International Journal of Current Trends in Engineering & Technology
ISSN: 2395-3152
Volume: 02, Issue: 03 (MAY-JUNE, 2016)

Lightweight Prevention of Black-hole Attack using Local Route Maintenance in MANET

Khushbu Patil
M. Tech. Scholar, Department of SCSIT
DAVV Indore, India
khushbupatil57@gmail.com

Prof. Pankaj Jagtap
Department of SCSIT,
DAVV Indore, India
jagtap03@gmail.com

Abstract – A Mobile Ad hoc Network is a set of mobile nodes forming a temporary multi-hop connection without any supervision of any centralized authority. The absence of any authority is invites many attackers that modified data, loss data and degrades the utilization of resources. The nodes are mobile in a MANET with different mobility speed; links between the nodes are created and destroyed in an unpredictable way, which makes quite challenging the determination of routes between a pair of nodes that want to communicate with each other. The black hole attacker is the routing layer packet dropping attacker that replies fake route information to sender nodes that forward request to attacker for secure communication black hole attacker is drop the data after link establishment. The proposed Local Repair Maintenance based Lightweight IDS for better communication is provides the novel secure Intrusion Detection System (IDS) against routing misbehaviour of Black hole attack in MANET. The proposed IDS are not determining whether the losses are caused by link errors or any other reason. It determines the loss due to malicious nodes or packet dropping nodes. In this research we are especially interested in the detection of attacker and that is possible due to identify the nodes that not forward the packets to destination after route establishment. The proposed Lightweight IDS is indented that nodes and blocked these nodes for providing secure communication. The basic idea behind the proposed security scheme is that even though malicious dropping may result in a packet loss rate that is much degradable as compare to normal channel losses. The watchdog security scheme is also applied on proposed scheme and observes that it is also completely secure the network but in proposed scheme Local Route Maintenance is improves the routing performance after blocking attacker malicious activities. The simulation of all the modules is done in network simulator-2 and performance is measures through performance metrics.

Keywords: Black hole attacker, MANET, Lightweight IDS, Routing, Local Route Maintenance, NS-2.

I. INTRODUCTION

Mobile ad-hoc networks are composed of autonomous nodes that are self- managed without any infrastructure. They usually have a dynamic topology such that nodes can easily join or leave the network at any time and they move around freely which gives them the name Mobile Ad hoc Networks or MANETs. They have many potential applications, especially in military and rescue operations such as connecting soldiers in the battle field or establishing a temporary network in place of one which collapsed after a disaster like an earthquake [1]. In these networks, besides acting as a host, each node also acts as a router and forwards packets to the correct node in the network once a route is established. To support this connectivity nodes are use routing protocols such as AODV (Ad hoc On Demand Distance Vector Routing Protocol). Mobile ad-hoc networks are usually susceptible to different security threats and malicious node attack is one of these. In this attack, an attacker node which absorbs and drops all data packets makes use of the vulnerabilities of the on demand route discovery protocols. In recent years, application domains of mobile ad hoc networks have gained more and more importance in non-military public organizations and in commercial and industrial areas. Security in Mobile Ad-Hoc Network is the most important concern for the basic functionality of network. The availability of network services, confidentiality and integrity of the data can be achieved by assuring that security issues have been met [2]. MANETs often suffer from security attacks because of its features like open medium, changing its topology dynamically, lack of central monitoring and management, cooperative algorithms and no clear defense mechanism. These factors have changed the battle field situation for the MANETs against the security threats.

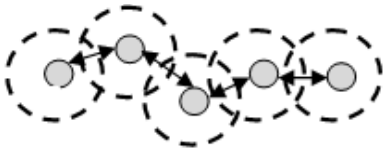

Fig.1.1 Ad hoc Network

II. PREVIOUS WORK

Tarun Varshney, Tushar Sharmaa, Pankaj Sharma [1] "Implementation of Watchdog Protocol with AODV in Mobile Ad Hoc Network" in this paper a network performance and reliability is broken by the attacks on ad hoc routing protocols. Many mechanisms have been proposed to overcome the Black-hole Attack. A malicious node or black-hole node send Route Response (RREP) incorrectly of having route to destination with minimum hop count and when sender sends the data packet to this malicious node, it drops the entire packet in the network. The propose watchdog mechanism detect this black hole nodes in a MANET. This method first detects a black-hole node in the network and then provides a new route to source node. In this, the performance of original-AODV and modified AODV called as watchdog-AODV (or W-AODV) in the presence of multiple black hole nodes is find out on the basis of throughput and packet delivery ratio and routing and control load.

