Detection of Selective Forwarding Attack in Mobile Ad Hoc Networks

Under taken by

Gul Sahar

339-FBAS/MSCS/F07

Supervised by

Prof. Dr Muhammad Sher

Department of Computer Science and Software Engineering

Faculty of Basic and Applied Sciences

International Islamic University Islamabad

2012

بسم الله الرحمن الرحيم

In the name of Almighty Allah,

The most Beneficent, the most Merciful

Department of Computer Science

International Islamic University, Islamabad

Dated: 27-6-12

Final Approval

It is certified that we have read the thesis titled "**Detection of Selective Forwarding Attack in Mobile Ad hoc Networks**" submitted by **Gul Sahar, Registration No: 339-FBAS/MSCS/F07**, and found as per standard. In our judgment, this research project is sufficient to warrant its acceptance by the International Islamic University, Islamabad for the award of **MS Degree in Computer Science.**

Project Evaluation Committee

External Examiner:
Associate. Prof. Dr. Hafiz Farooq Ahmed
NUST, School of Electrical Engineering
And Computer Science (SEECS)

10/7/12

Internal Examiners:
Assist. Prof. Qasir Javed
Department of Computer Science
International Islamic University, Islamabad.

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

27-6-12

Dedication

My Parents: Bundle of thanks for supporting me, affection and steady love and believing in me. I will try my best to attain all your dreams.

My Teachers: Bundle of thanks for commitment, support and guidance that make possible my study.

My Siblings: Bundle of thanks for checking me, soothing me, always is with me, and raising my trust on that Allah (S.W.T) better knows what is best for us.

A Dissertation submitted to the

Department of Computer Science

International Islamic University Islamabad

As a partial fulfilment of requirements for the award of

The degree of

MS in Computer Science

International Islamic University, Islamabad

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. 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 his 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.

GUL SAHAR

(339-FBAS/MSCS/F07)

Acknowledgement

First of all, I would like to extend our sincere and humble gratitude to all mighty ALLAH whose blessing, help and guidance has been a real source of all our achievements in my life. Appreciation to our beloved Prophet Muhammad (PBUH) who is always a great source of inspiration of divine devotion and dedication to me.

We admit that our achievements are due to sincere and most loving parents, sisters and brothers who always pray for success. We pay thanks to our sincere colleagues for theirs contribution and support in our research work. Their moral support and encouragement in every step, made our research work valuable, easier and attainable.

I would like to thank our **supervisor Prof. Dr Muhammad Sher** for their endless support, valuable suggestion, encouragement, guidance and coordination while conducting our task.

I state my innumerable gratitude to all the people Faraz Atika Qazi and Lect. Gul Jabeen (KIU) 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 of Selective Forwarding Attack in Mobile ad hoc networks
Undertaken By:	Gul Sahar
Supervised By:	Prof. Dr Muhammad Sher
Start Date:	February 2009
Completion Date:	February 2012-02-01
Tools and technologies:	MS Visual Studio C++ and OMNET++
Documentation Tools:	MS Word, EDraw, MS Excel
Operating system:	MS window XP Professional
System used:	Laptop Core i3

Abstract

Wireless networks are gaining popularity to its peak today, as the users want wireless connectivity irrespective of their geographic position. There is an increasing threat of attacks on the Mobile Ad-hoc Networks (MANET). Selective forwarding attack is one of the security threat in which the traffic is redirected to such a node that actually does not exist in the network. The node presents itself in such a way to the node that it can attack other nodes and networks knowing that it has the shortest path. MANETs must have a secure way for transmission and communication which is quite challenging and vital issue. In order to provide secure communication and transmission, researcher worked specifically on the security issues in MANETs, and many secure routing protocols and security measures within the networks were proposed.

Previously the mostly works done on security issues in MANET were based on Black hole attack Different kinds of attacks were studied, and their effects were elaborated by stating how these attacks disrupt the performance of MANET.

The scope of this thesis is to study the effects of Selective forwarding attack in MANET using both AODV routing protocol. The hybrid approach impact of Selective forwarding attack on the performance of MANET is evaluated finding out which globally and locally is more vulnerable to the attack and how much is the impact of the attack on both locally and globally. The measurements were taken in the light of throughput, end-to-end delay and network load. Simulation is done in OMNET++.

Table of Contents

List of Figures

Abbreviation Used

Abbreviation	Acronyms
MANET	Mobile Ad Hoc Network
AODV	Ad hoc On Demand Vector
MAC	Message Authentication Code
DSDV	Destination Sequenced Distance Vector Protocol
OLSR	Optimizing Link State Routing
DSR	Dynamic Source Routing
RREQ	Route Request Message
RREP	Route Reply Message
DoS	Denial of Service
CLR	Clear Packet
DB	Distributed Bordercasting
LSA	Link State Advertisements
LDR	Label Distance Routing
LAR	Location Aided Routing
NS-2	Network Simulator-2
PDR	Packet Delivery Ratio
QRY	Query Packet
RFC	Request For Comments

RERR	Route Error
RIP	Routing Information Protocol
RQPD	Random Query Processing Delay
TTL	Time To Live
UDP	User Datagram Protocol
UPD	Update packet
WMN	Wireless Mesh Network
WSN	Wireless Sensor Network
ZRP	Zone Routing Protocol

Chapter 1

Introduction

1.1 Introduction

Mobile Ad-hoc Networks (MANETs) are self-ruling as well as distributed wireless structure [1]. MANETs include transportable devices which are easily moving inside or outside of network region. The systems devices are often consist of nodes Mobile station, mobile host such as laptops, PDA, mobile cell, personal computer and MP3 player. These devices share data on the wireless network and movable. The devices could function as a source as well as routers simultaneously. They can do randomly for their connectivity to each other in the network. Wireless devices had their own capability to configure it selves as well as message delivery. Now a day MANET is generally capable and fast growing technology that is based on lack of infrastructure and quickly developed network [3]. Due to all these features enormous link with other nodes are created huge network. It's similar that have faced security challenges because MANET contains little character such as mobile technology, limited power and bandwidth, high error rated etc. So the main security issue is that the routing protocols of wired networks can not using as well in wireless network. At this reason routing protocol is one of the challenging and interesting fields for research areas [2]. MANET [3, 4] has many routing protocols such as DSR, DVDR, AODV, OLSR etc.

1.2 Wireless Local Area Network (WLAN)

Wireless local area network is opposite of wire area network and the only difference between the two networks is that WLAN has no infrastructure: It has more advantages than wire area networking such as easy installation, mobility, expandability, productivity and cost. Its popularity has been increasing among home users. Its link is established among two or more devices. The link between devices is established through OFDM or spread Spectrum. For the reason, wireless devices are connected in a limited area or having a basic service set (BSS). This sets all the stations for communication across. BSS has two types: one is independent BSS which has no access points. It is not connected with other basic services sets. Unlike independent BSS, infrastructure BSS is able to communication with other stations by access points.

1.2.1 Peer to Peer Network

In peer to peer network or ad hoc network wireless devices communicate across without requiring the participation of central access point. It is independent basic service set. If wireless devices are within range and can find out and link directly with no access point. This process is used between two computers.

1.2.2 Distributed Connection System

Distributed connection system uses access points as repeaters in place of connecting all access points in a network using wire. The client packets across link between accesses are the main advantage of WDS's for Mac addresses. Access point can be act both a main base station and relay. The main base stations connected with wired Ethernet. And remote base stations accepts link form wireless clients and passes rely or main base station. Relay's data between wireless client and remote base station and other relay stations to the same or another relay base station. The connectivity among clients is using MAC addresses or IP addresses. Wireless distribute system refers to repeater mode because it appear to bridge or accepts wireless client at the same time.

1.3 Issues in MANET

In Mobile ad hoc network hidden and exposed nodes are observable fact of carrier rate and packet common sense MAC protocol. This protocol controls access through the method where nodes, be different from available, sense another node using the channel.

1.3.1 Hidden Nodes

A hidden node is that a node that does not within the range is receiving and they don't hear the transmission and as a result do not vary from attempting to get access. Because the transmission may be the distance or a problem in the broadcasting path and antenna strength without range of signals and be applying of changed code. if node A send message to node B, node C cannot receive node A. The node C want to node B and C senses free medium fail collision at node B and node A can't received the collision so node A is hidden for node C.

1.3.2 Exposed Nodes

The exposed node is very different to hidden node. It is hear several disjoint parts of a network and never catch the opportunity to satisfy because it is always deferring to someone. If the continuous tessellation of a nodes on a rectangular network, where all node hear communication up to two nodes missing in all way. Such a network can be unconnected into separations of communication nodes anywhere a node can be an exposed node at different times in it process. For example node B send to Node A node C desires to send to other channel not A or B then node C senses carries finds medium in use and has to wait if node A is outside the signal range of node C therefore waiting is not necessary so node C is exposed to node B.

1.4 Security Vulnerabilities in MANET

MANET has much advantages and disadvantages. Because MANET has self-directed or routers connected through wireless link main reason is lack of centralized control. It has mobility and having self configuration. Due to which it faces many security challenges such as control access, repairing, bandwidth limited, power changes, addressing technology discovering, control access, self organization, scalability and reliability etc so several routing protocols has been proposed. Routing protocols are essentially design for find and maintain routes provide it exists through power control and assume that the node are willing to cooperate to each other and security etc.

The MANET attacks are divided into two types such as Passive and Active attacks. Passive attacks violate networks confidentiality. This attack is very difficult to identify because it do not disturb network it just capture data. To prevent form this attack encrypted mechanism is used. Active attack changes the data or destroys in the network. It disturbs the whole operations of the network. It is further divided into two types' external attack and internal attack. The external attack is carried out by the node but they do not belong to the network and internal attack is carried out by the cooperation node that is actually part of network. It is very complicated to evaluate internal attacks.

The above weak spot of MANET security requirement is required. Such as availability network services are available at any time correct any failure occurs and establish connection. Confident ability data should be protected in network from access of unauthorized party. Authenticity message authorization guarantees that content of a message are valid Integrity [7] data should not change or transmitted data should be same. No repudiation (transfer to the denial by a node in a communication of having participated). More security requirement of a MANET is focused to confidentiality and integrity.

Ad hoc networking has three types of routing protocols such as proactive, reactive and hybrid. Reactive protocols using an establishment the connection path and these routing protocols not perform maintain the network data and also not perform replace routing information like clockwork [2]. The sub categories of reactive routing protocols secure version the first is DSR i.e. QoS route discovery, SQoS route discovery and Confident and the second version is AODV i.e. CORE, SAODV, SAR other are TORA, ABR, SSA, FORP, LAR etc. The last version is hybrid i.e. ZRP and SLSP merge the greatest feature of in cooperation reactive and proactive protocols [8].

Distributed system [9] is the type of nature of scheme. This system has many advantage as well as disadvantage such as it has not needing sever so there set up are more complex. The distributed system facilitates private work in a way that is bad for the network. The private workflow as touted by this system is an anti-feature. The highest wireless useful throughput is dividing after the first retransmission (hop) is made. Dynamically allocated and revolve encryption keys are typically not hold in a distributed communication.

The major drawback of centralized system [9] which all authority is taken by top management and its lower nodes have a little authority such as sometimes some decisions are to be taken immediately at the spot time but due to central control system the decision can't be made without permission of managers.

1.5 Motivations and Challenges

In MANET security is the basic agonize used for the essential functionality of wireless network [5]. Essential security issues of a MANET are focused to confidentiality and integrity. MANET is vulnerable from security attacks such as it opens domain, dynamic nature, distributed system, cooperative algorithm and no protective defence method. So these issues have transformed the combat field of MANETs beside the security factors.

The MANET nodes communicate with each other nodes at the source of common reliance in the bases of decentralized administration. These rules MANET have faced more issues to be exploited by malicious nodes in the network. MANETs open medium also make more vulnerable to attack because it easier for opponents to go inside the network and search out to the ongoing links. Therefore the more nodes cooperate within rang the wireless link is very overhead.

In MANETs both communication and transmission are must secure so this way challenging and critical issue rapidly fast threats of attack in the mobile networks. Now a day security is most important, so to provide secure transmission and communication the researchers must know that all attacks and their vulnerabilities in the MANETs. These all attacks whose are following here are causes to break the security vulnerabilities like black hole attack, selective forwarding attack [6] gray hole attack, wormhole attack, flooding attack, Sybil attack, selfish attack, sinkhole attack denial of services etc. MANET communication is based on mutual trust to each other nodes. So there is no central access point for network control, dynamic changes, and limited resources such as power, bandwidth and unauthorized facility. Transfer of from source to destination in MANET is very sensitive for packet travelling. The performance of MANET is decreased due to this. Selective forward attack is the most difficult attack detection among all attacks [7]. Because it happened in internal network which may be a corporate node would call compromise node. It fall packets selectively. Range of packets to drop is concern on measure they become smarter for not identification. This attacker select drop from packet then it based on contents or original address. There are many other reasons for packet drop selection.

1.6 Problem Domain

The routing protocol of Mobile ad hoc network assume that in MANET topology nodes is strictly follows the routing protocols and through these protocol that willing to forward packets for other nodes. Mostly these routing protocols handle well with the dynamically changing topologies. Still they do not find the problem when attacker nodes hijack the network.

Mostly this attacker observed are packets dropping. Due to this case the network performance is degrade. In a convenient MANET the forwarding packet device need too many lot of resources such as high battery power and unlimited computing. So for the sake of other nodes some devices would not resort to forward packets in the presents of attackers. These attacks means in the presents of network due to reason of congestion, collusion and QoS and delay etc. may be packet dropped by attacker as well as certain of channel error.

In uncertainty packets dropping leads to detection and identification is very difficult in the present of attacker nodes. So it is very difficult to understand that the packet dropping reason due to channel error or uncertainty. These packets dropped significantly decrease the network performance. Because the MANET has lacks of central infrastructure, limited bandwidth, battery time, computational power and network topology and relationship are randomly changing. So the protection of this mechanism such as control access, authentication complex algorithm, detection system and complex routing protocols etc. We know that if the attacker attack the network the whole security of the system is degrade so we have need to develop better security mechanisms.

1.7 Proposed Approach

In our proposed solution we develop hybrid approach which is periodical detection the malicious node. The central point of data transfer communication in a MANET is intermediate nodes which act a router to router data transfer which place at end-to-end delivery. The intermediate route that means the uncertain problems could happen but some of these in-between routers begins mischievous. This problem need security mechanisms to detection and identification these routers. There is much number of security solutions for both wireless and wired routers but these have many deficiency which can't be ignored.

