Detection and Identification of Unreliable Traffic in Wireless Ad-hoc Network during Congestion

MS Research Dissertation

By

Sumaira Seemab (442-FBAS/MSCS/S08)

Supervised By:

Prof. Dr Muhammad Sher

Co-Supervised By:

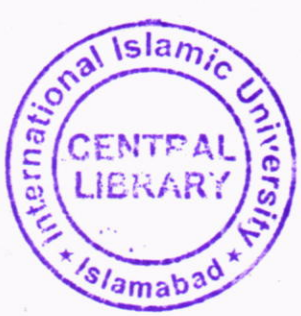
Mr. Khalid Hussain

Department of Computer Science

Faculty of Basic and Applied Sciences,

International Islamic University, Islamabad.

2011



Network operating system

A Dissertation submitted to the

Department of Computer Science

International Islamic University Islamabad

As a partial fulfillment of requirements for the award of

the degree of

MS in Computer Science

International Islamic University, Islamabad

International Islamic University, Islamabad

Dated: 02nd November, 2011

Final Approval

It is certified that we have examined the thesis titled "Detection and Identification of Unreliable Traffic in Wireless Ad-hoc Network during Congestion" submitted by Sumaira Seemab , Registration No: 442-FBAS/MSCS/S08, and found as per standard. In our judgment, this research project is sufficient to issue. It is accepted by the International Islamic University, Islamabad for the award of MS Degree in Computer Science.

Committee

External Examiner

Dr. Hassan Mahmood
Assistant Professor
Department of Electronics
QAU, Islamabad

Hasan Mahmood.

Internal Examiner

Dr Zunaira Jalil,
Assistant professor/Acting chairperson,
DCS&SE(FC),FBAS,IIUI

Supervisor

Prof. Dr. Muhammad Sher
Chairman,
DCS&SE, FBAS, IIUI

Co-Supervisor

Mr. Khalid Hussain
Assistant professor,
Riphah International University,
Islamabad

(Out of country)

Declaration

We hereby declare that this work, neither as a whole nor as a part has been copied out from any source. It is further declared that we have conducted this research and have accomplished this thesis entirely on the basis of our personal efforts and under the sincere guidance of our supervisor Prof. Dr Muhammad Sher and our Co-Supervisor Mr. Khalid Hussain. If any part of this project is proved to be copied out from any source or found to be reproduction of some other project, we shall stand by the consequences. No portion of the work presented in this dissertation has been submitted in support of any application for any other degree or qualification of this or any other university or institute of learning.

Sumaira Seemab

(442-FBAS/MSCS/S08)

Acknowledgement

I would like to thank my supervisor Prof. Dr Muhammad Sher and Co supervisor Mr. Khalid Hussain Khan for their endless support, valuable suggestion, encouragement, guidance and coordination while conducting my task. Their moral support and encouragement in every step, made my research work easier and attainable.

I would also like to extend my appreciation to all of my teachers in the department who have introduced new dimensions of knowledge. Their valid suggestion and support helped me in difficult time. Thanking Sir. Faraz for his views which helped me in improving the proposal and also Mam Ammara for not only their moral support but also providing the managerial and technical support as well.

I would gratefully thank my sincere friends for their contribution and support in my research work.

I would like to admit that my achievements are due to my sincere and loving parents who have always prayed for my success.

I state my innumerable gratitude to all the people who have helped me during completion this MS degree and hope to have this honour that they would walk along me throughout my life.

Project in Brief

Project Title:	Detection and Identification of Unreliable Traffic in Wireless Ad-hoc Network during Congestion
Undertaken By:	Sumaira Seemab
Supervised By:	Prof. Dr Muhammad Sher
Co-Supervised By:	Mr. Khalid Hussain
Start Date:	20-08-2010
Completion Date:	20-08-2011
Tools and Technologies:	OMNET++, VC++
Documentation Tools:	MS Word, MS Visio, MS Excel
Operating System:	Window XP
System used:	Pentium 4, 2.00 GHz dual core

Abstract

A temporary wireless network, set up by mobile nodes or computers is known as an ad-hoc network. These networks allow wireless mobile nodes and/or computers movement in areas with no infrastructure. The mobile nodes are able to communicate with each other by forwarding data packets to neighbouring nodes in the network. Nodes locate remote destinations with the help of intermediate nodes, via some routing protocols. With strong security mechanism, users gain advantages to an ad hoc network if these networks.

Under normal circumstances, wireless ad hoc networks are open to attacks targeted on nodes. These attacks include Wormholes, Gray holes, Byzantines, Black holes, and etc. Attacks and security problems have contributed to research in the field of security solutions to ad hoc networks to gain popularity, day by day. The focus of this thesis is to counter black hole attack in wireless ad hoc networks through detection and identification, thus pinpointing the attacker using coordination among nodes so that some isolation mechanism can be used to eliminate the black hole from further damaging the network performance.

The proposed methodologies to detect and identify a black hole attack in the ad hoc network are based on threshold values. Black hole attack is detected when overall packet loss exceeds a threshold value in comparison to average packet drop of the network. Whereas, for identification purposes, the neighbouring nodes coordinate against the suspicious member of the network before declaring it as fraudulent.

We have successfully simulated congestion and black hole attacks using the OMNET++ environment. An enhancement in existing AODV routing protocol is suggested to avoid the formation of black holes and congestion (sink) in the network. For this purpose, we present methodologies which enables the detection of congestion and black hole attacks in an ad hoc network under AODV protocol.

Table of Contents

CHAPTER 1

INTRODUCTION

Wireless [27] communication enables data to be transferred between users with waves. Waves are used to transformation of data to mobile users during the usage of communication. In wireless communication, wired infrastructure is not used. The air is used as a medium for these electromagnetic waves to travel.

Types of Networks

Three [27] types of wireless interconnection have been defined according to coverage area. These are Personal Area Networks (PANs) and Local Area Networks (LANs) and Wide Area Networks also.

Personal Area Networks

It is used for communication between devices such as Telephones. Another example is a PAN network. Bluetooth, sensor networks and zigbees are all known as PAN networks.

Local Area Networks

These networks allow communication in a local area and this Communication may be includes in a building. In wireless LAN, for medium purpose nodes used air.

Wide Area Networks

These networks allow communication in large geographical areas. WANs basically include multiple LANs.

1.1 Wireless Local Area Network (WLAN)

Wireless Ad-hoc network have number of nodes which able to communicate with each other through waves as a medium without a pre-specified networking infrastructure. It originates from battlefield communication applications, where infrastructure networks are often impossible. Wireless nodes have set of wireless devices, which connects dynamically, and transfer information. Wireless nodes can be personal computers (desktops/laptops) with wireless LAN cards, Personal Digital Assistants (PDA), or other types of wireless or mobile communication devices.

WLANs transmit information over wireless mediums rather than wires. These networks are an alternative solution to conventional LANs which connect nodes in wired environments. A

WLAN is a communication network that shared information with wireless links which are to be received by numerous stations due to broadcast data. WLANs mainly used for connecting the Internet. Internet access points present in coffeehouses and other areas are known as "hot spots". Such networks have expanded popularity among mobile users who need to access information.

1.1.1 Transmission of Wireless LAN

Wireless LAN [35, 36] is used for a wireless transmission medium. Wireless LANs which allow nomadic access to cross buildings are used in a cluster of buildings as well as Ad-hoc networking. Some essential requirements for wireless LANs include nodes, areas in which data perform, battery power and utilization, transmission strength and security, dynamic configuration, handoff or roaming as well as collocated network operations. Wireless LAN can operate both with, and without a base station. IEEE has defined the state of wireless LAN, named IEEE 802.11. This is used for covering the layers that is physical and data link layers. The design of IEEE 802.11 categorized with two sets: a **basic service set** (BSS) and an **extended service set** (ESS).

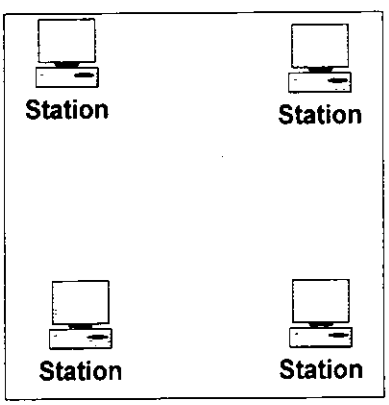


Fig 1.1: Ad-hoc Network (without an AP)

A BSS is a set of stations that is used for managing with single coordination function. BSS's may be isolated or connected to a central station that is base station and known as an access point (AP). A BSS that is not including an AP is known an **Ad-hoc architecture**.

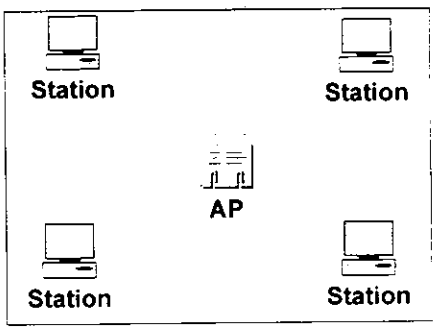


Fig1.2: Ad-hoc Network (with an AP)

On the other hand, **infrastructure network** is making with BSS and with an AP. ESS is not made with single BSS but made with two or more basic service sets with APs.

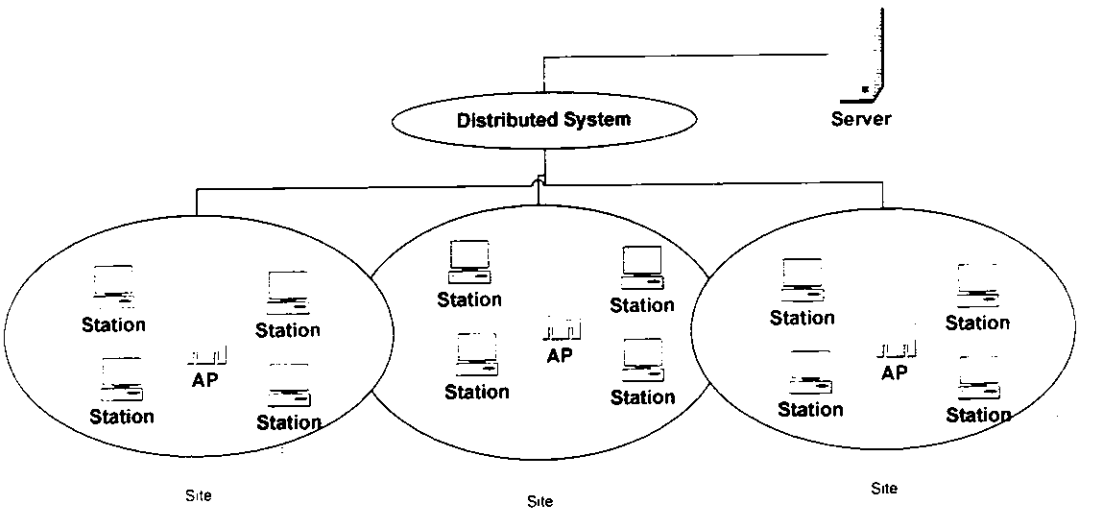


Fig 1.3: Distributed System

The IEEE 802.11 MAC layer includes three different areas: security, access control and data delivery with feasibility. Wireless LANs using IEEE 802.11 have layers with two types: a physical layer, and an MAC layer.

Factors such as Noise, interference, congestion, malicious and other different effects effect in loss of data. This can be countered by consistent mechanisms, not include at a lower level but at a higher level, as like TCP. For this accurate purpose, IEEE 802.11 includes frame that is used for exchanging protocol. When data is received by one node to another node, the receiving node sends an acknowledgment (ACK) frame to sending node. The other station is not interrupted during this stage. Hence this transmission is treated as an atomic. If the source nodes do not receive ACK within a specific time (usually a short one), the source data

retransmits the frame. This can be caused by either a damaged data frame, or a damaged ACK frame.

1.1.2 DATA TRANSMISSION

In **data transmission [36],** IEEE 802.11 has an exchange of two frames. For enhanced consistency, the exchange of frames carried out is four. Such an exchange requires the source to first issue a Request to Send (RTS) frame that transfer data from source to destination. The RTS alerts all nodes, present that an exchange is in progress. The destination from the nodes responds this frame with clear to send (CTS). In the same way, the CTS prepared all stations which are in range about the exchange in progress. After receiving the CTS, the source node retransmits the data frame and the after receiving data, the destination node responds with an acknowledgment. The RTS/CTS portion is a function of the MAC that is used for data transmission, but it is possible to disable it.

Suppose that node A is a source node that is used for transmitting data to node B, as shown in figure 1.4. if node C feel the existence of medium, then it will not allow to hear the data of specific node A because node A is not in range, excluded node A from this information, and node A mistakenly conclude that it can transmit data to node B. if node C also include in transmission and does start transmitting data, it means it will interfere at node B, clean out the frame from A. The problem that station is not able to detect a probable challenger for the medium is called **hidden station problem** because challenger is far away.

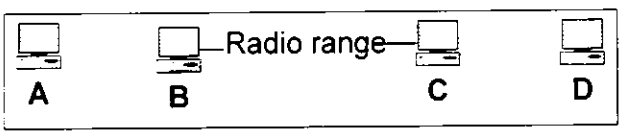


Fig 1.4: Hidden Station Problem

For dealing with hidden station problem, 802.11 support two operations. First is called distributed coordination function (DCF) that is distributed and does not use any type of central device. Other one is called Point coordination function (PCF) that is used for central point and focus on base station to control all activities in it.

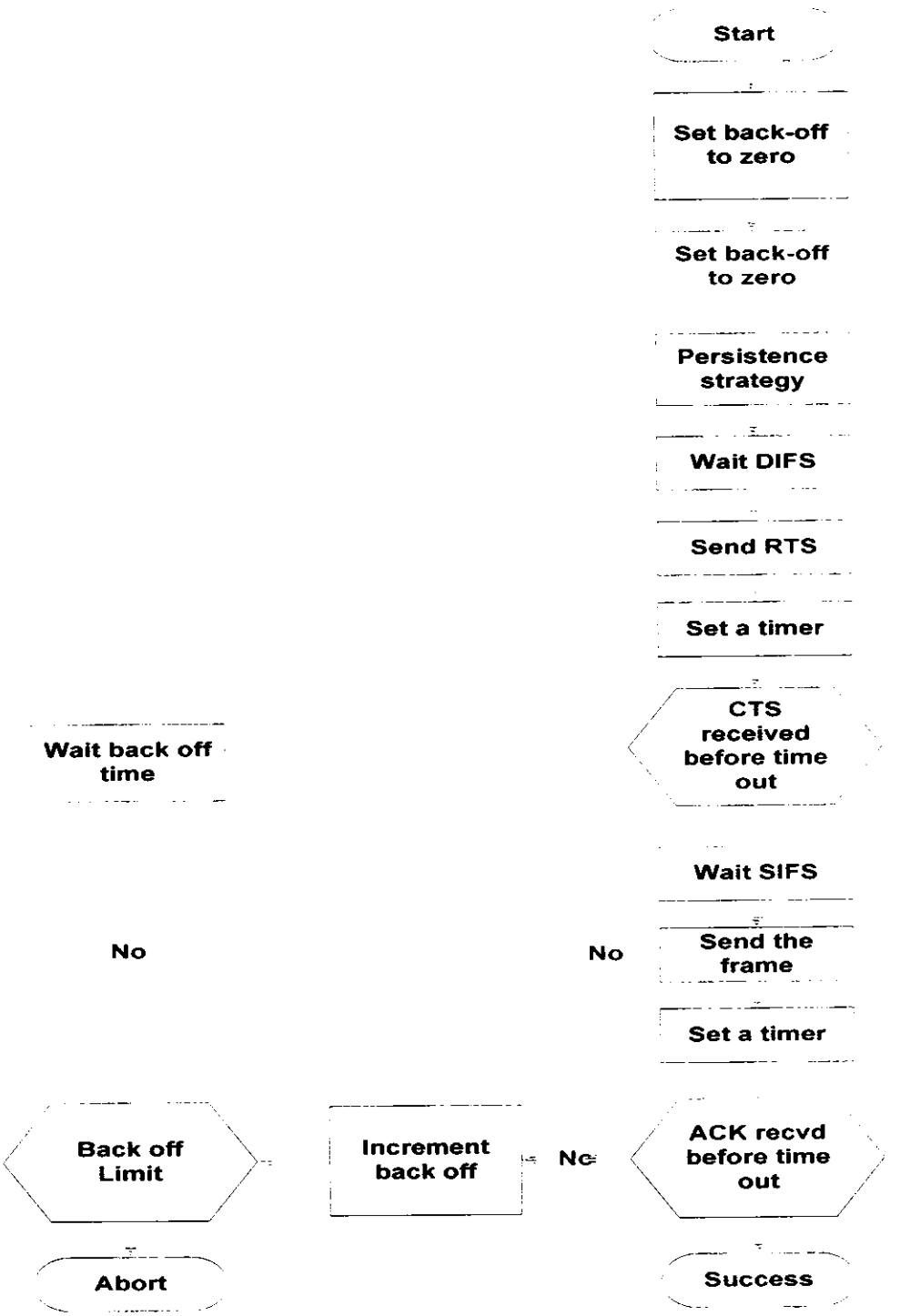


Fig 1.5: CSMA/CA flowchart [35]

DCF that used distributed function and have contention algorithm that is used for providing access to all traffic without any type of disruption. On the other hand, PCF provides services that's purpose is contention free. It is built on the top of DCF. When DCF is doing work, 802.11 use specific protocols that is called carrier sense multiple accesses with collision

avoidance and called as CSMA/CA. PCF is a method that is not a necessary method and this can be implemented in an infrastructure network. It cannot be used in an Ad-hoc network and mostly used in time sensitive transmission. DCF consist set of delays that have the opportunity used for priority scheme.

Consider a delay that is known as an inter frame space (IFS). By keeping the IFS in mind, we shall discuss the factors that are required during the exchange of data and control frame in time.