Akshai Aggarwal, Savita Gandhi et. al. [2] "Trust Based Secure on Demand Routing Protocol (TSDRP) for MANETs" in that work they proposed a Trust Based Secure on Demand Routing Protocol called "TSDRP". Ad hoc On-demand Distance Vector (AODV) routing protocol has been modified to implement TSDRP for making it secure to thwart attacks like Black-hole attack and DoS attack. To evaluate the performances.

S. Nishanthi, [3] "Intrusion Detection in Wireless Sensor Networks Using Watchdog Based Clonal Selection Algorithm", in this title we have discuss a tendency to opt for Bio-Inspired

Approach. In this paper, the clonal selection principle is implemented and develop the Watchdog based Clonal Selection Algorithm (WCSA).Using this WCSA, the intrusions in the network and monitoring multiple misbehaved nodes. Using this algorithm we can realize intruders and reduce the detector rate, and reduce generator value also will increase in throughput.

Silva, A.P.R.D., M.H.T. Martins, B.P.S. Rocha, A. A. F. Loureiro and L.B. Ruiz,[4] "Decentralized Intrusion Detection In Wireless Sensor Networks "In Rule-based intrusion detection schemes is proposed for WSN, also called specification based intrusion detection schemes. In these schemes, the detection rules are first designed by domain expert before the starting the detection process. Most of the techniques in these schemes follow three main phases: data acquisition phase, rule application phase and intrusion detection phase. In the following sub-sections, the key important schemes in this category are explored. Decentralized IDS in WSN propose the first and the most cited rule-based intrusion detection scheme for WSN to detect many different kinds of attacks in different layers. In this scheme, there are three main phases involved: data acquisition phase in which the monitor nodes are responsible of promiscuous listening of the messages and filtering the important information for the analysis; the rule application phase, in which the pre-defined rules are applied to the stored data from the previous phase, if the message analysis failed any of the rules test, a failure is raised and the counter increased by one; the intrusion detection phase, a comparison is taken place between the number of raised failures produced from the rule application phase with a predefined number of occasional failures that may happen in the network. If the total number of the raised failures is higher, intrusion alarm is produced.

A. Rajaram. Dr. S. Palaniswami [5] "Malicious Node Detection System for Mobile Ad hoc Networks" in this title, we develop a trust based security protocol based on a MAC-layer approach which attains confidentiality and authentication of packets in both routing and link layers of MANETs. In the first phase of the protocol, we design a trust based packet forwarding scheme for detecting and isolating the malicious nodes using the routing layer information. It uses trust values to favour packet forwarding by maintaining a trust counter for each node. A node is punished or rewarded by decreasing or increasing the trust counter. If the trust counter value falls below a trust threshold, the corresponding intermediate node is marked as malicious. In the next phase of the protocol, we provide link-layer security using the CBC-X mode of authentication and encryption. By simulation results, we show that the proposed MAC-layer security protocol achieves high packet delivery ratio while attaining low delay, high speed and overhead.

Dr. A. A. Gurjar, A. A. Dande, [6] "Black Hole Attack in Manet's: A Review Study" in this title we discuss Black hole attack is one of the possible attacks in MANET. In black hole attack, a malicious node sends the route reply message to the source node in order to advertise itself for having the shortest path to the destination node. The malicious node reply will be received by the requesting node before the reception of the any other node in the network. When this route is created, malicious node receives the data packet, now it's up to the malicious node whether to drop all the data or forward it to the unauthenticated nodes.

