoring the efficiency and performance of the network and its effects on entire communication. One question that always comes in our mind, the impact of confidentiality, integrity, authentication, privacy and availability of resources, results in the wastage of the reliable and expensive resources by getting access by the illegal user or attacker where there is no concept of security measures in network. That is why genuine users can not get access to the required resources and result in fail of communication that why security policies and protection mechanism is demanded against all such type of attacks and threats that facilitate the network to perform desire operations in any unfavorable condition that is obstacle in the performance of the network as well [7].

Proper security policy is required to achieve reliability, efficiency and performance to utmost level after detecting, preventing and recovering network from the malicious activity given below:

2.2.1 Attack Prevention

Prevention techniques prevent the network from any malicious activity or attack that can damage its performance. Implementations of these techniques also allow the attacker to intrude into the network then prevent it and secure the network from failure. These techniques are strong enough to fight against attacks and regulate the network as for example roll of firewall in "Infiltration attack" where malicious node enter into the network and occupies its resources for its own use, that prevent interference of malicious nodes into the network and also save the network from DoS attack. Another example of entering malicious nodes in the network is "Lying" where malicious node show off itself as a legitimate user. Prevention techniques are Digital Signatures, Access Control & Authentication, Authorization, Digital Signature, Non-Repudiation, Time stamping while Firewalls, Cryptography, Intrusion Prevention System and Anti-Viruses are main sources to save network from Infiltration [7] and also helpful to prevent it from risk of hacking. Prevention techniques try to provide maximum protection to the network but in some cases, when many fake queries are made theses approach fail and malicious intruder enter within the network and commit DoS attack.

2.2.2 Attack Detection

Once attack happened the next step is its detection and finding out all occupied resources by the attacker and recover it back so that authorized user continue its task by using required resources. For appropriate security measure a report of the attack and the damages caused by that attack are send to the network administrator

2.2.3 Detection Techniques

Some of the Attack detection techniques are as follows:

2.2.3.1 Intrusion Detection

In this technique, malicious nodes detected & prevented from entering into the network whenever intruder tries to enter into the network [7].

2.2.3.2 Quantum System

When encryption key broken by any intruder quantum system works discover and determine the quantity of that malicious deed

2.2.3.3 Watchdog, Processor, Polling, Beacons

To recovery the network in its original, state when any resources fail these techniques used for diagnoses of the attack or mishap.

2.2.3.4 Fail-Stop Digital Signature

This technique used for identifying, retrieving the resources back to the network and discard the treachery that bread the prevention techniques and entered into the network somehow.

2.2.3.5 Tripwire & Viruses Scanner

These techniques detect Infiltration attack not caught by the prevention techniques and recover the damages that occur because of that attack.

Some of the threats always exist in the network that is susceptible to many attacks that make their ways by using these techniques.

2.2.4 Attack Recovery

Techniques that used to repair the damaged network resources after the attack to its original state called recovery techniques that enable the network to work properly according to its original desired tasks. Lost information restored by these techniques for example if someone has encrypted his data by using any private key and placed that key in any storage like hard disk/

floppy disk that got damaged because of any reason then way to recover that key is the recovering techniques like Escrow, Rebooting or Restarting, Hot Swapping and Fail-Over [7]. Other recovering technique like Auditing, a great defense against malicious node that is pretending to be legal, and Certificate Revocation that re-allocate the certificate to all nodes to recover the network from damages occurred because of Infiltration.

2.3 Malicious node

2.3.1 What is Malicious Node?

If malicious nodes are present in a MANET, they may attempt to reduce network connectivity (and thereby undermine the network's security) by pretending to be cooperative but in effect dropping any data, they meant to pass on. These actions may result in defragmented networks, isolated nodes, and drastically reduced network performance [9]

In pure AODV protocol malicious node can be harmful for the network whether it is dropping, altering, modifying the packets or cause Denial of Service because of any reason like the one intermediate node are not working properly etc will down the overall network performance level [10].

2.3.2 Malicious Activity & Misbehaving Nodes

Malicious nodes in MANET greatly affected the availability of network services these are broken nodes having non-functional aspect in network. Malicious nodes are: that try to damage the network, misbehave nodes, try to change the network traffic by using the resources of the node or selfish node that got agree to transfer data but does not do that and drop packets by using network bandwidth and resources. Malicious nodes that selectively dropping packets can hidden within the network. It can add more packets into the network causing DOS attack as well [11]. While node misbehavior on network level can be of two types related either to routing or with packet forwarding [12]. In MANET IDS mostly used for the detection of malicious activity by data collecting and analyzing via malicious node and all other nodes within the network it may be collaborative IDS system working on schemes as cluster based voting, trust building and neighbor monitoring [13]. IDS can be misuse detection that detects only that attacks that recorded in its database unable to identify the new one other that is anomaly detection can detect on the bases of comparison of the sender and receiver behavior and its variation must be reported [14].

Bo-Chao Cheng et al write up in his paper about the malicious effects on the existing IDS that designed to detect any malicious activity within the Mobile Adhoc network [15]. Even appropriate mechanism of the IDS is still unable to get the desire results as the method / mechanism of the malicious node coverage within the network is not so strong. From the concept of containment strategies, for limiting the degree of the attacks the functionality of the IDS improved in this paper and new idea of AODV with the name of T-Sec AODV protocol that give repaid detect malicious node and discard its connection from the other nodes. Routing table reset as the alerts generated so that all nodes within the network remove all their connections to the malicious node and network performance does not suffer.

Getting efficiency in collecting data in large-scale mobile ad-hoc network that demand constant and supple clustered network structure but dynamic nature and sever resources limitation make is tough in MANET [16]. To overcome this problem virtual backbone made by cluster-head that decrease the path length between the nodes, the access time to remote counterparts for node is less and for a local range, network stability with node mobility is partial. Cluster head fixed to one hop and selected without considering network condition in clustering techniques in MANETs usually. To measure the link stability and connectivity that relies on neighborhood benchmark of mobile node, a technique proposed in paper that consists of equal size multiple hop clusters.

2.4 Malicious node detection strategy in MANET

Standard security solutions adopted for wired networks or structured wireless networks. Networks with backbone nodes providing access via physical networks do not extend naturally to ad hoc networks. Security methods such as public key infrastructure (PKI) and certification typically require a central infrastructure within the network, making them unusable in a MANET. However, the emergence of biometric-based user authentication for mobile devices motivates our investigation of the possible use of biometrics as a security measure for ad hoc networks. In some sensitive applications of MANET for example, in battlefields, biometrics could provide a crucial measure of security [24].

In MANET applications where authentication is not essential, there is still a need for mechanisms whereby nodes assured that packets delivered to their intended destination. To address this need, we are currently investigating the use of "creditability-based" routing tables to detect and isolate malicious nodes. In such a scheme, a node monitors its neighbors and assigns 'credit scores' to them according to their observed behavior and 'credit history.' Maintaining such a table at each node facilitates the choice of trusted routes rather than the shortest ones, potentially mitigating the packet losses caused by malicious nodes, even when authentication is not used. We are currently implementing this mechanism within the simulation system [24].

A malicious node cause the congestion in the network by sanding fake control packet as RREQs (Route request) and the processing of the RREQs results in degradation of the network performance that can be improved if all the resources are equally distributed among all nodes [17].

One mechanism is an adaptable method based on CoF for detection of misbehavior regarding packet drop and on other hand use of policy-based management (PBM) [18]. Such adaptability allows the system to judge the behavior of nodes and decide whether they should, or not, accused of misbehavior and penalized according to current network management policies. Proposed approach is deployed over a role-based wireless network, organized in a hybrid tiered manner [19]. Nodes assigned a role that defines the tasks they are responsible for as well as the policies that apply to them. For example, depending on their role, nodes may hold behavior information about their neighbors, a localized network section or the entire network.

2.4.1 Malicious Node Detection Strategy in WSN

Although there exist much malicious activity, detection techniques [31] but none of them gave appropriate results regarding security and architecture of the wireless. On the base of past related work a strategy is proposed where malicious activity decision is taken on the base of threshold value, auto-regressive predictor calculate roughly estimated values that is capered with the output of each sensor node each time and if a difference occur a decision block is activated to do action against it [21]. In scrupulous situations with high restrictions & liberty for dedicated methods with better applications it is thought to implement old IDS methods proved by the prior results of the work that is why AR prediction techniques are used here [21].

Design, testing, deployment and operation, different phases of life cycle of IT & C products where information security is a core part of budding requirements especially at the phase of deployment and operation. The behavior of all nodes may change depending upon preferred

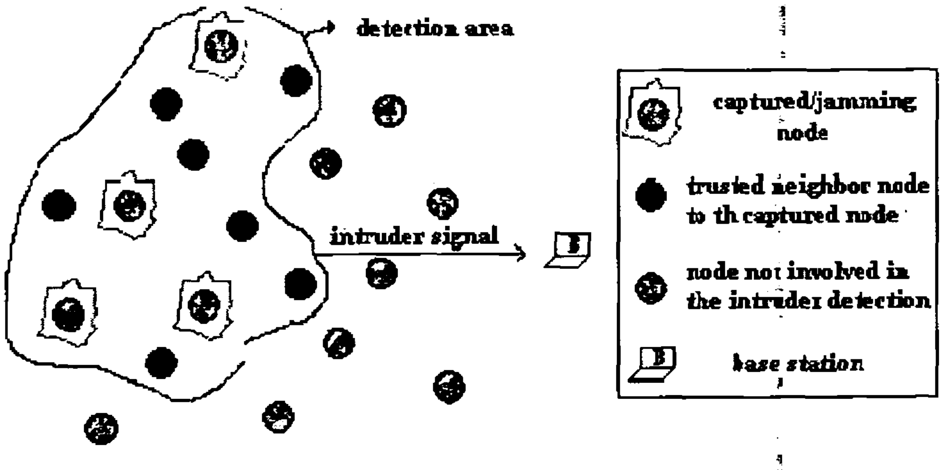
detection area
intruder signal
captured/jamming node
trusted neighbor node to th captured node
node not involved in the intruder detection
base station

Figure-5 Attacked Sensor Network [21]

reliability of sensor readings, commands from base stations, nodes proximity, and position regarding final deployment all these aspects considered at the designing phase of the architecture in sensor networks. Topology to give excellent efficiency in malicious node detection must have the following characteristics

(a) Each node in sensor network must know about its location either it deployed on ground or wireless environment that also detected by location process describer that do authentication of all sensor nodes in one time as they are deployed in the network [22].

(b) Based on the capabilities of communication and computation by using symmetric cryptography transmitting information is kept secure as in sensor nodes each node has capacity to maintain the encryption key

(c) Base station the main access point in the sensor networks considered not compromised as it is availing long lasting power.

Following strategies are being used to prevent the sensor node from attack like selective forwarding, sinkhole attack, spoofing, blackhole, Hello flood attack [31] etc

a) Inside data either small data or short messages (message send by the sensor or received by the base station) of the sensor networks are enciphered by AES, RC5 and Skipjack algorithm that reply on pre-distributed keys for getting efficient secure key cryptography and helpful to protect the network against attacks like eavesdropping and traffic analysis.

b) SENMA: when network is large (having a lot of sensor nodes) and Wireless Cellular Network (WCN) these two architectures are being used in WSN for the selection of topology

Both have the following features:

1. No multi-hope data transfer
2. Node-to-node communication does not exist they talk via base station.
3. Sensor nodes do not need for synchronization before starting communication
4. Use of intricate protocol is avoided
5. Sensor have low reliability, individually
6. It is not essential to re-configure the mobile nodes.
7. Protect network from
8. Network layer attacks like, spoofing, sinkhole, wormhole, Sybil etc attacks etc are can affect the network in the presence of the these two architectures.

c) By direct physical access, nodes capturing attack can get access to all sensor nodes depending on geographic deployment of the sensor. As it is not possible to get an access to all nodes in sensor networks that is way attack can easily affect the network having hundreds of the node and several kilometer range [23]. Attacker can gain un-restricted access to the high level communication by replace or damage the sensors very easily through getting cryptographic keys all because of that sensors nodes interference is opposed to, really. The attacker can get access to all over the network by applying techniques like reverse engineering that also used to find out bugs in the sensor networks that is almost using the same software and operating system.

By using the cryptographic keys, residing in the memory of the sensor node the attacker can send authenticated messages but that would not be in accordance with the specific or pre-defined specifications and will send invalid readings to the base station. Such type of the malfunctioning nodes detected by using linear autoregressive predicator (based on the past value of the sensor node) and either isolated or recovered from malicious activity [21]. Malicious node can also be detected by localization anomaly detection technique where all nodes get information of all other nodes in the networks and by itself as well and values are compared and declared as non malicious if the difference is so small.

Another idea for the detection of malicious node is signal strength way [24] where malicious node detected by monitoring the neighboring nodes in all over the network. In this paper signal strength of the originator is compared to the original signal strength of the node in its specific geographical position if it is same node is not malicious but this technique is not efficient and also time consuming with large overhead as it uses a lot of network bandwidth for comparisons.

2.4.2 Attacks

Routing protocol attacks can be:

a) Routing Disruption Attack: packets are routed to the located other than destination by making changes in routing mechanism.

b) Resource Consumption Attack: as clear from the name resources of the network used by the selfish/ malicious node by adding false packets in the network.

All possible attacks in MANET routing protocol are [21]:

a) Attack using modification as for example redirection by modified route sequence number

b) Attack suing Impersonation as for example, redirection by spoofing

c) Attack using Fabrication as for example route cache poisoning

d) Special Attacks as for example black hole

All depicted in Figure-6

2.4.3 Layer wise description of the attacks

As we know there are seven layers, one of them is physical layer we will discuss few attacks on this layer like Jamming: Collision distribution taken as an important aspect in networks that considered as indicator for the attack related to jamming [25]. For detecting this type of jamming attack authors, show the distribution in which first algorithm used for detection and other one used for competing terminals. Then show how to keep track of the number of competing terminals.

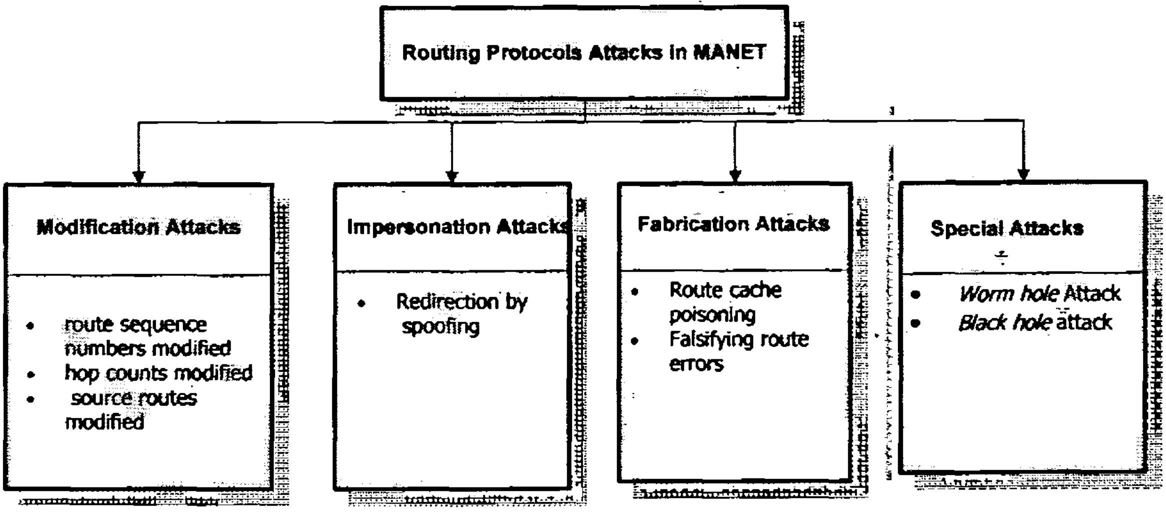

Figure-6: Classification of attacks on MANET routing protocols [21]

Other attack is Tampering: Unexpected context will be receiving when manually entered data, separated by the website because of any web relevant application attack is an example of tampering attack.

Other layer is transport layer having many attacks few of them are Flooding: In SYN flooding, server will never receive final ACK packets, which would declare the complete handshake process. This paper [26] describe about the source detection of attack like SYN flooding. That is one of the local detection methods of source in distributed DoS attacks. In TCP connection, for detecting the unusual behavior, architecture is dividing into 3 modules that are collection module, decision module and monitoring module. Collection module see the passively internet traffic and collects all TCP flow information in specific data structure. It represents the packets that have TCP flow information for identifying the nature of handshake. Second is Time synchronization attack: In this attack node try to deceive the neighboring node by proofing that the adjacent node having the different clock time required by the network that is main objective of the time-synchronization attack. De-synchronization Attack is also the type of the transport layer attack.

Application layer attacks are Node capture attack, JTAG, Bootstrap loader (BSL) and External flash. While few network layer attacks, is selective forwarding attack: one of the easiest implement and damaged attacks in multi-hop routing protocols.