1. First of all, the source node that is used for sensing medium through checking the energy level.
    - The medium then uses a strategy with back-off and this strategy is done until that medium is idle.
    - After detecting the idleness of station, the node waits for a period of time. This period is known as a **distributed inter frame space** (DIFS). After this period, the node sends an RTS frame.
2. After sending the Request to send, the source node waits for a period of time known as **short inter frame space** (SIFS) and the destination node reply this SIFS and sends a CTS frame. These CTS frames declare that the receiving node is ready to receive data.
3. The destination node receives data, and waiting for a time period that is equal to the SIFS, then destination node sends an acknowledgement which is used for indicating that transmitted frame has been received.
4. When the node sends a frame, it suppose to time duration for engaging channel. Nodes are always have affected by a timer that is known as the **network allocation timer** (NAV). The NAV illustrate about the time is missing before these nodes are allowed for the purpose of checking the idleness.

1.2 Ad-hoc Networks

These are networks that do not have any type of infrastructure, but still meet the required communication needs. If each node in this type network is supposed to be responsible by carrying traffic, then it participates in topology. Nodes within such networks may be mobile, meaning that they can be utilized within or out of the communication range. These nodes also support each other in processes such as the delivery of packets.

In MANET, wireless node has source, an intermediate node, or the destination which participates in data transmission. When a wireless node plays the role of intermediate node, it serves as a router that can receive and forward data packets. The nature of ad-hoc networks tends to cause wireless nodes to continuously move. Consequently, the network topology varies from time to time.

Ad-hoc network have advantages, which include:

- *Low cost of deployment*: Possible to deploy ad-hoc networks on the fly as they don't require any type of expensive infrastructure, such as copper wires or data cables.
- *Fast deployment*: Ad-hoc networks are very convenient and easy to deploy.
- *Dynamic Configuration:* Ad-hoc network configuration can change dynamically. When compared it to configurability of LANs, easy to change the network topology of a wireless network.

Users want the ability to communicate through wireless communication. Nodes are able to forward data/control packets from the source node to destination node in it. This form of network communication is limited by its transmission ranges.

- *Security:* It is an essential in scenarios such as a battlefield. The five goals of security – **availability, confidentiality, integrity, authenticity and non-repudiation** - are difficult to achieve in MANET, mainly because nodes in the network contributes equally in traveling packets.

1.2.1. Applications of Ad-hoc Networks

Some applications of MANET include: Soldiers who relay information to be aware and alert of the situation on a battlefield; sharing information in business during a meeting; attendance to participate in conference using laptop and by disaster relief personal who need to coordinate efforts during a disaster such as after an earthquake or fire.

A number of ad-hoc applications include:

Personal Area Networks

Personal area network is used to create a network which is stabilized by a number of nodes. Such nodes related with single person. Devices must be able to communicate with each other during use by a user or users.

Military Applications

The military operations require high survivability, consistency and fast communication recovery, but in an environment that does not acquire infrastructure. Ad-hoc network is the best solution for this application considering these essential features.

Bluetooth

Bluetooth is one of the commercial applications that utilized the concepts of Ad-hoc network. It can allow low-cost short-time links between wireless devices without depending on any infrastructure service for communication; hence, Ad-hoc network technology is the best solution.

Emergency Services

Ad-hoc network is very beneficial when infrastructure is broken because of natural disasters like earthquake or fire etc. Disaster recovery team requires a flexible communication network and they have no time to wait establishment of wired network. Ad-hoc network can establish communication network among disaster recovery teams very quickly.

1.2.2. Characteristics of Ad-hoc Networks

Infrastructure based, or fixed networks have their own characteristic set of properties. Mobile Ad-hoc networks, however, show properties which are different in many ways from properties of networks discussed above. These differing properties have made it harder to implement security services on such networks and because of them Ad-hoc networks are often considered by a dynamic topology (for quick changes to the topology). They are also thought to be bandwidth; energy constrained and also has limited physical security. But here we saw different types of characteristics that have importance for Ad-hoc networks.

Dynamic topology

One property of nodes includes the ability to move freely, which is used for change the network topology with randomly. This causes unidirectional and bidirectional links to be established.

Bandwidth-constrained

This refers to the amount of data obtained from wireless communication, with the presence of negative effects such as fading, noise, interference, and etc.

Energy-constrained operation

Nodes in an ad-hoc network can be built on batteries. Designing a system design criteria which optimizes energy conservation may thus be one of the most essential requirements for such nodes.

1.3 Ad-hoc Networks Routing Protocols

Routing protocols proposed for MANET and these protocols can be classified into two sub-parts, namely proactive protocols and second one is reactive protocols. **Proactive Routing Protocols** involve the maintenance of information in the form of a routing table by every node, while **Reactive Routing Protocols** involves obtaining routes when a demand is placed. The use of on demand protocol by a node requires a path to destination node and this means that node searching for the path may be forced to wait until the required route is found. It saves energy because it only works when the demand of route is placed on it. But has the disadvantage of the route not being immediately available as the route discovery takes some time. **Hybrid Routing protocols** have qualities of reactive routing protocol and also from proactive routing protocols, meaning that it can be useful for both above networks. During the establishment of routes, they are established with proactive manner with in the start, but later (after they have stabilized), they can serve as reactive routes.

a. Ad-hoc On-demand Distance Vector Routing (AODV)

This protocol is a well-known reactive protocol. Dynamic links are able to quickly adapt to this type of protocol. It also offers low processing and memory overhead and can determine routes to destination nodes within an Ad-hoc network, all of which are useful advantages.

The protocol uses sequence number of destination node for cover up the loop freedom for whole times (even with in the face of anomalous delivery messages). It can also help avoid problems like "counting to infinity", which are counted with distance vector protocols. The main purpose of the protocol is acquiring the shortest distance for completing communication that is for source node to the destination node during the route discovery process. Such

protocol has the route discovery process that is able to flood the network with packets of route request (RREQ). Consequently, the performance of the network can become reduced, especially when the nodes mobility is too much high. This means that communication can cause a route to become unstable, and ultimately the route may be lost. One solution to the mobility problem is to exclude high speed nodes. However, this may congest some nodes, while other nodes may be unutilized, causing poor network performance.

To counter this problem, the route discovery process should be changed to locate a stable route. This route should be able to balance the load among various routes. This may be done by using both nodes' mobility and traffic load to intermediate nodes is establish the most feasible route. Discovery process for route should then be modified to only allow slow speed nodes to forward the packets which are used for requesting the route, and the broadcast of the request packed is delayed according the business of the node (i.e. number of packets in its buffer). Results show that this scheme can perform better than the AODV with average end to end delay and the routing load.

When we focus about the operations of the AODV protocol then we see that it can be categorized into two functions that have the name of: Route Discovery, and Route Maintenance.

Route Discovery

Sending data to a new destination requires broadcasting a RREQ through the MANET. Doing this requires search techniques. When that RREQ is received through destination, then at that time receiving node creates a reverse routing entry with in the direction of the originator of RREQ. The destination node of the intermediate is then given by a RREP (route reply) unicast packet. On receiving the RREP, a reverse route entry is created.

There is a possibility of link breakages occurring in this process. To ensure that the nodes are aware of these breakages, a RRER (error) message is used. This message notifies the other nodes about the link breakage, indicating that the required destination is unreachable through the specific broken link. Performing this mechanism requires keeping a precursor list. This is done by the nodes.

Route Maintenance

With the broadcasting of HELLO message, any node can offer to connect the information. In the case of connect with the route; nodes only use the HELLO message. The link is broken when node doesn't gain the message or data packet (that is used for connecting) with the specific time from a neighbour. If the link failure node is near from the destination then local repair mechanism may be launched to rebuild the node towards the destination. On other hand RERR message is sent to neighbours.

b. Dynamic Source Routing (DSR)

An efficient routing protocol used in wireless Ad-hoc networks (WANET) containing mobile nodes is the Dynamic Source Routing (DSR). This protocol allows a network in use to organize itself efficiently, without the need of network administration or administration of any kind by any existing network. This can be done even in the presence of high mobility rates. DSR operates entirely on demand. To be specific, the DSR protocol does not require any type of packets at layer with the network being used.

This protocol is also established with the merging of two type mechanisms, which are known as Route Discover and Route Maintenance.

Route Discovery

This is the process in which a source wishing to send packets to destination through which obtains route that travel through source to destination node. Route discovery is only used when the source try to send data to the destination node through a source route.

Route Maintenance

This process is practiced by source nodes which are not able to detect the destination when using the source to destination (for finding route), for example destination. This can happen if the topology has changed, which in turn will make the link unusable. If a broken source route is detected while maintaining a route, the source may try to use another route to destination. Route maintenance for route will only be cover up when the source route is used for sending data to the destination node.

C. Optimized Link State Routing (OLSR)

The OLSR [27] protocol hopes to target large and dense MANETs. The main goal of OLSR protocol is to use multipoint relays (MPRs). These relays are specifically used for selected nodes. and they are mainly used to broadcast messages during flooding. This mechanism is able to reduce the message overhead by a greater amount than the flooding mechanism. from which each node try to again transmit messages as soon as the node receives the copy of message which is first one. This information is announced in the control messages of nodes that have been selected as MPRs.

MPRs are also used in route calculation from the route for any given node to destination node in the network. MPRs are also used to make possible flooding of control messages in the network.

The main benefit of the OSLR protocol is achieved when it is used for traffic patterns. where there is communication between a large, and a small subset of nodes. Using this protocol source node or destination node pair's change over a time period is also an advantage. This allows large and dense networks to achieve greater efficiency than classical link state algorithms. The protocol is able to enhance topological changes by decreasing the time interval before a periodic control message is transmitted.

1.4 Security Attacks on MANET

Security issues arise in different areas. Some solutions include routing and intrusion detection. physical security and key management: all of which are very important to a functional MANET. Ad-hoc networks are easier to target with the comparison of wired networks. The two fundamental types of attacks which routing protocols face are **Passive Attacks,** and other one is **Active Attacks**. First of all, passive attacks do not disturb protocol operations. Instead, they try to obtain essential information by listening to network traffic, while active attacks disturb protocol operations and try to gain authentication. This is done by injecting arbitrary packets where possible.

The general classification of security attacks against MANET. Passive attacks include eavesdropping, traffic analysis and traffic monitoring, while active attacks that is used for disturbing the protocol include jamming, impersonating, modification, denial of service (DOS) and message replay.

1.5 Security Solutions in MANET

A number of security techniques exist in the present era, and they are categorized by two types of approaches, namely static defensive approach and dynamic defensive approach. The static defensive approach provides authentication, access control, encryption, and digital signatures. These measures act as like defence that is first line, while the dynamic defensive approach behaves as like the second line that is also defensive. The dynamic defensive approach is based on detection of intrusion systems, and the cooperation of enforcement mechanisms.

a. Protective mechanism

The firewall behaves as a barrier between a computer, and the external cyber environment. The firewall allows the computer to stay safe from hacking, or cracking attempts generated by "bad guys". Many times instead of anti viruses, viruses can be attack. For prevention of these things, firewall is used.

Cryptography is based on authentication and encryption schemes, which includes both symmetric and asymmetric cryptography. Hash functions, threshold cryptography and digital signatures are cryptographic primitives. These primitives can enhance integrity, or hide data through dividing into a number of shares. They can also be used to provide authentication services.

Maintaining physical security is also essential. It is relatively easy for the host or small physical devices to be stolen, lost or damaged. Protecting sensitive data can be focus on security modules such as accessing data through PIN or biometric.

b. Reactive Mechanism

The intrusion detection mechanism (IDS) falls into the second line of defensive approach category. Such a mechanism is essentially used for the detection of any misuse and/or anomalies in the system. Anomaly detection expresses the detection of normal or expected behaviour, while misuse detection expresses detection of improper or unnatural behaviour. Such behaviour is usually based on the pattern of a number of well-known attacks. These approaches tend to prove effective against attacks when combined, and used alongside. The

reactive system usually indicates the termination of a connection, blockage of the IP addresses, and recovery.

c. Detective Mechanism

The [27] detection mechanism can be used to detect intrusions, attacks, misuse of resources, and malicious behaviour. First step for handling a malicious node is the detection of malicious behaviour. After such malicious node detection, next is to identify the node. The last step is the isolate malicious node from the network. All of these steps are carried out without any effect on the performance. The three main steps are explained in further detail below.

Detection

As stated above, when we talked about the handling of malicious node then the first step is to detect the presence of the "infected node". This detection process is usually done by searching for any different behaviour that is unexpected of normal behaviour, such as packet dropping.

Identification

As soon as defected node is detected, identification of misbehaving node becomes the next essential step. During identification, any abnormal behaviour of the node is searched for. After the misbehaving node is successfully identified, the remaining nodes that exist in the network are informed. This is mainly done to help the other nodes avoid the malicious node.

Isolation

Now that the other nodes alert about the malicious node because of unexpected behaviour, they can cooperate to isolate the malicious node by disconnecting any kind of service to it.

1.6 Motivation

The MANET has an active research area from the last decade, and it has attracted numerous researchers in the area for the purpose of research.

One of the fundamental problems that researchers are currently faced with is the control of attacks on a MANET. This has proved to be a challenging task. Mostly, research in MANET is based on simulation, which is done due to variety of reasons. This includes the high cost of

real life tests, as well as not being able to test maximum nodes in the real world as this is too infeasible. In hopes of finding solutions to security problems, security techniques have been proposed by researchers. However, techniques do not distinct the difference between congestion and attacks. This shows that there is a need to develop an extended routing protocol; one that will allow us to understand why packets are lost. We know so far that packets are lost by attacks, but congestion also leads to the same outcome.

1.7 Problem Domain

A common observed misbehaviour is packet dropping, which can cause network performance to significantly decrease. In MANET, forwarding packets consumes a large amount of resources. Certain mobile devices do not resort to packet forwarding for the sake of protecting others from any possible attacks or any sort congestion that may exist in the system.

Packets may be dropped by misbehaved nodes as well as certain link errors, and this uncertainty in dropping packets leads to the difficulty of identifying any misbehaving nodes. All of this is due to the lack of security mechanisms, which include access control and authentication.

As stated earlier, there are two types of approaches (static and dynamic) that are defensive which can be used to minimize potential attacks on Ad-hoc networks. There is a need for a deeper discussion which focuses on these approaches, since these approaches and the problems discussed above are closely related to each other. My focusing point of the discussion is enclosed in part of the following text.

Examples of static techniques for security solutions include firewalls, and encryption methods. However, these methods have their limitations. They are only able to provide security for the use of external threats, and so are considered to be the defence of first line as describe above. We know that if any node is comprised, entire security of the system becomes at risk of being compromised as well, showing that it is crucial we develop better security mechanisms; mechanisms that can protect a network from both external, as well as internal threats. This system can find out faulty and selfish activities within a network.

In this thesis, my main focus is to distinct nodes that have which are suspected of any malicious activity.

1.8 Proposed Approach

The central point of communication in a wired network is the router. Data which is meant to be transferred is done by the router to a router which is placed at the receiving end. This process mostly requires intermediate routers, which means that certain problems may arise if any of these intermediate routers starts misbehaving. Detecting and isolating of malicious node such bad routers is a current research topic. A number of researchers have presented solutions of security for both wired and wireless protocols, but these solutions also have deficiencies which can't be ignored.

Congestion and flooding attacks tend to hamper with the QOS of network layer, which results in the performance of the network layer being reduced. This problem indicates that developing a mechanism which would allow the victim of a flooded attack to select individual traffic, and stop its flow before the traffic saturates the network and decreases performance is compulsory. The mechanism should also be able to provide good performance to the remaining flows. There is no mechanism to differentiate the reliable and unreliable node and to identify the loss of reliable and unreliable packets during congestion. Due to loss of reliable packets, QoS is also decreased. Packet drop in wireless network may be because of two reasons; malicious node or congestion. Any of the reason consequently decreases QoS and network performance.

In our proposed system, extended AODV protocol will be proposed for crystal identification of malicious behaviour of the node. In our design, packet will pass form the Black and White (B/W) system, which provide the mechanism to stop packets when the node is malicious. This system can prevent legitimate communications from being disrupted network layer attacks. I have focused to implement network layer attacks in AODV protocol.

1.9 Thesis Structure

In chapter 2, I will discuss the related work with respect of my research topic in greater detail. I will also discuss the limitations or drawbacks of the existing literature overview in chapter 2. In chapter 3, I have mainly focus on analysis of requirement for the related proposed solution and the relative text will be about the analysis. I have also explored the problems associated with domains in greater depth. In Chapter 4, my proposed solution is discussed in detail. Implementation details will be given in chapter 5. Chapter 6 consist of

testing, simulation results, performance evaluation and also about results that is the proof of implementation. In chapter 7 consist of overall status of my research work and also include future work in it.

CHAPTER 2

LITERATURE SURVEY

In literature survey, I will discuss the papers of literature related to security of Wireless Ad-hoc networks. In this chapter, i have try to perform a broad and an important survey in order to make out the problem in existing literature. This chapter includes three sections. In part of 2.1, I have discussed different mechanism of how to handle congestion, in section 2.2. We focused on the papers that detected malicious node in network; whereas in section 2.3, different research papers according to security solution for wired network. Next section is according to wireless network and also deep analysis of internal attacks on network layer. Last part, in section 2.5 I have discuss about the drawbacks of existing literature/technologies and take summarize in the end.

2.1 Congestion

Congestion generally means crowding and network congestion occurs in data networking. Many research is going on it, we just take few paper that how to handle this congestion.

In this paper [40], authors focus on medium access mechanism at the medium access control (MAC) layer when the distributed coordination function (DCF) protocol is utilized. It is used to control protocol degrades when congestion and contention increase in Ad-hoc networks. A new contention-based congestion control (CBCC) method is used for detecting congestion information from MAC layer. It is used for detecting congestion by monitoring the number of one node entry the back off algorithm. Network congestion status can take from the back off state ratio. This method did not take the advantage of carrier sensing mechanism. The back off procedure invoked in different conditions, it is used when carrier sense (CS) mechanism is busy and nodes desire to initiate frame, or sender did not receive CTS frame successfully. When sender sends the (RTS) frame or sender did not receive the ACK frame successfully when sending the data frame or after completing the successful transmission, sender will also entry the back off algorithm. After giving attention to these issues, authors use the BSR (back off state ratio) to measure the level of congestion at a node. When congestion is occurring on medium then packet is not dropped blindly. This is the feature of this algorithm that simply marks the MAC layer when packet is dropped. This method can improve the hidden terminal problems among the nodes. This method improves the performance of TCP with channel of throughput and end to end delay. In this method, author did not focus mobility factor in it.