Hesiri Weerasinghe and Huirong Fu, [7] "Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks: Simulation Implementation and Evaluation" In this title , via simulation, we evaluate the proposed solution and compare it with other existing solutions in terms of throughput, packet loss percentage, average end-to end delay and route request overhead. The experiments show that (1) the AODV greatly suffers from cooperative black holes in terms of throughput and packet losses, and (2) our solution proposed in presents good performance in terms of better throughput rate and minimum packet loss percentage over other solutions, and (3) our solution proposed in can accurately prevent the cooperative black hole attacks.

Harjeet Kaur , Manju Bala, , Varsha Sahni [8] "Study of Black hole Attack Using Different Routing Protocols in MANET" This research effort focused first the comparative investigations of routing protocols under the various types of attack then to create scenario and simulate and investigate the performance metrics viz. Packet delivery ratio, average jitter, average throughput and end to end delay of reactive, proactive and hybrid routing protocols such as AODV and AODV with black hole attack, OLSR and OLSR with black hole attack and ZRP and ZRP with black hole attack for the different scenario under the different conditions.

Nitesh A. Funde, P. R. Pardhi [9] "Detection & Prevention Techniques to Black & Gray Hole Attacks in MANET: A Survey" in this title we have focus different techniques to prevent black & gray hole attacks in MANET. Mobile ad hoc network (MANET) is a self-configuring network of mobile nodes formed anytime and anywhere without the help of a fixed infrastructure or centralized management. It has many potential applications in disaster relief operations, military network, and commercial environments. Due to open, dynamic, infrastructure-less nature, the ad hoc networks are vulnerable to various attacks. AODV is an important on-demand distance vector routing protocol for mobile ad hoc networks. It is more vulnerable to black & gray hole attack. In MANET, black hole is an attack in which a node shows malicious behavior by claiming false RREP message to the source node and correspondingly malicious node drops all the receiving packets.

Dr. Bipul Syam Purkayastha, Dr. Prodipto Das, Rajib Das,[10] "Security Measures for Black Hole Attack in MANET: An Approach" In this title, we give an algorithmic approach to focus on analyzing and improving the security of AODV, which is one of the popular routing protocols for MANET. Our aim is on ensuring the security against Black hole attack. The proposed solution is capable of detecting & removing Black hole node(s) in the MANET at the beginning. Also the objective of this title is to provide a simulation study that illustrates the effects of Black hole attack on network performance.

III. PROPOSED METHODOLOGY

A) PROBLEM STATEMENT

The total security in the MANET is extremely tough to achieve because of its fundamental characteristics, such as limited functional resources, open medium, dynamic topology, limited range and. The foremost problem in dynamic network is that black hole attack is consumes and customized the authentic performance of routing in between sender and receiver and due to the absence of centralized absence and continuously

movement of mobile nodes, it is very difficult to find which node or nodes in the network creating an abnormal behavior. The black hole attacker is creating a problem in network is:-

- It replies the fake information to sender about the shortest path available up to destination.
- The attacker nodes are consumes all the packets of sender nodes that are in proper communication range.
- Due changing the location it is difficult to identified that location or trace their location in grid layout.

The packet dropping in network is enhanced by that routing overhead is also enhanced.

B) Algorithm Step for Lightweight Prevention of Black hole Attack using local route maintenance in MANET

In this algorithm we detect and prevent from black hole using local route maintenance based watch dog mechanism, in this section define the algorithm in step by step process.

Input:

M: mobile devices
S: Sender Nodes
R: Receiver Nodes
Watchdog node: w ϵ M
a ϵ M : attacker nodes
Threshold: Th

Output:

Infection percentage, throughput, PDR, overhead and data drop analysis

Routine

w provide open access ϵ M and watch behaviour of neighbour
a interact to w or send data to other nodes
a access w resource & data or capture data
if (an update data of s node)
{
Check update data by w
If(update > Th && modified receiver ID)
{
Identifies (infected data value, node number, symptoms)
While (symptoms != normal)
{
if (symptoms != black hole)
{
Identifies attacker a_n
Abnormal data set identification
Trace time
}
Else if (symptoms == new)
{
Watch symptoms behaviour
Attacker node a
New behaviour table generate
Assign-name of attacker
}
}
Prevention-manager (attack type, abnormal-table)
}
}
Prevention-manager (a-t, a-table)
{
Analyse attack type with abnormal table
Send normal treat msg to a
If (a profile == normal-profile)
{
a ϵ normal profile node
}
Else
{
Block the node with symptoms
}
Broadcast attacker node info and its symptoms to all connected node
New local route repair from predecessor of black hole node
Analyse the new network behaviour
Calculate performance of the network
}

The normal routing profile is shows the attacker free routing in network. In this network the attacker is not in active mode because the attacker is inactivate by secure proposed watchdog mechanism.

IV. SIMULATION & RESULT DISCUSSION

Network simulator 2 (NS2) is the result of an on-going effort of research and development that is administrated by researchers at Berkeley [12]. It is a discrete event simulator targeted at networking research. It provides substantial support for simulation of TCP, routing, and multipath protocol. The simulator is written in C++ and a script language called OTcl2. Ns use an Otcl interpreter towards the user. This means that the user writes an OTcl script that defines the network (number of nodes, links), the traffic in the network (sources, destinations, type of traffic) and which protocols it will use. This script is then used by ns during the simulations. The result of the simulations is an output trace file that can be used to do data processing (calculate delay, throughput etc) and to visualize the simulation with a program called Network Animator.

A) Simulation Parameters

The simulation is the tool that generates the scenario equivalent to real time scenario. The simulation of mobile nodes in MANET is completed on the bases of some input parameters. These parameters are used to decide the grid layout of simulation, number of nodes and much more. The simulation parameters used in this simulation is mentioned in table 1.

Table1 Simulation Parameter of Case Study

Dimension of simulated area	800×800
Mobile Nodes	50
Routing Protocol	AODV
Simulation time (seconds)	100
Attack Type	Black hole
Prevention Type	Watchdog IDS-Proposed
Transmission Range	550m
Transport Layer Protocol	TCP, UDP
Traffic type	FTP, CBR
Packet size (bytes)	1000
Number of traffic connections	10
Maximum Speed (m/s)	Random

B) Result Analysis

1. Routing Packets Overhead Analysis

The source and destination in MANET is also mobile and due to dynamic changing of topology the communication is really difficult. The routing packets are first flooded by sender to

confirm the destination. In MANET it is very rare that the destination is directly available in network in one hop count distance. The routing packets are confirming the destination and through minimum hop count route data is sending to destination. In this graph the routing packets analysis in presence of black hole attack, watchdog security and in presence of proposed IDS is appraised and the performance of proposed Lightweight IDS is really effective. The routing packets quantity is less in attack scenario but also packets receiving are also less and the watchdog disadvantage is routing packets flooding is more but in proposed Lightweight IDS it is just half of data packets receiving. That is the sign of better and secure performance.

2. PDR Performance Analysis

The PDR (Packet Delivery Ratio) is the performance metrics through which the packets percentage of receiving with respect to sending is measures. The better packets receiving in network is provides the better PDR performance. In this graph the PDR performance in presence of black hole attack, watchdog and proposed Lightweight IDS is evaluated and identified that the packets receiving in presence of black hole attack is completely negligible by that the PDR is only shown up to 26 seconds of simulation. The PDR performance of watch dog is about 82 % but the performance of proposed Lightweight IDS is really effective it is about 95% up to end of simulation. The Local Maintenance is really improves the routing performance of dynamic network.

