International Journal of Current Trends in Engineering & Technology
Received 1 February 2019, Revised form, 28 March 2019, Accepted 20 April 2019, Available online 26 April 2019
www.ijctet.org, ISSN: 2395-3152
Volume: 05, Issue: 02 (March- April, 2019)

Black Hole Attack Prevention Using Fake Sequence Number detection and Trust Based Routing in MANET

Chandan Kumar Mishra
M. Tech. Scholar, Dept. of CSE
TIT, Bhopal (M.P) India
mishrachandan85@gmail.com

Deepak Gour
Asst. Professor, Dept. of CSE
TIT, Bhopal (M.P) India
deepak.gour@gmail.com

Dr. Vijay Anand Sullare
Asst. Professor, Dept. of CSE
TIT, Bhopal (M.P) India
anandvijay111@gmail.com

Abstract Mobile Ad hoc Network (MANET) are forming a group of nodes that are communicated with each other in limited area. The attacker nodes in MANET are disturbing the normal routing performance that base the dynamic network performance. The malicious nodes are always stump intermediate nodes in routing procedure because these nodes are only received and forward respond of surrounding neighbor. The intermediate nodes work is very responsible in routing procedure with continuous movement. In this research we proposed Fake Sequence Number Detection (FSND) security algorithm against malicious black hole attack in MANET. The black hole nodes, the proposed security method of finding attacker is based on the identified the fake information of route in the network. The proposed scheme is detecting the attacker presence and also estimate the numbers of packets are dropped by black hole attacker in network. The packet dropping on link through node is detected and prevented by security system. The black hole presence is makeable in different node density scenarios and the single as well as multiple presences is detected by FSND scheme. This method not only identified the black hole nodes but also prevent from routing misbehavior of attacker nodes. Security is less effective on attacker/s. The performance of existing security scheme is comparing with proposed FSND and the performance of existing the proposed secure FSND is securing the MANET and improves the network performance after blocking malicious nodes in network. The network performance in presence of attack and secure FSND is measures through performance metrics like throughput, routing packets flooding and proposed secures routing is improves data receiving and minimizes dropping data network as compare to existing security scheme.

Key words:- Black hole Attacker, Routing, Security, MANET, FSND, Nodes.

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. 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 nodes which absorbs and drops all data packets makes use of the vulnerabilities of the on-demand route discovery protocols. According to the routing strategy routing protocols can be classified as Table-driven or Proactive routing protocols and on demand or source initiated.

Mobile ad hoc networks originated from the U.S. Government's Defence Advanced Research Projects Agency (DARPA) Packet Radio Network (PRNet) and SURAN project. Being independent on re-established infrastructure, mobile ad hoc networks have advantages such as rapidity and ease of deployment, improved flexibility, and reduced costs. Mobile ad hoc networks are appropriate for mobile applications in either hostile environment where no infrastructure is available, or temporarily established mobile applications, which are cost crucial. 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. The typical application scenarios include rescue missions, law enforcement operations, cooperating industrial robots, traffic management, and educational operations in campus.

II. Black-hole Attack

In this type of attacks, malicious node claims having an optimum route to the node whose packets it wants to intercept [1]. On receiving the request the malicious node sends a fake reply with extremely short route. Once the node has been able to place itself between the communicating nodes, it is able to do anything with the packets passing between them. In black hole attack, a malicious node uses its routing protocol in order to advertise itself for having the shortest path to the destination node or to the packet it wants to intercept. This hostile node advertises its availability of fresh routes irrespective of checking its routing table. In this way attacker node will always have the availability in replying to the route request and thus intercept the data packet and retain it. In protocol based on flooding, the malicious node reply will be received by the requesting node before the reception of reply from actual node; hence a malicious and forged route is created. When this route is established, now it's up to the node whether to drop all the packets or forward it to the unknown address.