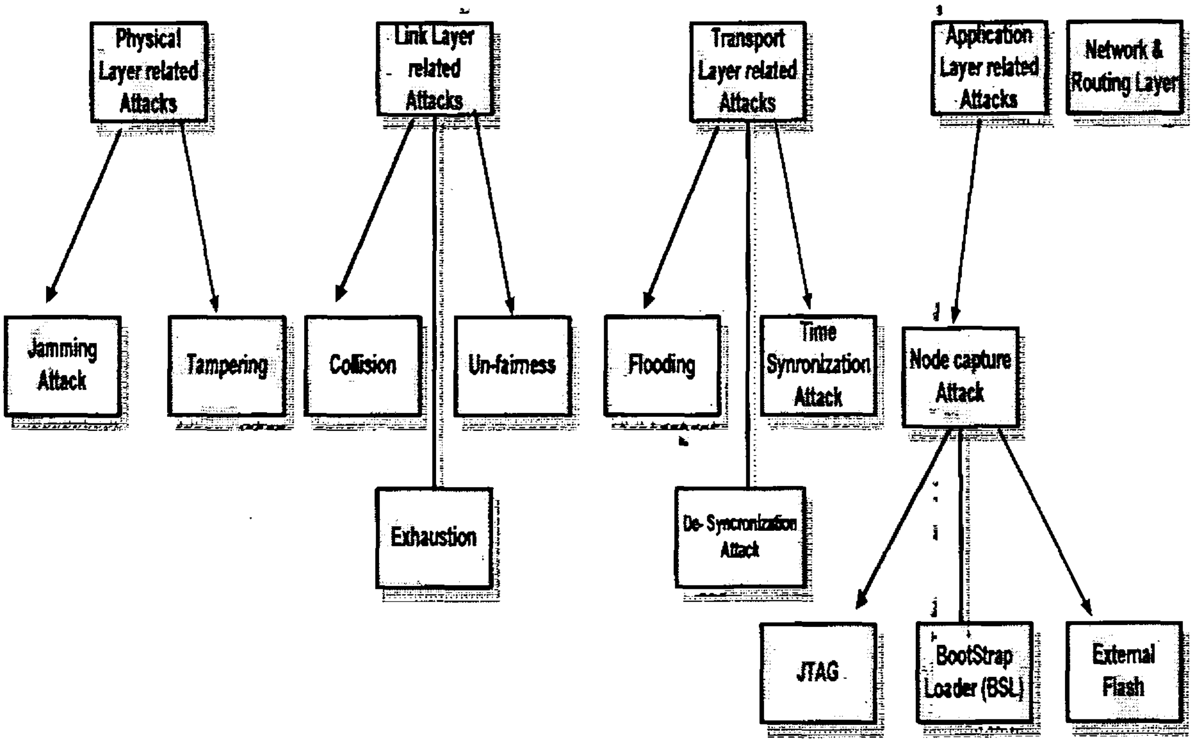

Figure-7: Layer Wise Attacks

In MANET nodes transmit, data to the base station through intermediate nodes due to their limited rang. Malicious node present in the transmission path selectively drops some of the packets. If the malicious nodes drop all the packets, then it is called as BH attack shown in figure-8. Selective forwarding is a more dangerous security issue. In blackhole attack, an attacker uses the routing protocol to announce itself as having the shortest path to the node whose packets it wants to stop. When the attacker receives a request for a route to the destination node, it creates a reply consisting of an extremely short route. If the malicious reply reaches the initiating node before the reply from the actual node, a fake route created. Once the malicious device has been able to insert itself between the communicating nodes, it is able to do anything with the packets passing between them [53]. A zero metric, known by all destinations that direct all data packets from all nodes toward zero metrics node that is acting as a blackhole and is liable to the AODV protocol its detail given in [58]. While in wormhole attack, a malicious node receives packets at one location in the network and tunnels them to another location in the network, where these packets resent into the network. This tunnel between two colluding attackers referred to as a wormhole. Other network layer attacks are Homing: Traffic analysis attack, Rate monitoring Attack, Time correlation Attack, Hellow flood attack [54], Sink hole Attack [54], Range change attack, Multi-impersonal Attack, Sybil attack, Silent Attack, Impersonation Attack and many more shown in Figure-9.

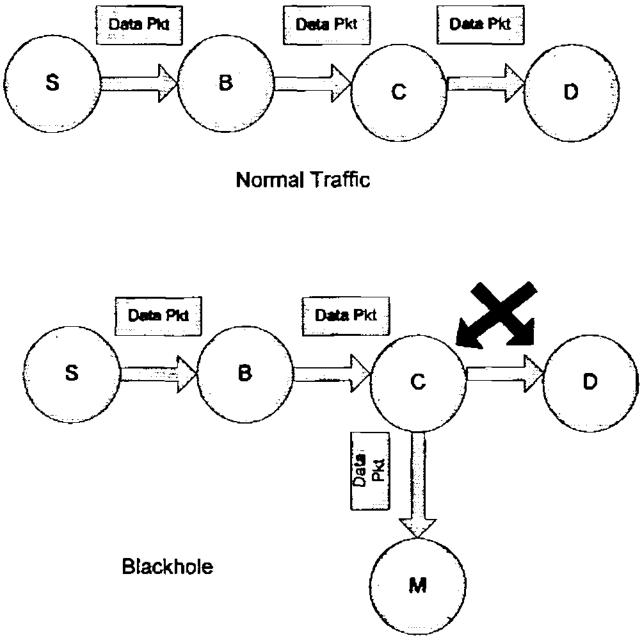

Figure-8 Black hole Attack scenario

In research topic i.e malicious CH detection mechanism in wireless ad-hoc sensor networks, CH is suffering BH attack and misbehaving by dropping packets and fake reporting to PCH. As CH is the central part for inter cluster communication and if CH compromised all communication suffered herewith.

2.5 Reactive Protocol (AODV)

AODV, an adhoc protocol [58] is made by the combination of DSDV and DSR as hop-by-hop communication and sequence number are derived by the DSDV while from DSR route discovery & maintenance is deal as AODV is a on-demand routing protocol having high scalability, effective use of the bandwidth that minimize the broadcasts and transmission latency.

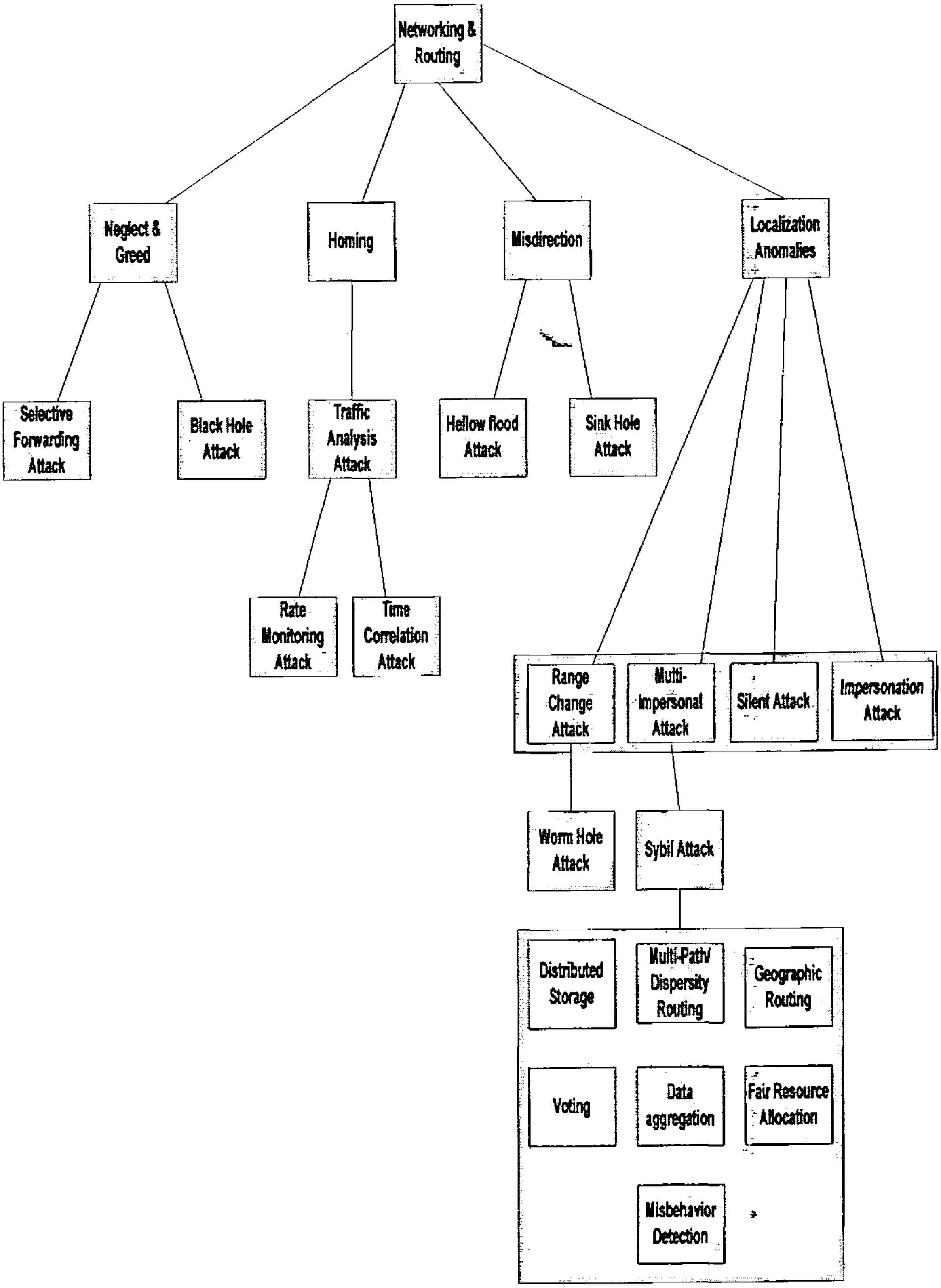

Figure-9: Network & Routing Layer Attack [54]

The objectives of AODV are:

- Local connectivity and topology are managed & maintained separately
- Broadcasts are discrete.
- Circulation made on mobile nodes if connectivity is going to be changed.
- Just like DSR route discovery messages are broadcasted.
- Intermediate nodes maintain the dynamic routing table

2.5.1 Path Discovery

Before the commencement of the communication path discovered by the source, sending a message called RREQ message to all of the network nodes that are maintaining two separate counters, first for sequence number and second one is for ID broadcasting. Messages propagate throughout the network and reach the destination, which replies the request via Route Reply Message (RREP).

2.6 Summary

In this chapter, we have concluded the problem, security threats with general issues in MANET by focusing network security aspects including prevention, detection and recovery techniques of attacks. Background briefly covered malicious node and misbehaving activities related to my problem in the light of layer wise attacks with used protocol for further assistance of research topic.

Chapter 3

LITERATURE SURVEY

Introduction

Problem domain related papers to gain knowledge about the existing work are included in this chapter so that we can update knowledge of the field and come to know about the problems in existing work. Different handling techniques of malicious node in wired & wireless discussed in both simple and clustered environment. Malicious node and Cluster head with various sachems regarding black hole attack handling are also focus. Our literature review divided into three sections, 3.1 related to malicious node in Wired & WLAN and different techniques to handle it, 3.2 covers malicious nodes clustering environment while 3.3 narrated malicious scenarios and 3.4 describe different black hole detection techniques.

3.1 Malicious / Selfish Node

Take reimbursement from the participating node without utilizing its own resources is the function of the malicious node [27]. Maliciousness can affect network in many form but we only focus on the black hole attack where a node acting as black hole pretend to be fake and shortest destination and all traffic routed towards that node. The presence of the malicious node that is dropping the data packets means it is avoiding security measures, having an impact on network performance so in case of multi-hop environment packet forwarding function should not be compromised as user is going to rely on his peer for forwarding the data to the desire location. If routing is not according to the routing protocol it is called routing misbehavior and if other network peer in unable for accurate transmissions of data packet it is forwarding misbehavior these are two types of network layer misbehavior [28].

Performance of the network is affected if network having defective nodes due to its malicious reason that force it to act as misbehaving node. Although many cryptographic techniques exist that handle all such issues but still all attacks and their countermeasures not given yet and issue of the faulty destination that is receiving that packet is still a big problem. Black hole causes the packet drop that is also a malicious behavior.

3.1.1 Techniques to handle malicious node in Wired Network

Probability of seizing data in wired network is less as it wrapped in a sheath than wireless network, which receives data from all direction before getting the accurate destination. Because of the wrapped sheath and its arrangement wired network can hinder any noise to make it reliable as compare to wireless network and achieving & detecting lossy channel watchers, CoF like techniques are used. Watchers scheme that rely on law of conservation of flow used for the prevention of attack, message authentication that is considered as one of the significant advantage for detection of route that is acting as malicious [29]. Watchers send data to all nodes expect exiting node it can detect almost all suspicious activity of the network like misrouted packets and the packets dropped selectively as in worm hole it can work in any situation like awareness of route that is best or having a connection with the best feasible route within the network. These assumptions are not so much applicable on the real world scenario attacks, ghost & source routing etc, that are not supported by the watchers are discussed. CoF is not supporting packets modification aspects, which handled at the data forwarding level. Whole routers can not be detected adequately by using per destination counter. Which flow is measured routers are not able to broadcast link state network status messages as conservation flow got fruitless here. Through which ghost routers can be possible. Packets handled out quickly in Hot potato attack where routers are not verifying IP header checksum. Good router labeled as bad in the presence of conservation of flow in Kamikaze attack. Next hop is check whether it comes within its range or not if not declared as bad in source routing. Premature age and many other attacks discussed in paper that bounded by the size. If router is malicious, it alleged to drop packets in the case of watcher. Encryption security payload is used detect modification in both header and payload at authentication header and destination level in IPv6 as there may be many different reasons of dropping packet in IP.

3.1.2 Techniques to handle Malicious Node In WLAN

In MANET, data transferred by using electromagnetic waves, as there is no well established infra structure as in wired network only air is source of propagation that facilitate everyone to get through it straightforwardly. Not necessary they are in the same place as in wired network case that become a great cause of intrusion and malicious activities results in congestion, contention, delay or packet drop etc must be handle to make network secure by any of the technique like

Confident or Watchdog etc [30]. Watchdog works on the base of passive monitoring as it can monitor communication of all nodes that are the part of the network and are in the same range. Detection of malicious activity or node is carried out by the neighbor monitoring method by maintaining a buffer regarding each node after comparing sending and receiving packets it take decision either to declare node malicious or not. If packet remain in the buffer for the specific interval of time and reached to pre-defined threshold for the malicious detection it consider neighboring node malicious but its flaw is that it monitor only one hop away nodes and can not detect all malicious nodes. Other schemes discussed here is pathrater that chose the best and shortest path for the transmission from source to destination by using DSR protocol on the bases of metric maintained regarding all nodes of the network for appropriate selection of the path.

Different intrusion schemes used for the detection of malicious nodes like Mob Intrusion Detection Schemes [31] that rely on the sensor deployment in parallel form to achieve higher security. Different values narrating positive and negative impact of the node are using by the name of positive and negative values that is used to calculate rating on local, combine and global bases. Rating are compared and on the bases of the rating decision is taken either node is malicious or not binary & iterative probing is used for solving MobIDS issues. Detection threshold used here if node crossed the fix threshold it declared as faulty node. It also relies on ACK concept if that is received within the required period its fine otherwise action taken. Two probing i.e binary and iterative are used for handing malicious activities.

If node is not meeting the requirement of the network or performing accurately, it can be selfish or malicious. Selfish nodes compromise the resources of the network while malicious nodes try to damage the network performance by dropping packets. Different schemes regarding the improvement of the network are proposed in [55, 56, 57] few of them are discussed below:

3.1.2.1 Scheme based on Token Method:

A combined security related to network layer is achieved by carry token by each node within the network that monitor all nodes that are the part of the network and if node not having an appropriate token type it can be discarded from the network by using RSA technique having a pair of public and global secret keys [32]. As all nodes carrying the token with signature so it renewed easily on the base of node performance and disowned if interrupting network performance. This approach is not suitable for link layer & physical layer only focus on the network layer security by monitoring all nodes with fix ID coming in its range. Integrity & confidentiality aspect are not considered in this scheme only reply on forwarding of data from required source to destination that may results in suffering of different attacks

3.1.2.2 Schemes based on Credit Method:

In virtual coining concept, each node has to pay for fixed nodes for using their services [33]. This approach is considered better rather than watchdog and pathrater because it related to the counter that are maintain on each node by using trust method. Nuglets resides in packet uses mechanism of cryptograph for getting security from intruders.

3.1.2.3 Scheme based on Reputation Method:

Another way related to detection of malicious node and its isolation is CONFIDANT [34] having these mechanisms:

- Monitoring
- Reputation System
- Robustness
- Fairness

These mechanisms meet the security requirements of the MANET and guide other nodes according to its experiences so that mistakes already happened & avoided by others and attack / error ration reduced.

3.2 Cluster Based Environment with malicious node

Group of nodes arranged into one group called cluster that diminish rate of transfer and overhead on network. In all groups that are making clusters, one selected as a cluster head. Cluster organization depends on the mobility of overall nodes in the network. Any node can join or leave the cluster any time or two clusters initiated from a single one with the selection of a central entity named cluster head, administrator of overall communication and selected random bases so that there are many chance that a malicious node also elected a Cluster Head [35]. Malicious node can affect the overall performance of the network by dropping packet or making any amendment in the desired data as in black hole attack the attacker reply the route request to show itself the shortest and more feasible path for transmission from source to destination and re-route all traffic to it shown in figure-10.

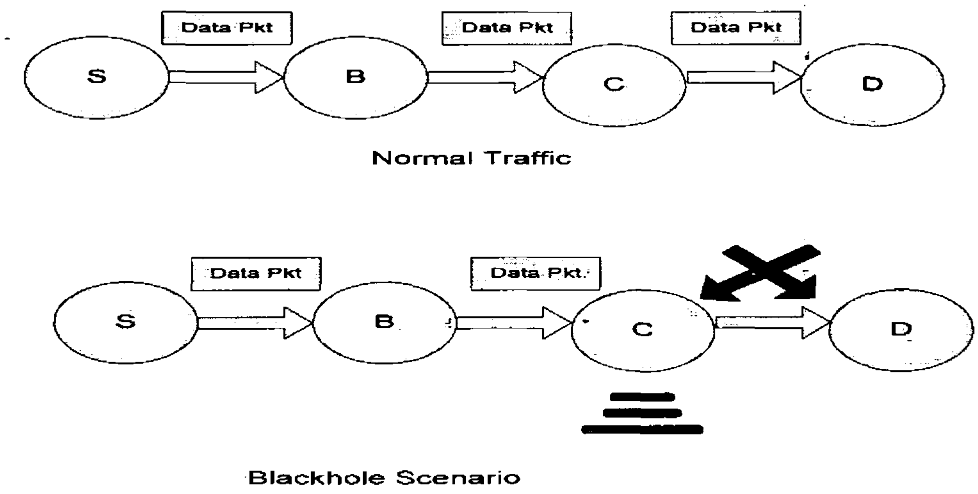

Figure-10: Black hole scenario

Node suffering black hole may misguide the source node towards the destination or may drop all data packets. Black hole reply all route request to behave like it is only one hop away from the destination that is main reason that is why source got compromised as it does not bother either neighboring nodes are monitoring it or not it continue dropping packets[36].