The Congestion and collusion are the security issues still in a normal wireless location. The packets drop in MANET may be two reasons such as malicious nodes or link break. So these reasons the network QoS is decrease the network performance. This research can later further investigate to identified malicious node and what are the reason for the packets drop by several existing algorithms of that specific purposes. Selective forwarding attacks harmfully involve the QoS routine of networks.

This research proposed a hybrid approach that extended AODV protocol will be proposed for crystal detection and identification of malicious node. The system model design, that give the method to discontinue packet drop after malicious node detection and identification and that will pass from the Black and gray list in system. This system can avoid justifiable communication from being disrupted network layer attacks.

1.8 Thesis Layout

We have a rest of the thesis is arranged as following.

In chapter 1 describe and explain the overview of Mobile ad hoc network and it security mechanism and issues.

In chapter 2 we will discuss the literature review in deep detail and we will also discuss the limitation of the existing techniques and preceding work of researchers interrelated to our problem domain.

In chapter 3 we have discussed a requirement analysis of proposed solution associated with domains in greater depth. Here we describe the problem definition and research objectives.

In chapter 4, the proposed scheme is discuss in details and methodology. Here we discuss about our proposed mechanism according to the problem that was fixed in the earlier chapter.

In chapter 5 belong to our Simulation details and including testing results and performance evaluation.

In chapter 6 concludes final remarks present and the future work.

Chapter 2

Literature Review

2.1 Literature Review

Nowadays security in MANET is important and fast growing technologies depend upon such self-configuration, self-managements topology, shared medium and lake of fixed control environment which make a MANET much more vulnerable to attack as compared to wired networks [10].

In this chapter examine the literature review related to MANET security issue. We present a broad, detail and essential vital survey in direct to make out the problem in existing system. In the reset of section 2.1 we talk about the several approaches of How to hold congestion and the section 2.2 we highlighting taking place the bases of pass literature related to security solution for wired and wireless networks whereas section 2.3 in this section is according to MANET and also depth analysis of selective forwarding attacks in MANET. At the end, in section 2.4 and 2.5 we focus on the restrictions of active technology scheme also summarize.

2.2 Congestion

In a mobile ad hoc network at shared medium if multiple senders send data to single destination or general means of congestion when the message is overload and so heavy that it show down the network performance and packets drops. Many researches are going on it but the specific possessions of MANET the congestion affect a whole network area due to the shared medium. We present few papers that show How to handle the congestion in MANET.

In this paper [11] the authors designed a routing protocol CASPER that performs routing intelligently and minimizes the delay in data transmission for congestion in MANETs. They control the network traffic through a suitable shortest path calculation algorithm that a less congested path and minimize the number of packets drops through data forwarding and avoid redundant delay. There proposed protocol has been compared with two link state protocol such as OSPF [12] and OLSR [13, 14]. They described OSPF and OLSR before comparison. The open shortest path first (OSPF) internal gateway protocol and it maintain state link database for well-organized routing connecting modes. During this process the data exchanges are called Link State Advertisements (LSA) [12] and every router stores the LSA's in its Link State Database. It is uses a shortest path algorithm to store and find shortest path from one node to another nodes. Dijkstra's algorithm contains the least cost path from a router to other nodes. Routers that share a link develop into neighbours and all neighbours are elected via exchange of Hello packets. The adjacency routers are responsible for database exchange and synchronization of their LSDB's. The OSPF have election of a Designated Router and a Backup Designated Router. This Designated Router as a central points as each router exchanges information. A Backup Designated Router is elected to replace the Designated Router in case it goes down. And they are an election through algorithm. The Optimized Link State Routing Protocol (OLSR) is MANET protocol that that as a table driven and proactive protocol. This uses hello messages to discover link state information between nodes in network and uses Topology Control (TC) [14,13] MANET. Each nodes is selected as Multipoint relays (MPR) by the node for forwarding control traffic. They proposed a circle based routing technique for forwarding data as an alternative of calculating and storing path source node to all nodes and also calculating the store the path from source to destination having only those in-between nodes. In the terms of throughput, the CASPER performs better than OSPF and OLSP. It is less congestion reduction mechanism get by constrained circular routing. The OSPF and OLSR are no such elimination of unnecessary nodes as compared to CASPER and it is also improvements in terms of throughput and packet delivery ratio during routing of huge data.

In this paper [15] the authors worked on transport layer and proposed end-to-end threshold-based algorithm which extended congestion control to deal with link failure loss in MANET. They have two phases. Firstly the threshold-based loss categorization algorithm differentiates losses suitable to link failure through approximating queue usage based on relative one-way trip time (ROTT) and secondly they regulates RTO for novel route through comparing facilities of novel route to the failure route using information in transport layer such as ROTT and number of hops. This paper shows the problem in-depth by concluding link failure loss state. The reinitialize case the ROTT must be calculated and compared with last maximum and minimum ROTT. The queue usage is compared with threshold. If threshold is exceeds redefined threshold it mean the congestion is occur. If timeout the data packets and ACK cannot reach to the end host that mean the link may be breakage. There implementation describe that the less percentage of three time ACK which come out directly after route recovery may be end result of route changes. The detection of link failure the RTO for reconstructed route through compared with broken route using information that are in transport layer. There simulation result are determined in three metrics the first metric determine threshold-based algorithm for loss classification accuracy. The congestion (AC) for accuracy in classifying loss, link failure (AL) and wireless channel (AW) be supposed to sufficient to prevent misinterpreting other losses for link failure loss. The other feature such as mobility, flow number and loss rare are in AC, AW and AI behave respectively. The simulation result is better than other approaches.

In this paper [16] the authors describe and shows the performance of two routing protocol such as AODV and DSR. In MANET needs more reliable routing protocols because it is critical issue for MANETs. In normal case the AODV was better than DSR. During the constrain situation the DSR was better than AODV. They say that the low performance or packet lose by network separation, link break, collision and congestion in ad hoc network. So the need of quick link recovery by the route maintenance is desirable property of routing algorithm. The DSR protocol have route cache when the most of route are fresh, so route renovate is restricted and it have additional method of route repair such are reply to route requests with cache routes, packet salvage, queued packets designed over a broken link as well route preservation. So they increase the AODV values parameters that have a high accessibility for different routes and decrease rate of elimination process. The algorithm is invoked before the dropping packet in AODV. The algorithm create other route away of all neighbour's present routes. The RREQ will create bye-pass temporary routes for this AODV packets dropping. In this paper the authors highlighted the importance of local route repair routing protocol because the earlier works that are not considered.

In this paper [17] the authors describe TCP congestion algorithm and their performance of mobile ad hoc networking as evaluate the wired networks. They are discus that TCP flow and congestion control mechanism reliable to data delivery. But TCP is not able to handle shared wireless medium such as frequent changes of the network topology and it create some critical issue. So their experiment on the existing TCP congestion control and it performance on MANET to design new algorithm. They have describe performance behaviour of BIC, Vegas scalable TCP congestion control algorithms and these algorithm analysis the efficient data transfer in wireless and mobile environment. The experimental scenario of these congestion control algorithm is very ideal condition without any cross traffic and any additional flows. In MANET scenario the scalable TCP algorithm provided good throughput as compared other algorithms.

2.3 Black hole attack

Black hole attack [18] is a malicious node it is the wrong way replies route request RREQ that it has route to destination node and then it drops the all packet. The harm was the serious at the black hole attack work together as a cluster. In the MANET, it can happen the when the malicious node path directly attacks on data traffic and it is able to change the packet to passing between them deliberately drops, delay and it may be possible to create a node to unrelated packets in the ad ho network. Another kind of black hole attack is to attack on the traffic routing control.

In this paper the authors [19] focus the behaviour of black hole attack of different scenarios, the performance of black hole attack on AODV protocol has analysis to the number of mobile nodes and black hole nodes. The analysis of black hold attack has the bases of different performance, such as packets loss, packet delivery ratio and average end-to-end delay. The authors take two scenarios firstly the total number of ad hoc network nodes are constants and secondly they have black hole nodes to total number of nodes remain constants. Their study focus on three performance matrices such as packet loss it is difference between packet send and received and loss packet counted by how many packet are not reach the destination than observed by black hole nodes, packet delivery ratio it the ratio between the number of CBR packets and the number of received by the CBR sink at the end destination and Delay. it is the average between end-to end sending packets by the CBR resource as well as corresponding of the CBR receiver. Finally the comparisons of these scenarios the black hole attach are effect on AOVD protocol. Effect on packet loss is less than as compare to effect on delay. They analysis the malicious node is the main security attack that effect the AODV protocol performance.

In this paper [20] the authors study the effect of black hole attacks on whole network performance. They use AODV routing protocol and enhanced new routing protocol that improve to reduce effect of black hole node as compared to previous protocols. They have simulation in two scenarios such as without and with black hole attack in the networks and introduced new routing protocol called BlackholeAODV. They used UDP protocol and CBR application at constant packets by the UDP link. The CBR packets size is 512 bytes and sent data rate is 1 Mbyte, the number of nodes is 20. As needs nod 18 and 19 are used to black hole attacks. They were count sent and received packet between each two nodes and then calculate dropped packets at every node including black hole nodes. In the normal simulation packets loss is low. The second scenario they have include black hole attacks in node 18 and 19 node. They assume that how many packets absorbed at black hole attack and calculate through the sent and received packets. The packets drop is the one reason as congestion in those black hole nodes. Final they implemented new routing protocol called IDSAODV. They used RREP message to begin the data transfer except when a second RREP message arrived then they used the new route. After they check there simulation performance improved and used all previously parameters.

In this paper [24] the authors' identify a lossy channel inside a wireless meshes network using conservation of flow approach. They know actually packets through a end to end node is routers and keep a context of graph theory, each edge have a capacity and each edge must be link the other edge for data travelling. A sum of data sent keen on a node should be equivalent to the sum of data received, except for only source and destination nodes. For the balancing of load and security purpose there are many protocols are presented which are floes of incoming and outgoing packets. The watcher is specially talked about conservation of flow in the wireless networks which is state that input must be equal to output. The watcher algorithm is detected to malicious routers, so all routers have to keep up six vectors for each neighbor nodes. The based on these vectors all data which is passing by router. Each router performs this test, on its neighbor that received the counter from each neighbour's neighbor. In this paper they have present and end to end delivery through metrics. Compare the number of total sending packets difference between the received packets and that check through threshold. But the rate goes over then the router is identifying as malicious. In wireless network as compared to wire network, there is collusion and packets dropped are greater. This problem arises through congestion, environment factor, loss channel or malicious nodes; these can be degrading quality of service and network performance.

2.4 Detection of Packet Dropping Attack

2.4.1 Packet Dropping in Wired Network

In this paper [21] the authors presented a distributed network monitoring protocol such as a watcher scheme for design to isolate and detection the network malicious routes. This scheme is same like the law of conservation of flow on the networks. When the all data sent in every node or not deliberate that node and attempt loss the node. As the watcher routing algorithm to detecting this misbehaving the routers it is to observe flows between the neighbours and to the end nodes. Watcher has met the following conditions that are designed to work on network. Such as link state condition: Each router must be agreeing on the accurate topology of the other router Good neighbor condition. Every router must be connected to at least one non-malicious router, Good path condition. Every router must be at least connected by a path of non-malicious router and Majority good condition. There must be majority routers are non-malicious routers. Watchers have two types of counter such as misrouted and transport traffic. Some time each router sum how bytes takes and leave. Each round contains two components. First communication request received and respond protocol and sue for authentication to digital signed. Second validation and conservation of flow by check neighbouring router.

The second component has three parts such as validation, starting checking and conservation of flow. The starting part has router received messages from frequent of routers because it has collected all the responses. In starting checking for the validation it first checks the packets behaviour and then cross-refers the neighbours counter. The neighbours counter for the testing router matches those values. Conservation of flow is through test router which is test on the router. The conservation of flow is used for the packets are properly consumed in the network and also find out and compute the packets difference between the sending and received packets. The total sending packets with on the router and total received packets minus then find out the differences but the rate higher as of threshold valve after the experienced router determine because malicious router. For the duration of detection of malicious route sometime hides its misbehaviour.

In this paper [22] the authors examined the watcher algorithm and show the conservation of flow as well as without adequate confirmation of its assumptions. They enhance the improvement through conservation law of flow. They talk about the different routing attacks because that crush the protocols such as packets modification, packets substitution, ghost routers, hot potato, kamikaze routers, source routing and premature aging that are the attackers. The packets modification the conservation of flow doesn't articulate to what packet keeps to destination and the packets substitution the conservation of flow does not change their ability because per destination does not counter sufficient to detect hole networks. The ghost routers about the conservation of flow nothing using interior configuration nodes to measure the flow, because the router are not only able to broadcast link-state network status messages. If the malicious router present on the network, so it can dropped the packets or controlling source routing. If the intermediate routes will check only whether the next hop is reachable, that intermediate routers arrived under the attack. It will be dropped the packets this router is not identified through watcher. The original watcher specification is very simplicity and this scheme is not to implement into real world networks. Its network size is small or bounded and identifies the malicious in routers drop packets through assumptions.

In this paper [23] the authors identify the problem of detecting routers and explore the design of protocol such as detector. This paper addresses the different threats, describe an efficient traffic validation functions. Finally they present a link-state routing algorithm through isolation of malicious routers. The traffic validation mechanism can be characterized as a predicate such as TV (π, infor ($Rb_{,\pi,}$ τ), infor (r_4, π, τ)). They require buffers to store packets information TV mechanism and also use bandwidth for retransmitting this information packet. This approach is a practically complex. They are divided into five different threats for bad behaviour of router such as packet loss, packet fabrication, packet modification, packet reordering and time behaviour. When the metrics of all these threats value are 0 that mean there is no faulty manner. Secondly synchronization such as collection of traffic information and for detection purposes and distributes the results. This problem solved by a protocol, which is proposed this paper called as π (K+2) protocol. The traffic validation based upon the routers collection information and determine the uncertainly which routers is faulty. The detector router is based on the calculating traffic over time period by pair (r, τ); the mean r was broken down for the duration of time period τ. The collapse detection is found on traffic in sequence through unreliable routers. The π is a path segment so the detector failures return a pair (π, τ). The π (K+2) TV applied only end path nodes segment in Pr. Each x-path segment through a router keep track which is one of end nodes, for some value of x. the proposed path point finding of algorithm with the intention of raising the mistrustful set of routers. This detection the malicious nodes and isolate through these nodes and eliminate the entire pathway that is exceptionally costly designed for realistic implementation.