International Journal of Current Trends in Engineering & Technology
Received 1 February 2019, Revised form, 28 March 2019, Accepted 20 April 2019, Available online 26 April 2019
www.ijctet.org, ISSN: 2395-3152
Volume: 05, Issue: 02 (March- April, 2019)

III. Related Work

In this section the previous work that has done in this field is discussed. We are doing a work on attacks mentioned in Taku Noguchi, Mayuko Hayakawa [1] "Black Hole Attack Prevention Method Using Multiple RREPs in Mobile Ad-Hoc Network" in this title a new threshold – based black hole attack prevention method using multiple RREPs. To investigate the performance of the proposed method, we compared it with existing method.

Dr. A. A. Gurjar, A. A. Dande, [2]"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, [3] "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 [4] "Study of Blackhole 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 blackhole attack, OLSR and OLSR with blackhole attack and ZRP and ZRP with blackhole attack for the different scenario under the different conditions.

Nitesh A. Funde, P. R. Pardhi [5]"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 behaviour 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,[6] "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.

Ei Khin and Thandar Phyu[7] "Impact Of Black Hole Attack On Aodv Routing Protocol" In this title, we are simulating and analyzing the impact of black hole attack on Ad Hoc On-Demand Distance Vector (AODV) protocol. The simulation is carried on NS-2 and the simulation results are analyzed on various network performance metrics such as packet delivery ratio, normalized routing overhead and average end-to-end delay.

Rupinder Kaur and Parminder Singh [8] "Review Of Black Hole And Grey Hole Attack" This title deals with the study of analysis of delay occurs by these attack in Wireless Mesh networks and its types and also discuss about previous study by which we get idea about attack occurs in networks and also study various techniques to detect and prevent network from black hole and grey hole attack. Then we discuss about their result by using simulator OPNET.

Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon and Kendall Nygard [9] "Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks" In this title, we address the problem of coordinated attack by multiple black holes acting in group. We present a technique to identify multiple black holes cooperating with each other and a solution to discover a safe route avoiding cooperative black hole attack.

Vipin Khandelwal, Dinesh Goyal [10] "Black Hole Attack and Detection Method for AODV Routing Protocol in MANETs" In this title, we have investigated packet loss problem caused by a malicious nodes that performs the well-known attack called Black-hole attack in the network. To mitigate the effects of such attack, we have also proposed a detection technique that efficiently detects the malicious nodes in the network. We have done simulations using NS-3 simulator. Black-hole attack is also called sequence number attack because it is created using and modifying sequence number field in routing control packets. We have performed the attack and its detection method on a of the well-known and largely used MANET

International Journal of Current Trends in Engineering & Technology
Received 1 February 2019, Revised form, 28 March 2019, Accepted 20 April 2019, Available online 26 April 2019
www.ijctet.org, ISSN: 2395-3152
Volume: 05, Issue: 02 (March- April, 2019)

routing protocol known as Ad Hoc Distance Vector (AODV) routing protocol. We have simulated this attack and determined effect of this attack on network performance by different network scenario. Furthermore, we have implemented a detection method that helps to isolates the malicious nodes in the network.

Jaspal Kumar, M. Kulkarni, Daya Gupta[11] "Effect of Black Hole Attack on MANET Routing Protocols" In this title we have analyzed the effects of Black hole attack on mobile ad hoc routing protocols. Mainly two protocols AODV and Improved AODV have been considered. Simulation has been performed on the basis of performance parameters and effect has been analyzed after adding Black-hole nodes in the network. Finally the results have been computed and compared to stumble on which protocol is least affected by these attacks.

Ashish Sharma, Dinesh Bhuriya , Upendra Singh , Sushma Singh [12] "Prevention of Black Hole Attack in AODV Routing Algorithm of MANET Using Trust Based Computing" In this title we are focus black holes attack. TAODV is a secure routing protocol based on trust model for mobile ad-hoc network. We have taken TAODV routing protocol approach to focus on analyzing and improving the security of Black hole in AODV routing protocol. AODV is a popular routing protocol for mobile ad-hoc network. Our aim is on ensuring the security against black hole attack. The metrics energy, throughputs and packet delivery ratio are used to determine the performance of AODV, AODV with black hole attack and Trusted AODV. By using simulation tool on ns2, the energy of Black hole is more as compare to TAODV and throughput of TAODV is better compare to black hole AODV, similar to packet delivery ration is better compare to black hole AODV.