Victorious et al [41] proposes a mechanism for internet congestion control, especially with the use of random early detection (RED) and mainly focuses on active queue management in congestion control. They make RED as a feedback control system and mainly focus on governing traffic dynamics in TCP/IP networks. This is the system about the TCP flows that uses the channel passing through a common link. In RED, sender of TCP change with its sending rate with respect to drop probability p. this is the RED system with feedback control system. Controlling elements in this system are: drop module, signal of response, possibility of dropping and sending rates of TCP. Feedback system has RTT among the signals are sent by the control module (not a packet) and its sender of TCP reacts to that signal. Variation of sending rate produces through the variation of queue length at bottleneck link. this is discrete time dynamic system with time step of one round trip time RTT. Authors employed queue averaging algorithm to filter out brief queue changes. They also provide an averaging interval that provides good condition in which initially queue averaging algorithm and later rapidly change in round trip times are applied. They also determine that frequency of every queue size should be sampled.

Authors in [42] describe about the interaction of cross layer TCP and protocols in multi hop Ad-hoc IEEE 802.11 networks. On-demand Ad-hoc routing protocols respond in whole networks with events such as channel sound and blockage due to the reason of link loss. They control and hold this problem from different aspects; namely, how transport layer hosts affect at lower network layers (at the end) such as routing and MAC layers. If the congestion-driven link loss clearly distinguish from channel then this technique require some related information from other respective layers. For addressing these problems, two schemes are used in which first one TCP few schemes that is is abbreviated as fractional window increment and the second one is Route-failure notification with the use of BUlk-losS Trigger (ROBUST) policy. In TCP fractional window increment, choose value of K and alpha values for controlling operation of TCP range with preserving of basic TCP window mechanism. If values of alpha are chose then it can achieve very loss rate with small average window. TCP few scheme is used to reduce the congestion with driven link loss and also preventive solution. On the other hand, Route-failure notification using BUlk-losS Trigger (ROBUST) policy is a solution that makes on-demand routing protocols to repress reactions persuade by the destructive TCP behaviour. Two things are used in it. B which is link failure sensitive parameters and number of link failures (that are in series) is counted and take action when

exceeds from threshold value B. Both mechanisms try to improve the system performance without changing the basis TCP window or the wireless MAC mechanism.

2.2 Malicious

Malicious node are the unwanted nodes that desire to cause harm during routing or data forwarding or through any other type. Malicious Participants disturb or take control some subset of parties and disturb the protocol by extracting any possible sensitive information, and protocol does not reveal it regularly. Malicious participant tries to illegally obtain information by proving fake inputs to others or may collude with each other for destroying the secret information. For understanding how to manage it in networking, we investigate some papers that are described below.

Nidal et al [15] present IDS that is used for Discovering Malicious Nodes specifically for MANETs. In this paper, authors describe about the IDS in which they overcome the weaknesses of Watchdog. The role of Watchdog is technique to focus about the node in the path that is used for forwarding the data path or not. If not forward then it will treat intermediate node as a malicious. The role of Pathrater is to find the reliable path from the result generated by Watchdog. Mainly in this paper, they discover the malicious nodes which can be make the reason of partition the network. Every node makes a table that record about the packets, also about the node that sends forwards or receives respectively. Author extends the watchdog system by making table that used for store about source, destination entry, path, in which sum is the total packets that the current node sends, used for forward, or receives using the path as source, intermediate node or destination respectively. And route path is the specific route that is used for the exchanging data between source and destination. Whenever a node detects that coming next hop is ambiguous, the source node will not act rapidly. It will send packets from source node to destination node using an alternate path in the route table. After receiving message, destination node will search out its table to see that is there any match or not. After match found, it contrast the sum field of the message. If the sums are equal, then it means that the malicious node forwards all packets that the source node sends thus it means that node are not malicious. In case, if there is not a matching, it means the node is malicious. Through this technique, false misbehaviour can be detected. But it is difficult to detect he defected node.

Ping YI et al [17] present the detection of malicious node in Ad-hoc Networks with the use automata in timing. In this paper, authors propose intrusion detect approaches that is based on timed automata. This timed automaton technique is applied on every node and detects the real time attacks. One node should monitor and that node must have chance to check itself. The timed automata algorithm has two parts, which is the selection phase and second one is maintain phase. In selection phase, the checking is done by competition. When a monitor is selected then maintain phase will be started. In this paper, DSR protocol is used and through timed automata that is based on IDS and this protocol can also detect attacks. When they forward the packet, they set out the timed and apply condition on specific node that if the node is maliciously modified, drop packets, impersonation and fabrication, they can detect it and adopt another suitable way. In this paper, they can detect the intrusions without any type of signature. Authors did not discuss about the delay of nodes that they create using the timed automata because manner authors have create this algorithm on every node in a detail.

Wormhole Attack

Yih-Chun Hu [28] highlights the Wormhole Attacks in Wireless Networks. This paper is focused on wormhole attack. Wormhole attack is achievable if the attacker has not cooperation with any one node, and even if all messages of transportation provides legitimacy and secrecy. This attack act as a defector node or an attacker records, check or see packets (or bits) at specific location in the network, change them to another location, and resend that packets or bits into the network. The wormhole attack can be considering a huge type of defect in networks, against many routing protocols and location-based security systems. For avoiding this type of attack, authors introduce a mechanism which is considering as packet leashes and present a protocol, called TIK stands for TESLA with instant key disclosure that implements this protocol and gave authentication for broadcasting communication to whole network. TESLA with instant key is based on efficient cryptographic primitives and requires accurate time synchronization. For detecting the wormhole attack, Hu et al represent packet leashes to restrict distance of a packet that can not be gain maximum distance. TIK is used within the conjunction of time stamps and tight clock synchronization. Within the combination of these two things, TIK can prevent wormhole attacks. Clock synchronization can be complete in wireless LAN with the use of commercial GPS receivers.

Byzantine Attack

Saju P John [19] presents Byzantine-Resilient secure Protocol mainly for Wireless Ad-hoc Networks. Authors make a framework which takes action when any authenticated nodes disrupt the service as like drop packets, change packets and misroute packets. They propose a new Byzantine-Resilient Secure Routing Protocol (BRSR) that provides flexibility for defending Byzantine attacks which provides authentication for internal, external and also with selective data forwarding attacks in MANET. For source authenticity, each working node of the network has a pair of keys (that can be private or public) and a node record that take public key or private key from its IP address. The source node uses a one-way hash function for broadcasting and use broadcasting for token authentication in the complete network. Some malicious hosts that have large distance but they had present that they are at distance of the source node (that are shortest hop). For solving this problem, they use one-way hash function. For solving modified route request, they did the sign with the use of its private key and also consist with its node id and sequence number that is requested. Data forwarding attacks were also the main problem. The source node broadcasts the information that is used for data transferring in the form of a message after signing it. Any nodes in the whole network which receive this message add their transmission rate in the message and save the copy of the last received. This whole information of message is used for helping the node to detect the forwarding attack. It also adds the information of its own id, its distance from the source and forwarding hop count verification information (that is also necessary) along with its estimated rate. Authors did not try to solve the overhead and waiting scheme of that specific protocol.

2.3 Security in wired network

Watchers

Bradely [2] presented protocol that detects and isolates malicious routers. Basically they use watchers scheme in which it is basically based on law of transmission of flow in a network. Watchers sent data (in the form of bytes) from the originator of the node and this technique does not feasible for exiting node. Watchers have many techniques that have significant advantage in which first is message authentication for prevent attackers. Watchers technique can have opportunity to detect routers that have the drawbacks of packets as like dropping or misrouting and can detect suspicious behaviour.

Watchers are designed to work in networks with following condition.

Link state condition:

This protocol is very beneficial in which each and every router have the information of every other router.

Good neighbour condition

In a network, every router related to it must have at least one good router.

Good path condition

Every router should able to broadcast message to any other router.

Majority good condition

Many routers are used and these routers in it are good. So prevent defected routers that are used for cause the new round of protocol.

Watchers protocol requires 7 counter packets that directly connected to router. Let two adjacent routers x and y. Define three things Transmission $_{X,Y}$, Source $_{X,Y}$, Destination $_{X,Y}$, Transmission $_{Y,X}$, Source $_{Y,X}$, and Destination $_{Y,X}$, that describe about the transiting, source and destination counters.

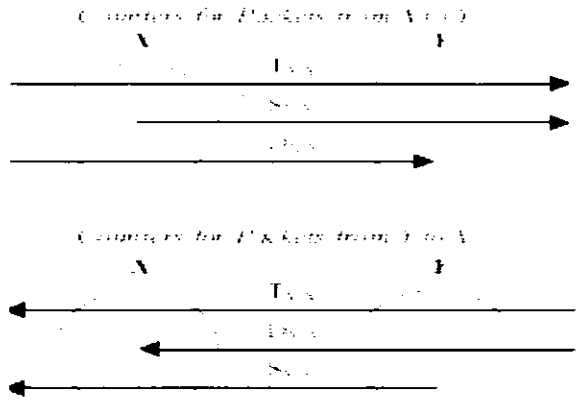


Figure 2.1: Transmit Packet byte Counter [2]

Watchers maintain two types of counters for transport traffic and misrouted traffic. After specific time, each router calculates calculation of bytes that how many of packets in it that has been received and how many bytes leave in it. Each round of transmission has two main parts. For communication, transmission of request, transmission of receives and responds protocol used. Secondly, check neighbouring router for validation and conservation of flow. In first component use digital signed for authentication.

In second component, use three parts in which preliminary checking, validation and conservation of flow is used. This part starts when router received message from routers and collected all the responses that it requires. In preliminary checking, it checks the behaviour of

packet and cross-refers the neighbours counter for validation. This neighbour's counter value matches those of the testing router. Testing router perform conservation of flow in which perform test on router. Conservation of flow is used information for determination and calculates the distinction of packets between the packets originated and consumed within the network properly: originated packets with that router and incoming packet detect packets intended for that router should match. The difference of incoming and outgoing values should be less than the fault tolerance threshold. If value exceeds from threshold value then tested router diagnosis as bad router.

During detection of bad misroute, sometimes router hides its misbehaviour. For covering this problem, router keeps two sources and two transferring counters for per destination and per neighbour. After the detection of malicious router, protocol broadcast the information within the autonomous system and discards all related links that is used in malicious route from the network.

Authors [10] show conservation of flow and see that their assumptions don't accurately model in real network. They discuss about the several attacks that defeat the protocol. Packet modification, packets substitution, ghost routers, hot potato, kamikaze routers, source routing and premature aging are the attack types. Flow doesn't speak that which number of packet forwards to the destination which can cause about the packet modification. Packet substitution can be occurring due to destination counter. Every destination counter is not feasible to detection about the whole information of routers. Conservation of flow says nothing using which flow is measured so message status of the link state network can not be broadcast through routers. Through which ghost routers can be possible. In source routing, intermediate routes only check that next hop is reachable or not. If that intermediate routes is under the attack then it will drop packets through which that type of router will be declared as faulty. In premature aging, time to live field is focused through which packets can be discarded. These weaknesses declare lacking of its formal specification.

Watchers specification is simple and thus two successive bad routers could defeat the counting. This scheme is only bounded on size of the network. In watchers, routers drop packets because it is supposed to be faulty or malicious. But node of IP may be act asdrop packets due to many reasons.

Fatih

This [8] paper is about the detection and isolation of malicious routers. The solution of this problem can be categorized into different problems i.e validation of traffic, take detection in

distributed manner and response against faulty procedure. From these sub problems, traffic validation has main part of the information of traffic through which detects the behaviour that is anomalous. Anomalous behaviour can be detected when a part of the traffic differs from the other one part what is expected. They saw about the whole working of the traffic in the network rather than individual packets. This information is predicted by TV (π, info (ri, π, τ), info (rj, π, τ)) that tells about the path segment and information about the traffic and router forward. It requires buffers to store packets information. Router r consists of two counters and each counter counting the number of packets in two directions along the path of π. Then pass these counters of packets is used for collecting information from other routers about π. In authentication of traffic, authors use set of packet (that is used as fingerprints) with other routers through which detecting packet modification. With the using of fingerprint, packet reordering can be detected.

In second sub problem synchronization that is used for taking the information of traffic and for detection purposes, distribute the results. Detector through which failure implements, has been accurate with two properties that are accuracy and completeness. A detector of failure considered to be accurate if correct router suspect (r, τ). It is mandatory for router r to check all paths segment through which r is at ending point. For solution of this protocol, present π *(K-2) protocol.* In which bad (k) holds and taking the value of K minimum then value of x that is used for satisfying constraint is k+2. k+2 path segment is not enough accurate. All path segments don't have requirement of k+2 long. This approach simple distributes the traffic and then uses this information for failure detector in each router. So detector of this router is based on evaluating the traffic more than period of time through (, *r*, τ) which means r was considered as faulty during time interval τ. Router computes hashes of packet content. They propose path level detection of algorithm that also increases the suspicious set of routers.

Once path is detected then take some countermeasures. Best way is to isolate malicious node from network and remove all the paths related to it. This protocol is very expensive for practical implementation.

Sats

Authors [1] present a mechanism through which they detect secure forwarding. Secure Split Assignment Trajectory Sampling (SATS) is the system that detects routers (that are faulty or malicious) on data plane. Assignment Trajectory Sampling can detect doubtful routers through the packets matching with the predicted paths. This is work on traffic measurement

with the use of packet sampling. They also consider that the first router on a path and also the last router on a path are correct. SATS can detect set of malicious routers between these correct routes. SATS use split range assignment function to assign hash rages to routers through which they can detect the weakness or any type of challenge. Then these router samples packets that are based on its sampling range. Next functions are not by routers: rest of packets is carried by backend engine. Hash labels and keys of that sampled packets are used for the backend engine. Backend engine used for reconstructs trajectories of packets after each interval. In aggregation of trajectories, SATS detect anomalies. In aggregation, Trajectories with the same routers of ingress and destination with routing prefix pair done. SATS focus on wrong trajectories that are different from their guess of trajectories.

In SAT, hash range change ranges of sampling from router to router. These routers are unknown to other routers and for this reason distinct sampling ranges are assigned (by the backend engine) through security channel. This assignment is not random sampling and more than one router assigned the same sampling range. In case of routing change, it is able to trace packets. Hash values are assigned to each pair of routers.

Inconsistent trajectories can be detected if packets are manipulated. They use the ending of normal trajectory for detection of packet dropping and packet modification.

Use of CoF for detecting lossy channel

Faraz et al [9] presented method a conservation of flow with in wireless Ad-hoc network. We know that router is the main focusing point of transmission. Data is transferred towards the destination with router. In context of graph theory, each edge connected to another edge for data travelling. A flow have restriction that quantity of the flow into a code equal to the quantity with flowing of data out of it, except either it has source node or destination node. There are protocols that declared about the flows of coming and outgoing for the lake of security purposes. A watcher is the one that talks about the conservation of flow. This technique is used for analyze network protocol for security purposes. In this perspective, each and every router has maintained six vectors for each neighbour host. These vectors depict that either this type of information which are being sent or data that is planned for the router or data is passing through that router. This test is performed on its neighbour that received the counter from each neighbour.

They present an end to end delivery with metrics. Compare the number of coming packets intended for router with the number of outgoing packets minus packets creating with that router and check it from threshold value. If value exceed then router is diagnosed as

malicious. Total packets were delivered to the destination or dropped but conserved with the network resulting in conservation of flow. There are number of reasons through which packet drop cannot be successful. May be any environmental factor can be included. Lossy channel or malicious node can be the reason of packet drop. Through which QOS and network performance also decrease.

2.4. Security in Wireless Network

Pathrater

Nasser et all present Intrusion Detection System for Discovering Malicious Nodes in MANET with in maximum detection. In this paper [5], author describe about the detection of intrusion system in which they overcome the weaknesses of Watchdog. The role of Watchdog is to watch that the next hop that is used for forwarding the data path or not. If not forward then it will take as a malicious. The role of Pathrater is to find the reliable path from the result generated by Watchdog. Mainly in this paper, they discover the faulty nodes which can cause to separation the network. Every host arrange a table that records the about quantity of packets of sending node forwards or receives. Author extends the watchdog system by arranging table that records about the entry of source node, destination node, and also about the path specification. In which sum is the number of packets that the current node send data, forward data, or receive data using the path of the route as source node, intermediate node or destination node correspondingly. And path is route that is used for the transferring data between source node and destination node. Whenever node detect that next node is faulty, then originator node will not act rapidly. It will send data from source node to destination node with the use of an alternate path in the routing table. After receiving the data from source node to destination node, destination node will search its table to see if there is any match. If there is, then evaluates it with the sum field of message. If these sums are equal, means that the defected node transferred packets that the source node sends. If there is not a matching, then it is considering that node is defected or selfish.

Watchdog and pathrater [31] presents a mechanism used for noticing faulty nodes and increasing their efficiency that impact in wireless Ad-hoc networks. Watchdog that discovering defected nodes and the scheme of pathrater that is used for routing protocols mainly for the purpose of avoiding these type of defected nodes. Watchdog technique listen with passive acknowledgment and also maintains a buffer that have receive the information

malicious. Total packets were delivered to the destination or dropped but conserved with the network resulting in conservation of flow. There are number of reasons through which packet drop cannot be successful. May be any environmental factor can be included. Lossy channel or malicious node can be the reason of packet drop. Through which QOS and network performance also decrease.

2.4. Security in Wireless Network

Pathrater

Nasser et all present Intrusion Detection System for Discovering Malicious Nodes in MANET with in maximum detection. In this paper [5], author describe about the detection of intrusion system in which they overcome the weaknesses of Watchdog. The role of Watchdog is to watch that the next hop that is used for forwarding the data path or not. If not forward then it will take as a malicious. The role of Pathrater is to find the reliable path from the result generated by Watchdog. Mainly in this paper, they discover the faulty nodes which can cause to separation the network. Every host arrange a table that records the about quantity of packets of sending node forwards or receives. Author extends the watchdog system by arranging table that records about the entry of source node, destination node, and also about the path specification. In which sum is the number of packets that the current node send data, forward data, or receive data using the path of the route as source node, intermediate node or destination node correspondingly. And path is route that is used for the transferring data between source node and destination node. Whenever node detect that next node is faulty, then originator node will not act rapidly. It will send data from source node to destination node with the use of an alternate path in the routing table. After receiving the data from source node to destination node, destination node will search its table to see if there is any match. If there is, then evaluates it with the sum field of message. If these sums are equal, means that the defected node transferred packets that the source node sends. If there is not a matching, then it is considering that node is defected or selfish.