2.4.2 Packets Drop in Wireless Networks

In this paper [25] presented a watchdog and pathrater mechanism through detecting malicious nodes. There mechanism has two components, first pathrater to avoid those malicious nodes on the routing protocol and each node maintains other node information in the network. Second the watchdog which is make out misbehaving nodes and this technique eavesdrop through passive acknowledgment as well as it keep up buffer of in recent times packets sent and also evaluate each overhead packet through buffer packet. If packet matches, then its entry in the buffer is removed. The packet is present in buffer long time then watchdog not detection this failure, it is detects misbehaviour only forwarding level, not link level. The watchdog have several disadvantages such as ambiguous collisions, receiver collisions, false misbehaviours and congestion etc. watchdog does not work properly it have just hop by hop information routing protocol. The weakness techniques of watchdog are intrusion detection system [26]. The watchdog technique is to watch the next hop of the path and forwarding data this oath or not It well is a malicious node if data is not forwarding. Pathrater will find out reliable path from the watchdog created result. In this paper network division is based on malicious nodes which were found. Every node will maintain a table of number of packets sent and received. Watchdog scheme was develop by maintaining totals entries of source and destination data.

The path is route which is used for the transfer between the data to source and destination. If a node is not forwarding the received data a node detect the malicious node. The source node not send packet to that node and It will choose the alternate path in the route table to send massage to the destination. When destination node will received a source message it will search and compare route table and match some field of message. The value in sum field is equal it means there is not any malicious node else there are chances of malicious node.

In this paper [27] authors are proposing a routing protocol which is detecting and isolating malicious node. The CONFIDENT protocol idea is creation misbehaviour unattractive and to detect faulty behaviour. This is checking the behaviour of nodes. This protocol use the checking misbehaviour through neighbour nodes that watches either listen the passive ACK or receiving the protocol behaviour. The malicious behaviour node information is shared with other nodes.

The CONFIDENT protocol has five different components such as Monitor. Trust manager, Reputation manager path manager. ALARM messages are control by trust manager and also inform nodes about ALARM messages. The ALARM message contains all information of network nodes. Information will be sent to reputation manager when malicious node will be detected. The reputation systems manage an all entries from nodes and used this information for rating. The rating is depending upon the threshold value. Reputation manager update the routing if define threshold is exceeded. When the node rating is change by reputation system than the ALARM message is received by monitor component after this message is passed to trust manager. Significances will be evaluated if the node is doubted to be malicious. CONFINDENT scheme based on detection, alteration and reaction for malicious node

2.5 Selective Forwarding Attack

In [42] the authors proposed an algorithm to defending against the selective forwarding attacks in WMNs on based on AODV routing protocol. They have described two phases; in first phase algorithm identification will be done at threshold counting based. Each node have counter for a packet received from source node. This detection scheme have two types of control packets such as control packet and control ACK. the received packet counter through control packet and compare threshold detection value and than sending control ACK to source node. If positive control ACK packet from destination to the source node, it's means that no malicious node present in network. If the negative control ACK from destination to source and the packet are les then sent packets, it's means that the malicious node are detection. When the source node not received the control ACK from the destination after the Timeout, then the destination node may be malicious or Packets are not reached there, so the source node will originate the Query based localization algorithm. In this paper they presented the estimate of performance on the bases of different scenarios such as A single attacker present in the forwarding path, colluding attackers present in multiple forwarding paths between source and destination and analysis of detection threshold, relative routing overhead of proposed algorithm.

In this paper [28] authors proposed a sequential mesh test scheme, which detect selective forwarding networking and this scheme is working over cluster base network. The scheme nature used is centralized. In a fix interval data message not forwarded. They select another path and identify the dropped and inform cluster head. The sequential mesh test base scheme is run on cluster head and the packet; identify the malicious node which drop packet. To run sequential mesh test select small quantity of samples. They select a sample as to select as whole. It decides if continue the test or not based on the test results until the final conclusion. After sending the data packets in wireless sensor node should identify to the networks selective forward attacks. If the source node absorbs after a fix time of period its intermediate node drop packets. The sequential mesh test base scheme runs on cluster head against the malicious node after receiving the packet dropped, and small quantity of samples to run the test this sequential mesh test, instead the whole time of test. The decision in based on test not based on conclusion. To detect the selection forwarding attack [29], wireless sensor nodes should listen to the network after sending their data packet. If sender node observed has not observed that packets are not forwarded for a fix time, after the period it suspects that the intermediate drops packets, this report is transmitted to cluster head using another route. This detection scheme is based on sequential mesh test method. Basically this is a hypothesis test, it depends upon the ratio of packets dropped and cluster head decided either this node is selective forward attack or not. This detection scheme's packet drop rate is higher than any other packet drop scheme.

In this paper [29] the authors' proposed Channel-aware algorithm will use to build this algorithm which will identify the selective forwarding node. This detection algorithm has two phases such as channel estimation and traffic monitoring. The normal failure is detection through the process of estimation channel and real loss rate is check by traffic monitoring. However the monitored loss rate at certain bound go over the estimate normal loss rate, these individuals nodes included will be recognized as an attackers. Furthermore they take away analytical learned shows that to establish the optimal detection entities that reduced the summary of false alarm and missed detection possibility.

In this paper [30] authors proposed a Channel Aware Detection algorithm for detection of colluding selective forwarding nodes in wireless mesh networks. The first phase it detects malicious nodes using channel-aware detection (CAD) algorithm used in identifies malicious behaviour of the node from losses. The second phase is detection of colluding nodes and used the analysis the suspicious nodes which is already detected in the first phase. The main objective of first phase is channel estimation and traffic monitoring. The channel estimate calculate upstream/downstream optimal detection threshold. The first phase, two types of packets, PROBE and PROBEACK are use to detection of attackers. Furthermore this method provides better detection of attacks in WMNs.

In this paper [31] the authors present a location aware multifunctional key management framework of implementing data security in wireless sensor networks. They detect the selective forwarding attack as well as information for large scale in WSN. The area is divides in to two groups such as gird and cells. The location aware area is without troubling end to end data security that effectively cooperate their surrounding nodes. The both ends and node to node authentication guarantee through multifunction key management framework. They have done an extensive analysis using the design that demonstrates highly resilience that is against the increasing no of compromising nodes. That is effective for energy savings. This model saves more than 85% energy without any changes in model. Further those in paper two algorithms have been used MD5 and HMAC. Those are efficient for data security ways. MD5 algorithms generates HASH, which is called "Digest" HMAC gives a message authentication but HMAC also generate which is called "Message Digest" and that is dependent on message length. Which is send by node? Send time is lass and data delivered at authorized user. These two algorithms have many advantages. Such as Code runs fast because of use of Hashing technique, HMAC algorithm developed confidence between sender and receiver and the sensor energy utilized minimum, save energy.

2.6Auxiliary Approaches

In this paper [32] the authors have presented a light weight defence scheme for selective forwarding attacks which is distributed in nature. The proposed lightweight scheme uses neighbour nodes to monitor the communication of every packet to detect selective forwarded attacks between two nodes. The source node detects the even packets through even packet communication and originated it and forwarding this packet to next hop node. This even packet determined through OPA_uvmts algorithm. The next hop node called intermediate node which received even packets. At that time the neighbor nodes monitor all around data that sending and receiving. The even packet is forwarding through intermediate nodes. The monitor node is responsible to detect the selective forwarding attacks. When selective forwarding is detected then it again the even packets generate and transmit to destination node and generate an alarm message to all around neighbour's nodes for notifying the location of attacks. It starts a time for attackers through monitor Deal algorithm. If the even packet relate the timer in the cache, the monitor generate a new route which is different from old route and forward even packet to neighbor through the route. The neighbours give location from which neighbor get packets. The process of the notice packet is that the monitor node finds the attacker and generates the notice packet which includes the notice packet which includes location of the attacker. The monitor sends clock wise the packets to neighbor which are adjacent to attacker. The neighbor nodes adjacent to attacker receive the notice period and neighbor nodes indentify the attacker node, they stop the notice periods to send to that direction. In this paper the authors made some assumptions for network model. Like after development, the location of node will not change any more, the active node listen packet from one hop node. Finally the even packet transmission process from source node to destination node may be the packet suffer from selective forwarding attack.

In this paper [34] the authors designed an intrusion detection to detect black hole and selective forwarding attacks in WSN, based on local information, They introduces a specification based intrusion detection system where policy is describing which drawing behaviours to normal and abnormal. There IDS based approach for detecting selective forwarding and black hole attack search only be a rule on the number of packets being dropped by malicious node. They structured the network model as a tree. In tree structure the whole network is grouped into clusters. In WSN have different characteristic such as each nodes have certain information that help in detection of attacker in network, associate surrounding node, nodes work together with cluster head and monitor surrounding nodes for detect malicious nodes. The clusters have moderately overlapping and each cluster has a leaf of the tree and the parent of the cluster is a part of the cluster called a cluster head. There network contain four types of nose such as Malicious node (not functioning properly these are helper nodes for malicious node to break in the security of network), Watch Dog (watch the communication link their neighbours and details their pointer to Cluster Head for decision making), Cluster Head (based on feedback from watch dog, it have decide any a node is performing normally or abnormally), Normal Node (back bone of WSN for transmitting the data to the base station). In the simulation they have set the parameter values such as 100 communication node, 30 Watch Dog, 10 Cluster Head, 10 number of Clusters and 100m of length and width. In the simulation they have 10 watch dog nodes per cluster if increasing the number of watch dogs increases the detection of probability and simulation show that 3 watch dogs per cluster are sufficient to detect the attack. This future scheme contains instruction detection, decision making, calculating the potential through watch dogs and calculating the possibilities thou WSN [35] is being used in different environment like military, emergency, natural and embedded environment with respect of security. WSN is deployed in unprotected and open environment so different preventive mechanisms are used to protect it from different attacks. Sometimes tough methodology is applied in the environment where attack detection is not easy so IDS is defensible in such situations as the chances of DOS attack. A preliminary Intrusion Detection System (IDS) for WSNs is proposed in paper that handles security aspects of DoS attack and fulfil security demand and restriction of the WSNs. During the DOS attacks network availability and WSN is becomes big issue IDS with limited number of nodes is design to help communication without involving malicious nodes and it also secure from threats for achieving this goal more research can be done. Radio interference is considered one of the possible methodology for DoS attacks and an algorithm similar to radio interference detection and avoidance algorithm is also used. Path-based DoS attack can also be handled with it and a non agent based wireless sensor node that shows network status at the time of DoS attack by detecting attack is also implemented. In Future by generating dynamic base line of network traffic anomaly detection pattern can be made better in Active IDS implementation that can be vigorously compared precisely by current measurement of network load to determine DoS attack that dipping the rate of false positives during the use of our IDS.

MAC addresses or uniquely generated hardware IDs can be used in implementation of unique identification mechanism to find out malicious node precisely that is used in encryption to enhance security. An encryption scheme that based on Real WSN environment can also be implemented and in spite of performing notification and communication by broadcast message throughout the WSN message can be send to the desire node that will reduce the traffic load in between wireless sensor nodes.

2.7 Limitation of Existing System

Now, approximately all of mobile ad hoc networks protocol has lack built-in security mechanism. The real networking environment these routing protocol are often expensive.

In hughes [22] observed the watcher [25] protocol, for the detecting misbehaving routers. As watcher algorithm is not suitable to be a security mechanism in routing protocols, the watcher is design only assumption identifies through the conservation of flow so it is defeated. The watcher strength is examining through applying different attacks on router such as packet modification, packet substitution, ghost routers and source routing etc. All router evaluating the protocol result the network topology and there is not broadcast packets presently accounted which in the watcher algorithm.

In Manet's research area the major problem focus on the black hole attacks. The attacker used the shortest path or highest sequence number whose packets it's wanted to drop. In [confident,] have also some limitation. The confident scheme is also follow the watchdog scheme and it change minor changes. Another side this scheme is also improves other protocols. In MobIDS used the threshold values and those automatically detecting malicious nodes during operation. They have expansive sensor nodes develops cause for detection is very quickly and fast.

In [15,23,24] even if detection of previous approaches is a good but the malicious node still present in the network and some other countermeasures need be hold to detect and isolate them form network. Furthermore, detection of malicious node scheme must be intelligent sufficient, thus that they can differences between packet dropping through malicious node and other reasons such as congestion, network failure, collision, buffer size full and bad ratio detection etc.

2.8 Summary

The literature review shows that the majority of work done the detection of black hole and selective forwarding attack in wireless sensor network. For few paper work done only mobile ad ho networking. The black hole attack detection process is easy as compare to selective forwarding attack because it is intelligent just drop few packet. The mechanism of simple wire we never used in MANETs. We have to require a speared scheme which can use for MANET. According to previous work our attack is more intelligent because it stay on network as long and its detection also difficult than others attacks. There are lots of proposed scheme but these are not enough.

Chapter 3

Problem Domain

3.1 Introduction

A mobile ad hoc network is a group of mobile nodes that lack infrastructure and are decentralized in nature. This lack of centralized structure and type of their realtime model having dynamic topology, leads MANET to be more vulnerable to several types of attacks than other network types of wireless. In effort, to secure communication a number of security techniques have been proposed to solve these vulnerabilities and malicious actions, in near past as discussed. However, still the presented approaches have their limitations and that is the very point where we intend to target for a more robust solution.

In this chapter we will focus on the requirement analysis of our research problem. The rest of section 3.2 we will discuss the network attacks in depth. We will discuss about problem statement in section 3.3. The focus of research will be highlighted in the section of 3.4. The section 3.3 will contain the final observations in the form of summary.