Sushil Kumar Chamoli, Santosh Kumar, Deepak Singh Rana, [13]"Performance of AODV against Black Hole Attacks in Mobile ad-hoc Networks" In this title, performance of AODV is evaluated in presence of black hole attack (malicious node) and without black hole attack with cbr traffic under different scalable network mobility. For this analysis RWP model is used.

Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto [14] "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method" In this title, we propose an anomaly detection scheme using dynamic training method in which the training data is updated at regular time intervals. The simulation results show the effectiveness of our scheme compared with conventional scheme.

IV. Proposed Work Description

After reading various researcher work discussed in this papers in field of security in MANET, we motivated to work on packet dropping attack in MANET. One of the simplest way for an attacker node to perturb the good function of MANET is to announce better routes (to reach to other neighbor nodes or just a specific one) than the other nodes. In addition all these vulnerabilities there are the existence of security routing protocols which make them secure and attacker infection free networks there by admiring the ultimate aim of researcher in field of Mobile Ad hoc networks. I proposed the variable consistency-based security scheme to identify the attacker on the basis of actual route selection. The actual route is identified by Intrusion Detection System (IDS) in presence of malicious attacker and identified the trust value of ach node with high sequence number. The proposed security system with its working is mentioned in algorithm in presence of attacker. The proposed scheme works to count whole length of path from source to destination. If more than one path is established then select shortest path in between Source to Destination. In this figure 2 the receiver replies to sender about shortest path but malicious node forwards the false route information of receiver to sender. Malicious nodes do not use this process and instead, they immediately respond to the source node with false information as though it has fresh enough path to the destination. Therefore source node sends its data packets via the malicious node to the destination by assuming it is a true or factual path. Explain it in more detail as we have already explained the AODV protocol. MANET that uses the AODV protocol, a Black Hole node absorbs the network traffic and drops all packets.

A. Proposed Algorithm:

In this section describe about algorithm to prevention black hole attack using fake route detection and trust-based route decision-based methodology, for that we develop the procedure to apply step by step process in mobile ad hoc network and provide reliable path. Fake Sequence Number detection and Trust Based Routing

Input:

M: mobile node
S: Source node
R: receiver node
ack: acknowledge packet
S_p: suspicious symptoms (sequence very higher, data drop, ack not send)
B: black hole node
F_s: fake sequence number
r-pkt: route packet
T_r: trust calculator (pdr base)
P_s: neighbour nodes watcher and trust calculator
Ψ: radio range 550m
R_p: AODV

Output: *attack detection, packet delivery ratio, throughput, routing overhead, end to end delay*

B. Methodology:

S initiate route request packet (AODV)
Bind AODV(S, R, r-pkt)
If *M_n in Ψ & M_n != R* ***Then***
M_n ← generate routing table (M_{n_id})
If *M_n as B* ***Then***

International Journal of Current Trends in Engineering & Technology
Received 1 February 2019, Revised form, 28 March 2019, Accepted 20 April 2019, Available online 26 April 2019
www.ijctet.org, ISSN: 2395-3152
Volume: 05, Issue: 02 (March- April, 2019)

M_n generate F_s
Instant generate reply packet send ack to S
S send(M_n , data)
Else
M_n forward routing packet to next hop
End if
Else if *M_j in Ψ & M_j == R* ***Then***
R receives route packet
Select shortest path
Generate reverse path
R send reply packet to S
Else
R not found or out of Ψ
End if
#Prevention Module *P_s nodes watch the M_j nodes*
If *P_s detect M_j generate F_s* ***Then***
Instant block M_j
P_s send block information to S node ***Else if*** *S send data by M_j node* ***Then***
M_j receives data and not forward to next hop
P_s watch neighbour activity
P_s calculate T_r
T_r ← M_j(send/receives)
If *T_r of M_j is < 80% & queue is ideal* ***Then***
P_s set M_j as S_p
Critical analyze the symptoms
If *symptoms is hseq & high data drop & ack not send* ***Then***
Block M_j by P_s
P_s send block information to S node
Else
P_s Only watch M_j
End if
Else
M_j behave normal
Else
M_j is a true route
End if

V. Simulation Parameters

The simulation of attack presence, existing and proposed Fake Sequence Number Detection (FSND) security scheme is evaluated on the basis of following simulation parameters mentioned in Table 1. The simulations of all the modules are done in four different node density scenarios of 20, 25, 30 and 35. The all nodes are movable and using Random Waypoint model. The number of black hole nodes are considered for simulation is 1,2,3 and 4 i.e. used in respective node density scenarios.