Watchdog and pathrater [31] presents a mechanism used for noticing faulty nodes and increasing their efficiency that impact in wireless Ad-hoc networks. Watchdog that discovering defected nodes and the scheme of pathrater that is used for routing protocols mainly for the purpose of avoiding these type of defected nodes. Watchdog technique listen with passive acknowledgment and also maintains a buffer that have receive the information

of recently sent packets and comparing each coming packet with the packet in the buffer for securing the duplicacy. If packets match with store packets then packet is removed from the buffer entry. If packets stay in buffer for long time then watchdog increments a failure. Watchdog technique detects misbehaviour at the level of forwarding; it is not only handled at the link level. This technique might be not perform good detection or have disadvantage in the presence of ambiguous, receiver collisions, false misbehaviour and collusion etc. watchdog have the information of hop by hop routing protocol and it doesn't work properly if it doesn't have this information.

In pathrater mechanism, which run by nodes and each node arrange rating mechanism for every node that is in the network. It is calculated the average ratings of the node through path metrics. This type of metric gives the similarity of whole feasibility of different paths and permits the following shortest path algorithm and uses highest metric with the selection of choosing the path. This mechanism mainly focuses on knowing the path (that is accurate) of packet that has been traversed. During calculation of pathrater metrics, a negative path value indicates the defected behaviour of nodes in the path. A node that has negative ratings should have compulsory point that increased their ratings with slowly. In metrics, they use throughput and also the effects of false positives watchdog. In this scheme they gain with the maximum number of routing nodes and also gain with the minimizing effects of defected nodes.

MobIDS

This [29] paper is focused on sensors that are used to detect defected nodes in MANET. Different types of sensors are used for finding the selfish hosts. Here author used the scheme that is Mob IDS. This scheme enhanced the overhearing and develops sensors, that type of sensors can be used in parallel for achieving with the higher rate of detection that is also accurate. Sensors generate two types of value: positive value or negative value. Positive value is used for positive behaviour and negative value is used for non- cooperative behaviour. Sensor rating is calculated by ki and kj. These sensor ratings are calculated into local ratings. Then these ratings are distributed to neighbouring nodes and take node averages by all local ratings that are the result of global rating. After global rating, nodes isolate that node from the network. For improving MobIDS sensors, authors use activity based overhearing, binary probing and iterative probing that tries to overcome the problems of MobIDS sensors.

In this paper, an author use different aspect that is activity based overhearing, binary probing and iterative probing is used in Mob IDS. In activity based overhearing, authors have improved the detection accuracy and introduce detection threshold. When it senses certain number of packets being dropped then monitoring node will generate an alarm. Through this activity based overhearing positive value will be generated. In MobIDS, probing is used to detect defected nodes in a route of MANET. When any type of acknowledge is missing between source S and destination D then S simply probes to selected nodes. This type of binary searching is called binary probing. But this type of probing has some drawbacks: that is encryption and decryption and this method is no reliable method of detection for dropping packets. For covering these problems, authors use iterative probing. In iterative robbing, different probe packets are sent but after the receiving reply from node.

Author's use sensors are different that exist in similar location and malicious node is used for detection of these multiple sensors, which are the good indication of the network. They use threshold value and set it manually that is used for good detection results.

Confidant

This [30] paper present a protocol that is used for detecting and isolating misbehaving nodes in wireless Ad-hoc networks. The main purpose of CONFIDANT protocol is making misbehaviour unattractive. Approach of this protocol is to detect faulty behaviour. For checking the behaviour, this protocol takes neighbourhood watch through observed behaviour. Neighbourhood watches either listen the passive acknowledgement or observing the protocol behaviour. And also learn from reported behaviour through which share information of malicious behaviour with other nodes.

CONFIDANT protocol has different components that describe with details. The trust manager is also used in it. Trust manager is used for incoming or outgoing ALARM messages and can warn the node an alarm message. This message that is sent contain the information of number of occurrences observed, addresses of reporting nodes, address of node and also about the destination node. When anomalous behaviour is identified, then this data is given to system of reputation. Reputation system arrange table that is used for saving entries of nodes and also save their ratings. Threshold value is used in it. When threshold value exceeds, the reputation system updates the nodes rating. When this rating level becomes high then this data is passed to the path manager. Path manager discard the entire

relevant path that containing the malicious nodes and all information according to receiving request for a route from defected node. When reputation system change its rating then alarm is received by monitor component, then pass it to trust manager. If the node is suspected to be malicious then this information is forwarded to the system of reputation where it is used for implication. CONFIDANT scheme is used for detection, alerting and reaction for malicious node.

Security Solutions for Gray Hole and Black Hole attack in MANET

Gray hole attack is a distinction of black hole attack, in which each node act as an accurate node during discovery process and then silently drop data packets. Identification of gray whole attack is harder due to its selfish nature. In this paper [33] author propose an algorithm in which total data traffic divide into small size blocks. Before starting the communication of data packets, source nodes send a message to the destination. Destination receiving message will be the announce for incoming data packets. Node of Destination sets a timer of incoming communication (about the end of transmission) and also starts quantity of the no. of packets received. After finishing the transmission source node, destination message send to source. then source node check the no. of packets from that message. If no. of packets is unequal then it detects about the starting point and deletes the defected nodes in the route. This methodology takes threshold value for data loss rate μ and uses this threshold value at each node. Firstly source node check that it is the neighbour of the next hop node in route or not. If it is consider as the next hop node in the route then start action of that specific host. During action, firstly initialize quantity of the number of data packets that is transmitted by the node. Through this copy of neighbours routing table can also maintain and also establish the next hop node for forwarding the packet. If any source appends that node in its find malicious table, then check it for predefined threshold value and broadcast it.

Sun et al [11] work on detection of black hole attack in MANT. After the completion of discovery procedure of path in routing protocol, originator node send control packet that is request neighbour set (RQNS). RQNS is used for send request to destination that is current neighbour set. With the reception of every RREP, originator node sends this packet to it. Each node replies this special packet with reply neighbour set (RPNS). It starts comparing neighbour set when a node receives more then one RPNS in certain period of time. But if the difference is greater than the threshold vale then it is presented as black hole attack. After detection of black hole attack, cryptography based authentication method is used for true

destination. Through this technique, the number of encrypted and decrypted operation for authentication is much reduced.

Dokurer et al [3] see the performance affected by the black hole attack on the network. Nodes which will adopt this protocol will be marked as black hole nodes and behave like black hole. Authors see the total packets by the originating node and received by destination and check that how many packets could not reach the destination due to black hole attack. Check a RREP message from black hole and the about the destination node. In IDSAODV protocol used the mechanism in which first message of route reply used to originate the transferring of data but new route adopted when second RREP message arrived. Through this technique, does not require any extra overhead.

Authors [4] see about the identification of black hole attack through sequence number. In this scheme, they try to remove black hole attack. When originator broadcast the route request message for destination node, black hole node rapidly respond with that reply message containing sequential number. Dokurer show that black hole node use greatest sequence number for achieving information from neighbour node. Then a black hole node takes all information for dump and dumps it. In black hole node, node that sends data understand that there is error in medium because did not receive ACK packet. Source node discards all other RREP messages. If TCP data packets send and discover fresh route for forwarded data to destination, that node again send message to sending node.

2.5 Limitations

In Hughes, watchers protocol detecting misbehaving routers. It uses COPF as a test and it is not suitable for security mechanism in network protocols. In this scheme, conservation of flow mechanism is not proofed, so they can be defeated. Authors try to improve many attacks on routers as like packet modification, substitution, ghost routers and source routing. But memory requirements and performance costs of watchers are still to be calculated and broadcast packets are not calculated in watchers protocol.

Black hole problem in [40] MANET is major problem that is used for solving in research area. In black hole, a defected node uses the shortest distance of the node whose packets malicious node wants to disturb. In [30, 29] have also some limitation. In Confidant protocol, extension of its implementation of other protocols is stated as future work. In MobIDS, authors try to evaluate threshold values that adjust automatically during operation and use to develop an additional sensor that will use to detect selfish nodes. Payal et al describe about the prevention scheme and authors did not discuss how to avoid theses type of malicious

nodes. Very few researchers have analyzed that how to avoid from the malicious nodes and how to avoid different type of attacks. Junahi et al did not discuss about the mobility of nodes and can not handle the unlimited message authentication with the switching of one-way-hash chains.

Khalid et al present the model that can be extended through RTS or CTS mechanisms and can be use through back off based on the traffic load and dynamic back off window size. Do sun did not perform about the non cryptography based method to true destination and there is much more need to improve the response and detection mechanism within the packet throughput. Through this technique, false misbehaviour can be detected. But it is difficult to detect the defected node on paths with specific source node and destination node. So this will be the outlook. In lossy channel, there does not include a cutting edge. Authors can extend metrics and can use load balancing and traffic analysis type algorithms.

Dokurere don't perform about the TCP ACK packet. They only discuss about the UDP packets. Black Hole attack is detected through IDSAODV. Many more techniques of AODV are existing but they discuss only one technique. Marti technique can be increased by explicitly trusted nodes and also with the increment of throughput values. Confidant approach is the detection, alerting and reaction scheme and also learns through neighbourhood and with the experience of friends. Authors didn't check about the behaviour with over time. TCP few simply limiting the heavy traffic through which overall performance can be improved.

2.6 Summary

In this whole description, I discuss about the congestion and malicious and also discuss that how it can be cover up in different paper. Malicious routing behaviour is a serious problem in wireless network. So in this chapter, I mainly focus on the security solutions of wired and wireless network in MANET. In the end we take limitations of these papers.

CHAPTER 3

REQUIREMENT ANALYSIS

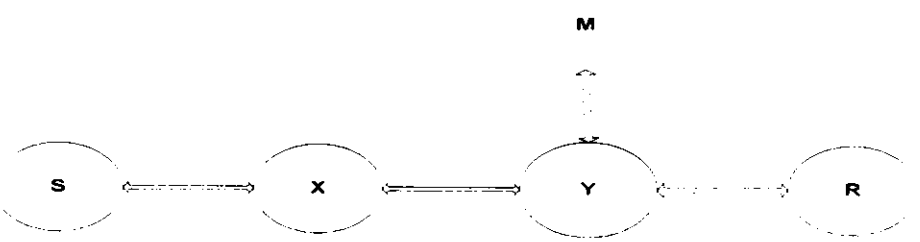
Ad-hoc networks are developed in sensitive environment in which security is a main point to focus. With the popularity of Wireless Ad-hoc networks security deficiencies has been detected. For save the system from these types of deficiencies and selfish activities, different types of security techniques have been proposed from previous work. However, these authentication techniques don't incorporate real time scenario or are limited to single problem only.

3.1 Introduction

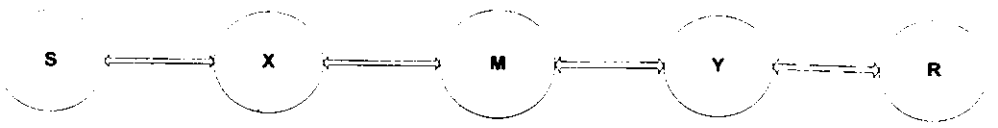
In this chapter I will mainly focusing on the necessities of my research work. Before that, section 3.2 will contain about the network layer attacks in detail. I will focus about problem domain in section 3.3. The problem statement will be described in part of 3.4. The section 3.5 will describe about the proposed solution in detail. Our main contribution of thesis will be declared in section 3.6. The section 3.7 will include the concluding remarks in the form of summary.

3.2 Network Layer Attacks

Number of attacks has been identified on network layer and mainly focusing in research papers. By misbehaving the routing protocols, attackers can disturb the whole network through insert them into the path connecting between the source nodes, destination node and arranging the whole network traffic. As in figure 3.1.In this figure a malicious node can introduce itself in the routing path between sender S and receiver R.



(a)



(b)

Fig 3.1: Attacks injection

In AODV, the attacker introduce itself a route with smaller distance or longer distance or change the route and discards all routing updates from other nodes. Some attacks on network layer are wormhole, black hole and Byzantine attacks. Their brief descriptions are given below:

Gray Hole Attack

Gray hole [33] attacks is a type of network layer attack in which attacking node try to send data from own side. Primarily, this attacking node behaves as like the normal node and replies correct RREP messages to nodes that originate RREQ message. If neighbouring node break out the connection to destination then it may try to find it again through broadcasting RREQ message. Always an attacking node performs as like establishes a route and sending RREP messages from its own and continue this process until it success. This type of attack is known as routing misbehaviour. Dropping packets or changing packets are also one of the behaviours of failed nodes.

Wormhole Attack

In wormhole attack [28], a malicious node receives packets at one side of the network and changes that transmission to another location in the network. This path that existing between two attackers is depicted to as a wormhole. These attacks have serious threats to MANET routing protocols. For example, when this attack is used against on demand protocol as like AODV, then at that time attacks could save the discovery of any routes other than through the wormhole.

Black hole Attack

In this attack [33], an attacker mention its routing protocol as shortest path for the purpose of saving whole packets of the network and then for dumping these packets. In black hole attack, when the attacker receives a request from destination node, it always creates a reply on its own and mention own routing protocol with the declaration of short route. If that

selfish or faulty reply reaches at the originating node before the reply from the actual accurate node, from this faulty route reply a fake route gets created. Malicious route can do message passing when the malicious route has been able to insert itself between the sending and receiving nodes. In black hole attack it may be possible that a node creates different unrelated packets within the network. An attacker changes the packets from some nodes, while lefting before the data from the other hosts unaltered which limit the doubt of its wrong doing.

Byzantine Attack

In this attack [19], an intermediate node involve in it and this node works in collusion and this attacks are grow up such as the generation of routing loops, forwarding packets on non-optimal paths and dropping packets which results in disruption routing services and degradation of the whole performance of the network. The detection of Byzantine failures is too much hard and complex.

3.3 Problem Domain

Mobile Ad-hoc network (MANET) is a hot research area since the last decade. Different aspects such as security, routing protocols development, safety related applications development, etc have been targeted by researchers. MANET has different challenging characteristics that differentiate it from other type of networks. One of the challenging characteristics of MANET is security. Security is challenging because it has great impacts on the performance of network. Security in the MANET is very hard to achieve because of its fundamental characteristics such as topology that is dynamic, open medium, power that is limited and also bandwidth that is limited. The prevention method like authentication and cryptography techniques are not able to provide complete security to these types of networks. Identification and isolation of attacks are efficient intrusion detection.

This mechanism is used to decrease the amount of routing delay, but takes the system as a target of malicious node. The defected nodes easily disrupt functioning of the routing protocol. Malicious node doesn't need to check its routing table when sending false message and the response is more likely to reach the source node first. Through this way, source node thinks that source discovery process is complete and send packet to that specific node. Consequently, all the packets through the selfish node are simply inspired. We call this type of problem as black hole problem. Through this way, lots of packets are consumed or

dropped and this thing affects the whole network. Remember that. Packets are dropped due to malicious activity or sometimes due to congestion

3.4 Problem Statement

Congestion and flooding attacks are the causes to hamper the QOS of network layer; so network layer performance is also decreased. Here, need for such a technique that enables the main focusing point of a flooding attack to choose traffic that it wants to stop these flows before they stuck the whole network and decrease the whole efficiency and even to gave efficiency to remaining flows. There is no mechanism to differentiate the reliable and unreliable node and to identify the loss of reliable and unreliable packets during congestion. Due to loss of reliable packets, QOS is also decreased. Black hole attack adversely affects the performance of whole network working under AODV protocol. I have focused to implement black hole attack in AODV protocol as AODV routing protocol is vulnerable to this type of attack. Need was to come up with an approach to identify black hole attack and differentiate it with congestion in AODV protocol.

3.5 Proposed Solution

My proposed solution consists upon two parts.

Phase 1: To analyze all those nodes that degrade the performance during congestion.

Phase 2: To identify the nodes that is having under the black hole attacks.

Phase 1

In phase 1, I first identified the node is congested. In this phase we analyzed the nodes which are affected by congestion. For checking congestion, we put the analyzer in receiving buffer through which we check the level of threshold (T.H) value. If Queue limit is increased from T.H then it generates a trigger and waits for a while and again sends packets. After some time, if same situation is occurs repeatedly then node can adopt to choose another path.

Phase 2

If the dropping packets are greater than double value of threshold then that node is detected to be malicious and make it as Gray mark and if this value is greater than double then Gray

mark value, then node is identified as black hole. It is just the identification of malicious behaviour of the node. If the node is detected as a black hole then we apply check on that node. We declare that node in B/W (Black and White) system which provides the mechanism to stop sending packets when the node is detected as black hole.

3.6 Contribution

Contribution of this research can be categorized as follows.

- It is a mechanism to develop an extended routing protocol that can cover the reasons for the loss of packets. The loss of such packets is thought to be mainly from attacks. but these losses are also caused by congestion. Reasons of packet losing are detected.
- A malicious node is criticized when all nodes are congested, then that particular node is underprivileged from the network membership and isolated in the network.
- This technique permits the victim of a flooding attack through which stop flows with that particular node before they stuck the whole network. And even to provide efficiency to the remaining flows.
- In order to cover up the loss of reliable packets, QOS is also increased.

3.7 Summary

A detailed description of the problem domain, my problem statement and solution that is proposed for problem statement is described in this chapter. Isolation of malicious attacks like black hole attack is very important for MANET because packet loosing is reduced and QOS is also increased through this. Our proposed solution will be used identify the defected node and separate it from the whole network and also detect the packet loosing due to congestion.

CHAPTER 4

SYSTEM DESIGN

Designing phase of the system creates structure of that system. In system design phase, I present a system, which is used as that how to construct the system and what is the main point through which architecture will be complete. This design phase is helpful for implementation of the software.

The focusing point of my research project is, to provide different and useful mechanism for the purpose of security in Wireless Ad-hoc networks. Any type of security in Wireless Ad-hoc networks needs to perform special consideration as like barriers or limitations because it has great impact on network performances.

4.1 Introduction

Fundamental needs of the proposed solution will be identified in this phase and that scheme will be beneficial in the system building. The design requirement of my proposed scheme is highlighted in section 4.2 and proposed architecture will be discussed in section 4.3. I will discuss about the algorithm in section 4.4. Section 4.5 concludes the remarks of this chapter in the form of summary.