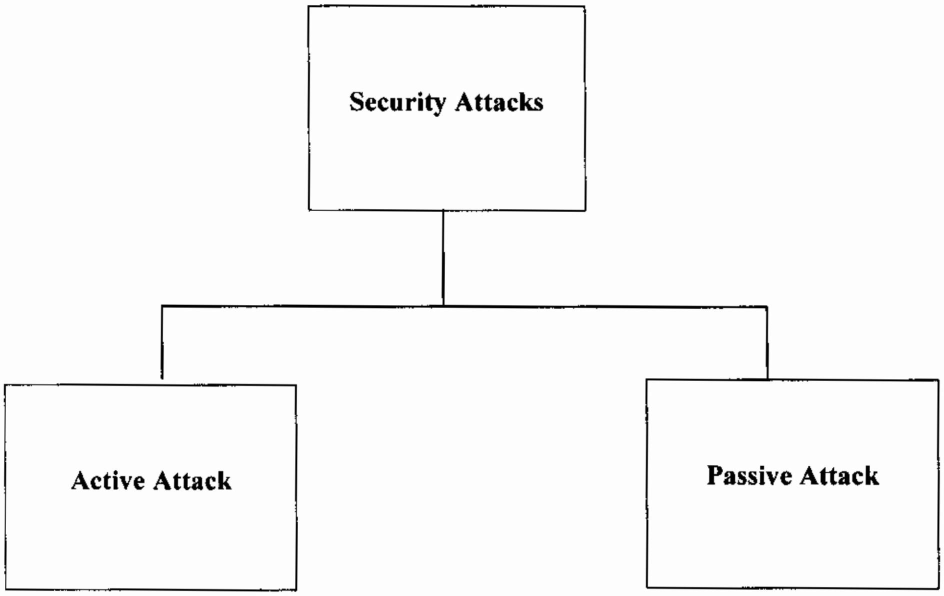

Figure 3.1: Classification of Network Attacks

3.2 Network Attacks

In mobile ad hoc network attacks [8] are a lot additional hard to detect as compared to wired networks. The MANET attack can be classified into two major categorizes, as shown in figure-3.1, on the basis of the source of the attacks such as internal or external and on the behaviour of attack such as Active or Passive attack. Passive attacks do not disrupt or exchange data in the normal operation of the communication network. It just listens to ongoing communication to get useful. In active attack the opponent disrupt the whole performance of the network. It involves information modification, fabrication and interruption. This attack can be both internal or external attack such as infection of the external attack is meant to destroy the network performances, whereas internal may be to get more share of the inclusion for itself.

3.2.1 External Attacker

Figure 3.2 shows the external attack which is actually present outside the network. It is not part of the local network, but wants to be part of the network. Once it gets part of the network, as disrupt the performances of the whole network such as starts sending it bogus packets, drop the packet and all denial of services that affect the network. The counter comes of this attack to implementing security measures such as firewall etc.

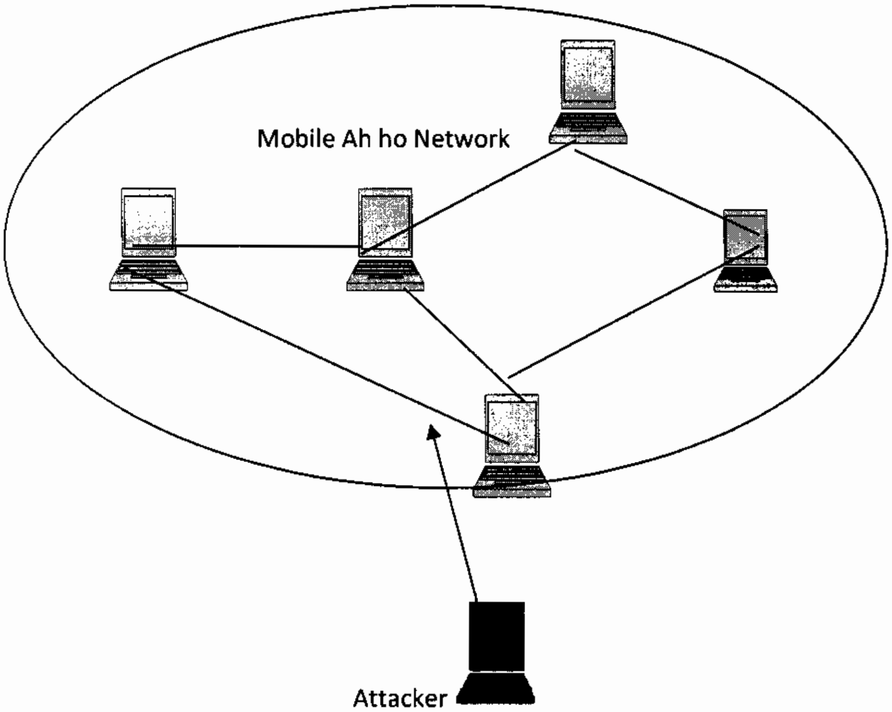

Figure 3.2: External Attacks in MANET

3.2.2 Internal Attacker

Figure 3.3 shows the internal attack where the opponent wants to attain normal nodes right of entry to the network as well as join in the normal actions of the network. These attacks are not intended to join in the network operation but the aim is to create network congestion, denial of services or disrupt the whole network operation. The internal attacks are launched formally by the misbehaving nodes. It is more severe type of attack than external attacks.

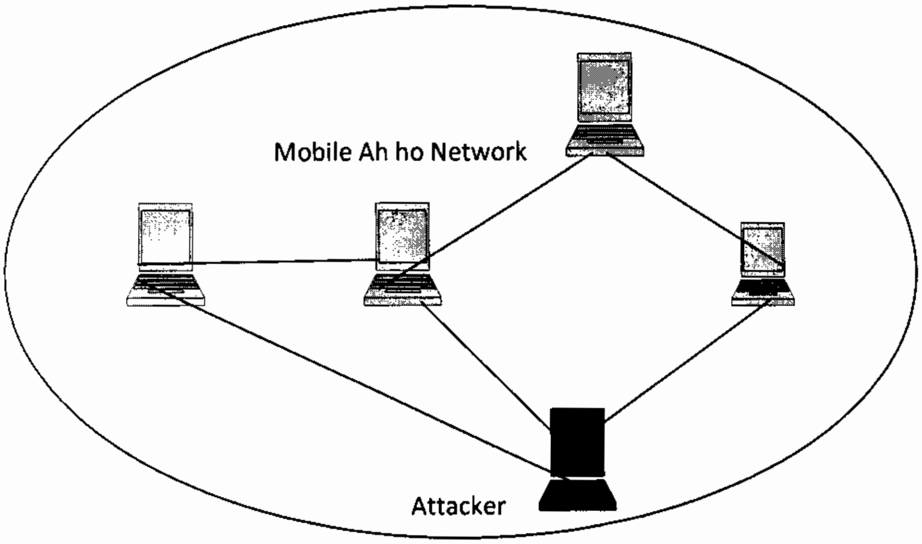

Figure 3.3: Internal Attack in MANET

3.2.3 Typical Routing Attacks

MANETs are critically vulnerably to diverse type of attacks. The fully network decentralization, absence of support infrastructure and dynamic topology increases a more vulnerability such as black holds attack, selective forwarding attack and wormhole among others.

3.2.3.1 Black Hole Attack

Black hole attack is very dangerous for ad hoc network. It affects the performance of whole network [39, 40]. In this malicious node plays a bluff and shows it has a smallest path to the destination. For example node S wants to send message to D during route request process node E which is malicious would claim that it has original and small route to D. The node "S" will think that this is the shortest path of the route and then ignores all other responses and will send the packets to node "E". The malicious node "E" after receiving all packets will drop. Looks, it repeats whole process after nodes too,

3.2.3.2 Selective Forwarding Attack

As compare to black hole attack the selective forwarding attack [33, 37] is very hard to detect because it not first time dropped all sending packets. A malicious node can be selectively dropping only few packets without forwarding them to destination. When a source send to transmit packet to destination it first send broadcast route request to the neighbouring nodes. The malicious node tries to join the element of network and get the route request message. The source node is after get the RRQ by the destination it transmits the packet. Malicious node is also present in network and it gets packets and drops them.

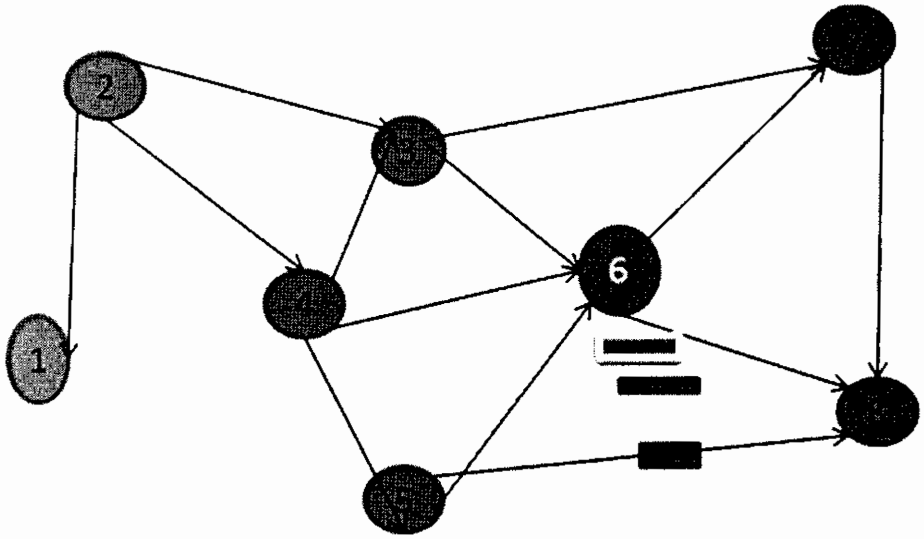

Figure 3.4: Selective Forwarding Attack

3.2.3.3 Wormhole Attack

Wormhole attack [38] are malicious threats to MANETs routing protocols, an attacker recorded a packets at one location in the network and replays them in a different parts. So routing protocol may be disrupt and the channel between two conspire attackers is referred as a wormhole attacks.

3.3 Problem Statement

Based on the analysis of the related literature the problem we intend to get a serious hybrid approach that detects the selective forwarding attack in ad hoc network, an intelligent attack where the attacker disrupts communication for much longer period without being detected easily [2]. Generally such type of attack is found in WSN but our objective is whether the said attack is also applicable and efficient in MANET where no central entity like cluster head exist.

In MANET forwarding packets go through many resources. Misbehaving nodes drop a packet as well as some connection errors create uncertainty due to which misbehaving nodes identification is difficult [9]. Due to lacking of authentication mechanism and access control network performance is also be affected. Due to protection some mobile devices don't rout to packet forwarding [8].

Several security issues and threats exist in MANET where nodes are independent and communication is by means of cooperation via neighbours or intermediate nodes that are our focused issue. While selective forwarding occurs due to cause of congestion and collision. Where the malicious node drops selective packet without forwarding them to the destination that is called selective forwarding attack. With the purpose of reason to hamper the QOS of network layer; so network layer performance is also reduced [3, 42].

3.4 Research Objectives

The focal points of this study can be summarized as:

- To develop a solution for handling intelligent attack in MANET and its effect.
- In view of the existing techniques, discussed earlier, need is either to enhance an existing technique or come up with a hybrid approach.
- In the absence of a central entity, the proposed methodology should be distributed in nature.
- Once, the proposed technique is tested for its reliability and robustness, can be optimized for energy constraints and lightweight; thus can be deployed to other forms of WLAN.

3.5 Summary

In this chapter a specified study on the problem domain is presented. There are many schemes being used for detection of malicious nodes such as selective forwarding attack. It is very important for MANET because packet dropping is degraded and QOS is also affected of the legitimate nodes, being member of the network. However, the need is to come up with a proposed solution which not only is based on fewer assumptions but is robust in a sense that minimizes the false alarms.

Chapter 4

Proposed Solution

4.1 Introduction

In design phase we had given an architecture which is require for any application level implementation. Main reason of design implementation is to design and test it within in actual boundaries which will be encountered in real environment. This research was conduct to find out strong security mechanism in Mobile Ad hoc network as they are used in uncertain and not fixed environment. Security in mobile ad hock requires specific attention as it has great effect on mobile networks function. Therefore, it is the requirement of the time to have a dynamic and real time security mechanism for wireless ad hoc networks.

The purpose in this chapter is to identify the basic requirements and needs of the proposed scheme, which will held in the system building. The need of the design and reference architecture of the proposed scheme is talk about in section 4.2 and 4, 3 respectively. The methodology/algorithm will be discussed in the sections 4.4. The closing remarks of this chapter are concluded as a summary in the section 4.5

4.2 Design Requirements

This research design handles malicious nodes as well as congestion in mobile ad hoc network. In this section, log files, threshold and routing table, the basic needs of proposed architecture will be discussed.

4.2.1 Log Files

In mobile ad hoc network each nodes have actions and tasks. If the nodes is malicious it is identify through the collection of all node information. Effected nodes are removed from network this loss of packet is considered due to attack but it was caused by congestion. Reason of packet loosing will be detected..Node will maintain log file for its normal function records.log fill have all record of incoming out going and number of packets.

4.2.2 Threshold

The threshold mean, which the network traffic level that within the host of network. Network eccentricity is due to malicious movement and congestion happens due to it. In this architecture different threshold value will be used.

4.2.3 Routing Table

The packet loosing are shows the routing table of the level of network traffic. The network traffic eccentricity accepts to be a malicious movement or due to congestion happen. The all nodes packet record is putting the routing tables and comparison among the all node table box.

4.3 Reference Architecture

Several security issue and threat are exits in MANET. In MANET all nodes are independent and communication is controlled by neighbours or intermediate nodes that are our focused issue. While selective forwarding occurs due to cause of congestion and collision. Where the malicious node drops selective packet without forwarding them to the destination that is called selective forwarding attack. If all packet drops then that is called black hole attack. .

- If the number of packets received by node exceeds its Queue size, they will be dropped.
- If the node will be out of rang or off due to power then it will not be able to receive and forward the packets.
- If the multiple nodes send packets to the node in same time the node will be exposed.

4.4 Proposed Approach

We have proposed a hybrid approach that detects the selective forwarding attack in MANET. Our scheme is based on traffic validation of transmitted data, either on the basis of acknowledgement received or passive monitoring in TCP & UDP based traffic, respectively. Our scheme comprises of a hybrid mechanism through which packet dropping will be tracked on lossy nodes and thus will be able to differentiate between congestion and attack.

We propose a system which tackles all these issues, after detecting the attacks. Data flow chart shows the process of our research work for controlling selective forwarding attacks or the tackling process to this issue.