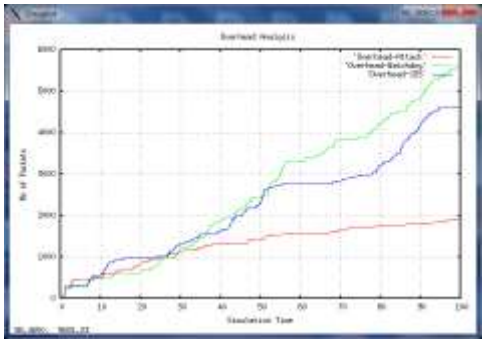

Figure: 4.1 Routing Overhead Analysis

3. Throughput Performance Analysis

The better performance of network is measured through number of packets received at destination in every instance of time. The packets sending is affected in network if the packets receiving is affected because sender it is not possible to sender start the next transmission of data without completing the first one successfully. In this graph the throughput performance in presence of black hole attack, secure watch dog scheme and proposed Lightweight IDS is measured and recognized that throughput performance of proposed IDS is about 1400 packets/second up to ending of simulation. The performance of watchdog is in peak point on time 25 to 40 seconds is only 600 number of packets/second and at last the worst performance is calculated in presence of black hole attack is about negligible in MANET. The Local Route Maintenance of IDS improves the network performance.

4. Attacker Loss Analysis The attacker in decentralized network is affected the performance easily and observe that their malicious activities is performing routing misbehaviour in dynamic network. The attacker loss percentage in network is the only performance of network in presence of attacker. In this analysis the watchdog and proposed Local Route Maintenance based Lightweight IDS performance is counted zero means no attacker infection is presence, attackers are completely blocked in network. Because of that the only in attacker presence loss of data is counted and this is about 24%.

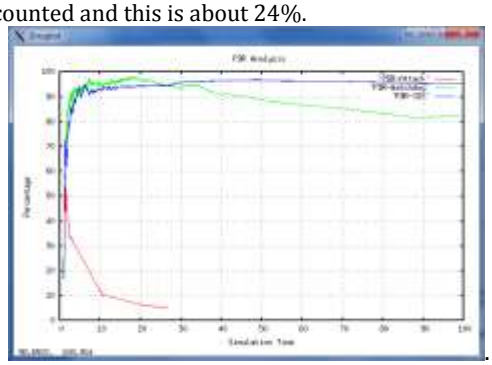

Figure 4.2 PDR Performance Analyses

That means the rest of original data us also affected due to loss of some data from it. The security scheme is removes the attacker infection and provides secure communication in decentralized network.

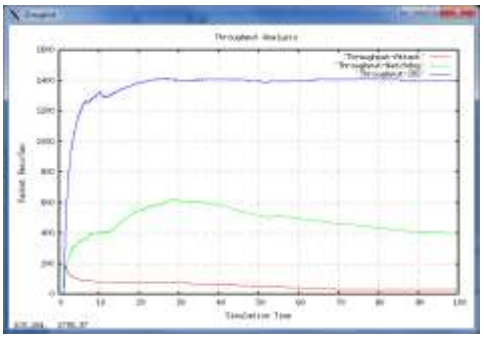

Figure: 4.3 Throughput Performance Analyses

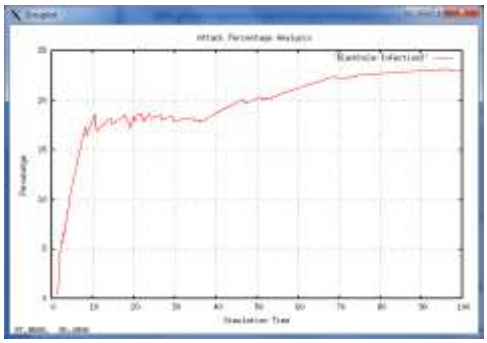

Figure: 4.4 Attacker Loss Analyses

Packets received and send in network. The packets sending and receiving in network in presence of proposed Lightweight IDS security is much better due to Local Route Maintenance in dynamic network.

5. Concluded Analysis of All Scenarios

The watchdog method is really effective in to protect the dynamic network from packet consumption black hole attack.

The watch dog method is effective but the flooding of routing packets in this method is more as compare to number of packets received and send in network. The packets sending and receiving in network in presence of proposed Lightweight IDS security is much better due to Local Route Maintenance in dynamic network.