3.3 Malicious Scenario

There can be two malicious cases:

- When node acting as malicious
- When Cluster Head acting as malicious

Now we have a look on them one by one:

3.3.1 Node Acting As Malicious

In clustering environment network is distributed into groups are called cluster that overcome the lack of infra structure in MANET by providing security. Algorithm & specific protocols are used for the configuration of the cluster and its maintenance animatedly as the is equally chance of any node to be selected as cluster head or any node having malicious behavior like black hole can become the part of the network that de grade the overall performance of the network[37].

Different situation having malicious node acting as a black hole considered below, shown in figure -11, 12:

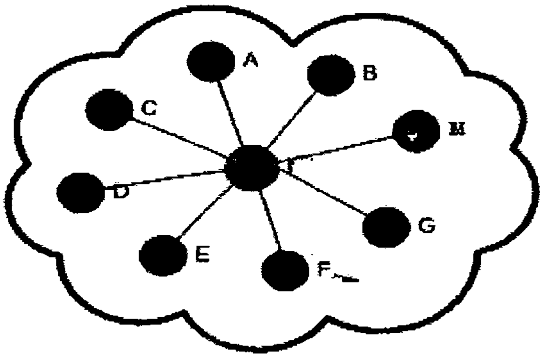

Figure-11: Malicious node Scenario in Clustering Environment [11]

Malicious node having an attack of black hole mislead the nodes whose packets it want to drop that is a considerable issue. CONFIDENT & MobIDS give and extension regarding its solution by using sensor nodes related to malicious node detection. A lot of work has done related to the detection schemes in MANET but how to solve it or identify the reason is still an issue [38] with only minor solutions. Khalid et al proposed a scheme related to traffic load and window size of the data following request/ clear to send method. Do sun did not consider throughput of the packets that is why his method also have some gap for improvement with respect to detection. Although these techniques are providing false detection method but in real time detection of malicious node still become a hot topic on another hand lossy channel algorithm related to traffic analysis and load balancing are not explained as in Dokurer paper only UDP traffic is considered by considering one of the AODV techniques. If trust & throughput of the node got raised Marti techniques improved as confident dealing reaction related to detection following neighboring nodes monitoring avoiding over time behavior in TCP performance made good if we can control heavy traffic load on the network.

3.3.2 Cluster-Head Acting As Malicious

Two clusters combined to form a single one or may split to form more clusters having one leader called cluster head. Cluster head (CH) is responsible for overall activities within the cluster that why many resources are consumed by it like battery etc. If CH is compromised all the network performance got down and cluster connection may be broke down with other clusters as in

WiMAX network consumption of power is considered much and it is controlled by avoiding un-necessary traffic within the network [39]. Energy consumption reduced by the clustering techniques by sending only aggregate values not the actual data that make system energy efficient. Each node having its own public & private keys that compared to get accurate data

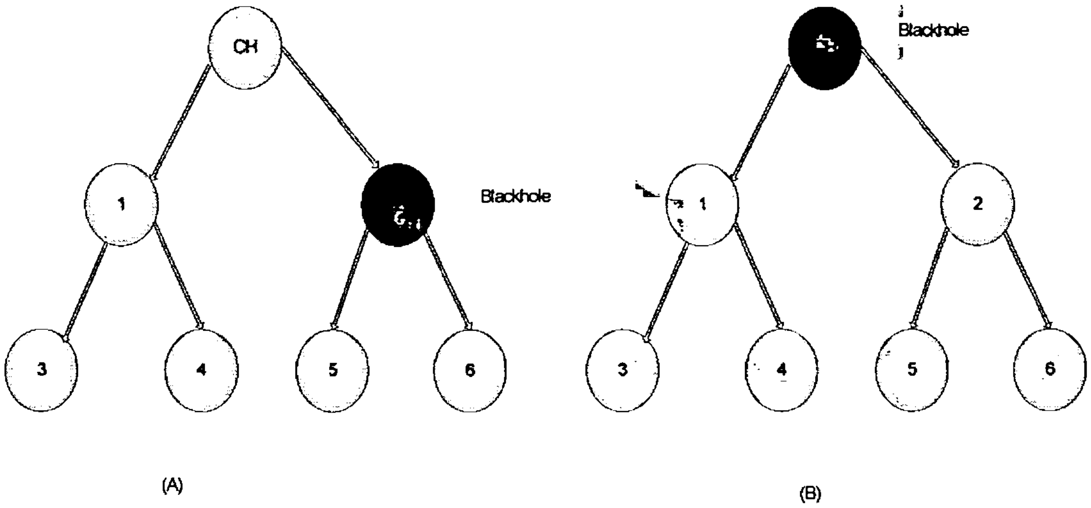

Figure-12: Blackhole Depiction

Comparison of two approaches: witness and direct voting prevent group head from attack that is responsible to get data from BS and to pass data towards it for smooth communication within the network. On the other side a secure protocol supporting communication and play a role in IDS in clustered based environment that is free of any dependency on BS [40] as keys are randomly distributed and packet transmission is limited for the detection of CH that is acting as malicious. Different parameters, considered by the nodes like connectivity security and energy to detect the malicious behavior of the CH.

Attack performance and behavior noticed in hierarchical WSN by using isolation method based on table for detection having two CH: primary & secondary. SCH do the monitoring of all nodes, part of the cluster and PCH as well. PCH isolation table carried out for collaborated IDS, can be said RTID, that pre-assume all the nodes are only single hop away from the CH. Routing tables are altered by the attacker to discard the CH in a state when less number of nodes are alive and threshold level is squat. Having only one problem that is, PCH is point of attack by the intruder then whole network will be compromised [41].

In this paper, routing protocol secured by a court-like Cluster-based IDS (CCIDS) [42] that divide the network into one-hop cluster. Each cluster does monitoring: detection & full protection achieved by per node per CH monitoring. Investigation: to know the trust, CH takes ID of that alleged nodes and launch an investigation process on them. Deference: From malicious nodes, suspicious message taken as evidence, which results in the signature of condemning. Alert issuing: alert issued by the CH only when it goes validity checking on each node to prevent the malicious alerts that result in the reduction of false positive rate and malicious alert avoidance with low detection delay with suitable communication overhead. It also offer precise detection of link spoofing and link deletion attacks.

On the base of trust node able to get are number of nodes trust selected as a CHs that is responsible for overall activities of the network [43]. CRTRP provides nodes the sure path for transferring data by informing them about the malicious nodes in the route on the bases of its trust level and updates the packet route dynamically so that all malicious routes identified. In this scenario trust level gradually changes on the bases of interaction frequency and time and every node save the right to elect the trustiest neighbor as an acting CH and its entire member nodes communicate through it as they make sure a safe path on the bases of the trust on their CH. No routing request or communication from a malicious node is entertained here as each node monitors the activity of its neighboring nodes and updates its trust table on the bases of their observation and in a case if CH got malicious, affiliate nodes re-select new CH on the base of trustworthiness.

Triggering of event is also a best way for the detection of malicious activity in cluster-based Intrusion Detection System [44] has some strong points as CH selected in a case if it has high battery timing in the whole cluster. Detection accuracy is high in Cluster-based IDS architecture. It consists of multiple layers for detection but flaw in this techniques are a node that is malicious can also utilize the election of the CH selection that is why it can suffer many attacks like man in the middle and other blackmail attacks like blackhole etc as our CH is being considered a point of the malfunctioning. On the other hand, CH selection process increases the overload on the network that result in increase of the processing and communication overhead. Detection accuracy and false positive ration greatly affected because of the mobility of the nodes.

Detection of malicious nodes on the base of game theory, rely on the hierarchical intrusion system. Where selection of CH, based on high battery time and self-monitoring of the CH for malevolent behavior with other nodes, are its pros but cons. As CH selection is a process that waste the computational power, results in increase of communication and processing overhead. If CH fail or corrupt because of any reason or attack it can damage the communication of the nodes from the network but selfish node can not be CH in the mean while malicious node that exist in that network may show itself as legitimate CH for behaving maliciously[45].

Voting scheme for the detection of any mal-functioning activity reduce processing and communication overhead but disadvantage of the voting scheme here is; a malicious node can also determine the legitimate node as a malicious node whether it is not uses mechanism of detection rely on collective decision . Here point of failure can also be the monitoring node and only the specific attacks can be detected in this scheme because of high node mobility that cause high packet loss and ratio of false positive and detection accuracy decline [46].

In optimal hierarchical IDS architecture [47] a node selected as CH who can vigorously survive in the network of high mobility as CH is a head that last longer in the cluster. It also gives multiple detection levels that increase the detection accuracy but CH comes at lower level overloaded. Overhead related to communication in the presence of different attacks increased. One of malicious nodes can also elect as a CH that can easily mislead IDS system. If CH is a malicious node then it can easily declare a normal node as a malicious node or its behavior as a false behavior.

In clustered anomaly detection architecture [48], workload of processing equally distributed among the nodes as CH is rotating in this scheme and CH after selection can monitor a lot of the network area that results in accurate detection and decision regarding that action. But in this detection scheme processing capabilities of the node in the election process is greatly neglected and malicious node, if selected by other nodes or set of malicious nodes as a CH it can declare a legitimate node a malicious node easily. It can also mislead the IDS system effortlessly.

On the base of the papers we deduced that different ways are used to improve the detection accuracy where sometimes monitoring is done by the selected CH or CH keep occupied by the large portion of the network for monitoring or multiple layer detection patterns is being used [44]. On the other hand, CH rotation or battery timings of the nodes kept into account for balanced processing of workload among nodes [45]. Some prefer the voting scheme or high battery timing of the node for detection schemes that result in processing and communication overhead reduction [46].

Different attack are entertained in all like malicious node hinder or mislead detection, black mailing attack and many more [44]. in few papers mobility negatively affect the network that is a cause for few detection of attacks[48] in many cases creation and maintenance of CH cause a high overhead in regard of the processing and communication [46] CH can be cause of the failure in some cases [45] and it selection is overloaded unfairly [47]

3.4 Different Handling Schemes Regarding BH

Security is an important issue regarding networks. There are many checks regarding energy, power of processing, used storage and consumed bandwidth suffering low battery timings, circuit integration, and other aspects of routing and processing of signals [49]. These aspects counted in the research challenges that must be handed by any technique may be algorithmic, IDS or agent based.

3.4.1 Schemes Regarding Detection Using Agent

Agent can work independently as in intrusion detection system of MANET that can perform any activity as local response, monitoring, detection, analysis etc and can respond on local, network or global level [50]. It works on neighbor monitoring after observing the behavior of the node it report the authority and take appropriate decision accordingly. Figure-13 shows some of the agents.

On each sensor node, local & global agents installed that monitor the activities of all neighboring nodes and help in misuse and anomalies detection in hybrid environment [51]. In IDS used for cluster based environment local monitoring carried out and against each node rules, that predefined checked on the bases of entries that made in the buffer against each node movement that comes within its range. All the nodes within the route of source and destination are checking the signature of the node on packet if that have rule against it they pass it otherwise declare it malicious. However, local & global monitoring workload on the network is inversely proportional to the lifetime of the network shown in figure-13.

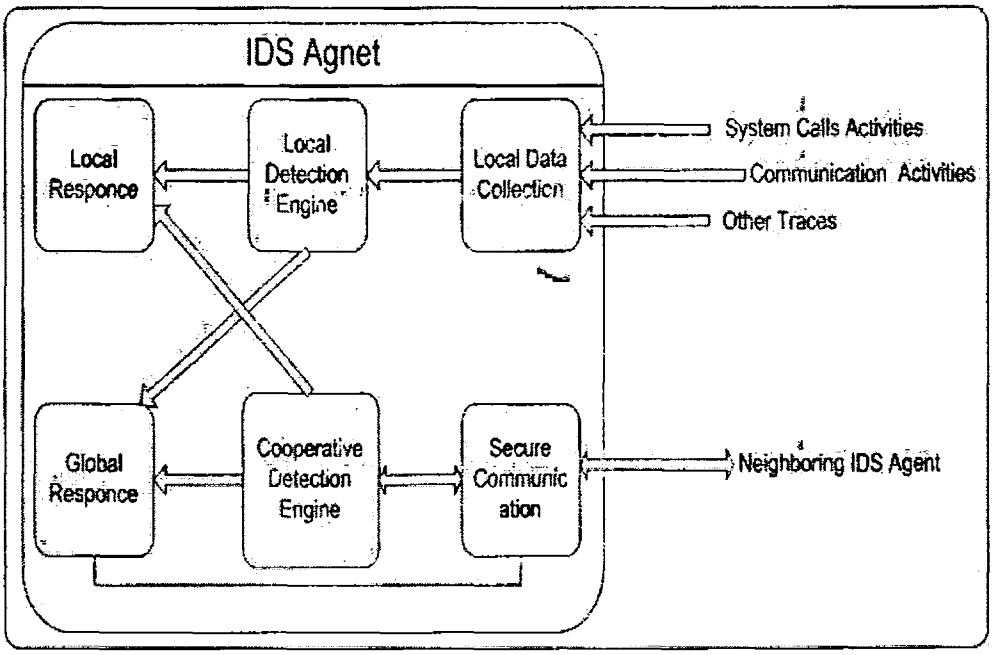

Figure-13: Theoretical Model for IDS Agent [50]

An architecture having different agents like pre-processing that is taking data from recorded database. Reasoning agent that find the actual reason of the attack while decision & update agent take decision on the bases of circumstance and update their database for further assistance while communication agent is responsible for all collaboration between local and global agents and over all communication units, called State Transition Analysis Tool [52]. But deployment of this architecture is not feasible as installation of five agents on each node within the network is not real time as it increase network load and consume a lot of battery time and efficiency got reduce as memory utilization increases.

Four different agents installed on each node for detection [53]. Sentry agent for monitoring and for the identification of intrusion analysis and response agent that take action accordingly and fourth one agent relate to the management of all communication aspects, intrusion and counter measures against it. This scheme relies on the monitoring of the neighbor and if that is malfunctioning, whole network suffer here and it is not feasible to deploy four agents on individual nodes. Its solution is given by using watchdog technique for monitoring but selection of watchdog in also another over head on the global agent but it reserve energy aspect because only one global agent monitor the traffic as packets are transmitted from one node to another within one hop distance.

Another IDS detection scheme in WSN is Slipper algorithm where data trained before transmission repeatedly. Detection carried out on the bases of alarm, if any deviation occurs after monitoring local data. Network try to recover it according to slipper algorithm as trust relation does not exist here that is why it is not too much accurate and tough to deploy on each node as there are many constraints related to network resources that why no verification regarding scheme is given in this paper [54].

In this section, different detection schemes/mechanisms are discuss in [50,51,52,53,54] where on each node more than one agents are deployed for detection of malicious node. Having different functionality of nodes, increase the burden on network and decreases the efficiency and quality of services. Too many resources consumed, as battery timing of sensor is less so there is need of such mechanism that uses fewer resources and give reliable transmission rate with the deployment of single agent for overall network.

3.4.2 Schemes Regarding Detection Based On IDS

A lot of work has been done related to achieve the security goal in MANET in the form of secure protocol / mechanism/ algorithm / techniques of SAODV, SSL IPSec etc that is being used for detection purpose another way is IDS latest way to detect attacks [55]. Distributed Intrusion detection schemes also given for monitoring the behavior of node and taking action on behalf of the situation but no these are still fulfilling the requirements of the security in MANET.

Different strategies like core, boundary and distributed defence that select nodes on central point, boundary and voting schemes respectively for detection of malicious nodes. But cluster inside can suffer attack in the case of core in the same time distributed defence consume large amount of energy as cluster size going to increase while in boundary case false alarm rate got raise as because of increase in cluster size. This IDS scheme base on voting having two parameters regarding one hop & how many numbers of hops exist in between intermediate nodes from source to destination. This scheme is not efficient because of energy consumption.

Other way of IDS for detection in clustering environment is the use of gNode that monitor over all network activities and report the CH on the base of warning tickets it make a check like if the node is normal node pass its data otherwise make a warning and send report to CH then CH take decision accordingly. This mostly used for some type of attacks like negligent attack and DoS attack but this scheme is valid only on the network having many gNodés not for all types of the network [56].

In this section, we consider some of the IDS techniques in distributed & clustering environment [55, 56] where different schemes proposed like deployment of gNodes. Defence schemes and security protocols to make the transmission secure by the detection of attack but these schemes are restricted with constraints like energy consumption & network over load that is way not efficient in performance. Therefore, there is need of lightweight solution for the detection of malicious nodes within the network.

3.4.3 Countermeasures against Attacks

In blackhole detection method, when route is established routing protocol send a route request message to destination node. RQNS sent for making neighbor set from source to destination then all neighbor set send RPNS. After getting all RPNS source node, compare the requested and received neighbor set if number of sending and receiving neighbor sets are same its safe route. If it crosses the fix threshold, it declared as black hole then a cryptographic algorithm applied for confirmation of attack named true detection [57].

Effect of black hole attack on the network handled after its detection, by comparing number of sending & receiving packets. Different protocol used to monitor this ratio if that vary, declare it as a black hole node. In intrusion detection schemes, security protocol like AODV is used which provide the advantage in such way that after receiving first RREP it wait and after getting second one start transmission that reduce the network overhead and increase the reliability of the network performance [58].

Another way for the detection of black hole is sequence number where black hole node must gain the highest sequence number and in response of the route request it reply fast and re-direct all traffic towards it by showing itself shortest and feasible path even though the source consider this situation just like the link error are discard other RREP. New route is established when no ACK regarding delivery of data is achieved. As this scheme rely on ACK and if source not receiving ACK route request is again send by using AODV protocol [59] shown in figure-14.