When problem occur to detect that problem we design a matrices in which total sent packet are equal to received packets. If these are not same then malicious node is present in network, we will detect this node by using the matrices, we propose two layers to detect this malicious node. First we consider whole network as global, in which we check whether a malicious node has been detected or not. If it has been detected then we see local position of malicious node. For this whole process we use a hybrid approach.

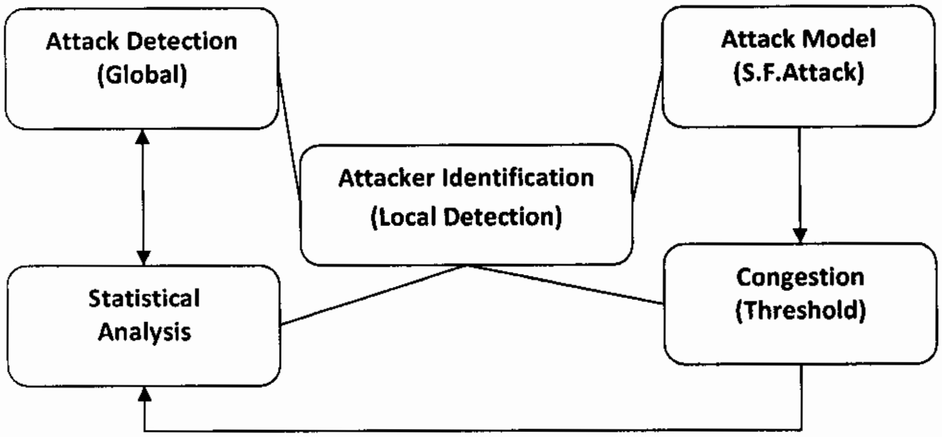

Figure 4.1: Hybrid Approach

The figure 4.1 shows the proposed hybrid approach used for improving the security solution for ad hoc networks using AODV routing protocol. Our approach can detect and identify the selective forwarded attack in networks.

In this hybrid approach we use techniques of confident [27] and lossy [24]. To find the selective forwarded attack we use threshold on node. The congestion environment formed in two ways. First is normal congestion and second is congestion with attack. If the packet drop rate is less than a particular threshold, it will be considered as normal congestion. When packet drop -rate crosses that threshold it will be considered as congestion with attack, and localizes the nodes/ area where problem occurred, later our identification method is triggered in that area only; to minimize network packets and overhead.

4.4.1 Methodology

We intend to adopt hybrid approach for detection of selective forwarding attack, to our proposed hybrid methodology. We have selected this methodology because it take care the performance of networks to communication process that we have highlight in the literature review. First we consider a whole network as Global in which we check the selective forwarding attack detection or not.

Tested for congestion with attack environment classify in to two main categories.

- Global Detection
    - Avg.Packet Drop x 'X' > threshold then node is malicious

    - Start Monitoring

- Local identification
    - Avg.Packet Drop x '2X' >threshold then node is selective forwarding attack
    - Black lists the malicious node.

The proposed methodology will take as input data from the attack model and will statistical analysis those input data to establish a particular type of thresholds. The different thresholds will be defined to detect the selective forwarded attacks. Final we designed a matrices through statistical analysis [31], which total send package is equal to the total received package, such as we consider whole network as a global, then we see local position of malicious node [30].

4.5 Flow Diagram

In this research we detect the malicious node through threshold (T.H).firstly we check our normal threshold value and congestion value are same. If our threshold value is lower than normal value then it is declare as NORMAL scenario. If our threshold value is double of normal threshold value it means malicious node exits in network. If our threshold value is double of our detection threshold value it starts malicious node identification process. This identification process is done by watchers.

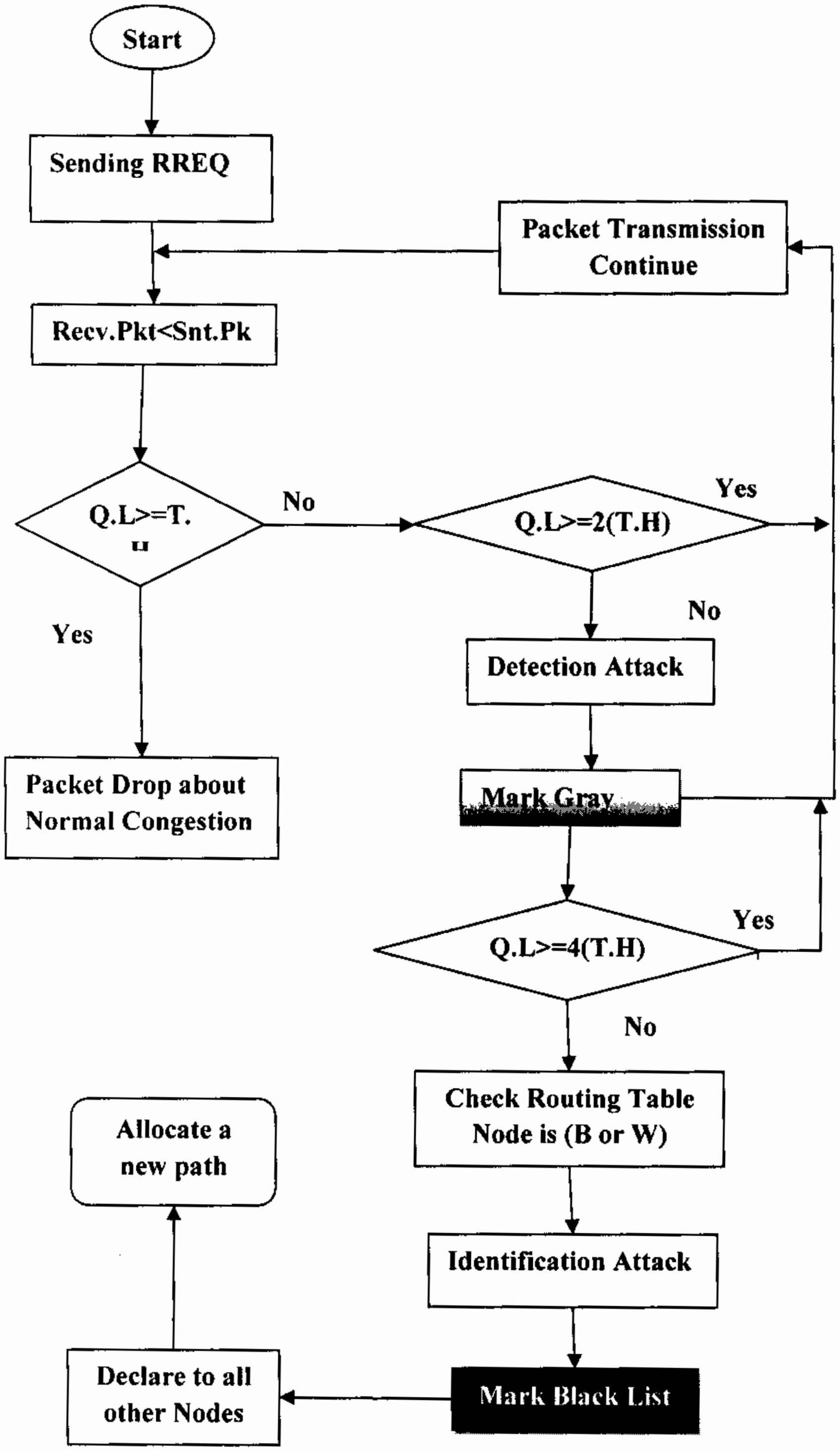

Figure 4.2: Flow Chart of Proposed Architecture

4.6 Proposed Algorithm

In this mechanism source node used fresh route to the destination by checking it in routing table. Source node broadcast RREQ message. Attack node has highest sequence number in RREP message. As it has highest number source node sends data by considering it as destination or intermediate node. Black will eventually all packets and start dropping it and destination will not receive them.

QL:	Queue Length
Th:	Threshold based on congestion
NL:	Node-list
MNode:	Malicious Node

Pseudo Code

```
    Initialize Network();
    Setup Routes ();
    Init Normal_Comm();
    Set QL;                  // for congestion
If (QL > TH)
   Normal Scenario;
Else
   Congested Scenario;

If (QL < $\alpha$*(TH))                           // where $\alpha$ = constant
    Keep Montior (period);
Else
        Init Global_Detect(NL);

Repeat:
If (Globlal_Detect == TRUE)
{
   Locate Packet_Drop (node);
   If (node != clean)
      Init Local_Detect (node);
}

Period:
   If (Q.L< $\beta$* (T.L))                            // where $\beta$ = constant
       Local_Detect (MNode);
  Else
  {
       Black List;                            // Identified Malicious Node
       Enqueue (Arr_pkt); Succ_Drop_pkt ();
    }
```

4.7 Summary

MANET can play an important role in our daily life. In the MANET there are more security issues as compared to others due to its lack of infrastructure and dynamic technology. That why it is more unsecure. Here a data this can transfer from source to destination by intermediate nodes. These intermediate nodes use as a router. If any misbehaving or incorporated these nodes with others then data will never send. So our network performance comes to degrade. They are different form if the attacker is black hole then it completely drop all packets. And it is selective forwarding attack then it will drop packets selectively who live/ stay here for a long time. if the attacker id grays it drop the packet certain nodes. So there arc different forms of attackers which are effective on the network. In this research we have set numerous goals or objectives. We are represented a specific hybrid idea which we have include some other scheme features. We have included some parameters and use analysis this attack for global and local. According to the result between local and global we detect attack for different scenarios. We do the analysis of result as layered wise because we implement hybrid scheme on each nodes.

Chapter 5

Simulations and Results

5.1 Simulations

In this work, we have tried to evaluate the effects of the selective forwarding attacks in the wireless ad hoc networks. Different simulators are used to design MANETs, i.e., NS-2, OPNET, GloMoSim and Omnet++ use for designing MANETs. In our statistical part, we have used Omnet++ version 1.1 to design mobile ad hoc networks.

5.1.1 OMNET++

It is a discrete event network simulator, which is object oriented modular; the simulator used the following features.

- Modeling of Routing Protocol
- Network Modeling queue
- Network tele- communication is traffic modeling
- Hardware architecture.
- Other system modeling which discrete approach is suitable.
- Distributed hardware systems.

The interface tools of OMNET++ [41] are portable, they allow network model to be ease. It also +works on UNIX system and used in windows as well in different C++ compilers. Parallel distribution simulations communication frame is provides C++ compiler.

The OMNNET is hierarchically nested module. The nested module mean it allow logical format of actual real system easily. Parameters are passing through communication to each other is very complex in the messages. Theses parameters are modified for topology behaviour. Parameters are like a gates and sends messages and communication through every module.

There is some OMNET++ simulations feature that changing user interface of function such as debugging expression and batch execution. These can be very helpful in simulation projects development. The demonstration of model working is also assist by user interfaces.

The various C++ compilers are used on both windows and multiple UNIX, as simulators can operate in both of above operating systems because of that the simulators are portable. The distributed parallel simulation is also supported by OMNET++. To establish communication between partitions of parallel distribution simulation OMNET++ can use several mechanisms.MPI and pipes are some of the examples. It is easily extended simulator and these models do not need any special instruments to be run in parallel. For parallel simulations GUI is also used.

5.2 Hierarchical Modules

Basically the OMNET++ is contains step by step modules. This model is communicates by connecting system to anther system. The initial level module is the system module that can also consists by sub modules. This kind of module is not limited by user that allows reflecting the logical structure of the actual system in the model structure.

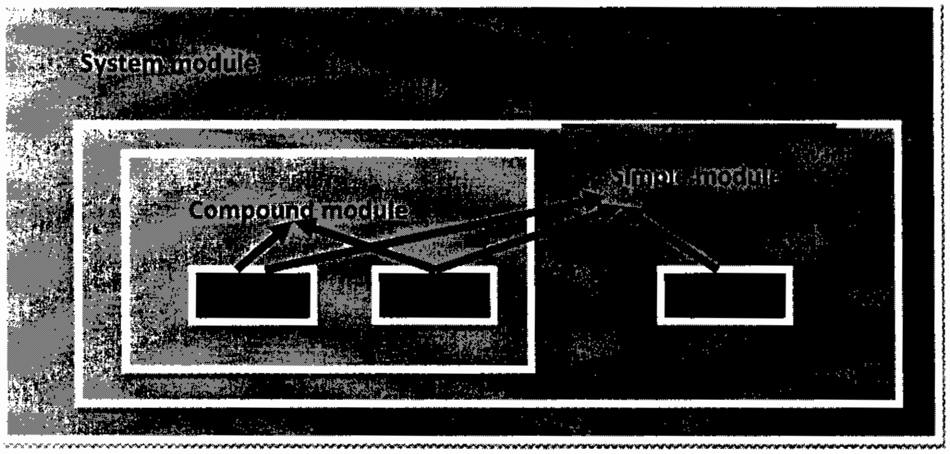

Figure 5.1: Compound and Simple Module

Modules are divided into sub modules called compound module, which is in opposite to the simple modules. According to the module hierarchy simple modules are at the most lowest level.

5.2.1 Module Types

There are two module types such as simple and compound. If we telling the model, the user classify module types; the example of modules types provide because the component for further difficult module types. When users work on system module it is also used of an earlier module types. It is no partition whether it is a compound or simple module because the uses of building block. In actual usage module type stored all files separately, for this means the user can uses the existing group modules and libraries.

The module hierarchy which is create with single level for each link. One in compound module each connects the two sub Modules. The messages move through sequence of connection, originating or reaching due to the structure of hierarchical method. The router whereas as connection go to simple module to simple module. Compound module is called cardboard boxes. Which represent the transparently communicating between inside and outside world?

5.2.2 Modelling of Packet Transmission

The communication network modelling, for this connection there are assign three different parameters and these are optional, such as propagation delay parameter, bit error rate and data rate. The message arrival channel is propagation delay parameter. The bit rate is identifying noisy channel and incorrect travel bit. The determining the transmission rate of packet is bit per second through data rate.

OMNET++ provides technologies, protocols, communication devices for academic research, assessment and improvement. It is efficient, robust and highly reliable which grant the user the ease of graphical interface, developing and running the simulation and validation of the results.

5.3 AODV Routing Protocol

The Ad-hoc On-Demand Distance Vector (AODV) [3, 4] routing protocol is created for use in Mobile Ad Hoc Networks. It is a reactive protocol, if route are needed then create a routes. The AODV important feature is that maintenance of time-based states in each node and not use expired routing entry. The neighbours can be identified in the case of route is broken. The presented networks are bases on the AODV implementation. Figure 5.2 shows the route discovery in AODV.