4.2 Design Requirements

This system is designed for covering defected or selfish node, congestion and destructive activities in Ad-hoc networks. In this section, I will describe about the log files, threshold and Routing table which are the basic requirements of my architecture.

a. Log files

Special type of tasks and responsibilities are assigned to every node of the network. The information that is received or arranged from these nodes is used for detection about the attacks and trigger is generated if node is malicious. Nodes that are affected from the attacker then isolated it from entire network. The dropping of such packets is thought to be mainly from attacks, but these losses are also caused by congestion. The objective of nodes is to detect the reason of packet loosing which is either the node is malicious or congested. Each node arranges or organizes a log files for the reason to secure its normal activity. In log files, keep the record of incoming, out going and about the number of packets.

b. Threshold

This value is basically used to show the flows of network traffic and also tells about the variation of network traffic following inside the host and the whole network. The variation or ups and downs in the network traffic assume to be a malicious activity or due to congestion occur. In our proposed architecture we used a threshold value that is depicted according the overall percentage. If the queue limit is greater than the threshold value then it means node is congested.

c. Routing Table

The routing table also shows the network traffic flow as depicted in threshold and also about the packet loosing. The variation of the network traffic assumes to be faulty or selfish activity or due to congestion occur. In routing table keeps record about the packets and put check on the B/W box.

4.3 Proposed Architecture

In this architecture, we put the analyzer in receiving buffer through which we check the level of threshold (T.H) value. If Queue limit is increased from T.H than it generates a trigger and if not increased then packets move to routing table. In buffer routing table, receiving packets matches with sending packets, if receiving packet is less than sending packet then system will put B/W check on that node and declare it to malicious. I will try to develop the protocol which identifies the cause to hamper the QOS network layer and to mitigate or filter out the packet loss ratio at network layer and enhance the performance as well. In our proposed system, extended AODV protocol will be proposed for crystal identification of malicious behaviour of the node. In our design, packet will pass form the B/W (Black and White) system, which provide the mechanism to stop packets when the node is malicious. This system can prevent legitimate transmission (among the source and destination) from being disrupted the network layer attacks. And also save the legitimate transmissions that is disrupted by congestion. In this architecture, congestion is detected through the level of threshold value. We will fix the threshold value in receiving buffer and if the queue limit is increased from that threshold value then it means congestion is occurring. When a node is detected that congestion is occurring then the node will stop packet sending for a while and send packets again after passing sometime. After trying 1 or 2 times, if same situation is

occur means still congestion problem is existed then sending node wants to send packets from another route that is appropriate. That route may be long but it will be efficient if packets are saved. Through this network traffic will be save and enhance the performance as well. The following figure 4.2 declares the present architecture.

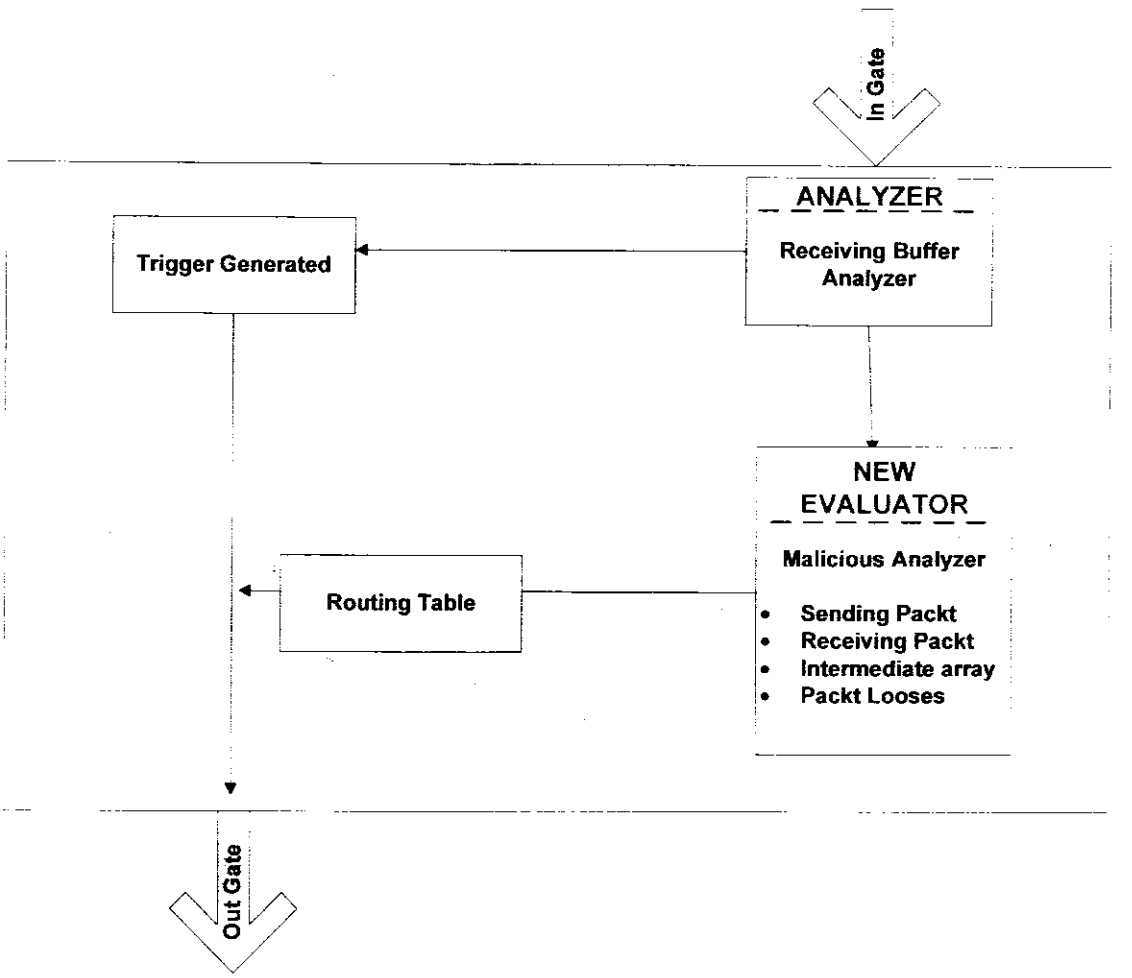


Fig 4.1: proposed architecture

4.4 Design Methodology / Algorithm

This technique helps in constructing the architecture of a proposed scheme. My algorithm builds with two distinct phases. They are named as initial phase and detection phase also. The description of congestion and malicious phase are given in part of (a) and (b) respectively.

occur means still congestion problem is existed then sending node wants to send packets from another route that is appropriate. That route may be long but it will be efficient if packets are saved. Through this network traffic will be save and enhance the performance as well. The following figure 4.2 declares the present architecture.

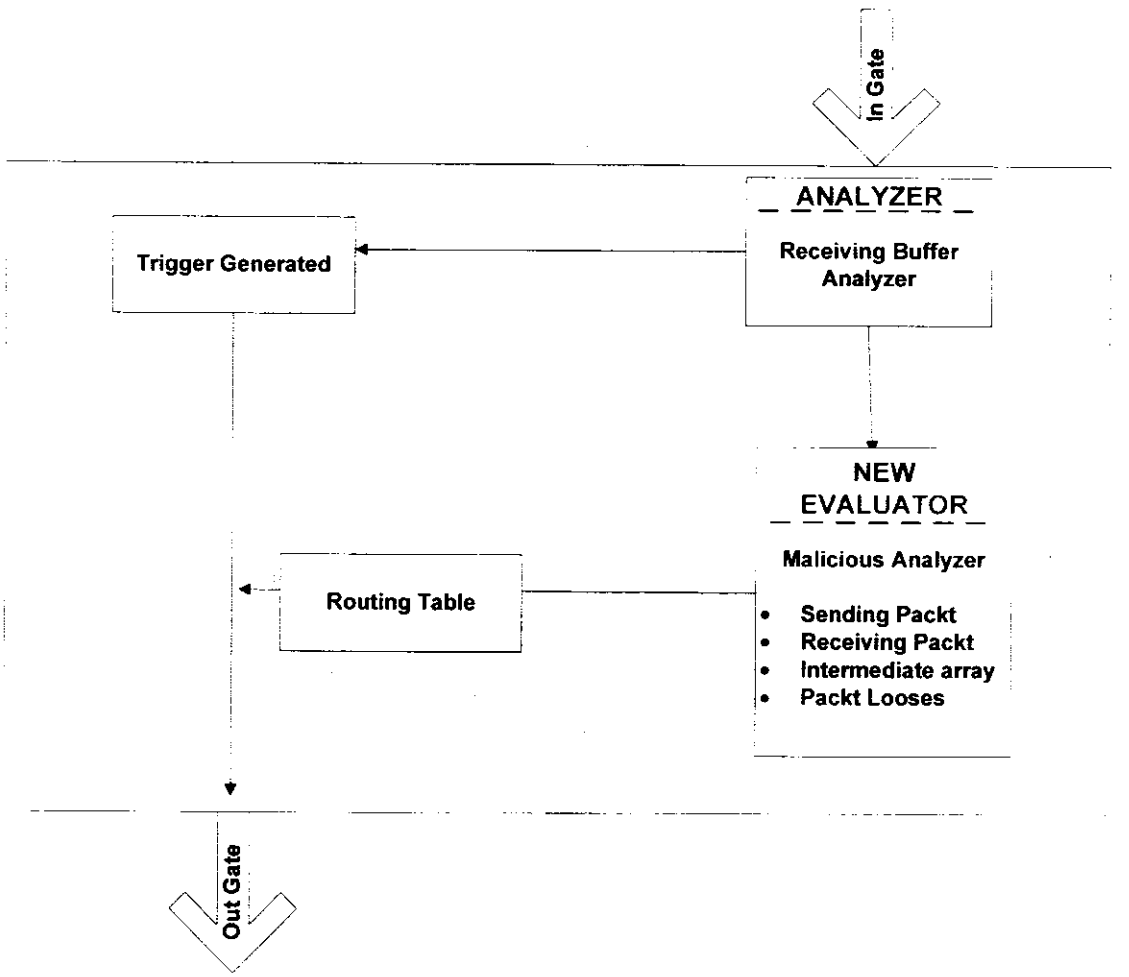


Fig 4.1: proposed architecture

4.4 Design Methodology / Algorithm

This technique helps in constructing the architecture of a proposed scheme. My algorithm builds with two distinct phases. They are named as initial phase and detection phase also. The description of congestion and malicious phase are given in part of (a) and (b) respectively.

a. Congestion Phase

The rules are fixed into the database with in this initial phase. During this phase of the system is considered the queue limit value means the packets that can be embedded in a node. Threshold values are also consider in this phase. For checking the node that either the nodes have ability to receive packets or nodes queue limit have full. For this phase we apply a check that that queue limit is greater then or equal to threshold value, if yes then it means node is congested. The job of node is to feel the packets of data about flow of data traffic, number of coming and outgoing messages.

b. Malicious Phase

In this phase system is tried check about detection of system and also about the handling of selfish and harmful activity or not. Continuously, node checks the whole network traffic. The intrusion activity is detected when routing table is received. In routing table we have sending array, receiving array, intermediate array and number of packets that will be dropped. After receiving that table, we can check that our receiving packets are greater than sending packets. If yes then it means those nodes is malicious and check on that node in black and white system. And broadcast this message to all other nodes. After it sending node will adopt another route which is appropriate, that route can also be long but this thing can be acceptable.

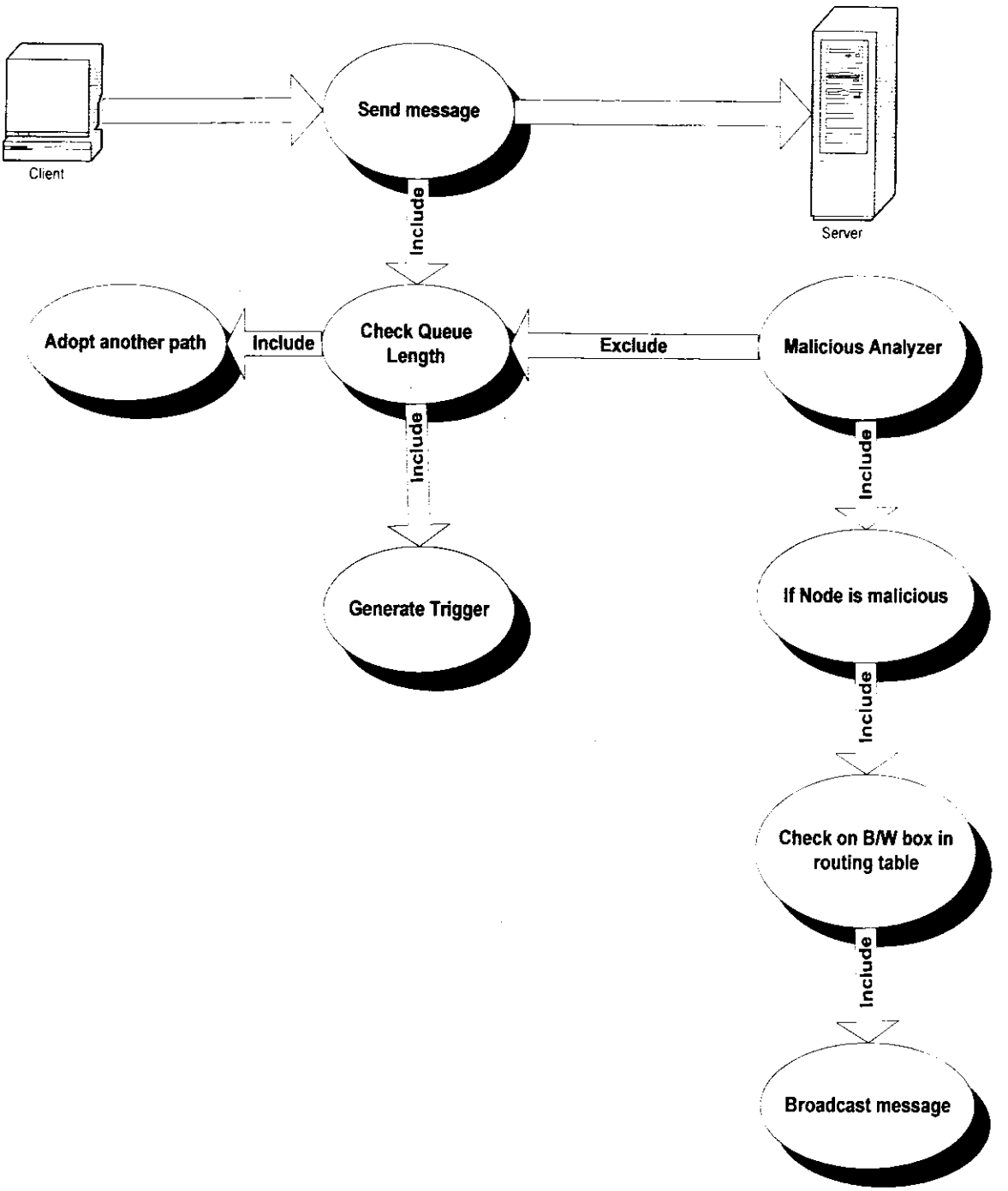


Figure 4.2: Use case Diagram

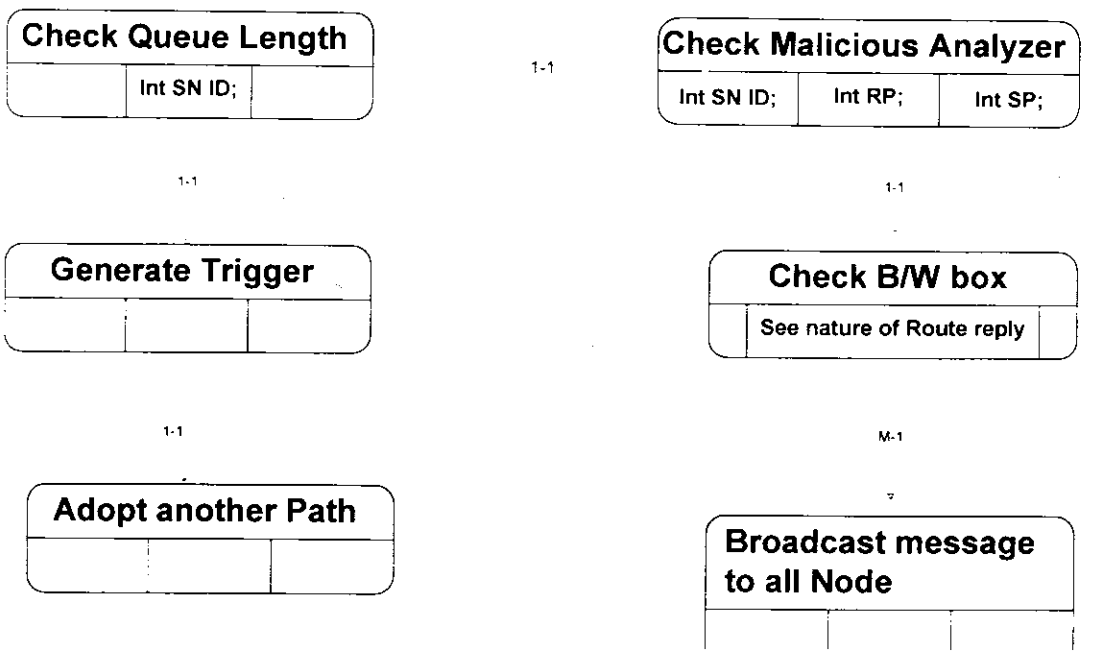


Figure 4.3: Class Diagram

4.5 Summary

In system design section, I have proposed Detection and Identification of Unreliable Traffic in Wireless Ad-hoc Network during Congestion and during identification of malicious node. This proposed scheme provides strong security mechanism with the purpose of minimum network resources and also tries to cover up the security of the control messages in the network. The proposed solution is based on isolation technique which is apply after detection of malicious node or can be apply after detected the congested node.

CHAPTER 5

IMPLEMENTATION

The main objective of the section of implementation is to clearly describe about the proposed system which reflects the working of whole system. Many dimensions are considered that help to determine how much the objective is being met. I have not required maximizing every measure to obtain the desired goals and objectives. My objective is to create a balanced relationship among such measurement attributes.