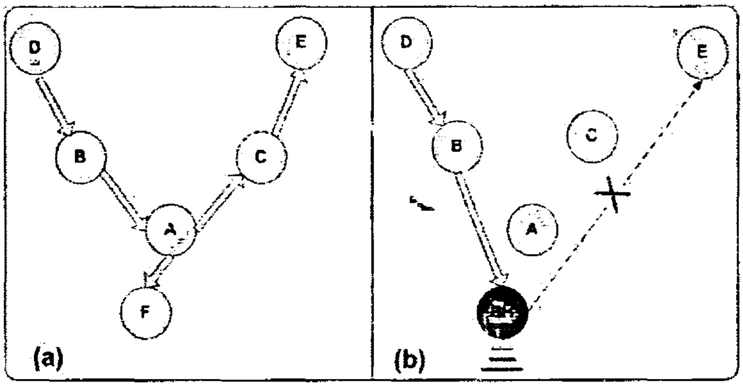

Figure-14: AODV protocol Limitation for malicious activity. (a) Normal traffic flow. (b) Data dropping because of BH [59]

SAR protocol is also a suitable way for the detection of black hole attack in this scheme a trust level in security metric attached with the RREQ message that is propagated trough the network. To reach the destination, this packet move from one node to another node. Only those nodes reply for the request that satisfied with this trust level and send the RREP to next one. This process continue until it reach the destination that reply the source by attaching another security metric and if destination not able to meet the requirement of the trust it send back message to the source to set security metric again. This is a secure method for packet transmission and detection of attack as encryption decryption techniques used by each node but it increased the workload on the network [60].

On the base of the above-mentioned discussion, black hole and its countermeasures discussed. Protection mechanism like probability based, shortest path also seen. Cryptography based authentic action and many algorithms / techniques like threshold based, sequence number based, time stamp and clock synchronization used for detection, identification, isolation and avoidance of blackhole, cooperative blackhole, gray hole and wormhole attacks in MANET.

3.5 Summary

Chapter shows malicious node with different handling techniques in Wired & WLAN environment. Malicious node in cluster based network with two scenarios: first node acting as a malicious while in second cluster head is considered malicious are discussed with different handling schemes and their solutions regarding blackhole.

Chapter 4

RESEARCH DOMAIN & OBJECTIVE

Adhoc and sensor networks commonly deployed in sensitive environment therefore security considered much for the sake of privacy and confidentiality. Much vulnerability explored in MANET and WSN by its growing usage in day today life. Therefore many techniques and mechanism are launched to make them secure from these vulnerabilities and malicious activities but most of these techniques are not compatible with the real world scenario as they are made for only the considered problem scenario or similar ones; as evident from the literature.

4.1 Introduction

As clear from the literature, survey different schemes used for the detection of malicious activity within the wireless network by either using IDS, agent based or any other technique. These techniques though differ in terms of threshold and conditions along with the assumptions considered, but the common target being the malicious packet dropper detection. However, the variance is provided in terms of simple and clustered scenario in the presence of black hole attack but all these schemes have some fault to some extend regarding efficiency, reliability, node burden, power consumption, overhead or network load etc. So there is a need to have such schemes to deal with reliability of the network as well; with the detection and identification of blackhole attack suffered by the cluster head which is backbone of the clustered environment of the network.

This chapter focuses on the provision of my research work, dividing chapter into sections here section 4.2 covers network layer attacks while 4.3 & 4.4 narrate problem domain & problem statement and 4.5 & 4.6 covering proposed solution and basic contribution of my work in last section there is a summary cover all about the chapter.

4.2 Problem Domain

An infrastructure-less network is made by connecting mobile stations via wireless link in MANET that is an autonomous system as it does not follow any pre-defined infrastructure. Within the range, all nodes can communicate with each other. If one node wants to communicate with the other, who is not within the prescribed range, multi hop communication is required [60]. Transformation of information carried out based on topology as it can be changed randomly due to mobility or node-failure; especially in WSN. Trust and cooperation are the keys elements of functioning among nodes in MANET with most important features like variable link capacity, limited energy and physical security with dynamic topology and bandwidth constraint that are attractive features for different type of attacks. Many methods that are made for detecting intrusion in wired network can not be used in MANET because of the behaviour of medium and usage of the wireless technology. At network and data link layer, MENET is susceptible to attacks as in network layer. When nodes are affected by some attack they may behave maliciously by dropping packet or making amendments in data, or may be fail to forward the data to the desired location, or may attempt to jam the communication channel in case of data link layer. Congestion and flooding attack affect network layer performance that is a great obstruct in its proper functioning and misbehavior detection.

The threats in the case of attacks can be alleviated by using clustering where all communication is carried out by the cluster head so malicious node can be stopped to interact with other nodes in the cluster which avoids the network nodes from mal-functioning. Research focus is on identifying and detecting Malicious Cluster Head (MCH) suffering black hole attack & dropping packets. For this purpose, the aim is to come up with an algorithm that is efficient enough for different types of traffic along with negligible false positives.

4.3 Problem Statement

Wireless Sensor Network is an up-and-coming technology. Inadequate amount of energy, processing capability and storage capacity considered some of the restrictions of the WSN. Because of these restrictions traditionally, security mechanism of the ad-hoc network are not adequate for the WSN. Self-protecting approaches in WSN may be static like firewall & encryption and dynamic like first line of defense that facilitates external threats only. While we need security mechanism regarding both internal and external threats to make our system reliable and efficient because if cluster head got compromised the whole cluster will suffer.

Suspicious and malicious activities detected by different techniques like Intrusion Detection System (IDS) that is dynamic in nature. Efficient resource consumption is compromise if network security enhanced as the strong security and efficient resource utilization of sensor nodes have inverse relation cleared from my given literature.

As in clustering environment, the communication carried out through cluster heads and if cluster head is compromised the entire network compromised so malfunctioning of cluster head detected and indentified so that it discarded and network works smoothly and securely. To handle this issue we propose "Malicious Cluster Head Detection Mechanism in Wireless ad-hoc and Sensor Network" that provide reliable transmission of data.

4.4 Proposed Solution

Every forwarded packet routed by intermediate nodes in a wireless network, listened by the sender itself too named as watchdog technique. This technique is better one as here passive monitoring carried out in the absence of an acknowledgement in UDP traffic. Generally, one or more entities are dedicated controlling authorities in WSN and similar in our assumptions. In clustered based environment, the controlling authority, PCH, is assumed to be focal point of inter and intra-cluster communication. Additionally, it is assumed that PCH can not be compromised.

These assumptions based on studies discussed earlier and yet are the least of all. In our mechanism, we use watchdog technique that monitor all the nodes, their communication & behavior laying on PCH, if watchdog observes that packets are going to be dropped, it detect that something is going to be wrong in the network and report the PCH. Now an agent deployed on malicious SCH, by using the resources of SCH agent report PCH and PCH declares it malicious. After detection and identification of MCH, PCH select the new SCH from one of the nodes nearer to the previous one and at the distance of one hop having maximum number of nodes attached with it.

We set two pre-determined thresholds by using watchdog technique on PCH, one for detection and other identification of malicious behavior of cluster head i.e.

- First threshold called detection threshold
- Second threshold called identification threshold.

When packet drop ratio increases from this threshold monitoring and reporting agent report the PCH and got dissolve.

4.5 Contribution

Thesis contributions are

- We have focused malicious cluster head detection and identification, which is core part in clustering environment where communication carried out through cluster head.
- Detection and identification of malicious activity of cluster head will make the traffic smooth and reliable
- Reliability achieved with the inclusion of a secure entity, like PCH.
- As discussed earlier, the earlier studies have majorly focused on TCP communication, however for applications using UDP traffic the authenticity of such algorithms has not been tested. This study focused mainly on UDP traffic.
- For UDP traffic, where no Acknowledgement exists for the successful delivery of the packets, passive monitoring technique is used.
- Lastly, fake reporting by the malicious entity incorporated, so that it can survive longer on the network and avoid/ delay detected as malicious.

4.6 Summary

In this chapter, we have discussed network layer attacks focusing on black hole attack, problem domain, problem statement and its proposed solution. Malicious cluster head i.e dropping packets because of blackhole, its Identification, detection and isolation mentioned in proposed solution. That will make our network reliable by decreasing number of dropped packets and provide us maximum security.

Chapter 5
PROPOSED SOLUTION

In design phase, system architecture considered where the features of the system judged to make a system design that help in the software implementation. Boundaries and the limitations of the physical and social environment considered to make a proper design that is the main aim of the system design phase.

Due to limited resources, distributed nature and constraints of the computing in Wireless Sensor Network and MANET the security is deliberated specially that is the focus of this research project. Reliable security mechanism is required because of the inverse relationship between efficient network resource utilization and the strong security mechanisms.

5.1 Introduction

For system, building basis requirements of the anticipated scheme notified in this chapter. In section 5.2, 5.3 & 5.4 design requirements, topology and proposed architecture narrated while communication between PCH & SCH, Rotation of new CH, design methodology will be conversed in section 5.5, 5.6, 5.7 and conclusion/ closing remarks in the form of summary given in section 5.8.

5.2 Design Requirements

Malicious cluster head detected in the clustering environment where all the communication carried out through cluster heads [35]. Watchdog technique [30] used to monitor the network and agent [50] that sense unauthorized, harmful and malicious activities in ad-hoc-sensor network that used for detection and isolation of malicious cluster head. Detection & identification thresholds are the essential need of our proposed architecture.

5.2.1 Thresholds

Inside the host and network, the threshold shows level of network traffic flow. Malicious activity as deviation in network traffic will be auxiliary investigated. We set two threshold frequencies in our proposed solution: threshold one for detection & threshold two for identification of malicious CH.

5.3 Cluster topology

Topology is an essential aspect of the communication it can be star, tree etc. In cluster based hierarchical approach, group of nodes form a cluster and one node among them acts as an aggregated node or cluster head (CH) that collects data from specific cluster nodes and transfer it accordingly, is supposed to have large battery time and supervisor node to control the communication between all other nodes.

Depending on the WSN deploying scheme each secondary cluster head (SCH) must he connected with the primary cluster head (PCH). The functionality of the PCH & SCH is almost same but the additional feature is that it connects different secondary cluster heads. Collected data is send to PCH for analysis. Energy efficient protocol needed because of limited amount of battery and low cost processor. Battery time of the sensor node can be reduced by the reduction in communication messages as overall messages between sensor nodes and PCH is reduced, the basic concept of the cluster is shown in figure-15 our proposed architecture also have the cluster tree.

5.4 Proposed Architecture

We proposed Malicious Cluster Head Detection Mechanism in Wireless Ad-hoc Sensor networks, in this scheme we use watchdog technique to check the level of threshold if packet drop ratio increases from threshold it detects that something is wrong in the network. Normally packets move to routing table where receiving & sending packets matched, if number of packets did not match, they considered as suspicious. A mechanism that improves the network performance and decreases the number of packet drop at network layer level designed in this thesis. Malicious behavior detected by the use of AODV protocol as well. For getting pure transmission, Black & White system used in our design for the termination of transfer of packets in a case if node is malicious. In this architecture, MCH detected, on the base of threshold values. Two threshold values are set one for detection, second for identification of MCH and one agent named, monitoring & reporting agent that monitors the activities of the suspicious CH.

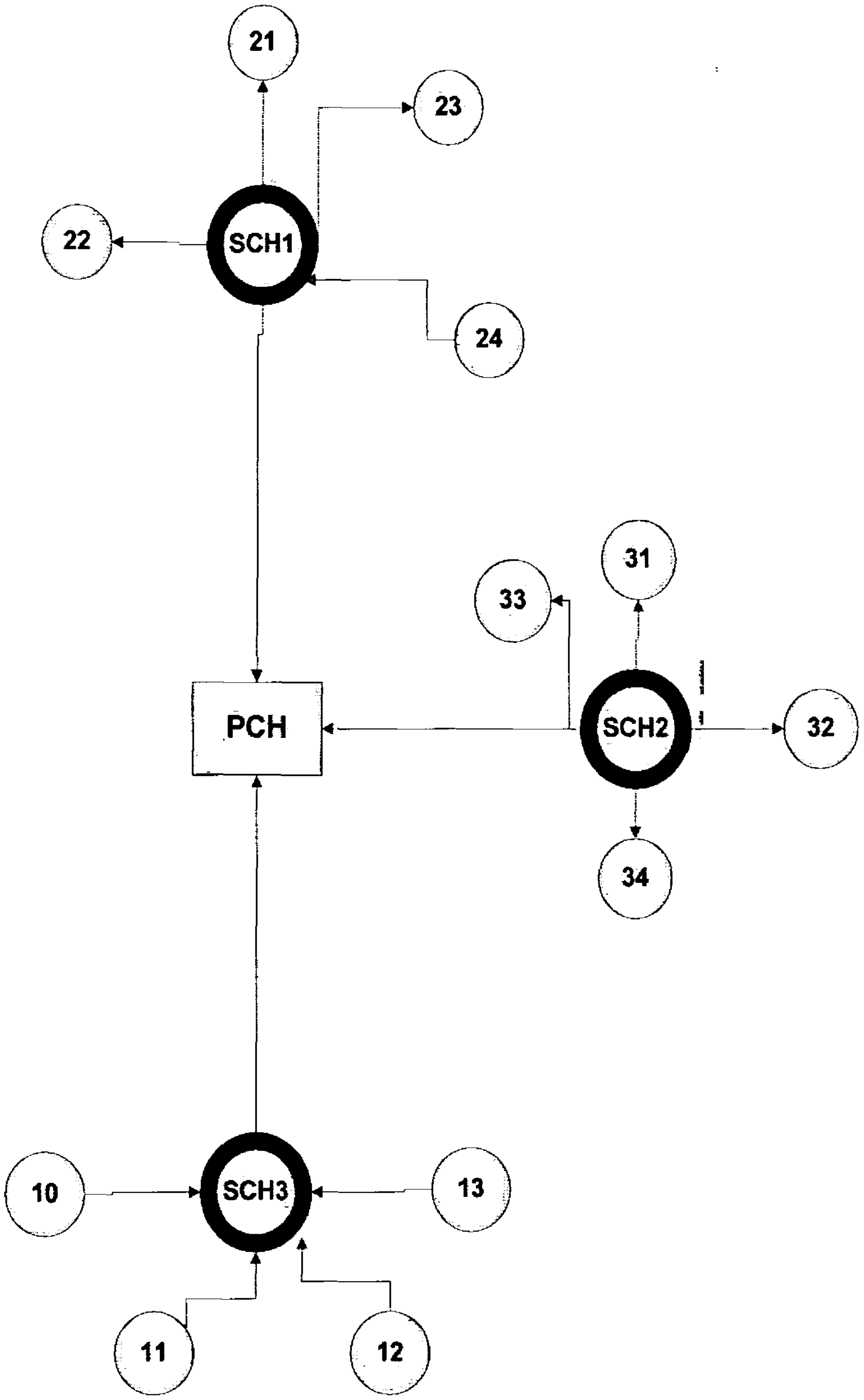

Figure-15: Cluster topology

In the case if intrusion / attack occur on any SCH a copy of the Monitoring & Reporting Agent sent to the doubtful SCH, by using victim resources Agent confirm the occurrence of the intrusion/ attack on the base of second threshold, now Monitoring & Reporting Agent report the PCH and dissolves.

Sequence of the proposed approach narrated in flow chart that is representation of working flow in the system & activities taken place during the whole process shown in Figure-16.

5.5 Communication Structure of SCH with PCH

When malicious activity detected by analyzing agent, message is send to primary cluster head that takes it as a novel intrusion and after taking appropriate action it sends report to the secondary cluster head that generate rule, save intrusion in database for future work shown in Fig-17.

All SCH send IR to PCH that reduces the network load on PCH and minimizes the security control messages that results in saving resources of all nodes. Network lifetime increases if the communication load minimizes, that make network efficient. In another sense, time and resources saved if the same intrusion/ attack occur in future because now PCH takes the same decision without deploying an agent.

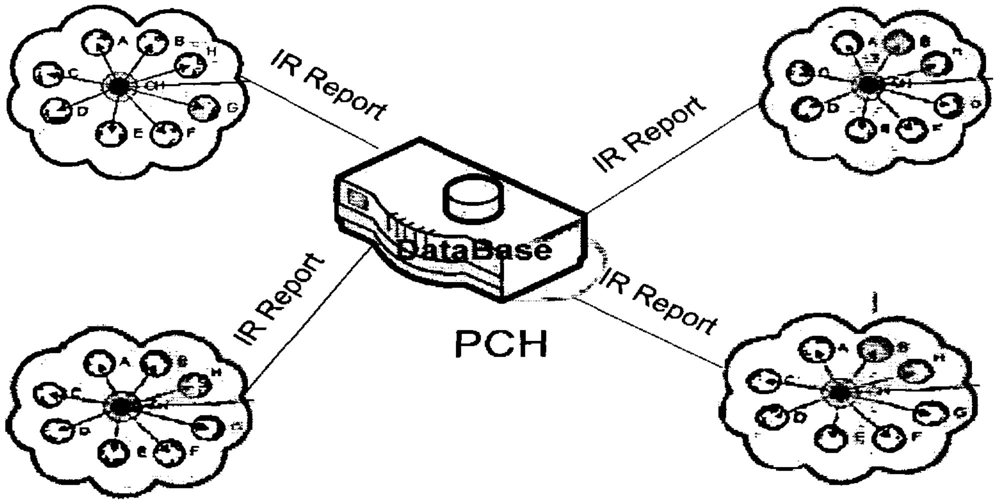

Figure-17: Communication Structure of SCH with PCH

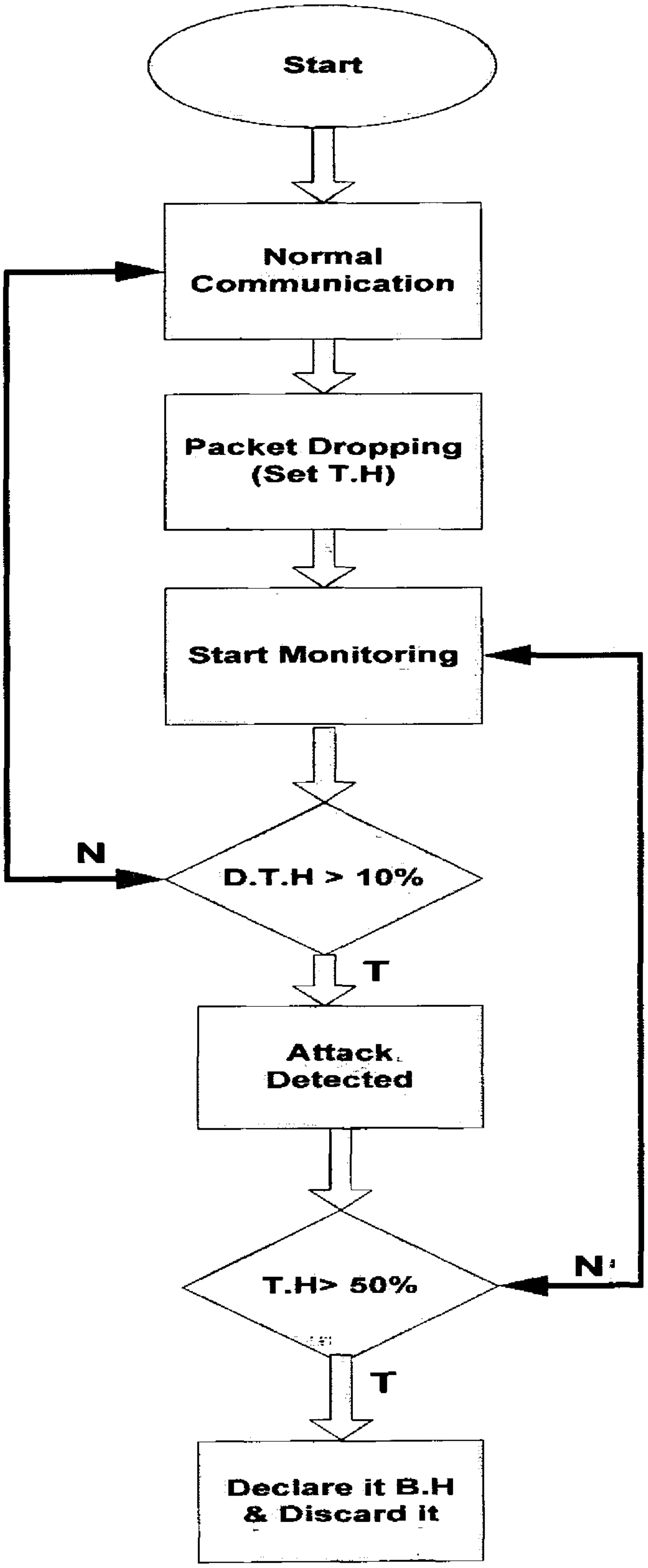

Figure-16: Proposed Architecture

5.6 Rotation of New SCH

Two major technologies used to detect attacks are CID and RTID [50]. Within the cluster a node acts as a CH is supposed to have large battery time than other nodes where CID generate a cluster duty cycle, as it continuously monitor the intrusion in network being as intrusion detection system, that is used for SCH selection after a specific interval of the time. IR messages from all SCH are collected and saved in database when the rotation of the new secondary cluster head occurs after selection primary cluster head send all saved IR to the new elected secondary cluster head shown in Fig -18. The main advantage of our proposed scheme is that during the election of new secondary cluster head previously intrusions would not be lost.