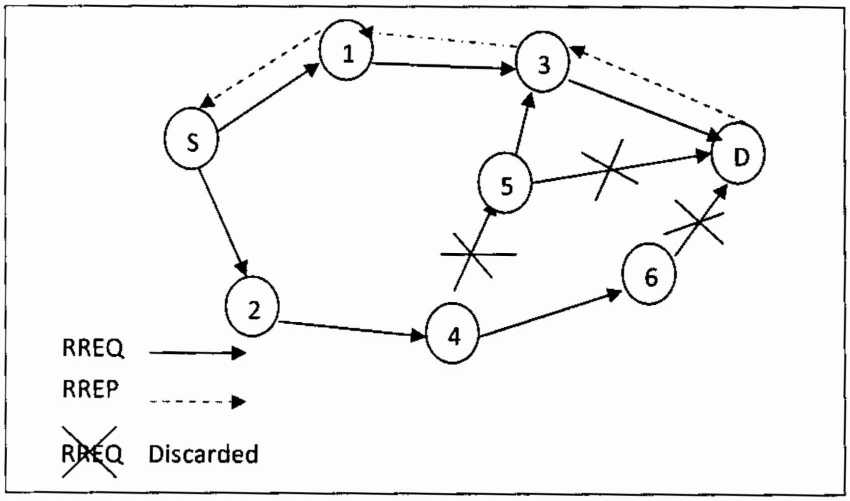

Figure 5.2: Route Discovery in AODV

Figure 5.2 each network nodes maintain a routing table entry for each destination. Routing table maintain the following data.

- Destination node
- Next hop
- Number of hops
- Sequence number for destination
- Active neighbors for this route
- Expiration time for this route table entry

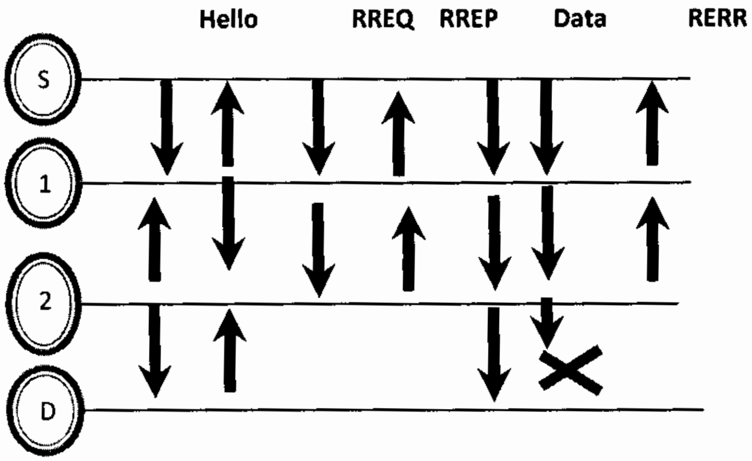

Figure 5.3: Messaging Exchanges of AODV Protocol

The figure 5.3 illustrates the messaging exchanges of the AODV routing protocol. Firstly the hellos send for detect and monitor links to neighbours. Each active node periodically broadcast the hello messages for all its neighbours, if a neighbour node not passes to get hello messages as of a neighbour that indicates a link break. Secondly, when source send a data to destination, firstly it broadcast RREQ message for the destination. If the intermediate node is not destination, it rebroadcast the RREQ. If the RREQ message receiving node is destination, it create a RREP message, RREP message is uncast in a hop-to-hop way for a source. So a RREP message is transmission, each intermediate create to a route for a destination and then it records this information in routing tables and can being forwarding data and also select the route with the shortest hop count is chosen. Thirdly as the data transmits from the source to destination, each intimidate node along the routes table updates the timer with the routes to source and destination. Finally if the data is travelling and a link break detected, a route Error RERR message sent to the source of data in a hop-to-hop way.

HELLO and RERR messages are utilized route maintenance, while route discovery through RREQ and RREP messages. Figure 5.4 shows the basic AODV protocol flow chart:

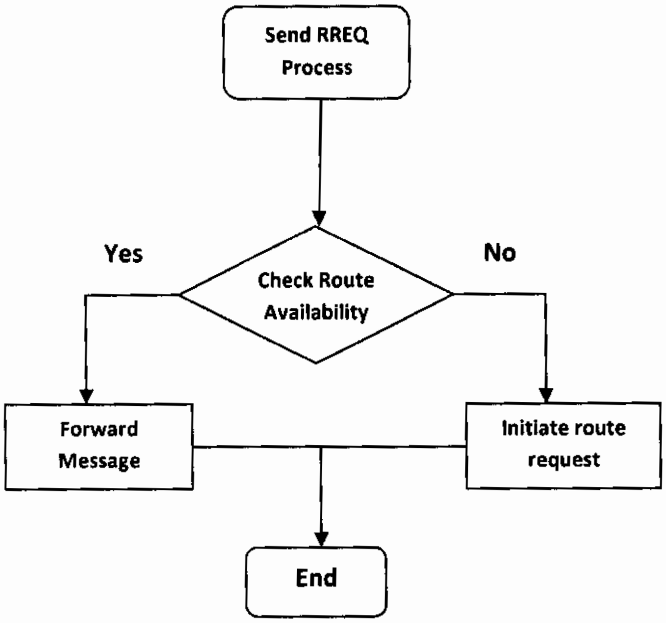

Figure 5.4: Basic AODV Protocol

The above figure 5.4 describe, if a source node A send a packet to a node F, firstly check route accessibility, then presumptuous the packet to the next hop. If it does not have a route, then it again initiates the route request by AODV protocol.

5.4 Simulation Environment

We have tested our implementation of the selective forwarding attack to see whether it is correctly working or not. To be ensuring the implementation is correctly working, we used the Omnet++ application. To test the implementation, we used two simulations. In the first scenario we did not use any selective forwarding attack on Mobile ad hoc networking. In the second scenario we added a selective forwarding attack in Mobile ad hoc networking. Then we concluded the results of the simulation.

5.4.1 Simulation Parameters

For simulation , the number of nodes is varied between 8 to 15 and are randomly deployed in a area of 250m*250m, simulation time is 15min, 20min and 25min respectively. Simulation parameters are shown in the table 5.1. Parameters considered for simulation that we take from different related literature such as lossy [24] and shila [42]. The metrics we considered from two forms such as global detection and local identification for comparison are packet delivery ratio and packet drop ratio in the presence and absence of selective forwarding attack.

Table 5.1: Simulation Parameters

Parameters	**Values**
No of nodes	8-12
Number of malicious nodes	1
World size	250m*250m
Packet Size	1024KB
Traffic	CBR
Routing Protocol	AODV
Wireless Standard	802.11b
Data Rate	2Mbps
Traffic Load	~5pps

Our first simulation scenario environment is ideal, where there are minimum amount of selective packets drops, which is consider in normal network scenarios and congestion. The second scenario we consider some congestion with threshold values in simulation. For simulation we have remove a selective packets drop rate on attack nodes.

5.5 Results and Discussions

In the first scenario where there is not a selective forwarding attack node, which is normal congestion case of a mobile ad hoc network. Whereas the second scenario where there is presence of selective forwarding attack, which is congestion with attacker. For sake of simulation, we have use a our hybrid approach that detection is from in two way such as first we consider the whole network as a Global in which we check whether selective forwarding attack are detected or not. If selective forwarding attack detected then we see local identification position of selective forwarding attack. Through this whole process we will try to statistical analyze the impact of selective forwarding attack identification use hybrid approach in an environment. The threshold value being consider in the this scenario is 7-9% error rate.

Since the selection of sender node, receiver node, the number of packet to be sent and packet drop rate are all random.

5.5.1 Case I: 8 nodes Scenarios for Congestion Environment

For an 8 nodes network topology a simulation of 15min, 20min and 25min are respectively was manipulated. For the sake of understanding, the normal congestion environment we test the three different scenarios. These different scenarios, we proof the normal congestion how actually packet will drop. In the normal congestion the packets drop rate is maximum 3% consider.. The network diagram is demonstrated as shown in figure 5.5.

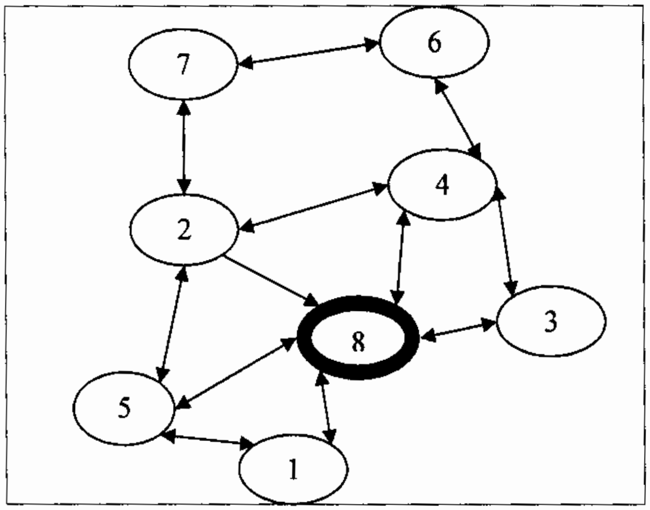

Figure 5.5: 8 nodes Network Topology for Simulation Case I

5.5.1.1 Scenario I: 8 Nodes, Simulation time is 20min

In this scenario the total sum of data pass through on the network is approximately 39,000, in this period the sum of total packets received at each node were approximately 38,000. Figure 5.6 shows the overall number of packets dropped by each node in different links; which make around 2.4% of the entire data packet.

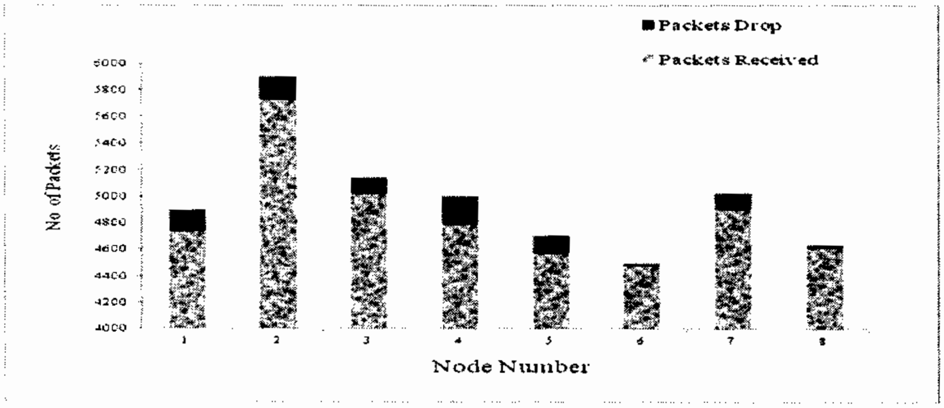

Figure 5.6: 8 Nodes Scenario I: Nodewise Throughput Packets Received and Dropped at each Node of 20min

5.5.1.2 Scenario II: 8 Nodes, 25min

Scenario II we just extend the time then again run in 8 nodes topology networks and environment is also normal congestion. Figure 5.7 shows the total data packet arrived in on the network is approximately 50,000, and received at each node were approximately 49,000 .in this duration the overall number of packets dropped by each node in different link; which make around 2.3% of entire data packets.

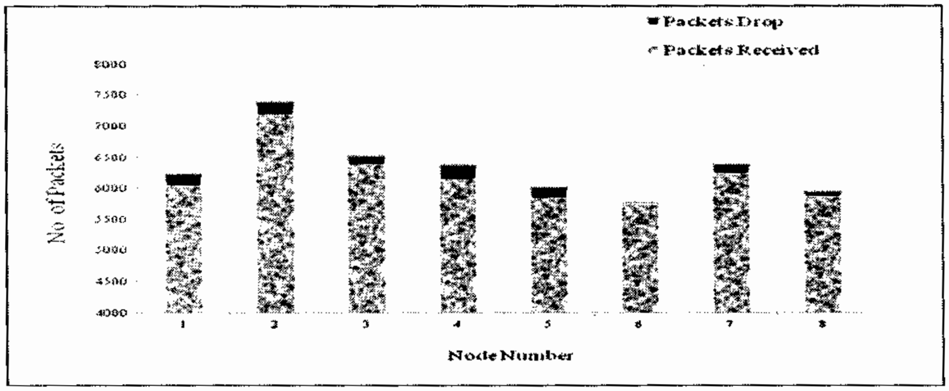

Figure 5.7: 8 Node Scenario II: Nodewise Throughput Packets Received and Dropped at each Node of 25min

5.5.1.3 Scenario III: 8 Nodes, 30min

In scenario III we have change the time about 30 min. Network topology is also same. Figure 5.8 shows the only packets arrived on the network is approximately 61,000, this duration the overall packets received by each node were approximately 59,000. In this figure shows Overall number of packets dropped by each node in different links. Which make around 2.4% of the entire data packet?

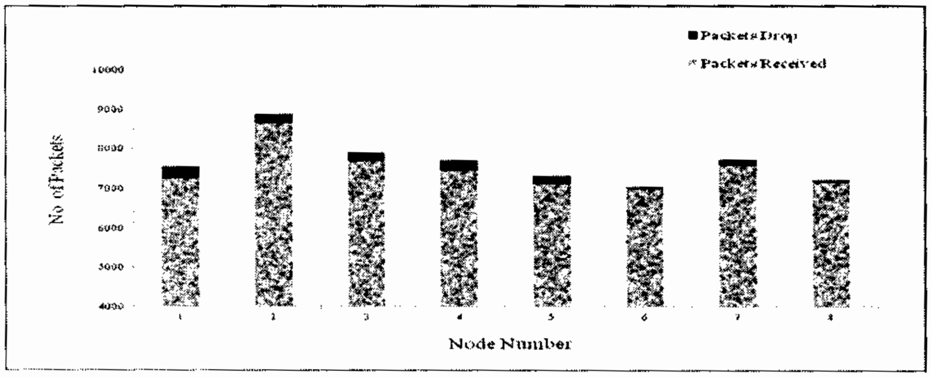

Figure 5.8: 8 Node Scenario III: Nodewise Throughput Packets Received and Dropped at each Node of 30min

It is observed from the figures 5.6, 5.7 and 5.8 that the normal packet drop rate in the absence of selective forwarding attack; which make around 2.4% of all the packets.