5.1 OMNET++

OMNET++ [39] is an object-oriented simulator. This simulator may be used for:

- Protocol modelling.
- Modelling queue networks.
- Traffic modelling for telecommunication.
- Authentication of hardware architecture.
- Modelling for any system where the discrete event approach is appropriate.
- Modelling multiprocessors and other distributed systems of hardware.

OMNET++ is portable, and they allow a network model to be built with ease. OMNET++ also works successfully on several UNIX types. It can also be used in Windows with the using of different C++ compilers. OMNET++ helps distribution with parallel simulations and provides transmission between parallel distribution simulations. OMNET++ is free to use for research purposes.

The OMNET++ model has collected a multiplicity of hierarchically nested modules. The module nesting depth is not restricted and allows realizing the logical format of system easily.

Modules can communicate message parameter to each other. Complex architecture may be contained within these messages. These parameters allow the modification of the behaviour, as well as the topology of a module. Each and every module in the model has its parameters for communication, and may send message parameters through gates, by forming a connection directly to the destination or along a predetermine route. The module copes up the behaviour and lowest level of module hierarchy.

OMNET++ simulations have feature that is used for varying user interfaces for purposes such as debugging, expression and batch execution. This can be handy in the expansion of projects that are simulated. User interfaces also make possible the display of models working.

The simulators are portable because they can operate on both windows and multiple UNIX with the use of different C++ compilers. OMNET++ also supports simulation that is parallel distributed, and it can use numerous mechanisms for transmission between separations of parallel simulation that is distributed. Some examples include MPI and named pipes. This parallel simulator can be complete easily. Models don't need any instruments that are used for running in parallel. Simulations can be run in parallel under the investigation of GUI which provides feedback about what is going on in detailed manner.

Modelling of Packet Transmission

While modelling communication networks, a connection can be assigned three parameters and all of these are optional. The parameters include delay of propagation, bit error and data rate. Delay of Propagation is the time of arrival that is delayed during message through which it travels through the channel. Bit error rates clarify probabilities for a bit being transmitted incorrectly, and for noisy channel modelling. At the end, rate of data is particular in bits per second and calculating the transmission time of packets. In data rate, sending of the message related to the communication of the first bit and the arrival of the last bit that is related to message transmission. This method is applicable at some time, not always feasible.

5.2 AODV Implementation

In MANET, there are several routing protocols, such as DSR, AODV or DSDV. The AODV implementation is the basis of the presented network. AODV implementation mainly consists of two functional channels. These

- Detect the route through a network, and
- Forward packets within the route.

Figure 4.3 is a simple packet flow within a single node. An agent allocates the data information and initializes the contents of that packet. After this, packet is handled by AODV routing mechanism. Initially, handler receives this packet and processes it locally.

OMNET++ simulations have feature that is used for varying user interfaces for purposes such as debugging, expression and batch execution. This can be handy in the expansion of projects that are simulated. User interfaces also make possible the display of models working.

The simulators are portable because they can operate on both windows and multiple UNIX with the use of different C++ compilers. OMNET++ also supports simulation that is parallel distributed, and it can use numerous mechanisms for transmission between separations of parallel simulation that is distributed. Some examples include MPI and named pipes. This parallel simulator can be complete easily. Models don't need any instruments that are used for running in parallel. Simulations can be run in parallel under the investigation of GUI which provides feedback about what is going on in detailed manner.

Modelling of Packet Transmission

While modelling communication networks, a connection can be assigned three parameters and all of these are optional. The parameters include delay of propagation, bit error and data rate. Delay of Propagation is the time of arrival that is delayed during message through which it travels through the channel. Bit error rates clarify probabilities for a bit being transmitted incorrectly, and for noisy channel modelling. At the end, rate of data is particular in bits per second and calculating the transmission time of packets. In data rate, sending of the message related to the communication of the first bit and the arrival of the last bit that is related to message transmission. This method is applicable at some time, not always feasible.

5.2 AODV Implementation

In MANET, there are several routing protocols, such as DSR, AODV or DSDV. The AODV implementation is the basis of the presented network. AODV implementation mainly consists of two functional channels. These

- Detect the route through a network, and
- Forward packets within the route.

Figure 4.3 is a simple packet flow within a single node. An agent allocates the data information and initializes the contents of that packet. After this, packet is handled by AODV routing mechanism. Initially, handler receives this packet and processes it locally.

Afterwards the route for the packet is detected. The packet is transfered to the next hop when suitable route is found.

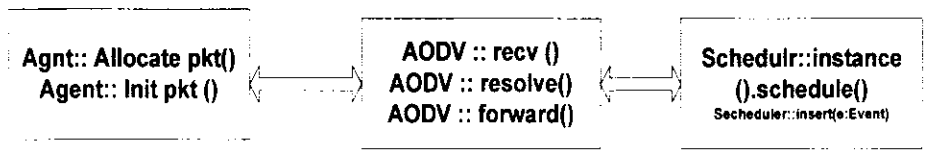


Fig 5.1: Packet Flow

- Recv () method is used for being called.
- After it, calls the resolve () and then forward () method.
- Forward () method used for calls the scheduler () method that is used for schedules and queues all the packets.

Fig 5.1 shows the process of transmission of packet flow. The packet is forwarded by each node on the route. In this process, scheduler method is used for forwarding. The resolve () method returns immediately, due to a cached response for the request.

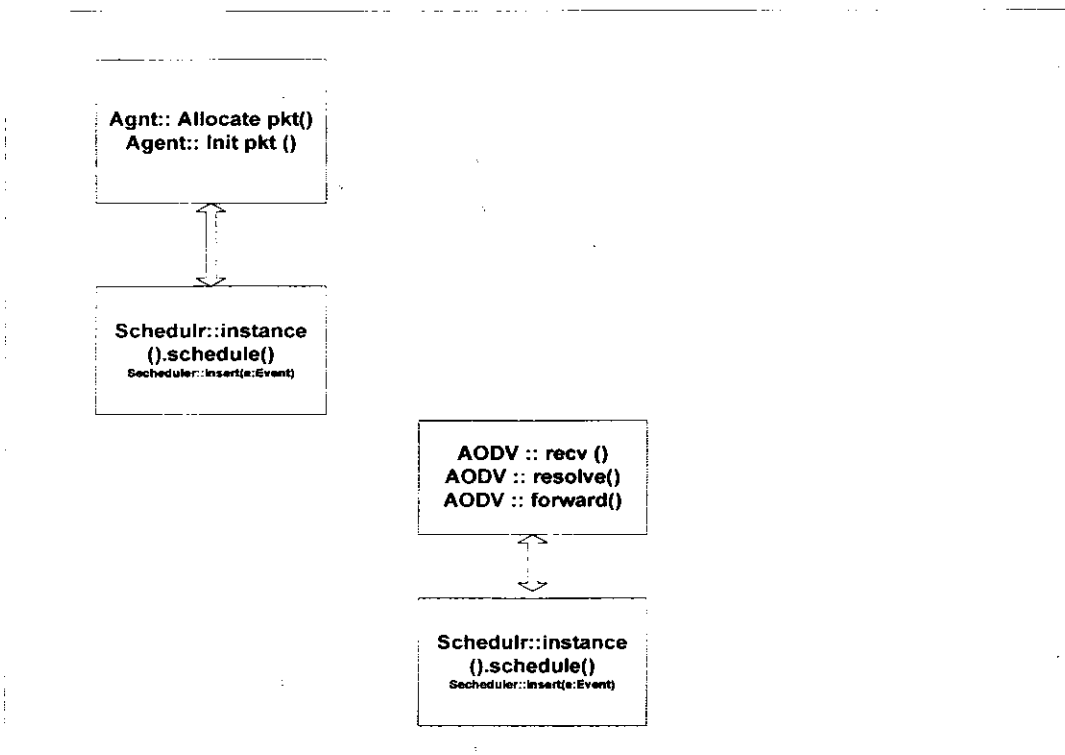


Fig 5.2 Transmission of packet flow

5.3 Flow Charts

In this architecture, we put the analyzer in receiving buffer through which we check the level of threshold (T.H) value. If Queue limit is increased from T.H than it generates a trigger and wait for some time and again send it to intermediate node. If again queue limit is increase then send it to another path. But if queue limit is not increased, then packets move towards the routing table. In buffer routing table, receiving packets matches with sending packets, if the packet that is received is less than the packets that are send then originating node does not receive route reply system and put B/W check on that node and declare it to malicious. I am trying to develop the protocol which identifies the cause to hamper the QOS network layer and to mitigate or filter out the packet loss ratio at network layer and enhance the performance as well. In our proposed system, extended AODV protocol will be proposed for crystal identification of malicious behaviour of the node. In our design, packet will pass form the B/W (Black and White) system, which provide the mechanism to stop packets when the node is malicious. This system can prevent legitimate communications from being disrupted network layer attacks. When the node is malicious detected then it will isolate from the network and declare or announce to other nodes that this node is detected as a faulty node and do not take transformation from this.

(a) Active Black holes Attack

In this mechanism when source node wants to start communication, it use fresh from source route to the destination route and it can be seen from the routing table. On other hand source node will broadcasts RREQ message. A black hole node uses highest possible sequence number in RREP message. Because of its highest possible sequence number source node starts sending data to that node thinking it as a destination node or intermediate node towards the destination node. Balck hole node receives all the data packets and start dropping the packet.

- SN: Source Node
- DN: Destination Node
- IN: Intermediate Node
- NH: Next Hop
- RREQ: Route Request

- RREP: Route Reply

Pseudo Code of packet receiving in Active Black hole Attack:

```
1) SN broadcast RREQ msg
2) {SN receives RREP msg
3) IF (RREP is from DN){
4) Route Data Packets
5) }
6) ELSE{
7) SN waits for RREP from IN
8) {Receive RREP from IN
9) RREP contains highest sequence number
10) SN starts forwarding packet to IN
11) }
12) }
```

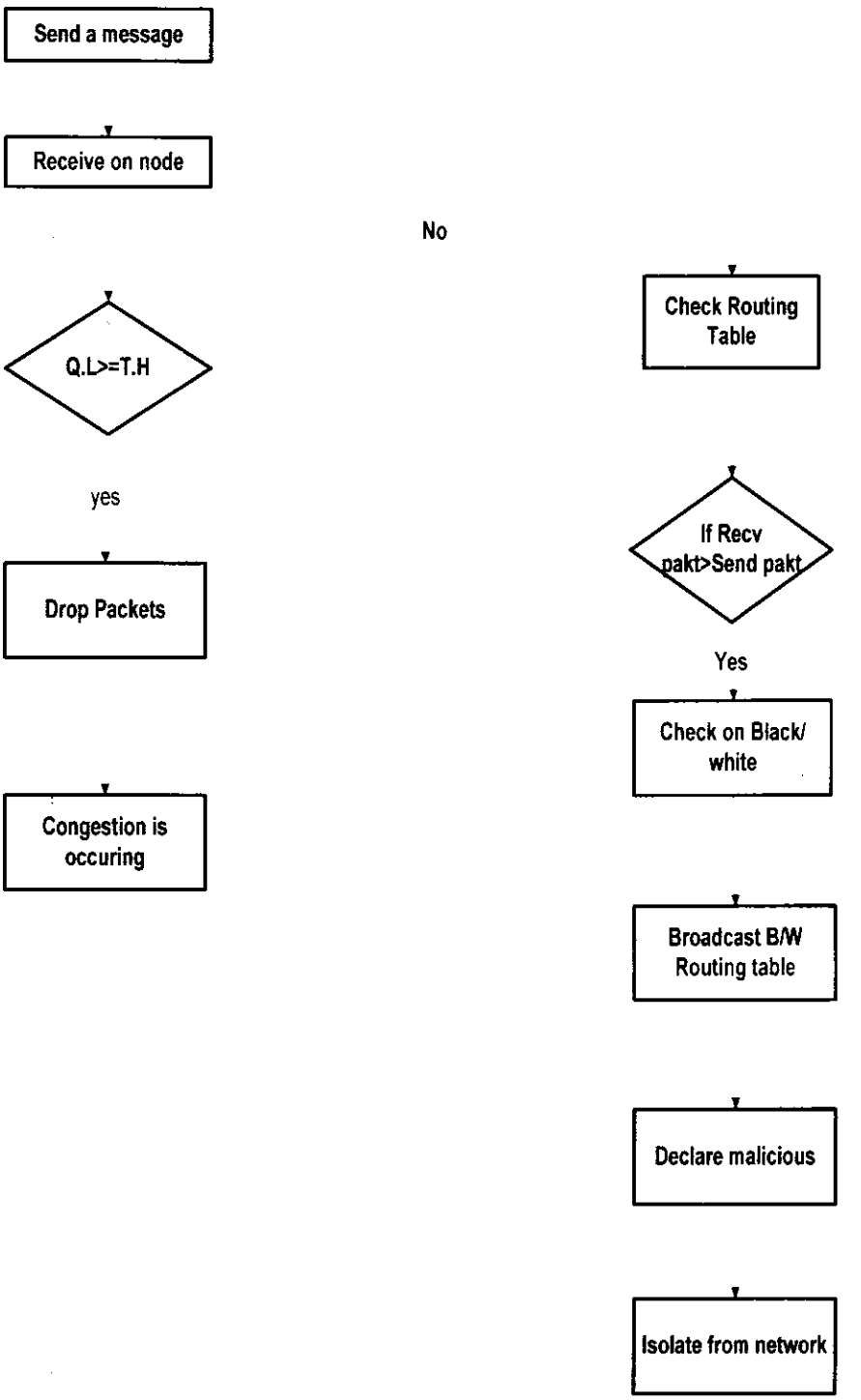


Fig 5.3 (b) Proposed Architecture

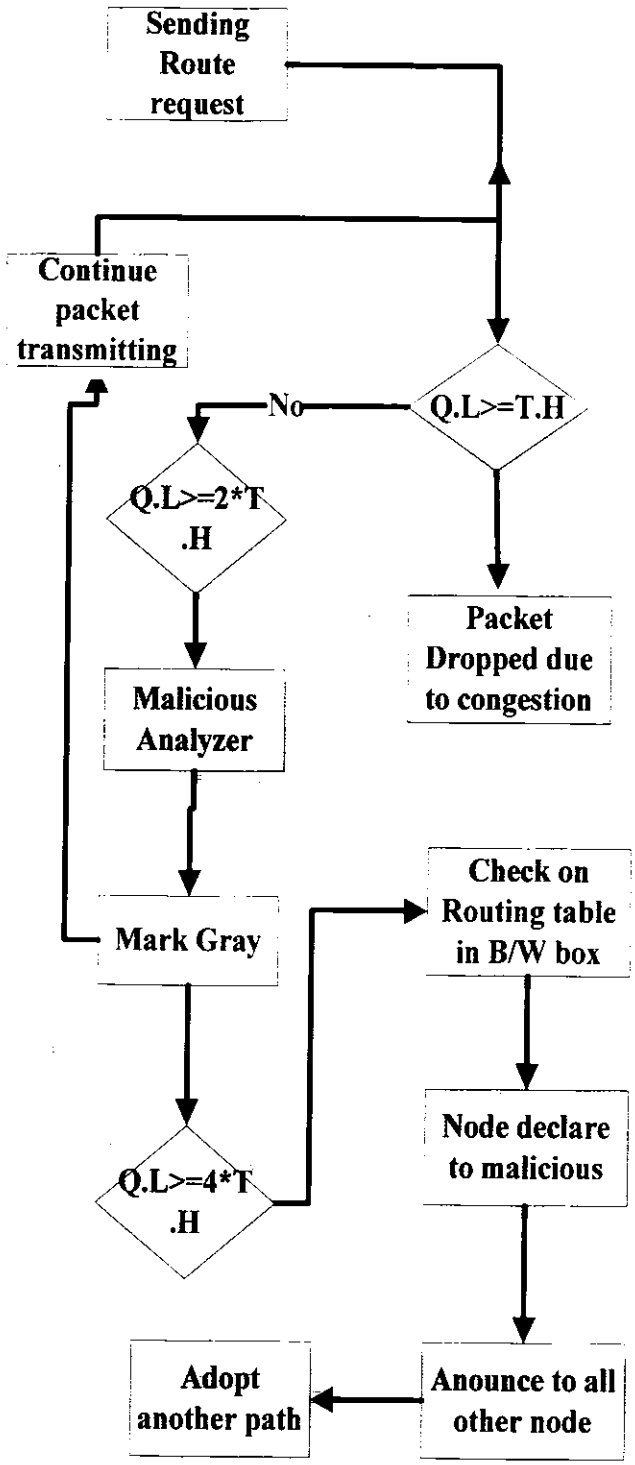


Fig 5.3 (c): Malicious Identification

5.4 Proposed Algorithm

Col_sum_check(ChkPoint)

{ for (j=1 to total nodes)

If col[j]> ChkPoint:

Mark Gray [j]:

}

Algorithm

Queue Length=Q.L

If (Qsize<QLength)

Enqueue (Arr_pkt); Succ_Drop_pkt ();

Else

{Drop_Pkt ();

}

Queue_Drop_ctr (Self);

Succ_Drop_ctr (Sender);

Time=t0:

Sum_neighbourNodeComm ();

Calculate AvgDrop ();

If (Drop_Pkt_repeated (n)== true)

{

for (i=1 to total nodes)

ChkPoint = threshold * (Avg_drop_rate)

If Row[i]> ChkPoint

{Col_sum_Check(ChkPoint)

Break:

} }

Same procedure is done on t1 and t2 with the multiple of threshold value and from this can detect the gray hole and black hole.