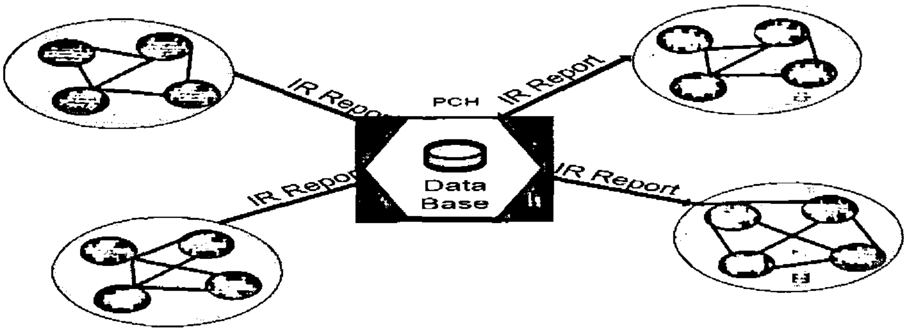

Figure-18: Rotation of new Secondary Cluster Head (SCH)

5.7 Methodology / Algorithm

Our proposed intrusion detection framework divided into two important phases: detection phase and identification phase that narrated below:

5.7.1 Detection Phase

Primary cluster head constantly monitor network traffic because intrusion can occurs on network either level or on SCH level by using watchdog technique. To verify either the system can detect and handle the malicious activity or not an attack launched in this phase. A report is sent to PCH if any deviation from the threshold frequency occurs, an excessive traffic generating node within network is also detected by it and taken into the consideration, that node is also monitored by a particular agent send by PCH.

5.7.2 Identification Phase

In identification phase, system is assumed safe and rules are embedded in the form of tuples into the database and two threshold frequencies are set, threshold one is set for identification of malicious cluster head and is used when packet drop ratio increases from 10% and threshold second is set for detection when packet drop ratio increases from 50%. Number of incoming & outgoing messages from each SCH and data packet flow within cluster is the responsibility of the PCH.

5.8 Summary

In this chapter we projected Malicious Cluster Head Detection Mechanism in Wireless Ad-hoc Sensor Network, that provide reliable communication by dealing fake reporting of the malicious CH acting as a black hole. Our proposed schemes provides a strong security mechanism based on two mechanism, detection and identification relying on two threshold

Chapter 6

METHODOLOGY

To get the desire result the proposed system implemented that is the basic goal in this chapter where we only set confident measurements to get desire goal instead of maximizing every measure but inverse relationship among measurements attributes may live in many cases. To achieve balance relationship among measurements attributes is our most important goal.

6.1 Introduction

Here we will discuss working environment that we have used for getting our results through simulation. User case class diagram & flow charts of the proposed approach to show the actual flow of the problem solution. Pseudo codes for the detection and identification of black hole attack on SCH & closing remarks of the chapter in the form of brief summary in 6.2, 6.3, 6.4, & 6.5 respectively.

6.2 Deployment / Environment

For examining and understanding the behaviour of architecture in a given scenario, environment impact more OMNeT ++ is a network simulator that we use to simulate our proposed architecture. Overview of OMNeT++, network simulation support & basic concept of building and running simulation of OMNeT++ , discussed in 5.2.1, 5.2.2, and 5.2.3 respectively.

6.2.1 What is OMNeT++

There are many simulation tools, some of them are not easy to implement and supportable for hierarchical model. Several are non-supportable for graphical environment and not user friendly while a number of tools use reusable components that are not supportable for large model and its simulation environment is not freely available. OMNet++ provides simulation environment to the researchers for launching their own framework. Additionally, it provides an educational version for students and academia, which we have used in this study. For doing experiments and building simulation model, we use OMNet++ as it is a modular having well designed and a system that is widely used. Source code of OMNet++ can be easily available.

Data collection process and simulation is not linear. To collect data, already existing models modified and re-run the experiment. In OMNet++ we have for NED topology description language there is a complier

- A simulation kernel
- Tools of plotting data
- Tools for documentation

For execution of simulation two types of user interface exits first is GUI and second deal command line. OMNeT++ developed by Andras Varga [26] and the purpose of its selection in my implementation is that it provide friendly environment for debugging, demonstration and batch execution by facilitating evaluating performance aspect of complex software system. There are many hierarchical modules with their own parameter for communication. Models are nested; communicate with each other by passing parameters cause to alter the behavior of module & its topology. Gates used to send the messages that linked directly to the destination or may follow pre-define.

6.2.3 How to Build and run simulation in OMNeT++

OMNeT++ has the following main parts.

- ***NED language topology description:*** module structure with gates, connection and parameters are narrated in the NED file that is written in NotePad/ WordPad saved with .ned extension
- ***Message definition:*** in this field, message and data field defined that translated in C++ that is the basic responsibility of the OMNeT++.
- ***Simple module source:*** these are C++ source file with extension .h

Two basic component of the simulation system are Simulation kernel & User Inter face. To create a simulation program following steps are involved:

- In first step definition file converted into C++ code.
- In second step converted file are linked with simulation kernel and library related to the user interface.
- By using NED tool NED file is converted into C++ at the start, steps shown in figure-19

6.3. Use Case Diagram

Sequence of the proposed approach is considerate by using use case diagram that is the representative of the working flow in the system and activities taken place during the whole process regarding detection and identification of malicious SCH in the presence of blackhole shown in figure-20.

6.4 Pseudo code of Proposed Scheme

Used abbreviations are:

- DTh= Detection Threshold
- IdTh = Identification Threshold
- N=Nodes
- C=Cluster
- CH=Cluster Head
- W=Watchdog
- NPD=Number of Packet Dropped
- DPP=Drop Packet Percentage
- NW=Network
- MRA=Monitoring & Reporting Agent
- BH=Blackhole
- PCH= Primary Cluster Head
- NSCH=New Secondary Cluster Head

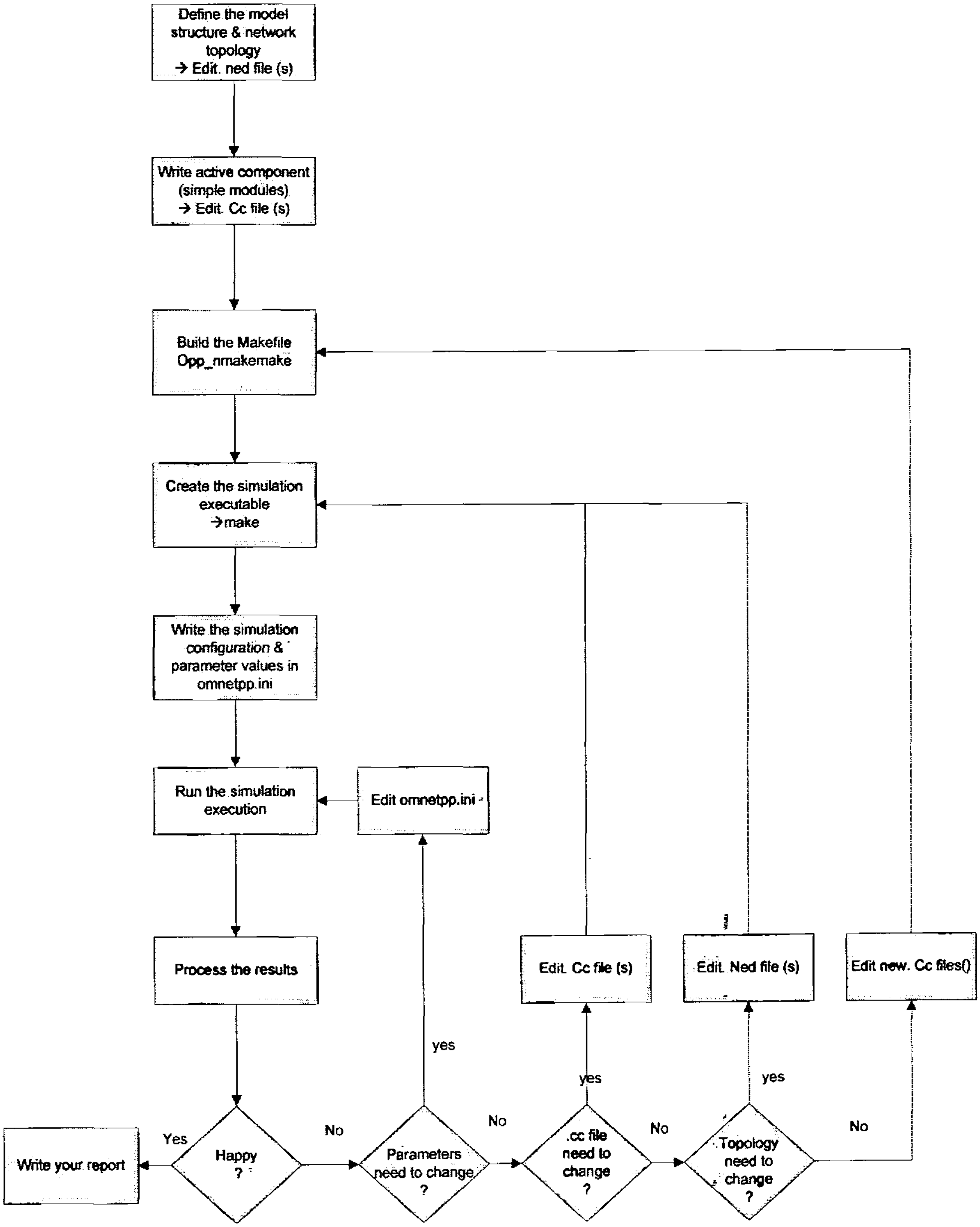
Define the model structure & network topology → Edit. ned file (s)
Write active component (simple modules) → Edit. Cc file (s)
Build the Makefile Opp_nmakemake
Create the simulation executable →make
Write the simulation configuration & parameter values in omnetpp.ini
Run the simulation execution
Edit omnetpp.ini
Process the results
Edit. Cc file (s)
Edit. Ned file (s)
Edit new. Cc files()
yes
yes
yes
Write your report
Yes
Happy ?
No
Parameters need to change ?
No
.cc file need to change ?
No
Topology need to change ?
No

Figure-19: Detailed flowchart of the OMNet++ Simulation Process

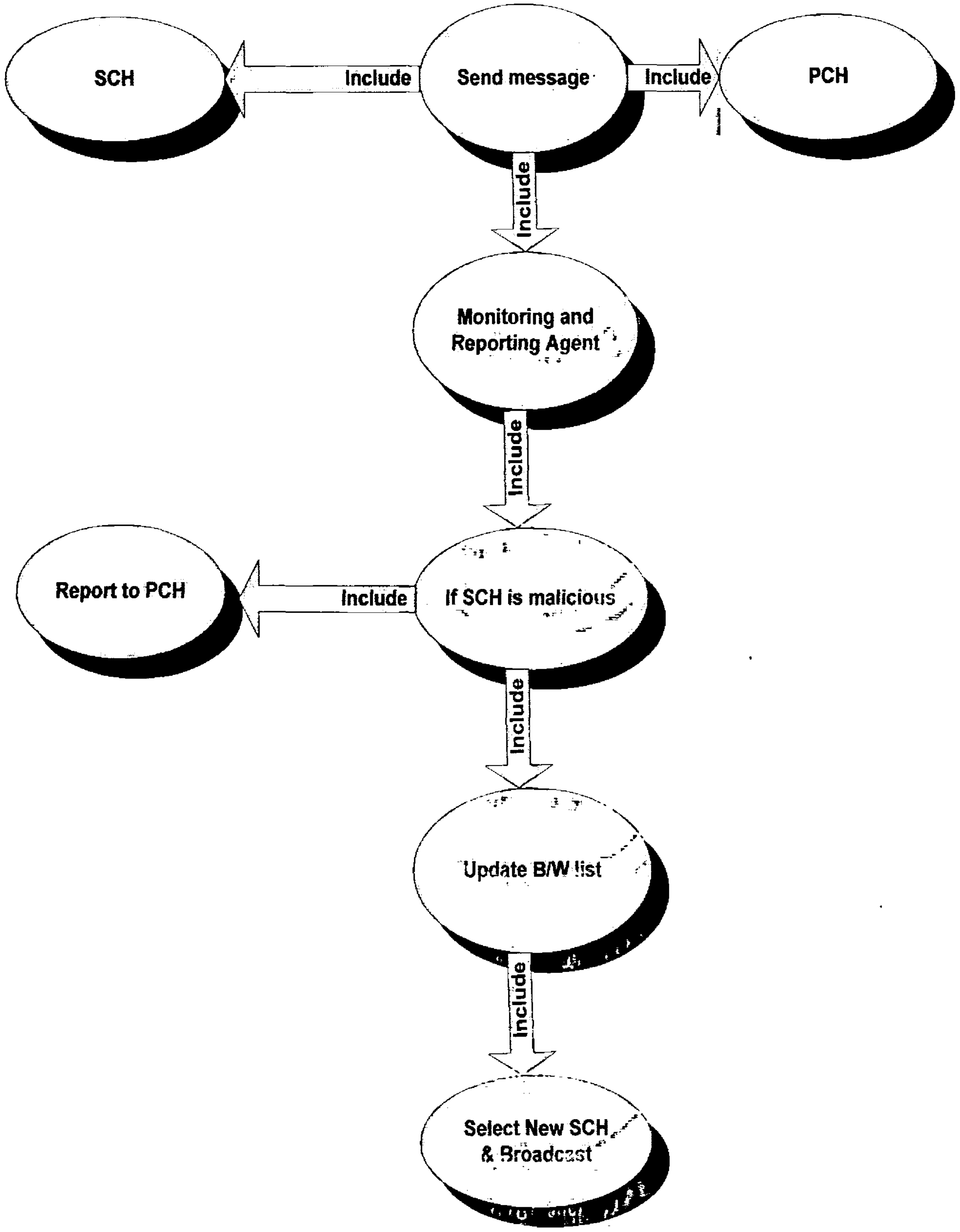

Figure-20: Use Case Diagram of Proposed Solution

Pseudo Code for detection & Identification of Blackhole

```
BEGIN
          ∀ N in C
          PCH monitors Inter-cluster traffic
          Repeat:
                    If (Packet drop ↔ True (using W) )
                              Wait till DTh
                    Else if (Packet drop > DTh)
                              Deploy MRA on Potential BH
          If (DPP > DTh) && (DPP < IdTh)
                    MRA: log drop packets
          Else if (DPP < DTh)
                    Report(clean)
          Else if (DPP > IdTh)
                    Report(malicious)
          PCH ☞ CH as malicious && Disown it.
          Select New CH.
```

Pseudo Code for selection of new CH

```
PCH monitors all neighboring node
Checks the condition NSCH == 1 hope away && maximum number of nodes are attached with it if true
Declare it as a NSCH
```

6.5 Summary

Simulation environment its introduction and working paradigm related user case diagram narrating my proposed scheme and description with pseudo code discussed in this chapter.

Chapter 7

RESULTS

7.1 Topology:

Our proposed topology containing 11 nodes two secondary cluster heads (SCH), named SCH1 & SCH2 and one primary cluster head named as PCH all the communication carried out between SCHs through Primary Cluster heads. Source & destination node selection, packets per node generation are random while number of nodes kept constant. We divide our simulation in different cases dealing different number of packet generating and dropping ration to fix our detection and identification threshold to diagnose black hole attack.