Table2 Complete Performance Analysis

Parameter	Black hole Attack	Watchdog	Proposed IDS
SEND	1758	2325	8318
RECV	28	1911	7925
ROUTINGPKTS	1914	5623	4616
Routing Attack	1228	0	0
PDF	1.59	82.19	95.28
NRL	68.36	2.94	0.58
Average e-e delay(ms)	114.95	170.72	126.92
No. of Packet Drop	1730	401	360

V. CONCLUSION & FUTURE SCOPES

The main benefit of proposed research is, it is protocol independent Mobile Ad hoc Network are susceptible from routing security attacks due absence of centralized monitoring and management, so it is crucial to protect them. In this paper they proposed the Local Repair Maintenance. Security in MANET is the challenging and complex area, in which auxiliary research is tranquilly performed and their result is to protect attackers in decentralized network. In black hole attack node behaves as normal as at the time of connection establishment. Their actual behaviour is highlighted at the time of data sending by sender in network. The proposed Lightweight IDS identified the packet dropping and loss percentage of attacker and block their malicious activities. The proposed Local Route Maintenance is improves the routing performance by providing the authority to intermediate nodes to take routing decision. Because of that every time sender is not re-established connection if the link is break. The watchdog method is also applied and it is also provides security from black hole attack but the overhead is more in this method because of that the packets receiving is more. The attacker malicious activities are blocked by Lightweight IDS and the performance metrics is shows the better results of proposed scheme as compare to watchdog method. In future we proposed work on collaborative attack of Sybil attackers and wormhole attacker that communicate with each other with original foam to confirm the trust factors by sender but for other nodes (Intermediate nodes generated the fake ID). Their detection is identified through proposed scheme. In future also try to work on the dynamic topology control system to control scheme. In this scheme we also observe higher mobility of mobile nodes and forward the message to every node.

REFERENCES

[1]. Tarun Varshney, Tushar Sharma, Pankaj Sharma "Implementation of Watchdog Protocol with AODV in Mobile Ad Hoc Network" 2014 Fourth International Conference on Communication Systems and Network Technologies.

[2]. Akshai Aggarwal "Trust Based Secure on Demand Routing Protocol (TSDRP) for MANETs" 2014 Fourth International Conference on Advanced Computing & Communication Technologies, 978-1-4799-4910-6/14 2014 IEEE DOI 10.1109/ACCT.2014.95.

[3]. S. Nishanthi, "Intrusion Detection in Wireless Sensor Networks Using Watchdog Based Clonal Selection Algorithm", IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 1, Issue 1, March, 2013.

[4]. Silva, A.P.R.D., M.H.T. Martins, B.P.S. Rocha, A. A. F. Loureiro and L.B. Ruiz, "Decentralized Intrusion Detection In Wireless Sensor Networks" Proceedings of the 1st ACM International Workshop on Quality of Service and Security in Wireless and Mobile Networks, (QSSWMN; 25), pp.: 16-23, 2005.

[5]. Xie, M., S. Han, B. Tian and S. Parvin, "Anomaly detection in wireless sensor networks: A survey" Journal of Network and Computer Application, pp.1302-1325, 2011.

[6]. Dr. A. A. Gurjar, A. A. Dande, "Black Hole Attack in Manet's: A Review Study" International Journal of IT, Engineering and Applied Sciences Research (IJIEASR) ISSN: 2319-4413 Volume 2, No. 3, March 2013.

[7]. Hesiri Weerasinghe and Huirong Fu, "Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks: Simulation Implementation and Evaluation International Journal of Software Engineering and Its Applications Vol. 2, No. 3, July, 2008.

[8]. Harjeet Kaur , Manju Bala, , Varsha Sahni "Study of black hole Attack Using Different Routing Protocols in MANET" International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering Vol. 2, Issue 7, July 2013.

[9]. Nitesh A. Funde, P. R. Pardhi "Detection & Prevention Techniques to Black & Gray Hole Attacks in MANET: A Survey" International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 10, October 2013.

[10]. Dr. Bipul Syam Purkayastha, Dr. Prodipto Das, Rajib Das, "Security Measures for Black Hole Attack in MANET: An Approach" 2012 Assam University.