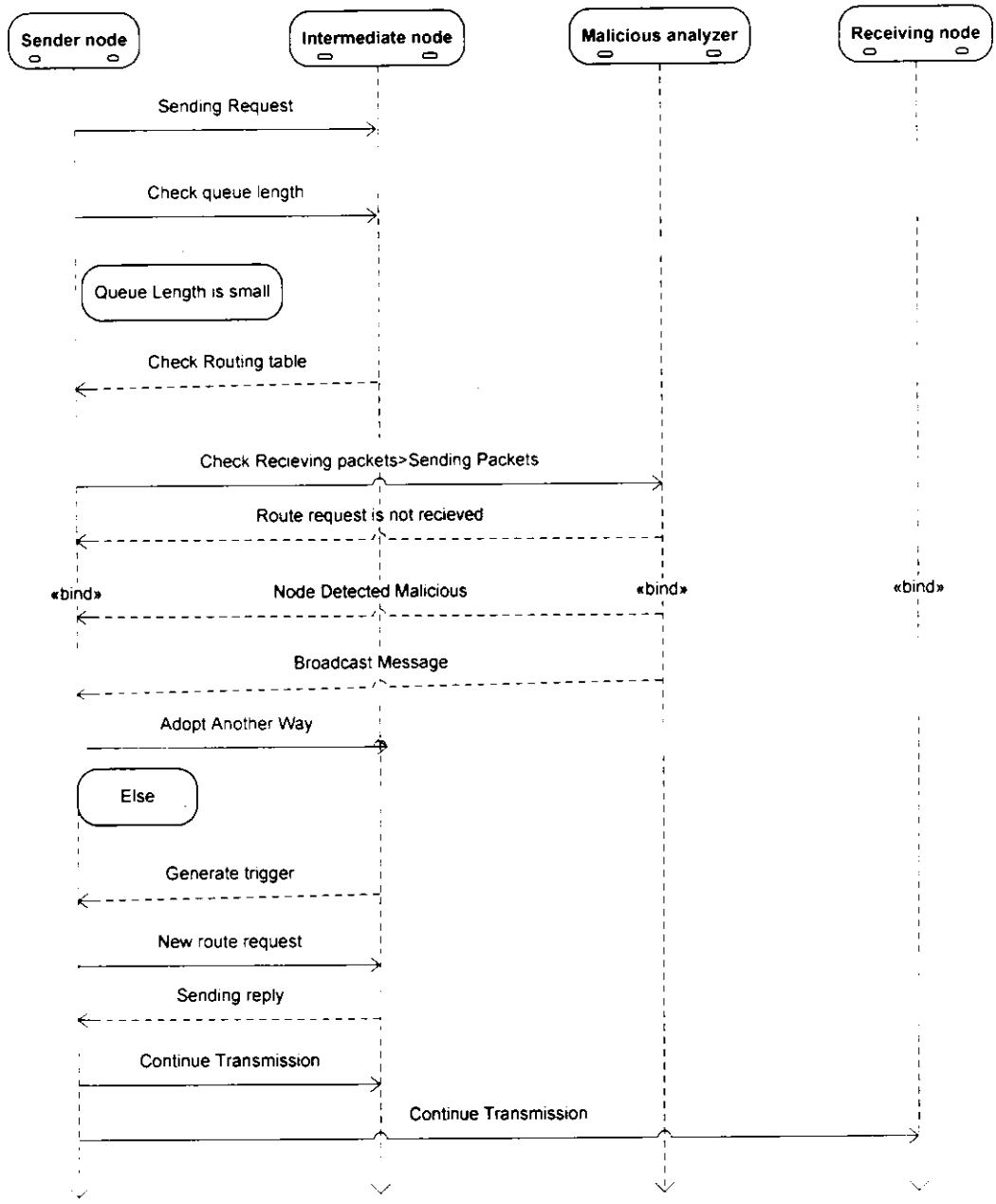


Fig 5.5: System Sequence Diagram

CHAPTER 6

RESULTS AND SIMULATION

6.1 Simulation Scenario in OMNET++

In order to test system model three different simulation scenarios are performed. The three scenarios differ in simulation time and number of nodes. The simulation starts and takes some time to setup the network topology and path discover with the basis of AODV routing protocol. The communication starts between the nodes when the paths are established. The sender and destination nodes are randomly chosen. Fro the ease of implementation and understanding, one node at a time sends packets on the network. In this scenario, 8 nodes are used in which firstly HELLO message are used for handshake. Through this links are established on physical layer. After this packets are generated through application layer. Routing layer is used for AODV and for table maintenance. On MAC layer, congestion and queue maintenance are used. After creates the route request generation, if route reply is not received for specific time then retries it and again packet generation is used. Route reply is also having broadcast nature as well as route request. On MAC layer we take matching that this packet is for which node.

6.2. Congestion & Malicious Simulation

For nodes of the network a simulation of 20 minutes was performed. The congestion is situated in our scenario in such a way that it basically divides the network into two logical networks. This partitioning can be seen in figure, where node 8 has congestion because it have many links and bridges two logical portions to make it a single network: if node 8 is removed from the network, the network is divided into two physical networks. Such a scenario is generally catered for the worst cases among research study. However, in this study it is taken for the ease of identification of a data moving to and fro between the two logical networks.

Figure 6.1 shows the corresponding graph of the packets sent by the senders and received by the intended destinations. In our scenario 2 to 5 percent congestion is performing. During congestion when packet lasting is increased then we detect that it is not the fault of congestion. And it is the fault due to any type of attack.

6.3 Congestion Simulation

In this case, show the congestion through which packets is dropped and two to three percent of packet loss is occurring.

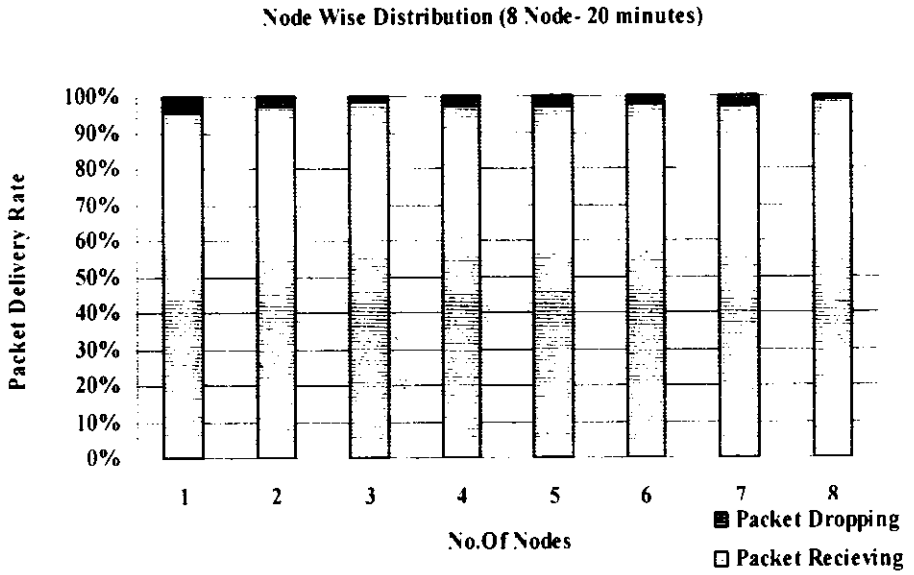


Figure 6.1: Packets Received at all nodes.

6.4 Malicious Simulation

Case 1

This can be seen in figure, where node 8 has black hole and bridges two logical portions to make it a single network; if node 8 is removed from the network, the network is divided into two physical networks. Such a scenario is generally catered for the worst cases among research study. However, in this study it is taken for the ease of identification of a data moving to and fro between the two logical networks.

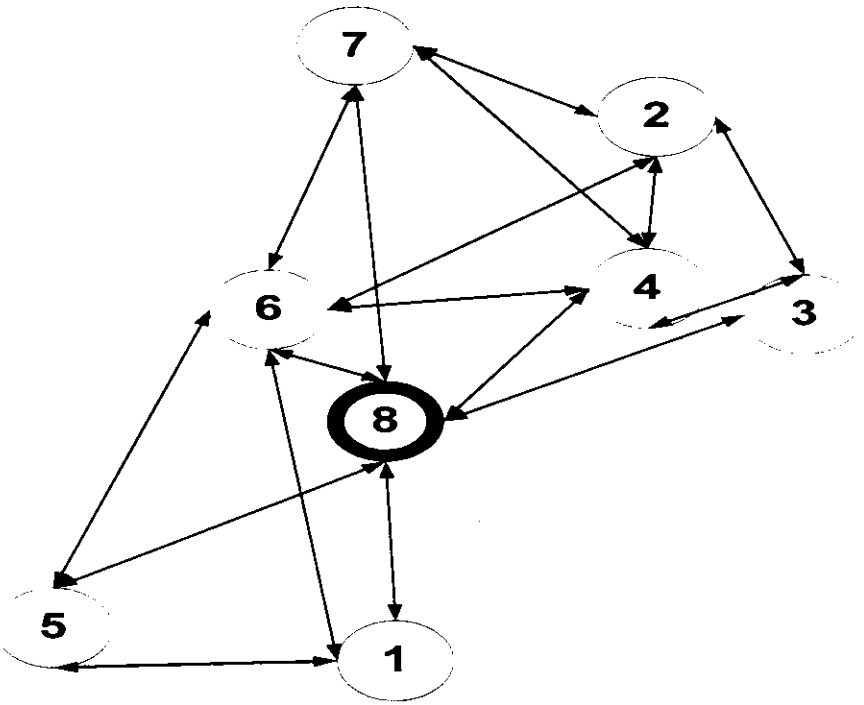


Figure 6.2: Topology of 8-node scenario

Figure 6.3 shows the corresponding graph of the packets received by the intended destinations. This is 8 node scenario and 25 minutes is taken. The difference is the dropped packets. In figure 6.4 total received packets show in which during black hole attack, packet dropping rate is increased. In this scenario, total 41,758 packets were sent, out of which approximately 5253 packets were dropped. Total 36505 packets were received in which just over 428 packets were dropped during the identification of malicious activity: the black hole. In this case, we take 3 packets of queue length.

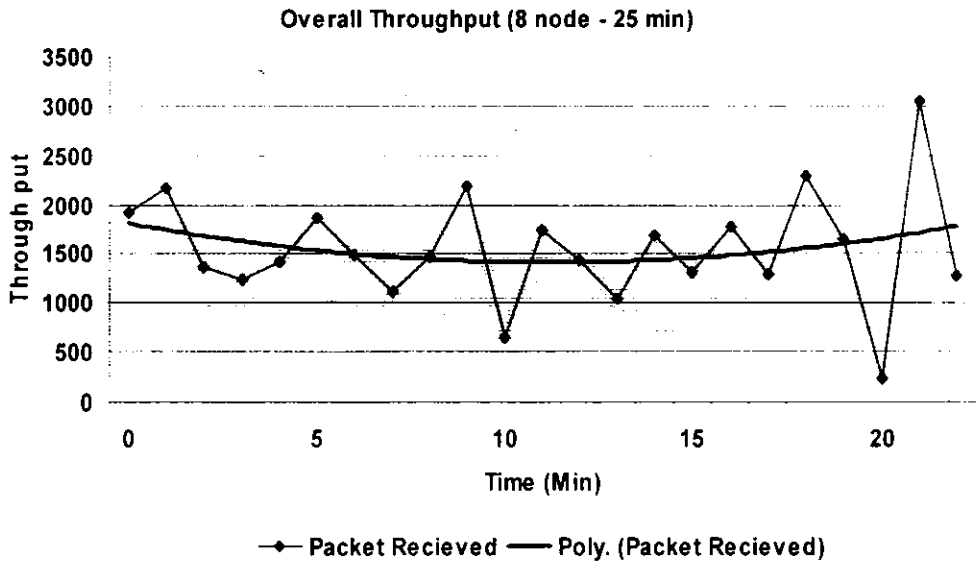


Fig 6.3: Packets Received at all nodes

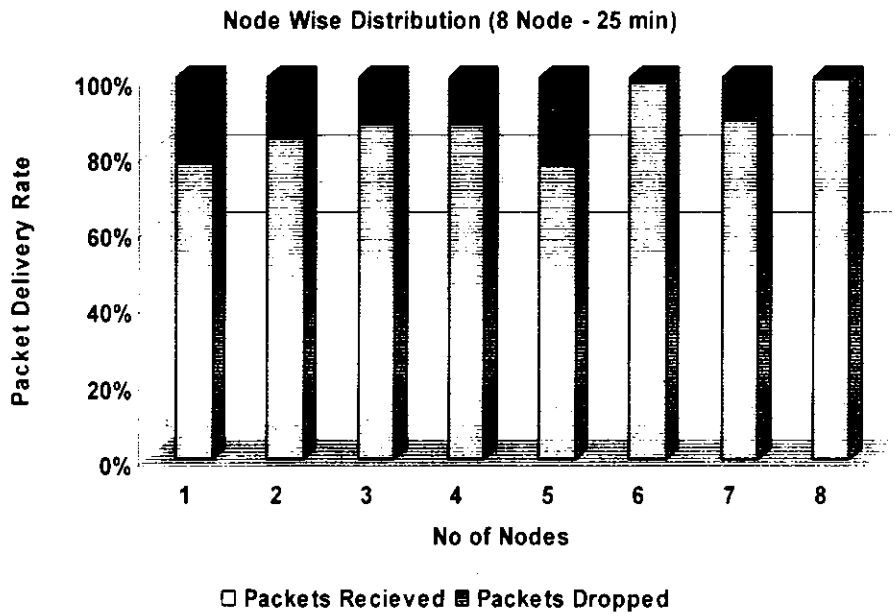


Fig 6.4: Packets Dropped During Transaction

For nodes of 8 in the network, a simulation of 50 minutes was performed. Figure shows the corresponding graph of the packets sent by the senders and received by the intended destinations. The difference is the dropped packets. In this scenario, total 41758 packets were

sent, out of which approximately 5253 packets were reported dropped due to malicious node and existence of black hole attack in the network. Besides, data packets are also dropped due to time limit reached.

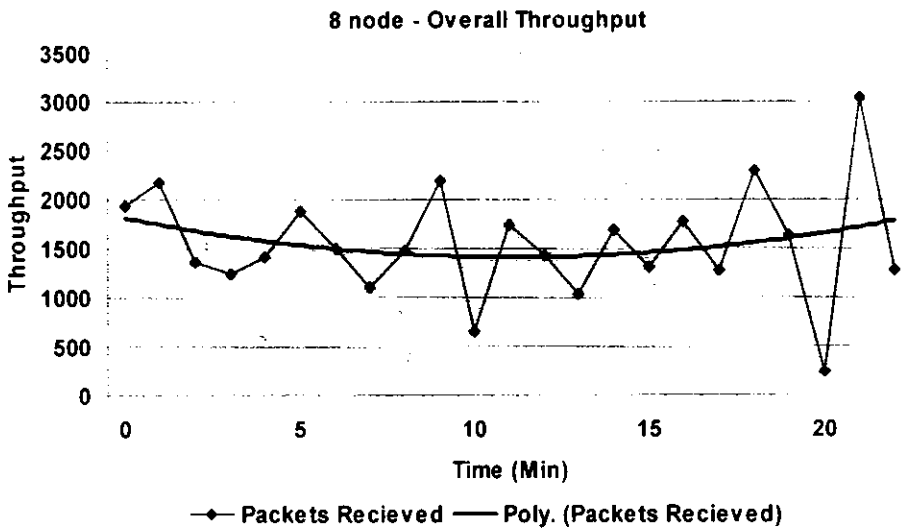


Fig 6.5: Packets Received at all nodes

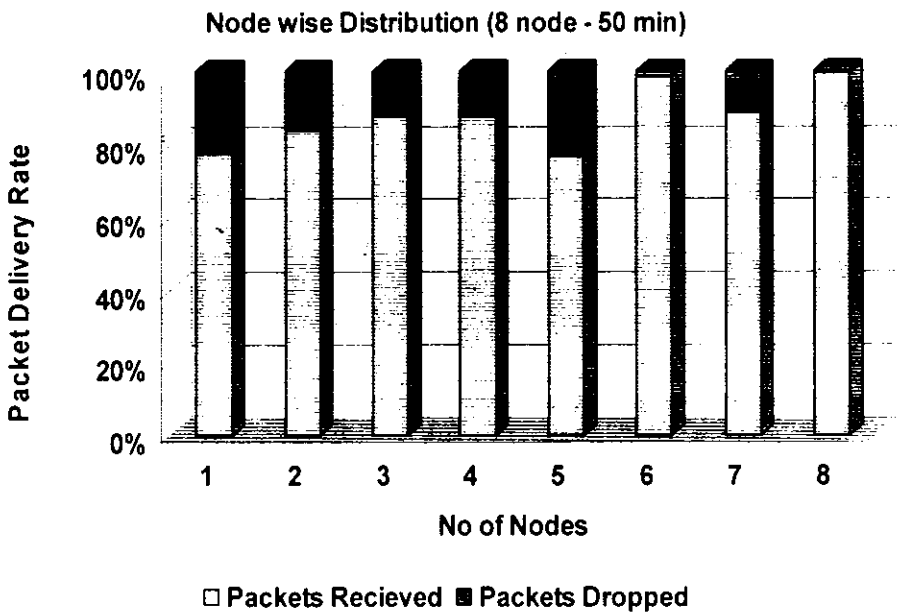


Fig 6.6: Packets Dropped During Transaction

Case 2

Figure shows the corresponding graph of the packets sent by the senders and received by the intended destinations. Here we take the 12 node scenario and 25 minutes is taken.

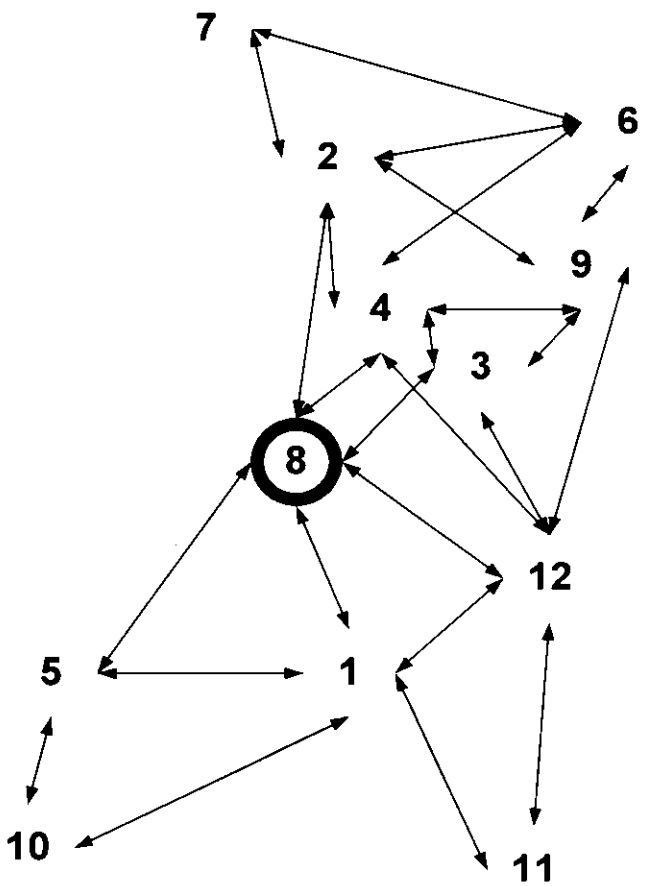


Figure 6.7: Topology of 12-node scenario

The difference is the dropped packets. In this scenario, total 62,598 packets were sent, out of which approximately 11376 packets were unable to reach the destination. 703 packets were dropped due to route selection through black hole. In this case, we take 5 packets of queue length and the threshold value is 10.