5.5.2 Case II: 8 nodes Scenario for Congestion with Attack Environment

For the sake of understanding, this phase our simulation act on congestion with attack, we have transplanted a packets drop rate on a certain threshold value. For a second time, we run our simulation and evaluated the result with previous one. By this we will find to analyze the impact of a selective forwarding attack detection mechanism in an environment. Detection of selective forwarding attack error rate is 4.5. The threshold value being considered to Global detection rate is making around 6% and local identification error rate is 12%.

5.5.2.1 Scenario I: 8 Nodes and Simulation Time is 25min

In this scenario the total sum of data pass through on the network is approximately 50,000, in this period the sum of total packets received at each node were approximately 45,000. Figure 5.9 shows the overall number of packets dropped by each node in different links; which make around 4.5% of the entire data packet. That means the selective forwarding attack is presence in network.

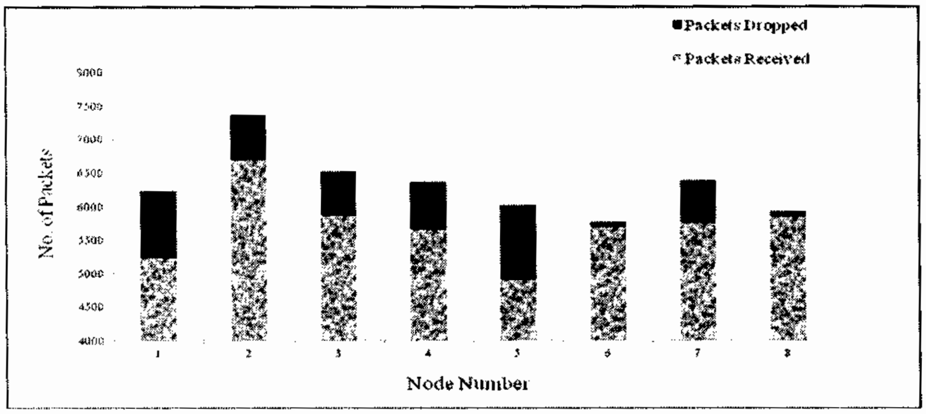

Figure 5.9: 8 nodes scenario I congestion with attacker Packets received and drop at each Node of 25min

5.5.2.2 Global Detection for Selective Forwarding Attack

For the sake of simplicity, we consider the whole network in which we check the selective forwarding attack detected or not by statistical analysis. In figure 6.10 illustrate the number of packets dropped by each node in different transactions; which makes around approximately 2000 of all originated data packets and drop rate is approximately 4.5%.

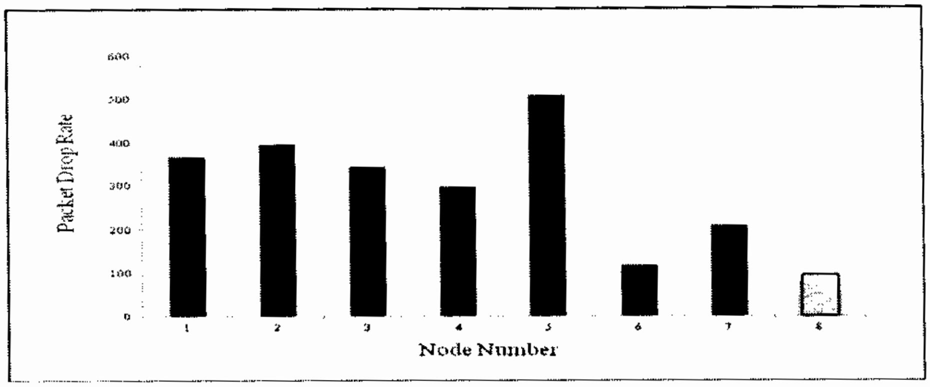

Figure 5.10: Packets Dropped During Transaction at Each Node for Global Detection

5.5.2.3 Local Identification for Selective Forwarding Attack

If selective forwarding attack detected globally then we see local identification position of selective forwarding attack. So the total data packets that travel on the network in this tin approximately 30000. Figure 5.11 illustrate that which nodes packets dropped by selective forwarding attack. Amongst the total initiated data packets rate make around 7-9%.

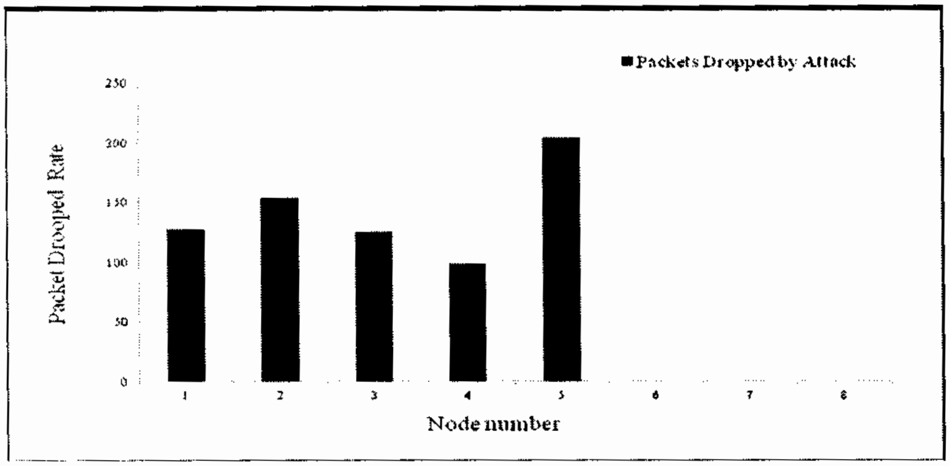

Figure 5.11: Number of Packets Dropped at each Node for Local Identification

It is observed from the figures 5.9, 5.10 and 5.11 that the packet drop rate in the presence of selective forwarding attack; which make around drop rate 7-9% of all the packets.

5.5.3 Case III: 12 Nodes Topology for Congestion with Attack Environment

In this scenario, was extended further to a network topology of 12 nodes network. This Phase our simulation act on congestion with attack, we have transplanted a packets drop rate on a certain threshold value. For a second time, we run our simulation and evaluated the result with previous one. By this we will find to analyze the impact of a selective forwarding attack detection mechanism in an environment. Detection of selective forwarding attack error rate is

6%. The threshold value being considered to identification error rate is 12%. The arrangement of 12 nodes is shown in the figure 5.12.

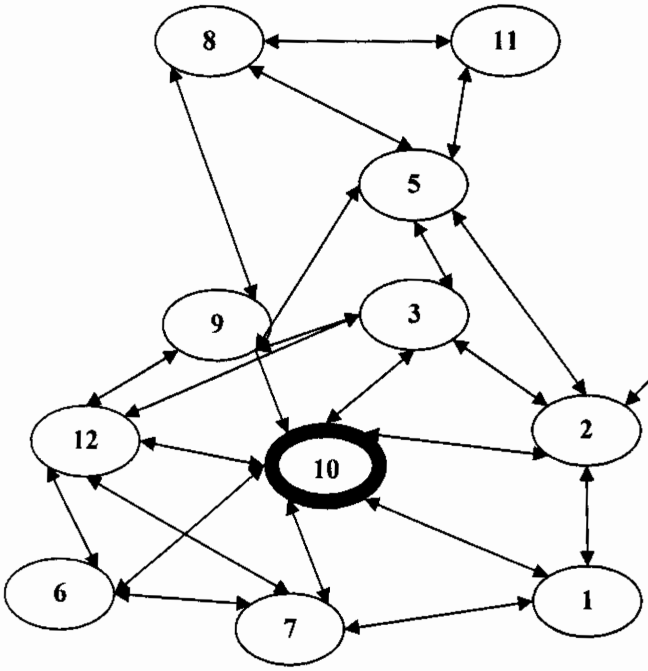

Figure 5.12: 12 Nodes Network Topology for Simulation Case III

5.5.3.1 Scenario I: 12 Nodes for Simulation Time 25min

In this scenario the total sum of data pass through on the network is approximately 66,000 in this period the sum of total packets received at each node were approximately 61,000. Figure 5.13 shows the overall number of packets dropped by each node in different links; which make around 4.9% of the entire data packet. That means the selective forwarding attack is detection now.

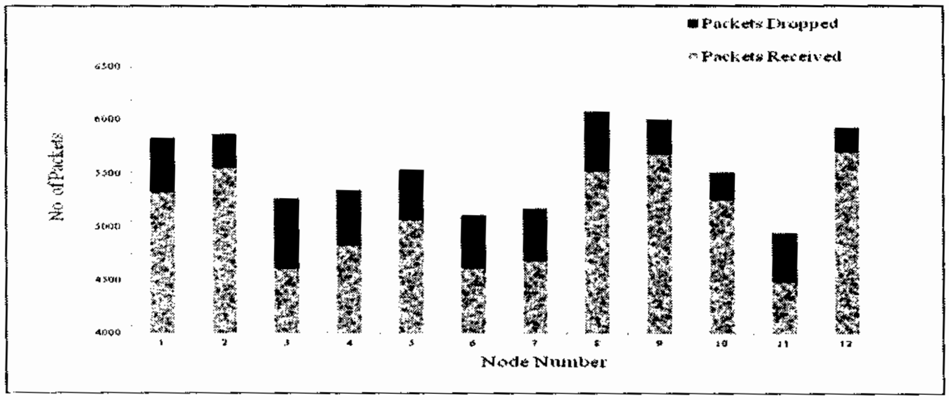

Figure 5.13: 12 nodes scenario II congestion with attacker Packets received and drop at each Node of 25min

5.5.3.2 Global Detection for Selective Forwarding Attack

For the sake of simplicity, we consider the whole network in which we check the selective forwarding attack detected or not by statistical analysis. In figure 5.14 illustrate the number of packets dropped by each node in different transactions; which makes around approximately 2000 of all originated data packets approximately 4.9%.

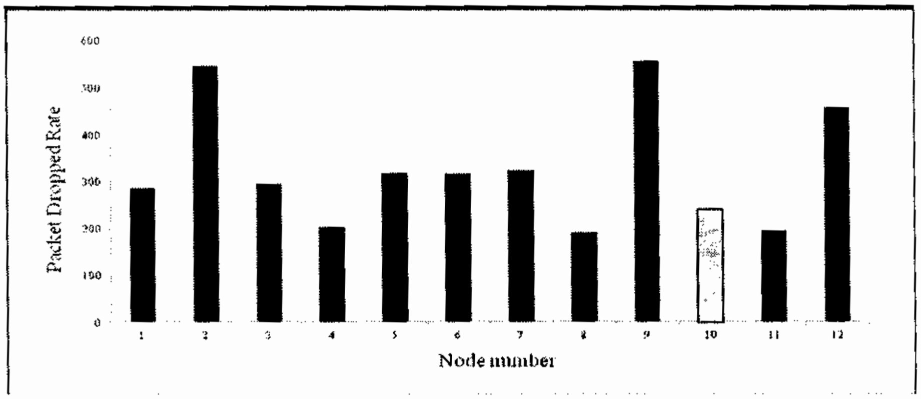

Figure 5.14: Dropped During Transaction at Each Node for Global Detection

5.5.3.3 Local Identification for Selective Forwarding Attack

If selective forwarding attack detected globally then we see local identification position of selective forwarding attack, the total data packets that travel on the network in this tin approximately 32000 figure 6.15 illustrate which nodes packets dropped by each node in different links. However, on the attacker between nodes one to node five, approximately 7.9% of the packet that pass by this link was drop.

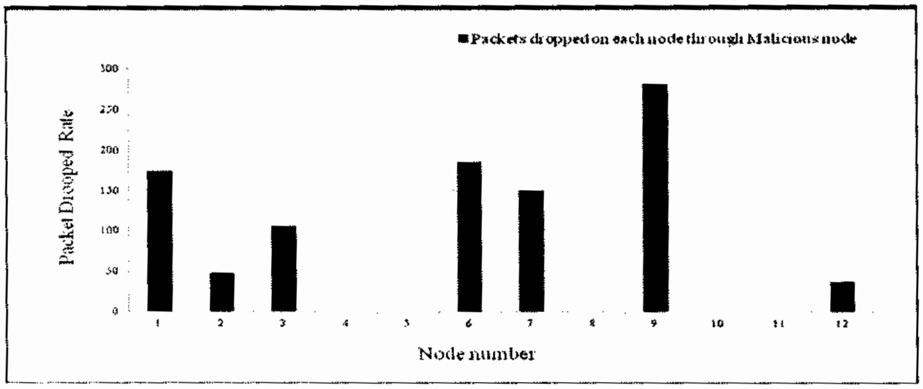

Figure 5.15: Number of Packets Dropped at each Node for local Identification

5.6 Overall Network Throughput for 8 and 12 Nodes Topology

It is observed from the figures 5.16 and 5.17 shows that the overall network throughput for 8 and 12 nodes topology. The trendline polynomial show as the time increase the throughput will be decrease if the selective forwarding attacks global detection. At this movement the network throughput degrade and packet drop rate across the normal threshold value. In which we check attacker detected or not. If it detected we see local identification position of attacker then now start Monitoring. When it locally identification the polynomial trendline smooth and throughput is normal.