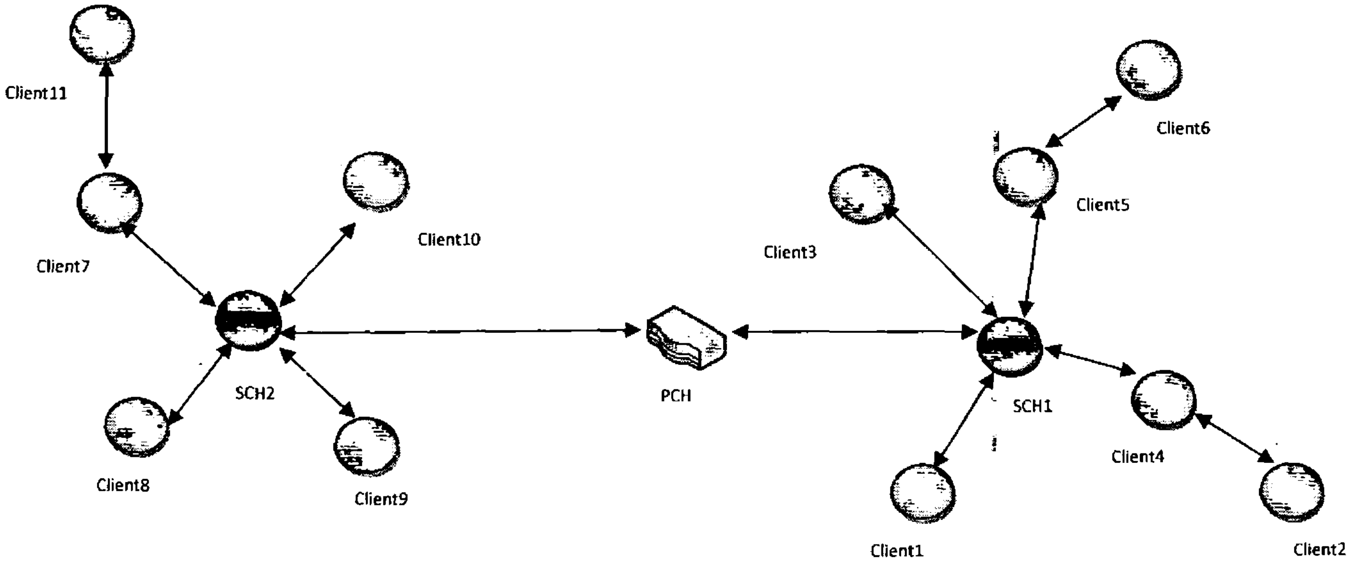

Figure-21: Proposed topology

The simulation parameters considered listed in Table-1. 700m x 350m span taken where both the clusters deployed. The transmission range of nodes and CHs is 100m whereas PCH can cover larger distance, i.e. 200m. IEEE 802.11b standard considered having channel bandwidth of 2Mbps while data rate is 34.6 Kbps with propagation delay of 10msec. Initially, the network is setup and normal communication takes place with CBR traffic. However, blackhole activates after 15seconds. Blackhole intensity is not high here so that it can survive longer on the network. This way, our methodology have verified for detection and identification of the malicious CH.

Parameter	***Values***
Number of nodes	*11*
Secondary Cluster Heads (SCH1 & SCH2)	*2*
Primary Cluster Head	*1*
Routing Protocol	*AODV*
Area/Span of the Network	*700m X 350m*
Chanel bandwidth	*2 Mbps*
Data Rate	*34.6 Kbps*
Traffic Generation Rate	*CBR*
Packet size	*1k*
Channel Error Rate	*2-3%*
Propagation Delay	*10 m.sec*
Blackhole Activation Time	*1/4-1/2 Simtime*

Table-1: Simulation Parameters

7.2 Simulation Results

First, to set our detection and identification threshold we tested our topology with different number of packet generation per nodes for different simulation time with and without agent deployment. There are two levels of detection; at one level, thresholds used while on second level agent deployed. First threshold called detection threshold and second called identification threshold. Now we compare the results with the actual packet send by the SCH and packet received by the PCH and observed that some of the packets are missing, as graph is not same for the sending and receiving packets. Through this, we will try to analyze the impact of intended packet drop in the presence of black hole attack.

If more than, 10% packets dropped by SCH considered that, something is wrong there and when drop rate crosses 50%, i.e. it is persistent in dropping packets, the said CH declared as blackhole. To verify whether our algorithm is working properly or not we tested our results with different throughput for different nodes and set threshold values of detection and identification.

Case-I:

In first case, simulation time of 15 sec is set for static number of node i.e 11 having packet size of each node is 4k. The true picture attained throughput illustrated in figure-22.

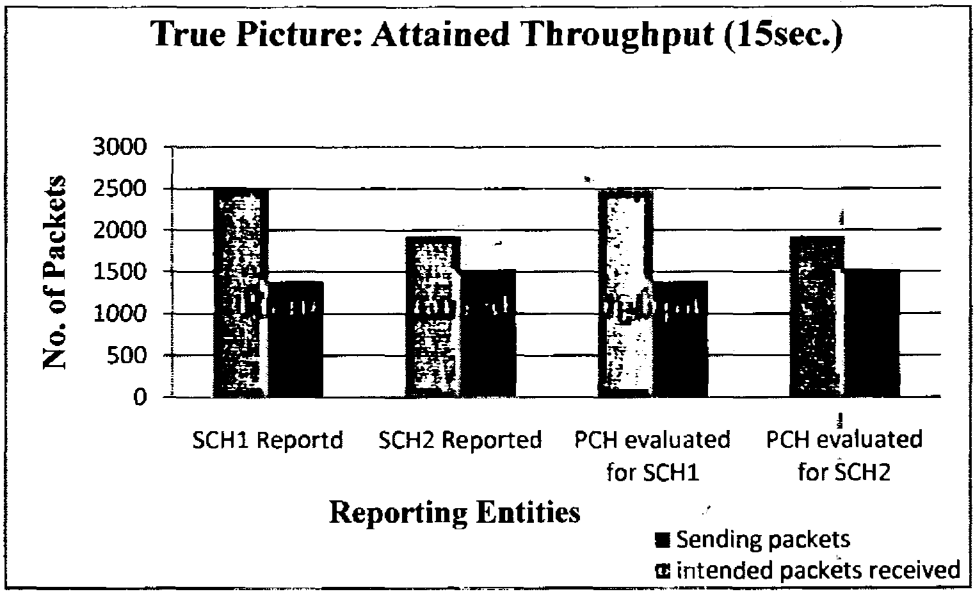

Figure-22: For 15sec. scenario – Originally packets handled by CHs.

Here blue bar shows the sending packets and red shown intended packets received. Where SCH1 reported packets and PCH evaluated for SCH1 are same and SCH2 reported packets and PCH evaluated for SCH2 are same that is a normal scenario where PCH reported results are same to SCH1 & SCH2 generated results. Now we set a threshold of 10% for dropped packets when it meets detection started and when threshold of 50% crossed, it declared as blackhole. In this case, when 66% packets dropped it declared as blackhole.

Figure-23 shows the number of dropped packets reported by the agent. Regarding each node, we used watchers technique to confirm any malicious activity. When detection confirmed crossing our first threshold that is 10%, we deploy an agent that monitor the activity of a malicious CH and when it cross second threshold that is more than 50%, it declared as blackhole.

Here, node number 2 & 6 are not showing intended dropped packets because of watchdog limitation that only monitor the nodes one hop away and if a nodes are two hops away then SCH only record the entry of passing data but did not consider its packet-dropping rate.

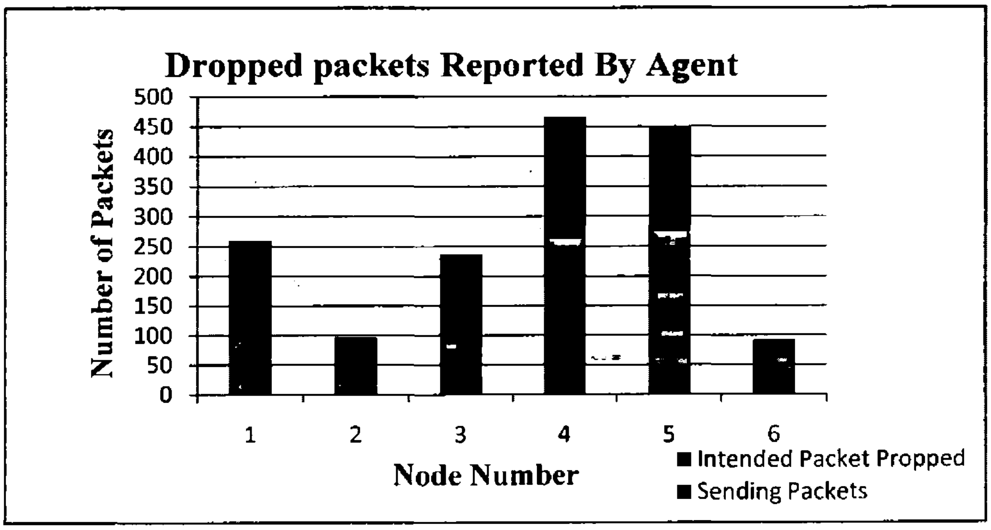

Figure-23: Dropped packets Reported by agent

Case-II:

The same scenario is extended for 20 seconds with different number of packets per node, true picture attained throughput is illustrated in figure-24.

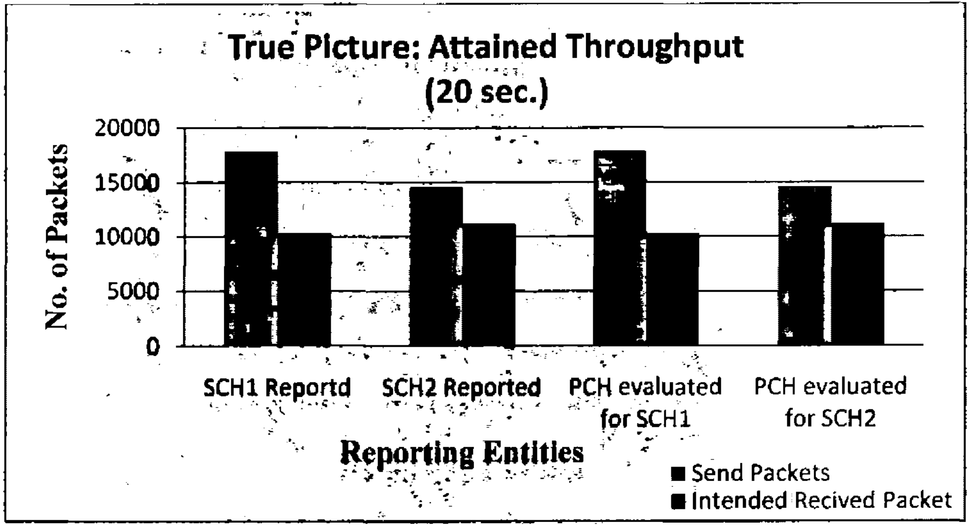

Figure-24: For 20sec. Scenario – Originally packets handled by CHs.

Blue & red lines are showing sending and intended received packets used to narrate that PCH evaluated results are against SCH1 & SCH2 are same as SCH1 & SCH2 are going to report while Figure-25 related to dropped packet per node that is being reported by an agent following detecting and identification threshold having the same condition for nodes 2 & 6.

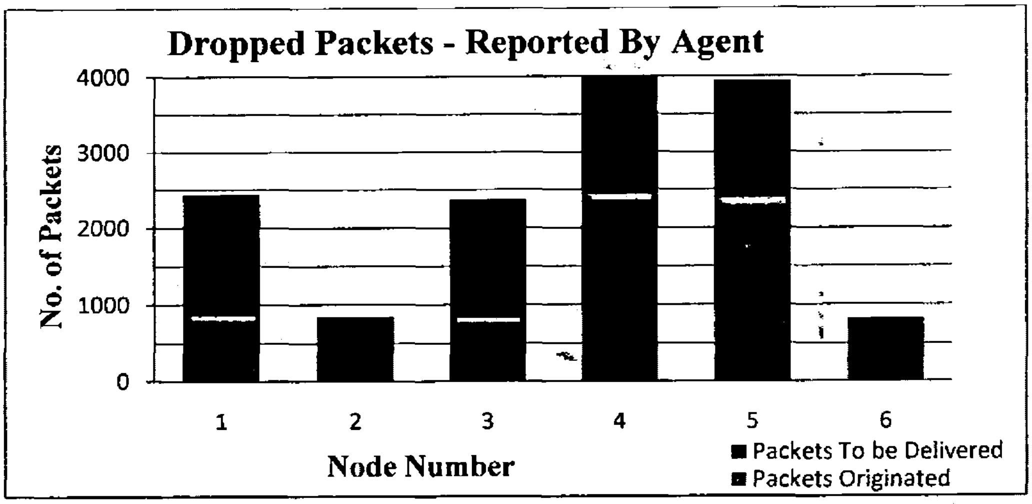

Figure-25: Dropped Packets Reported by agent

Case-III:

Same scenario of case-1 tested with simulation time of 25 seconds shown in figure-26, which monitor that the original packets originated by the SCH1 & SCH2 are not same as reported by SCH1 & SCH2 so there would be some gap or any malicious activity carried out because of blackhole that is dropping packet and not transferring actual quantity of packets. PCH is keeping the entries of data pass from it and updating its record in the routing table and make it show that

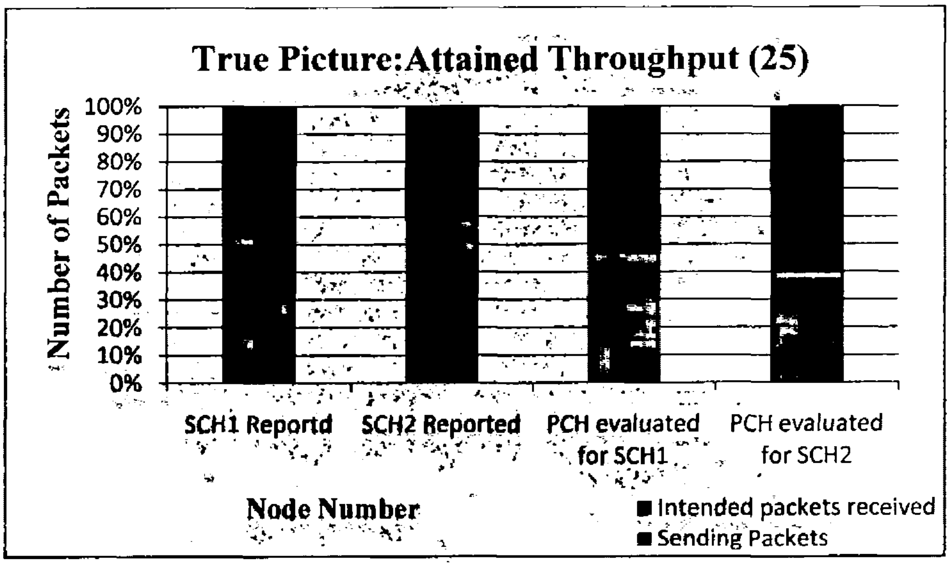

Figure-26: For 25sec. scenario – Originally packets handled by CHs.

data is coming from which SCH. PCH monitors either data is coming from one hope nodes or 2 hop nodes if it is coming from 1 hop nodes it counts its number of dropped packets and if it is coming from two hop distance it will take only its entry of passing data but did not consider its dropping packets.

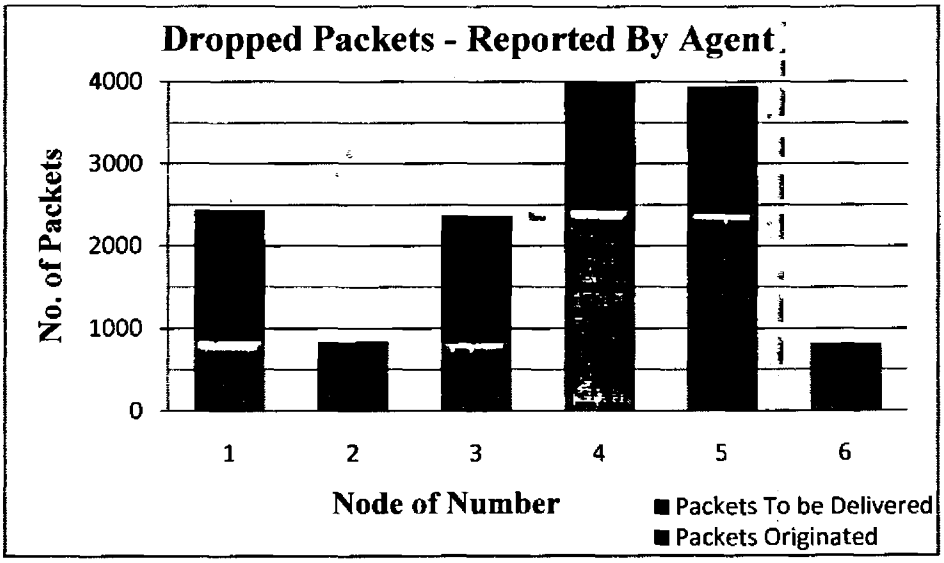

Figure-27: Dropped packets reported by Agent

Case-IV

Above cases scenario tested for simulation time of 50seconds for 4k packet size shown in figure-28

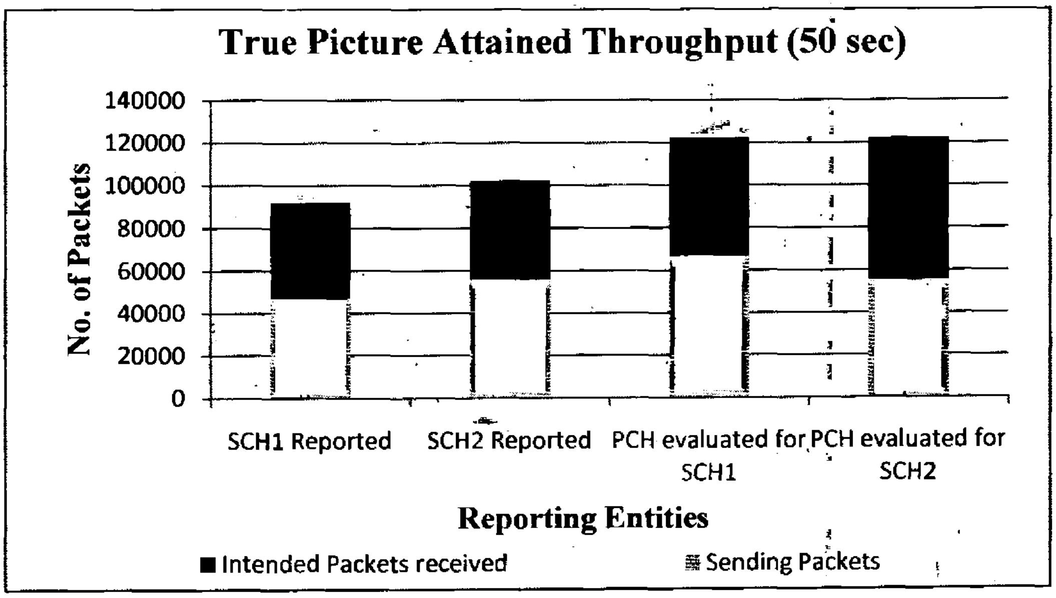

Figure-28: For 50sec. scenario – Originally packets handled by CHs.