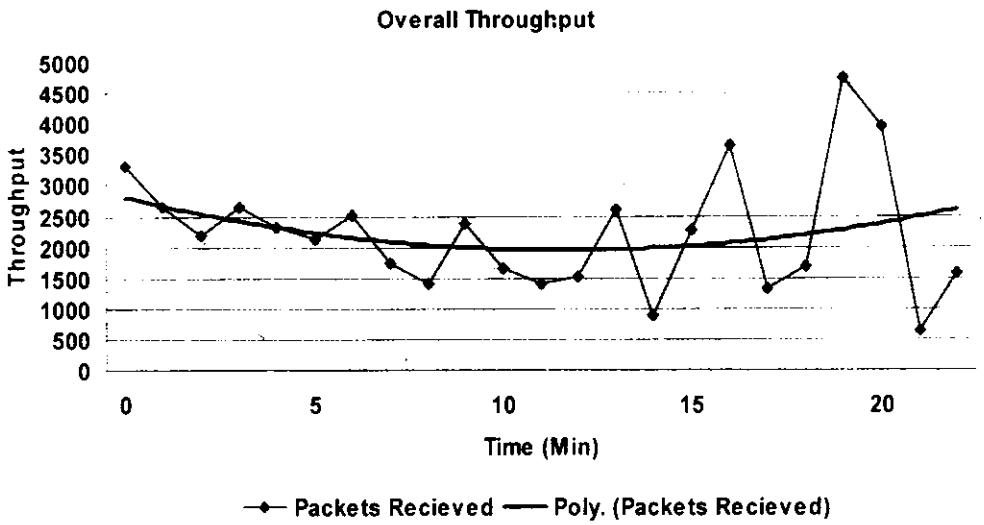


Fig 6.8: Packets sent and Received at all nodes

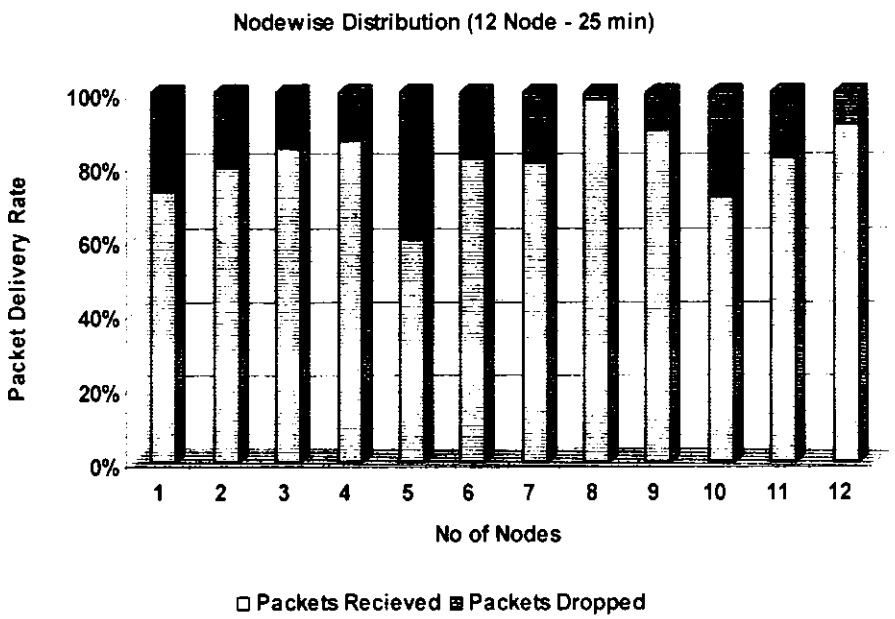


Fig 6.9: Packet Dropped by During Transaction

This is 12 node scenario and 50 minutes is taken. The difference is the dropped packets. In this scenario, total 125681 packets were sent, out of which approximately 23853 packets failed to reach desired target node. Even though a total 10, 1828 packets were received but still black hole node was able to maliciously disrupt and drop 1120 packets. In this case, we

take also 5 packets of queue length and take threshold value with 10. After 17 minutes black hole attack identified.

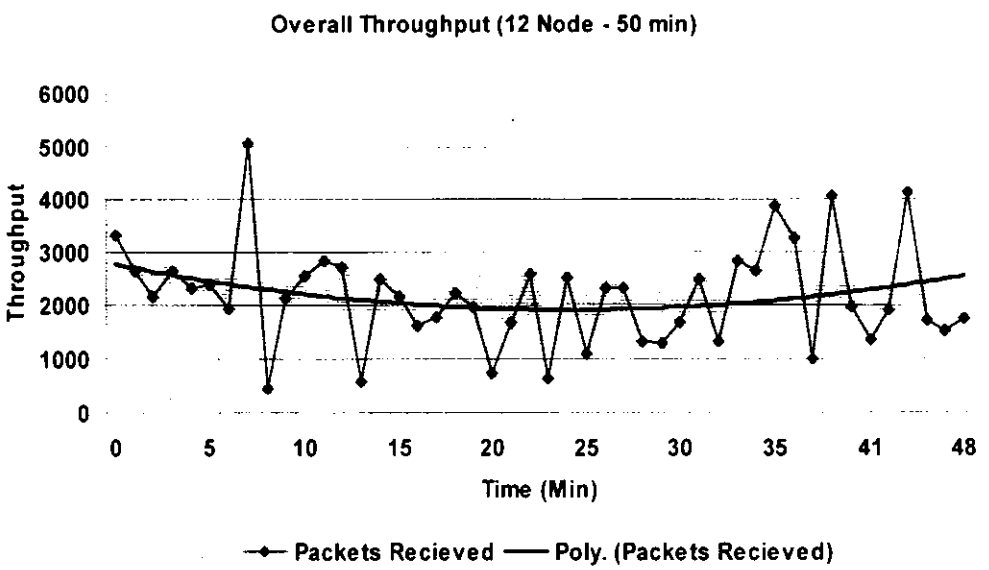


Fig 6.10: Packets Received at all nodes

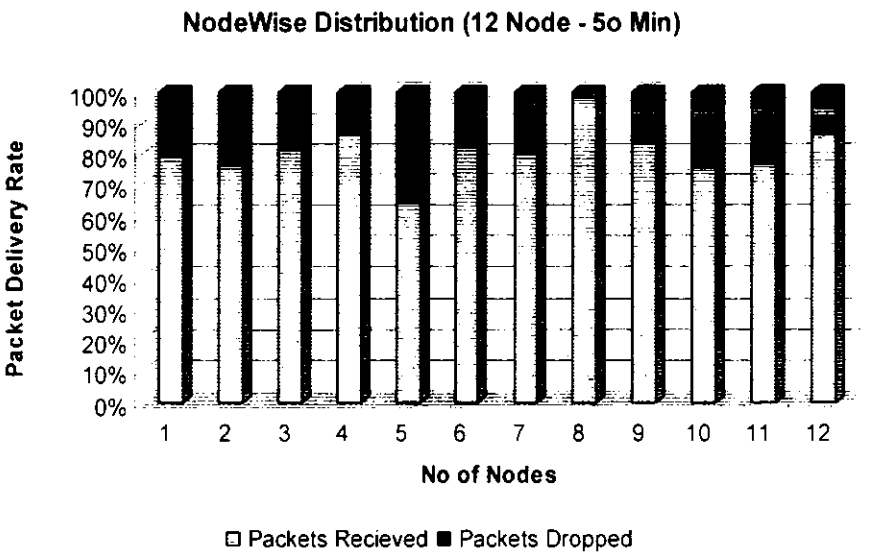


Fig 6.11: Packet Dropped During transaction

6.5 Results

Simulation results show that congestion and black hole attack implemented in network simulator. I have taken simulation scenario with different type of sender and receiver nodes.

As there is congestion and malicious node in the network, so graphs show that either in congestion or malicious attack, packets are dropped. In congestion, due to queue full packets are dropped and in malicious all the packets towards malicious node and drop all the packets thus decreasing network performance. According to my simulation results source node sends packets and are received by either queue full node or malicious node. All the packets and throughput of packets being dropped at the queue full or malicious node can be seen in the graph. We also change threshold value and also change queue size according to our scenario. And according to these threshold values, I can identify the node when treated as suspected and when treated as a malicious node.

CHAPTER 7

CONCULSION

A range of attacks intended for the network layer have been recognized and deeply research in recently research papers. By attacking on the routing protocols, attackers can take traffic and injects an illegal data into the path between source node and destination node. After injecting the path, attacker can control the network flow. In AODV, the attacker tries to find out a route with distance metric that is too much smaller and it is smaller than the actual distance. In this routing protocol, attacker can announce a routing update with a large sequence number. This thesis has focused on improving the security solution for Ad-hoc network using AODV protocol. I presented active black hole attack simulation for Ad-hoc network and congestion simulation using OMNET++. The corresponding results have been presented in relevant chapter. I have also designed an algorithm that not only detects black hole but also differentiates with congestion in Ad-hoc network environment when applied on AODV protocol.

Future work might include further optimization of the proposed algorithm to minimize packet drops and false alarms. Additionally, this solution my be applied on other type of attacks like wormhole, gray hole or Byzantine attacks. The implemented mechanism doesn't provide protection from all active attacks but it can provide Ad-hoc network from other type of attacks. This scheme can also be applied to other types of routing protocols that is my future work.

References

[1] Sihyung Lee Tina Wong Hyong S. Kim;" Secure Split Assignment Trajectory Sampling: A Malicious Router Detection System,"2006.

[2] K.A. Bradley, S. Cheung, N. Puketza, B. Mukherjee and R.A. Olsson, Detecting disruptive routers: a distributed network monitoring approach, in: Proceedings of the IEEE Symposium on Research in Security and Privacy pp. 115–124. May 1998.

[3] Dokurer, S.; Ert, Y.M.; and Acar, C.E. Performance analysis of ad-hoc networks under blackhole attacks. SoutheastCon, 2007, Proceedings IEEE, 148 – 153. 2007.

[4] Dokurer, Semih.Simulation of Black hole attack in wireless Ad-hoc networks. Master's thesis, AtılımUniversity, September 2006.

[5] N. Nasser and Y. Chen, Enhanced intrusion detection system for discovering malicious nodes in mobile Ad-hoc network, in Proc. IEEE Int. Conf. on Communication (ICC'07), , pp. 1154-1159. June 2007.

[6] Ahmed, Iffat; Ahsan, Faraz; Khadim, Nyla; and Hussain, Khalid, "Multimedia Traffic Engineering in Next Generation Networks" .CONF-IRM 2009 Proceedings. Paper 25.2009.

[7] C. Adjih, D. Raffo, and P. Muhlethaler, "Attacks Against OLSR: Distributed Key Management for Security," 2nd OLSR Interop/Wksp., Palaiseau, France, July 28–29. 2005.

[8] A. Mizrak, Y.-C. Cheng, K. Marzullo, and S. Savage. Fatih: Detecting and isolating malicious routers. In Proc. International Conference on Dependable Systems and Networks, Jun. 2005.

[9] Faraz Ahsen, Khalid Hussain, Nyla Khadam, Muhammad Sharif. Identification of a Lossy Channel in Wireless Mesh Network using Conservation of flow. Journal of Information & Communication Technology Vol. 1, No. 2, 60-70. Fall 2007.

[10] J. R. Hughes, T. Aura, and M. Bishop. Using conservation of flow as a security mechanism in network protocols. In IEEE Symp. on Security and Privacy, pages 132–131, 2000.

[11] B. Sun, Y. Guan, J. Chen and U.W. Pooch, Detecting black- hole attack in mobile Ad-hoc networks, in Proc. of the 5th European Personal Mobile Communications Conference, Glasgow, UK, April 2003.

[12] A. Boukerche, Performance comparison and analysis of Ad-hoc routing algorithms, Proc. IEEE International Conference on Performance, Computing, and Communications. , pp. 171–178. 2001.

[13] C. E. Perkins and E. M. Royer, Ad-hoc On Demand Distance Vector (AODV) Routing, IETF Internet draft, draft-ietf-manet-aodv-O2,txt, Nov. 1998 .

[14] Sreedhar C. Madhusudhana V. S and Kasiviswanath N. A Survey on Security Issues in Wireless Ad-hoc Network Routing protocols, International Journal on Computer Science and Engineering, Vol. 02, No. 02, p.p 224-232, 2010.

[15] N. Nasser and Y. Chen, Enhanced intrusion detection system for discovering malicious nodes in mobile Ad-hoc network, in Proc. IEEE Int. Conf. on Communication (ICC'07), pp. 1154-1159. June 2007.

[16] N.jasiankar, K.Durai Swamy. A Novel security framework for protecting Network Layer operations in MANET. 2009.

[17] Ping YI, Vue WU, Jianhua LI, Malicious Node Detection in Ad-hoc Networks Using Timed Automata.2007.

[18] Junhai Luo, Mingyu Fan, Danxia Ye, 'Black Hole Attack Prevention Based on Authentication Mechanism, in: Proc. of the IEEE Singapore International Conference on Communication Systems (ICCS), pp. 173–177, 2008.

[19] Saju P John and Philip Samuel, An On-Demand Byzantine-Resilient Secure Routing Protocol for Wireless Adhoc Networks, IJCSNS International Journal of Computer Science and Network Security, VOL. 10 No.1, p.p 201-208 January 2010.

[20] Payal N. Raj, Prashant B. Swadas. DPRAODV: A Dyanamic Learning System Against Blackhole Attack In Bodv Based Manet. In: International Journal of Computer Science Issues, Vol.2, pp 54-59, 2009.

[21] Idrees, M., Yousaf, M.M., Jaffry, S.W. Pasha, M.A. and Hussain, S.A, Enhancement in AOD V Routing Using Mobility Aware Agents . IEEE - International Conference on Emerging Technologies , Islamabad, pp 98-102, September 2005.

[22] S Madhavi, K Duraiswamy, B Kalaavathi, S Vijayaragavan. Survey of Attacks on AODV and MAODV. ICWET 2010.

[23] G. S Mamatha, S.C. Sharma. A Robust Approach to Detect and Prevent Network Layer Attacks in MANETS. IJCS 2009.

[24] Parul Tomar, Prof. P.K. Suri, Dr. M. K. Soni. A Comparative Study for Secure Routing in MANET. IJCS 2010.

[25] Sahu S. and Shandilya S. K. A Comprehensive Survey on Intrusion Detection in MANET, proceedings of the International Journal of Information Technology and Knowledge Management, 2(2), 305-310. (2007).

[26] Firas Al-Balas,Design and Investigation of Scalable Multicast Recursive Protocols for Wired and Wireless Ad-hoc Networks. january 2009.

[27] Nyla Khadam, Kalid Hussain. Detection of malicious node in MANET through Faith. 2008.

[28] Y-C. Hu, A. Perrig, and D. Johnson, Wormhole Attacks in Wireless Networks, IEEE JSAC, vol. 24, no. 2, Feb. 2006.

[29] F. Kargl et al., Advanced Detection of Selfish or Malicious Nodes in Ad-hoc Networks, 1st European Wksp. Security in Ad-Hoc and Sensor Networks, ESAS 2004, Aug. 5–6, 2004.

[30] S. Buchegger and J.-Y. L. Boudec, Performance analysis of the CONFIDANT protocol: Cooperation of nodes - fairness in dynamic ad-hoc networks, in Proceedings of IEEE/ACM Workshop on Mobile Ad-hoc Networking and Computing (MobiHOC). IEEE, June 2002. [Online]. Available: http://leawww.epfl.ch/Publications/LeBoudec/ BucheggerL02.pdf

[31] S. Marti, T.J. Giuli, K. Lai and M. Baker, Mitigating routing misbehaviour in mobile Ad-hoc networks, in: Proceedings of the 6th Annual IEEE/ACM International Conference on Mobile Computing and Networking (MobiCom 2000) pp. 255–265. (August 2000).

[32] Martine Bella¨ıche,Jean-Charles Gr´egoire "Source Detection of SYN Flooding Attacks" ESRGroups France 2009.

[33] Sukla Banerjee. Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Networks Proceedings of the World Congress on Engineering and Computer Science 2008 WCECS 2008, October 22 - 24, San Francisco, USA , 2008.

[34] A. Toledo and X. Wang, Robust Detection of MAC Layer Denial-of- Service Attacks in CSMA/CA Wireless Networks, IEEE Trans. Inf. Forensics Secur., vol. 3, no. 3, pp. 347–358, 2008.

[35] W. Stallings, Data and Computer Communications, 6th ed. Englewood Cliffs, NJ: Prentice Hall, 2000.

[36] B.A. Forouzan, Data Communications and Networking, 4th ed., McGraw- Hill Science, New York, NY, 2006.

[37] Y. Law et al., Link-Layer Jamming Attacks on S-Mac,Proc. 2nd Euro. Wksp. Wireless Sensor Networks, pp. 217–25, 2005.

[38] Rajani Muraleedharan, Lisa Ann Osadciw, Jamming Attack Detection and Countermeasures In Wireless Sensor Network Using Ant System, SPIE Defence and Security, Orlando, 2006.

[39] Andras Varga. Omnet++ - discrete event simulation system - version 3.2 - user manual, March 2005.

[40] Lin Ma, Jun Zhang, and Kai Liu. Contention-Based Congestion Control in Wireless Ad-hoc Networks. International Conference on Information, Networking and Automation (ICINA) 2010.

[41] Victor Firoiu and Marty Borden,A Study of Active Queue Management for Congestion Control in Proceedings of IEEE/INFOCOM, 2000.

[42] K. Nahm, A. Helmy, and C.-C. J. Kuo, Cross-layer interaction of TCP and Ad-hoc routing protocols in multihop IEEE 802.11 networks, Trans. Mobile Computing, vol. 7, no. 4, pp. 458–469, Apr 2008.