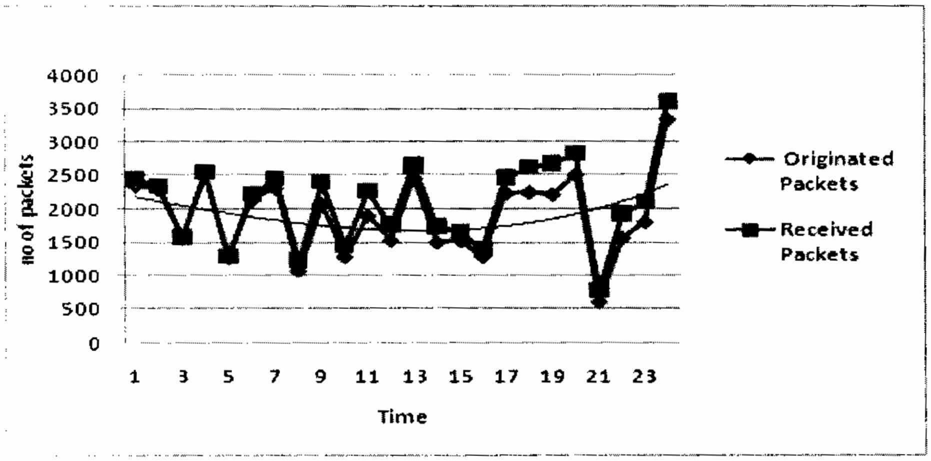

Figure 5.16: Overall Network Throughput for 8 Nodes Topology

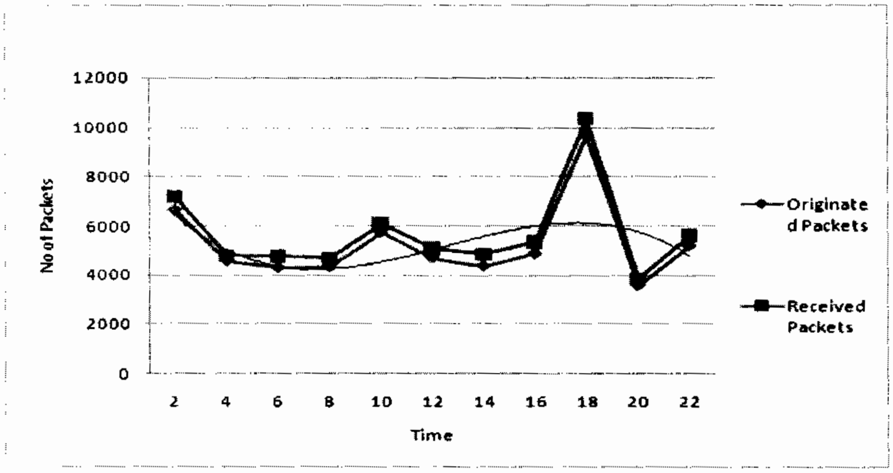

Figure 5.17: Overall Network throughput for 12 nodes topology

5.7 Analysis and Discussion

This simulation study has shown that in normal without attack congestion, there is a 3% error rate in packet delivery rate. However in case of 6 to 12 % an increased drop rate is observed which can be evaluate with respect to the total sum of sent packets is differences the total number of received packet verses the percentage of detection of malicious node. If received packets are less than send packets then we calculate total drop packet error rate of network. When the drop rate becomes higher than the sent packets, than we detected the attack on the basis of these drop rate. We use two topologies in our simulation which are 8 and 12 nodes topology. In 8 node topology the difference between the sums of sent packets and received packet is percent and it will be less than the congestion with attack error rate. When the same simulation was done on 12 node than the detection attacker rate will became 7.4% which is less than the congestion with attacker rate. In large amount of network nodes, still finding attacks rate this was knowable because in high amount of nodes the total sum of the traffic is high and it is not distinguish between the normal network's environment and under attacks environment situation.

5.8 Summary

In this chapter we are showing the result of simulation while using the OMNET++ and AODV routing protocol. Here we have used 8 and 12 nodes network topology and also mention two different scenarios. In first we are testing normal congestion environment and second we are using congestion with attack. If attack will detect and during the detection attack will gray and after it we are doing identification then here attack will black and w e add it in black list and we will delete from the network then apply new route. During the simulation we analysis or negotiated the performance of whole network about data transferring source to destination. We are showing simulation result in the sense of graphs.

Chapter 6

Conclusion and Future Direction

6.1 Conclusion

Mobile Ad-Hoc Networks has the ability to deploy a network where a traditional network infrastructure environment cannot possibly be deployed. With the importance of MANET comparative to its vast potential it has still many challenges left in order to overcome. Security of MANET is one of the important features for its deployment. In our thesis, we have analyzed the behaviour and challenges of security threats in mobile Ad-Hoc networks with solution finding technique.

Although many solutions have been proposed but still these solutions are not perfect in terms of hamper the QOS and degrade the performance of networks.

In this study, we analyzed effect of the selective forwarding attack in an AODV network. For this purpose, we implemented a hybrid approach is use to minimize false detection rate that behaves as selective forwarding attack in Omnet++.

The approach has been evaluated using the simulator and results are compared under normal congestion and congestion with attacker. Having simulated the selective forwarding attack, we saw that the packet drop is increased in the Mobile ad hoc network. In simulation results show the difference between the number of packet drop in the network with and without selective forwarding attacker. This also shows that selective forwarding attack affect the whole network connectivity and the data drop could show the existence of selective forwarding attack in network.

Finally, we opted for selective forwarding attack in MANET. Our hybrid approach from two way of attack detection such as Global detection because we consider the whole network as a Global in which we check whether selective forwarding attack is detected or not. If selective forwarding attack detected then we see local position of selective forwarding attack this called Local Identification.

Based on our research and analysis of simulation result we draw the conclusion that detection of selective forwarding attacker, at the cost of 5-7% as compared to [42] 25% and our hybrid approach is distributed coordination as well as periodic monitoring.

6.2 Future Direction

We simulated the selective forwarding attack in the Mobile Ad Hoc Networks and detection its affects. In our study, we used hybrid approach on AODV routing protocol. But the other routing protocol could be simulated as well. All routing protocols are expected to present different results. Therefore, the best routing protocol for minimizing the selective forwarding attack may be determined.

In out thesis, we try to eliminate the selective forwarding attack effect in the network. But we can find a solution on how to detect the multiple malicious nodes and how optimally and reliably we can alert neighbor nodes about the malicious node. In future, we can find a solution in dynamic approach using AI, rather than threshold and also apply proposed methodology on other networks.

References

[1] A. S. A. Ukey, M. Chawla, "Detection of Packet Dropping Attack Using Improved Acknowledgement Based Scheme in MANET", International Journal of Computer Science, 2010.pg 12-17

[2] K. P. Manikandan, Dr. R .Satyaprasad, Dr. K. Rajasekhrarao, "A Survey on Attacks and Defence Metrics of Routing Mechanism in Mobile Ad Hoc Networks", International Journal of Advanced Computer Science and Application (IJACSA), 2011.

[3] A. K. Mishra, B. D. Sahoo, "Analysis of Security Attacks for AODV Protocol in MANET" The institute of Electrical Engineers, Printed and published by IEEE, 2009.

[4] V. Kumar, V. M. A. Rajam "Detection of Colluding Selective Forwarding Nodes in Wireless Mesh Networks Based on Channel Aware Detection Algorithm", MES Journal of technology and Management, 2010

[5] S. Kaplantzis, A. Shilton, N. Mani and Y. Sekercioglu, "Detecting selective forwarding attacks in wireless sensor networks using support vector machines," in 3rd Conf. of Intelligent Sensors Sensor Networks and Information Processing, Dec. 2007, pp. 335-340.

[6] B. Yu and B. Xiao, "Detecting selective forwarding attacks in wireless sensor networks," in Proc. of the 2nd International Workshop on Security in Systems and Networks, April 2006, pp.1-8.

[7] B. Yu and B. Xiao, "CHEMAS: identify suspect nodes in selective forwarding attacks," in Journal of Parallel and Distributed Computing, Vol. 67, No. 11, 2007, pp. 1218-1230.

[8] G. Padmavathi, D. Shanmugapriya, "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks" International Journal of Computer Security, Vol. 4, No. 1 & 2, pp.117-125, 2009

[9] W. Z. Khan, Y. Xiang, M. Y Aalsalem "Comprehensive Study of Selective Forwarding Attack in Wireless Sensor Network", I.J. Computer Network and Information Security, 2011

[10] N.Bhalaji, Dr.A.Shammugam,"Reliable Routing against Selective Packet Drop Attack in DSR based MANET" in Journal of Software, vol. 4, no. 6, august 2009

[11] M.S. Obaidat, S. K. Dhurandher and K. Diwakar, "CASPER:Congestion Aware Selection of Path with Efficient Routing in Multimedia Networks", Journal of Information Processing Systems, Vol.7, No.2, June 2011 DOI 0.3745/JIPS.2011.7.2.241

[12] W. V. Wollman and Y. Barsoum. "Overview of Open Shortest Path First,version 2 (ospf v2) routing in the tactical environment", Proc. of IEEE MILCOM., Vol. 3, pp. 925-930, October 1995.

[13] T. Clausen, P. Jacquet, Project Hipercom, INRIA, RFC-3626: Optimized Link State Routing Protocol (OLSR), October 2003.

[14] T. H. Clausen, G. Hansen, L. Christensen, G. Behrmann, "The Optimized Link State Routing Protocol Evaluation through Experiments and Simulation", in Proc. of Wireless Personal Mobile Communications, Aalborg, Denmark, 2001.

[15] M.A Kheirandish, S. Karamizadeh1, M. Aflaki, " Enhancing Congestion to Control to Address Link Failure Loss Over Mobile Ad-Hoc Network, International Journal of Computer Networks & Communications (IJCNC) Vol.3, No.5, Sep 2011.

[16] M. Bhardwaja, S. Pandeyb, R.P Mahapatra, "Problem Analysis of Routing Protocols in MANET in Constrained Situation", International Journal on Computer Science and Engineering (IJCSE), ISSN : 0975-3397 Vol. 3 No. 7 July 2011.

[17] M.Jehan, Dr. G.Radhamani,Scalable TCP: Better Throughput in TCP Congestion Control Algorithms on MANETs, in International Journal of Advanced Computer Science and Applications, Special Issue on Wireless & Mobile Networks.

[18] B. Sun,Y. Guan,J. Chen,Udo , "Detecting Black-hole Attack in Mobile Ad Hoc Network" , The institute of Electrical Engineers, Printed and published by IEEE, 2003.

[19] A. Saini, H. Kumar, Effect Of Black Hole Attack On AODV Routing Protocol In MANET , IJCST Vol. 1, Iss ue 2, December 2010.

[20] S. Dokurer, Y.M. Erten, C.E. Acar, „„„Performance Analysis of Ad-hoc Networks under Black Hole Attacks", in: Proc. of the IEEE SoutheastCon, pp. 148–153, 2007.

[21] 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 (May 1998) pp. 115–124.

[22] J. R. Hughes, T. Aura, M. Bishop," Using Conservation of Flow as a Security Mechanism in Network Protocols" 2000.

[23] A.T. Mızrak, Y.C. Cheng, K. Marzullo and S. Savage," Fatih: Detecting and Isolating Malicious Routers", DSN. 05: Proc 2005 In't Conf. Dependable System and Networks(DSN), pp:558-547.

[24] F. Ahsen, K. Hussain, N. Khadam, M. Sharif." Identification of a Lossy Channel in Wireless Mesh Network using Conservation of flow" journal of Information and Technology, Vol. 1, No. 2. Pp: 60-70 2007

[25] S. Marti, T.J. Giuli, K. Lai, and M. Baker "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks" In proceedings of Mobile computing and Networking August 2000 pp: 255-265.

[26] 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), June 2007, pp. 1154-1159.

[27] S. Buchegger, J.Y.L. Boudec "Performance Analysis of the CONFIDANT Protocol (Cooperation Of Nodes: Fairness In Dynamic Adhoc NeTworks)", EPFL Lausanne, Switzerland. MOBIHOC'02, June 9-11, 2002,

[29] G. Li, X. Liu, and C. Wang, "A Sequential Mesh Test Based Selective Forwarding Attacks Detection Scheme in Wireless Sensor Network" Networking, Sensing and Control(ICNSC) International Conference on 10-12 April 2010, pages:554-558

[30] D. M. Shila, Y. Cheng, T. Anjali, "Mitigating Selective Forwarding with a Channel-Aware Approach in WMNs", Wireless Communication, IEEE, May 2010, pages: 1661-1675

[31] V. kumar, V. M. A. Rajam "Detection of Colluding Selective Forwarding Nodes in Wireless Mesh Networks Based on Channel Aware Detection Algorithm", Journal of technology and Management, 2010.

[32] V. Prema Tulasi, Prof. D Durga Bhavani, Prof. Dr. Ch.G.V.N Prasad "Implementing Data Security in Wireless Sensor Network's through Location Aware Multifunctional

Key Management Framework", Intertional Journal of Computer and Application (IJCA), 2011.

[33] W. Xin-sheng, Z. Yong-zhao, X. Shu-ming, W. Liangmin, "Lightweight Defense Scheme against Selective Forwarding Attacks in Wireless Sensor Networks', Cyber-Enabled Distribed Computing and Knowledge Discovery International Conference on 10-11, Oct 2009

[34] S. Kaplantzis, A. Shilton, N. Mani and Y. Sekercioglu, "Detecting selective forwarding attacks in wireless sensor networks using support vector machines," in 3rd Conf. of Intelligent Sensors Sensor Networks and Information Processing, Dec. 2007, pp. 335-340.

[35] M. Tiwari, K. V. Arya, R. Choudhair, K. S. Choudhary "Designing Intrusion Detection to Black Hole and Selective Forwarding Attack in WSN based on local Information" , IEEE, 2009.

[36] D. Martynov, J. Roman, S. Vaidya, and H. Fu, WSN "Design and Implementation of an Intrusion Detection System for Wireless Sensor Networks",Electro/Information Technology(EIT,IEEE), international Conference on 17-20, May 2007, pages: 507-512

[37] Bo Yu and Bin Xiao. "Detecting selective forwarding attacks in wireless sensor networks", In proceedings of 20th International Parallel and Distributed Processing Symposium (IPDPS) 2006.

[38] H-M Sun, C-M Chen, and Y-C Hsiao. Un- mask: Utilizing neighbor monitoring for attack mitigation in mul-tihop wireless sensor networks" Journal Ad Hoc Networks Volume 8,issue 2, March, 2010, pages 148–164,

[39] K. Biswas and Md. Liaqat Ali, "Security threats in Mobile Ad-Hoc Network", Master Thesis, Blekinge Institute of Technology" Sweden, 22nd March 2007

[40] G. A. Pegueno and J. R. Rivera, "Extension to MAC 802.11 for performance Improvement in MANET", Karlstads University, Sweden, December 2006

[41] Andras Varga, "OMNET++: Discrete event simulation system, Version 3.2 user manual", essay.utwente.nl/58509/1.scriptie_E_van_Eentennaam.pdf

[42] D. M Shila,,T. Anjali, “Defending Selective Forwarding Attacks in WMNs”,Electro/Information Technology, EIT, international conference on 18-20, May 2008, E-ISBN:978-4244-2030-8

[43] S.seemab, Dr. M. Sher “Detection and identification of unreliable traffic in wirless ad hoc networking in congestion.” MS thesis, Islamic International University Islamabad. 2011