Here the results are same as in the simulation of 15,20 & 25 second as the SCH & SCH2 reported packets are same as evaluated by the PCH regarding SCH1 & SCH2 following both threshold checks like 10% for detection and 50% for identification now we fixed our threshold value that is meeting our requirement of blackhole detection and identification. Figure-29 shows the number of dropped packets reported by the agent regarding each node.

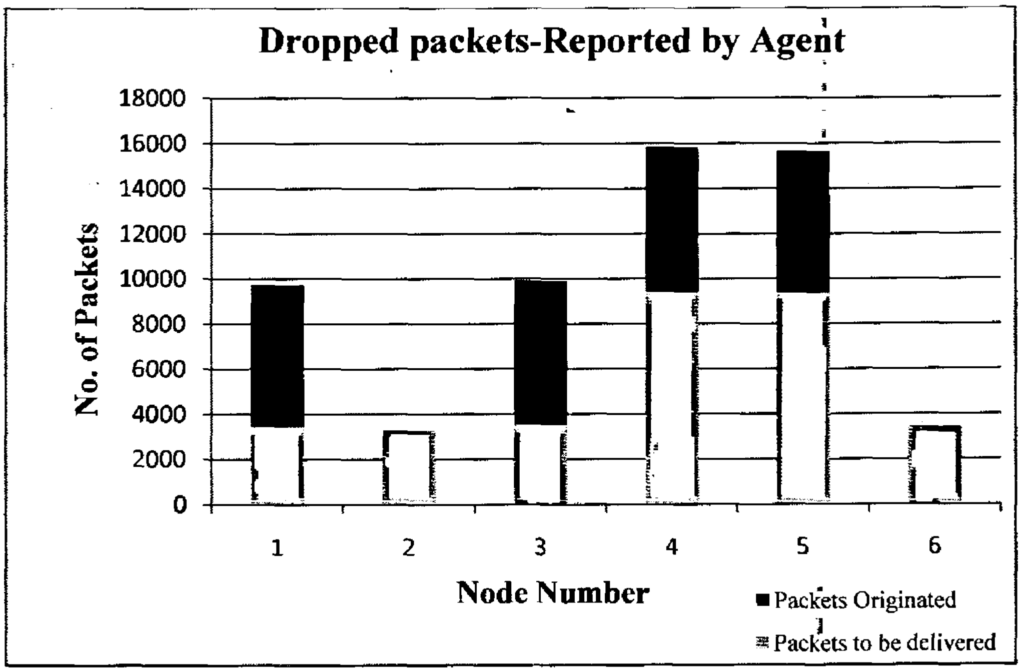

Figure-29: Dropped packets reported by Agent

Case-V

In the Figure-31, SCH 1 sending packets are same as receiving of SCH2 while sending of SCH2 is same as Receiving of SCH1 that is mean graph trend is same for SCH 1 & SCH2 in both sending and receiving case. In this case, simulation time is 60 second and black hole activation time is 10 second. Agent is deployed approximately after 20 seconds and it accomplish its detection regarding blackhole within 20-60 second time limit and the difference between sending and receiving packets of SCH 1 & SCH2 are evaluated as shown is Figure-32.

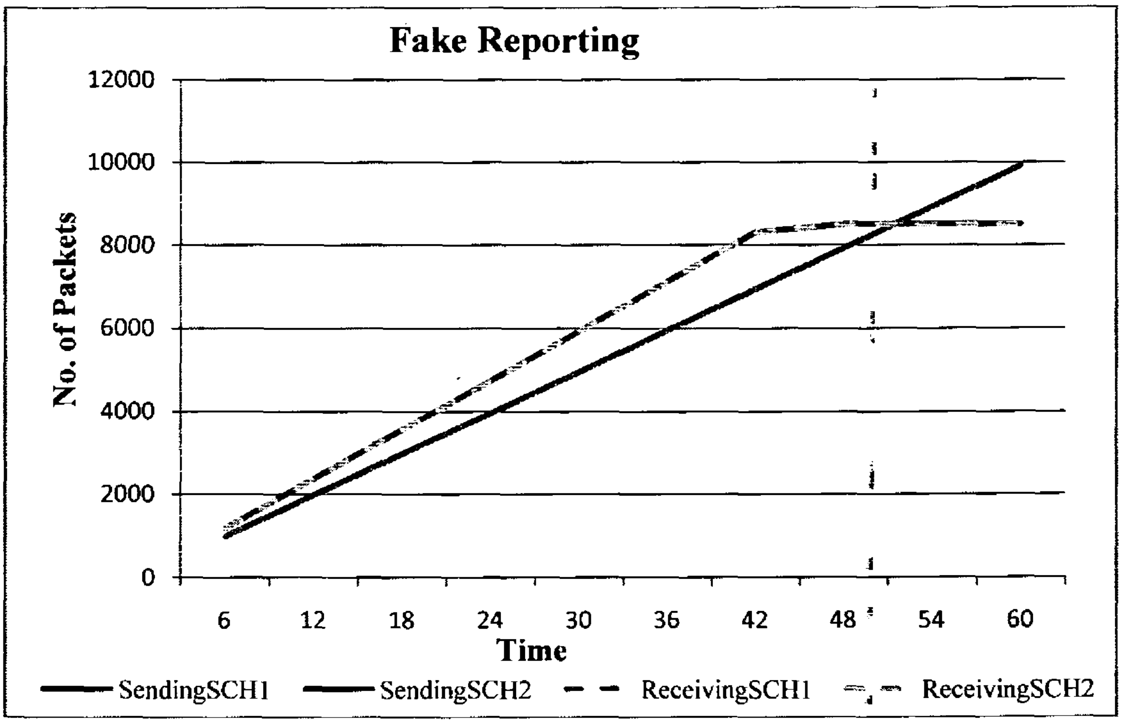

Figure-31 Fake Reporting By Malicious SCH

From Figure-32, it shown when blackhole got active after 10-second graph trend of receiving packets low, revealed that packets are not receiving completely as send by the SCH1 & SCH2

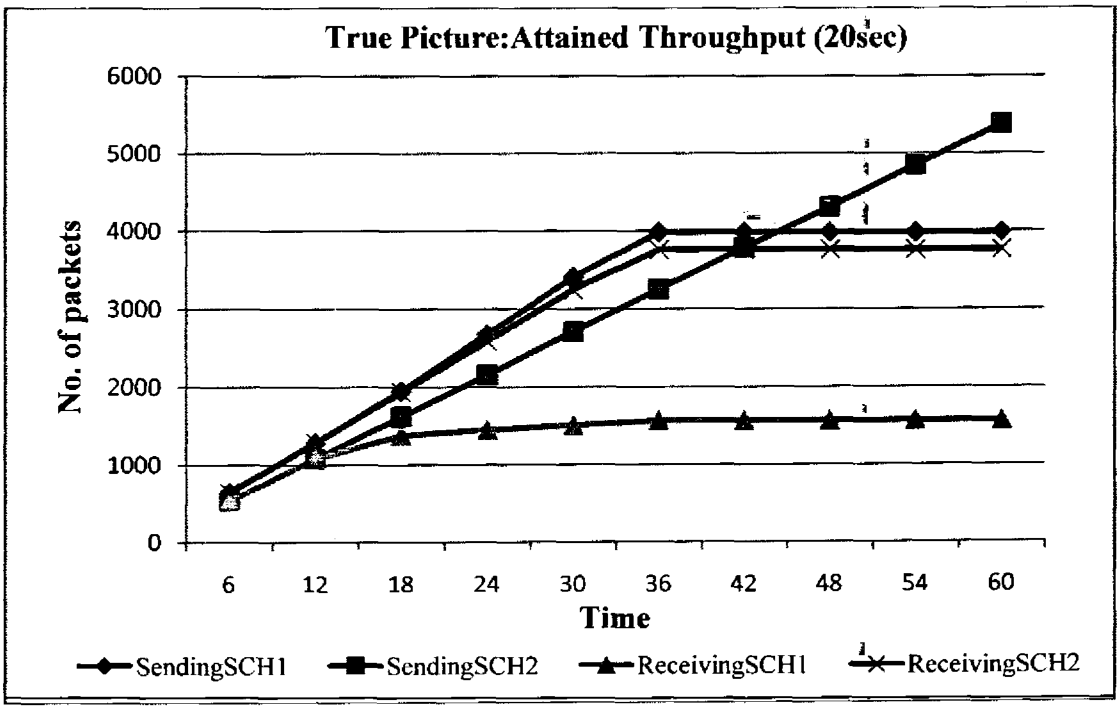

Figure-32: True Picture Attained Throughput (20sec)

While in graph-1 sending and receiving graph trend is same means there is no difference in the number of packets send and received by the SCH1 and SCH2 its mean there is fake reporting by SCH1 & SCH2. Actually, SCH1 & SCH2 are dropping packets but reporting PCH that packets are delivering appropriately that is what we detected and removed.

Figure-33 shows another aspect of time wise throughput where sending SCH1 and receiving SCH2 are same while sending SCH2 and receiving SCH1 are different. In this case, BH activated after 15-seconds and starts dropping packets. After 15-45sencond agent deployed and BH identified and disowned within period of one minute. While SCH2 still sanding packets but SCH1 in not receiving as it disowned PCH take the entry of sending data but it is not calculating the dropped packets.

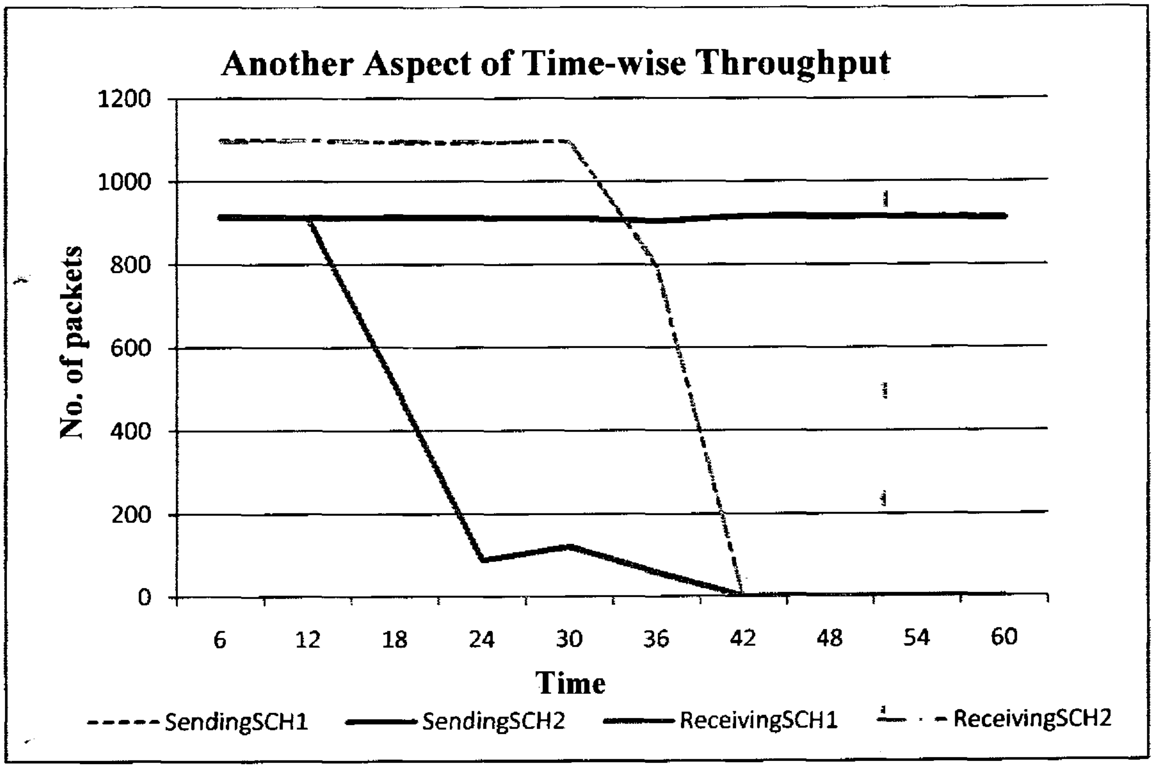

Figure-33: Another aspect of Time-wise Throughput

In figure-34, graph show number of packet dropped after agent deployment, between number of nodes and number of packets generated by each node. Different nodes are dropping different number of packets.

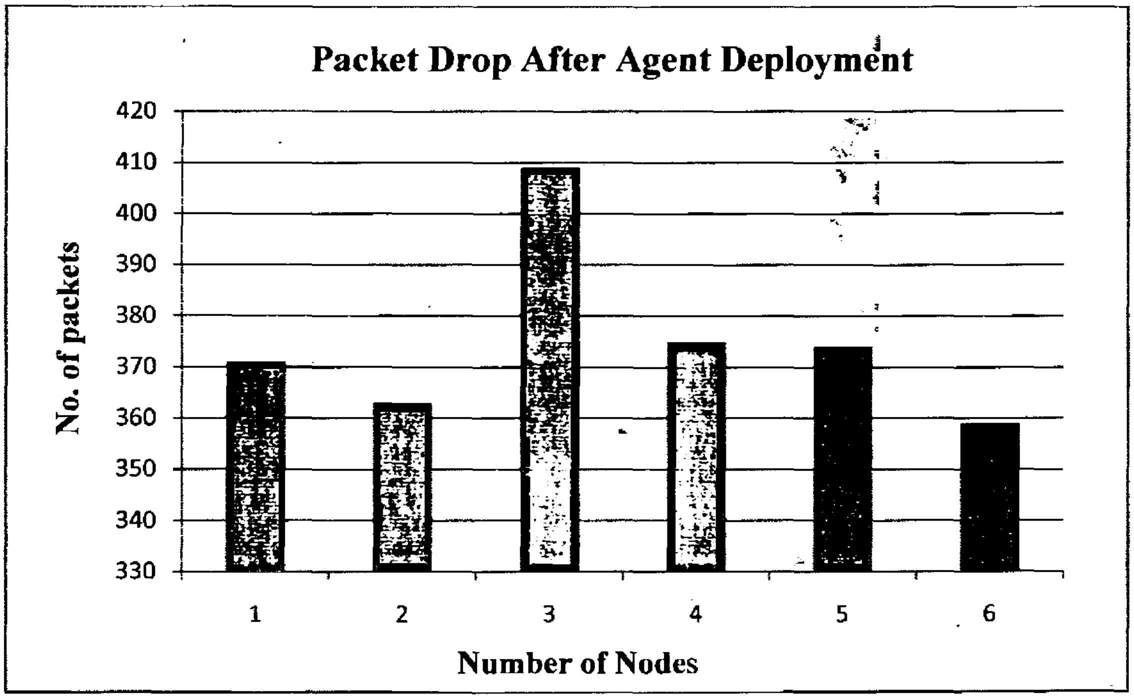

Figure-34 Packets Dropped after Agent Deployment

7.3 Results & Comparison

Here in figure-35 is a comparison of reported statistics to PCH, which monitor that the original packets originated by the SCH1 & SCH2 are not same as reported by SCH1 & SCH2 so there would be some gap or any malicious activity is carried out which is blackhole which is dropping packet and not transferring actual quantity of packets. PCH is keeping the entries of data pass from it and updating its record in the routing table whether it is coming from one hope or 2 hop but not monitoring dropping rate that why result are not same.

7.4 Analysis & Discussion

For setting simulation threshold for detection & identification, we considered different cases with different number of packets per node for simulation time of 15, 20 and 25 sec. we observe that in all cases graph trend found similar for varying throughput of packets per node. We verify our proposed solution by extending it to 50 sec simulation and changing the traffic generation rule to Exponential. This way, we utilized the available resources to the maximum and found out that our detection and identification threshold are working properly as graph trend remain same in all cases.

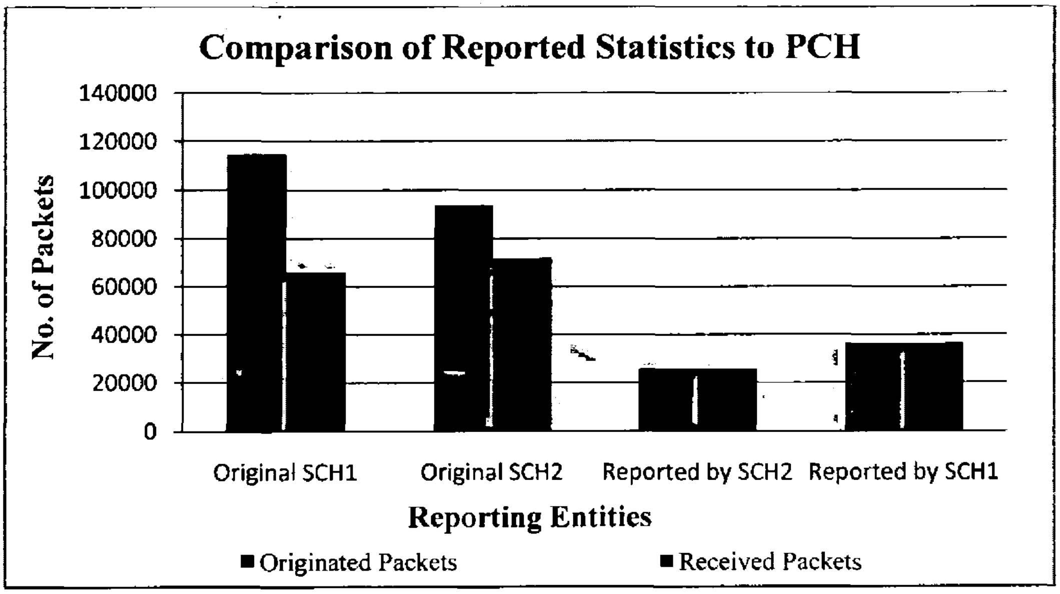

Figure-35: Comparison of Reported Statistics to PCH

In the end, we compare the results and observed that original number of packets send by SCH1 and SCH2 are now the same as reported by the PCH that is mean there is some malicious activity in the network that is causing packets not reaching successfully to the intended destinations shown in figure-35. Finally, the blackhole attack that launched by SCH1, after detection and identification that malicious CH disowned from the network and a new SCH selected for smooth transmission of the data within the network shown in figure-36.

Initially, we have tested our results to fix our detection and identification threshold with varying simulation times, from 15-50 seconds, and different number of through put. It observed that dropped threshold vary from 64-96% packets with CBR having bandwidth of 2Mbps while data rate is 34.6 Kbps with propagation delay of 10msec. BH is getting active in between 15-30 second where as packet per second is 10-30.

In the case when BH activation time is 15 seconds total dropped packets in the process of detection and identification is about to 47% of the total send packets while agent is sending approximately half of the packets received by it. Average BH activation and agent deployment time is about to 2.2 % while BH activation time and agent kill timings average is near about 19%. If packets per second vary to 20-30 then average BH activation and agent deployment time lies in between 2-3.6% while BH activation time and agent kill timing average remain 20-34% approximately here weighted average throughput of nodes is approximately 2.6 %.

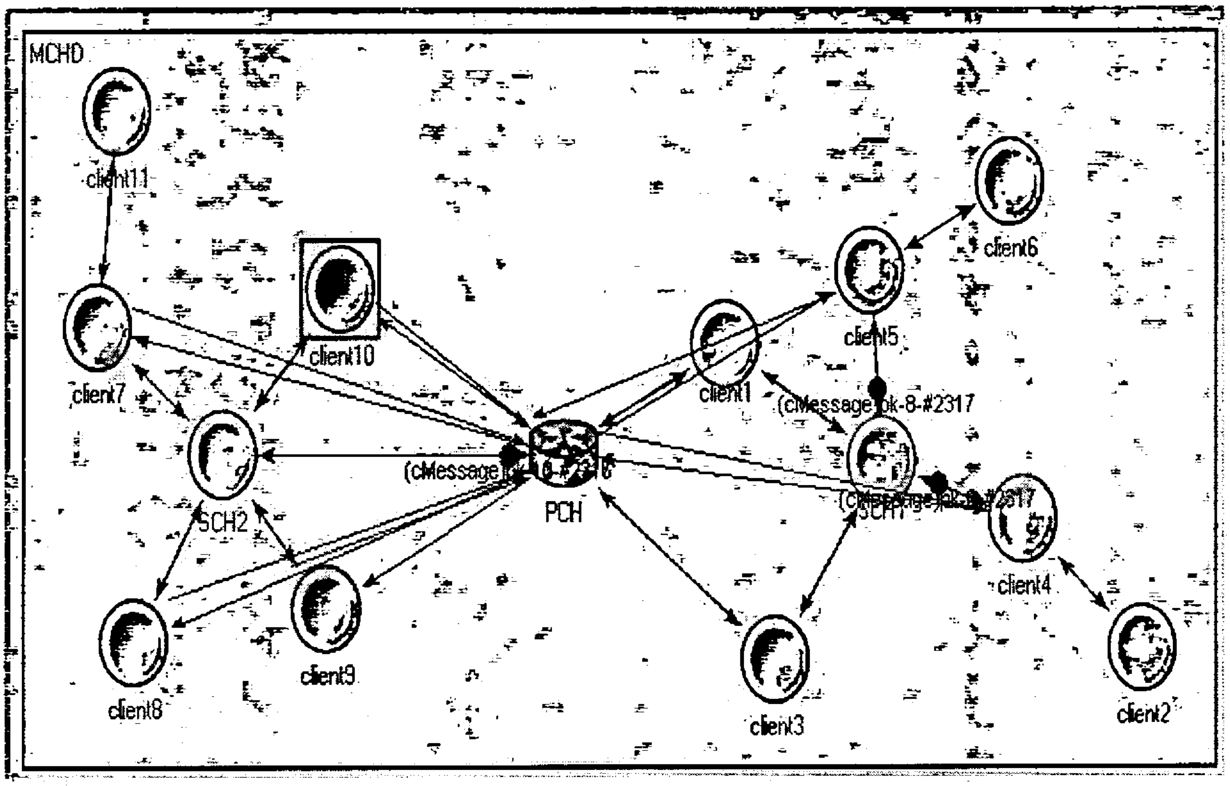

Figure-36: Simulation Snapshot, after old CH declared malicious and new SCH selected.

In the case of timeline graph when we considered total number of packets sent by the agent and average of BH activation time with agent killing time after dividing packet per second that lies in between 10-30, the weighted average throughput of nodes against timeline is approximately 27% is observed.

The weighted average throughput of nodes is approximately 2.6 % whether agent deployment and kill time is in between 17-34sec in the case when the BH activation time varies from 15-30seconds. Agent completes its identification process almost within time of 27seconds after the activation of Blackhole attack, disowns the malicious SCH, and selects a new SCH.

Chapter 8

CONCLUSION & FUTURE DIRECTIONS

In this chapter, we are concluding final remarks regarding thesis achievement and future directions

8.1 Achievements

Main achievements of this thesis are:

- We have focused the malicious cluster head detection and identification as it is a core part in clustering environment where all communication carried out through cluster head.
- Detection and identification of malicious activity of cluster head will make the traffic smooth and reliable.
- Reliability achieved by decreasing reliable packet loss.
- This security mechanism enhances level of security to great extend in clustering environment.
- As evident from literature survey studies main have considered TCP based traffic. As, this study having in cooperated UDP traffic load has the potential for further research and hopefully fulfill the existing gap in this area.
- Thesis diagnoses the fake reporting of the malicious Cluster head and gives a smooth solution to that problem.

8.2 Future Direction & Prospective

Our present work has highlighted many directions for future research. One of them is the use of same scenario for different type of networks like Mesh, Sensor etc. Secondly, increase in network and node size, like WSN, for the generation of variable data set so that AI based algorithms and data mining techniques can be applied to pin-point the behavior of malicious entities; such that verification of thresholds and their dynamicity can be applied for the detection of malicious nodes/ CH .

As we have simulated our scheme using OMNET++ in future, it can implement as a real testbed for analysis and its integration into IDS & IPS etc. In the meanwhile, the same mechanism tested for different infra structures. Finally, the proposed scheme can also be tested for different attacks type.

References

[1] J. Broch, et.al, “A performance comparison of multi-hop wireless ad hoc network routing protocols”, ACM Press New York, NY, USA, 1998, pp. 85-97.

[2] D. B. Johnson et. al “Routing in Ad Hoc Networks of Mobile Hosts ”, IEEE Workshop on Mobile Computing Systems and Applications 1994, pp. 158-163

[3] Wikipedia: The biggest Encyclopedia. www.en.wikipedia.com.

[4] J.K. Hart, et.al. “Environmental Sensor Networks: A revolution in the earth system science”, Earth-Science Reviews, 78. pp. 177-191.2006

[5] N. Li et. al., “Autonomic Fault Management for Wireless Mesh Networks,

[6] S. Lu, et. al., “Robust rate adaptation for 802.11 wireless networks”. In Proceedings of the 12th Annual International Conference on Mobile Computing and Networking, pages 146–157, Los Angeles, CA, September 2006.

[7] N. Daswani “Denial-of-Service (DOS) Attacks and Commerce Infrastructure in Peer-to-Peer Networks”, 2005

[8] MS Thesis on “Mobile Agent Based Hierarchical Intrusion Detection System in Wireless Sensor Networks” by Surraya Khanum, International Islamic University, Islamabad, 2011.

[9] F.Li et. al.“Malicious nodes seriously affect the performance of mobile ad hoc networks”Packet delivery ratios in wireless ad hoc networks deteriorate or break significantly with the presence of malicious nodes. 28 July 2006, SPIE Newsroom. DOI: 10.1117/2.1200606.0277

[10] P. Rathod et. al.“Security Scheme for Malicious Node Detection in Mobile Ad Hoc Networks” (Eds.): IWDC 2004, LNCS 3326, pp. 541-542, 2004,·Springer-Verlag Berlin Heidelberg 2004.

[11] C. Crepeau et.al.“A secure MANET routing protocol with resilience against byzantine behaviours of malicious or selfish nodes”

[12] H. Yang, J. Shu, X. Meng, S. Lu, “SCAN: Self-organized network-layer security in mobile ad hoc networks,” IEEE Journal on Selected Areas in Communications, vol. 24, no. 2, February 2006, pp. 261-273

[13] http://csrc.nist.gov/groups/SNS/manet/documents/Critical-Nodes-MANET.pdf

[14] D.I. Curiac et.al "Malicious Node Detection in Wireless Sensor Networks Using an Autoregression Technique", Ovidiu Banias, Octavian Dranga, Third International Conference on Networking and Services (ICNS'07) 2007 IEEE

[15] B.C. Cheng, et.al, "A Good IDS Response Protocol of MANET Containment Strategies" IEICE Transactions on Communications, 2008.

[16] S.S. Yau, et. al "Multi-hop Clustering Based on Neighborhood Benchmark in Mobile Ad-hoc Networks"2007.

[17] P. Rathod et. al."Security Scheme for Malicious Node Detection in Mobile Ad Hoc Networks" (Eds.): IWDC 2004, LNCS 3326, pp. 541-542, 2004, Springer-Verlag Berlin Heidelberg 2004.

[18] R. Boutaba, et. al, "Policy-based Management: A Historical Perspective", Journal of Network and Systems Management (JNSM), Vol.15, No. 4, Dec. 2007

[19] A.M.Hadjiantonis, et.al. "A context-aware, policy based framework for the management of MANETs", 7th IEEE Intl. Work on Policies for Distributed Systems and Networks, pp.23-32 (Policy 2006)

[20] P. Albers et.al., "Security in ad hoc Networks: A General Intrusion Detection Architecture Enhancing Trust Based Approaches", WIS'02 Proceedings, April 2002, pp.1-12.

[21] C. Karlof et.al, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", Elsevier's AdHoc Networks Journal, 1(2-3), 2003, pp. 293-315.

[22] A. Savvides, et.al "Dynamic fine-grained localization in ad-hoc networks of sensors", In Proc. 7th ACM MobiCom, Rome, Italy, 2001, pp. 166-179.

[23] A. Becher, et.al, "Tampering with motes: Real-world physical attacks on wireless sensor networks", SPC Proc., York, UK, April 2006, pp.104-118.

[24] W. Junior, et.al, "Malicious Node Detection in Wireless Sensor Networks," the 18th International Parallel and Distributed Processing Symposium (IPDPS'04), April 26 – 30, 2004, Santa Fe, Nex Mexico, USA.

[25] A.L. Toledo "Robust Detection of MAC Layer Denial-of-Service Attacks in CSMA/CA Wireless Networks". IEEE Transactions on Information Forensics and Security, Vol. 3, No. 3, September 2008.

[26] M. Bella et.al "Source Detection of SYN Flooding Attacks" 2009, ESR Groups France

[27] B. Awerbuch, et.al "Mitigating Byzantine Attacks in Ad Hoc Wireless Networks. Technical report, Center for Networking and Distributed Systems", Computer Science Department, Johns Hopkins University, 2004.

[28] P. N. Raj, et.al "DPRAODV: A dynamic learning system against blackhole attack in AODV based MANET" IJCSI 2009.

[29] K. A. Bradley, et.al "Detecting Disruptive Routers: A distributed Network Monitoring Approach" IEEE1998

[30] N. Khadam, et.al "Detection of malicious node in MANET through Faith" MS Thesis, accepted in International Islamic University Islamabad, 2008.

[31] F. Kargl, et.al "Advanced Detection of Selfish or Malicious Nodes in Ad Hoc Networks" Springer-Verlag Berlin Heidelberg 2005

[32] H. Yang, et.al,"Self-organized Network Layer Security in Mobile Ad Hoc Networks", ACM MOBICOM Wireless Security Workshop (WiSe'02).

[33] L. Buttyan et.al: "A Virtual Currency to Simulate Cooperation in Self-organized Ad Hoc Networks". Technial Report DSC/2001/001, Swiss Federal Institute of Technology - Lausanne, 2001.

[34] S. Buchegger et.al, "Nodes Bearing Grudges: Towards Routing Security, Fairness, and Robustness in Mobile Ad Hoc Networks", Proc. of the 10th Euromicro Workshop on Parallel, Distributed and Network-based Processing,Canary Islands, Spain, 2002.

[35] Y.-A. Huang et.al "A Cooperative Intrusion Detection System for Ad hoc Networks," In the Proc. of first ACM Workshop on Ad hoc and Sensor Networks, pp. 135-147, 2003. New York, NY, USA

[36] M. Hollick, et.al "On the Effect of Node Misbehavior in Ad Hoc Networks", IEEE Communications Society, 2004.

[37] [online] P. Sethi et.al" Dynamic Cluster Management in Ad hoc Networks" available: http://cse.iitg.ernet.in/gb/papers/clustercresq_pdp02.pdf

[38] P. N. Raj, et.al, "DPRAODV: A dynamic learning system against blackhole attack in AODV based MANET" *IJCSI* 2009

[39] M. D. Priya, et.al "ARPE: An Attack-Resilient and Power Efficient Multihop WiMAX Network" International Journal on Computer Science and Engineering Vol. 02, No. 04, 2010, 1201-1208

[40] L. Yao, et.al "A Clustered Routing protocol with Distributed Intrusion Detection for Wireless Sensor Networks" 2007.

[41] R.C. Chen, et.al "A New Method for Intrusion Detection on Hierarchical Wireless Sensor Networks" International Conference on Ubiquitous Information Management and Communication-09, January 15-16, 2009, Suwon, S. Korea, Published in ACM 2009.

[42] D. Zhang, et.al," A Novel Architecture of Intrusion Detection System" IEEE CCNC 2010 proceedings.

[43] H. Safa, et.al "A cluster-based trust-aware routing protocol for mobile ad hoc networks" Wireless Netw (2010) 16:969–984, DOI 10.1007/s11276-009-0182-1, Published online: 20 May , Springer Science & Business Media, LLC 2009

[44] C.X Ma, et.al, "A novel intrusion detection architecture based on adaptive selection event triggering for mobile ad-hoc networks," IEEE Second International Symposium on Intelligent Information Technology and Security Informatics, pp.198-201, January 2009

[45] H. Otrok, et.al, "A game-theoretic intrusion detection model for mobile ad hoc networks," Elsevier Computer Communications vol. 31, issue 4, pp. 708-721, March 2008

[46] N. Marchang, et.al "Collaborative techniques for intrusion detection in mobile ad hoc networks," Elsevier Ad Hoc Networks, vol. 6, issue 4, pp. 508 – 523, June 2008.

[47] K. Manousakis, et.al, "A stochastic approximation approach for improving intrusion detection data fusion structures," IEEE Military Communications Conference (MILCOM 2008), San Diego, CA, pp. 1-7, November 2008.

[48] H. Deng, et.al, "Agent-based cooperative anomaly detection for wireless adhoc networks," Proceedings of the 12th Conference on Parallel and Distributed Systems, pp. 613-620, 2006.

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

[50] S. Marti, et.al "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks", Proc. of the Sixth Annual International Conference on Mobile Computing and Networking (MOBICOM), Boston, 2000

[51] T.H. Hai, et.al "Hybrid Intrusion Detection System for Wireless Sensor Networks", Internet Computing & Security Lab, Department of Computer Engineering, Kyung Hee University, South Korea, LNCS 4706, Part II, pp. 383–396, Springer-2007.

[52] B. Dong et.al, "An improved intrusion detection system based on agent" Proceedings of the Sixth International Conference on Machine Learning and Cybernetics, Hong Kong, IEEE - 2007.

[53] W. H.bin, et.al, "Intrusion Detection for Wireless Sensor Networks Based on Multi-Agent and Refined Clustering" 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.

[54] Y. Zhenwei et.al "A Framework of Machine Learning Based Intrusion Detection for Wireless Sensor Networks" Department of Computer Science, University of Illinois at Chicago, Published by IEEE 2008.

[55] G.H Lai et.al "Detecting Denial of Service Attacks in Sensor Networks" Department of Information Management, ational Sun Yat-Sen University, Kaohsiung 804 Taiwan 2008.

[56] B Sun, et.al "Detecting Black-hole Attack in Mobile Ad Hoc Networks" EPMCC 2003

[57] P. N. Raj, et.al "DPRAODV: A dynamic learning system against blackhole attack in AODV based MANET" IJCSI 2009

[58] B Sun, et.al "Detecting Black-hole Attack in Mobile Ad Hoc Networks" EPMCC 2003.

[59] S. Dokurer, et.al "Simulation of Black hole attack in wireless Ad-hoc networks" Master's thesis, Atılım University, September2006.

[60] S. Yi, et.al, "Security-Aware Ad-hoc Routing for Wireless Networks". Report No.UIUCDCS-R-2002-2290, UIUC, 2002.

Acronyms

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**
IDA:	**Intrusion Detection Agent**
IDS:	**Intrusion Detection System**
IP:	**Intrusion Prevention**
IPS:	**Intrusion Prevention System**
J-Sim:	**Java Simulator**
PCH:	**Primary Cluster Header**
PKC:	**Public Key Cryptography**
P2P:	**Point to point**
SCH:	**Secondary Cluster Header**
SKE:	**Symmetric Key Encryption**
WSN:	**Wireless Sensor Networks**
NSCH:	**New Secondary Cluster Head**
MCH:	**Malicious Cluster Head**
MSCH:	**Malicious Secondary Cluster Head**
BH:	**Black Hole**
CBR:	**Constant Bit Rate**