VI. Result Description

A. Packet Delivery Ratio Analysis

The packets percentage performance is measured through of Packet Delivery Fraction (PDF). In this graph the PDF analysis in case of black hole attack, previous security scheme and Fake Sequence Number Detection (FSND) is evaluated. The normal routing performance is only evaluated to stint the network performance after applying proposed security scheme. The effect of black hole attack in network is 8 % in 20 node density and after that the percentage of receiving is improves but it is count maximum up to 19% in 35 node density. The proposed FSND scheme is improves the network performance and provides secure routing. The performance of network almost provides 79% PDF, that are improves after applying security scheme against attack. The proposed security scheme is improved the performance in presence that is also better than existing scheme in MANET.

Table 1: Simulation Parameters

Parameters	Value
Network Type	MANET
Simulation Time	100 [s]
Nodes/Devices	20, 25, 30, 35
Network Area	800*800 [m]
Mobility Model	Random Waypoint
Physical Medium	Wireless
Data Packet Size	512 [bytes]
MAC Layer	802.11
Routing Protocol	AODV
Prevention Method	Fake Sequence No Detection & Trust Based Prevention.
Traffic Type	CBR, FTP
Number of Connection	Random
Propagation radio model	Two ray ground
Number of black hole nodes	1, 2, 3, 4
Rate	10 Packet/s

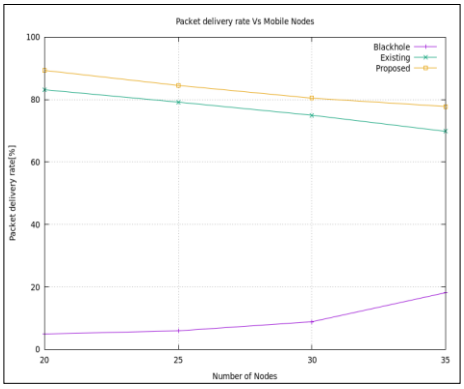

Figure 1: Packet Delivery Ratio Analysis

B. Normalized Routing Overhead Analysis

The overhead in network is enhanced due to the loss of data packets and the loss of data is also enhance the overhead. The loss of data is also improving the control overhead performance because of retransmission of control packets. The number of attacker nodes presence are enhancing the overhead due to loss of almost complete data packets. The overhead performance of existing security scheme is showing the overhead less than one in network. The performance of proposed FSND is improves the performance that's why the overhead is minimum. The

International Journal of Current Trends in Engineering & Technology
Received 1 February 2019, Revised form, 28 March 2019, Accepted 20 April 2019, Available online 26 April 2019
www.ijctet.org, ISSN: 2395-3152
Volume: 05, Issue: 02 (March- April, 2019)

overhead in presence of attacker is also maximum or relay almost more than six time more as compare to proposed scheme. The higher overhead performance is showing the degrade in packets receiving.

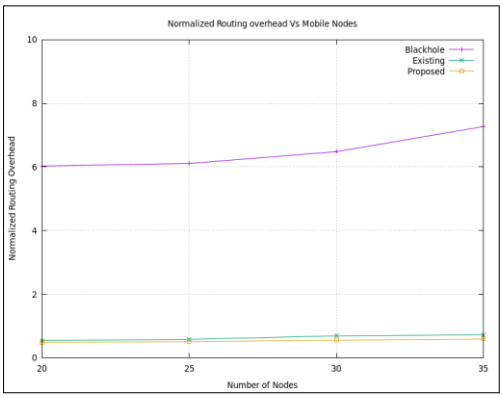

Figure 2: Normalized Routing Overhead

C. End to End Delay Analysis

The End to End delay analysis is measures in presence of attacker, in existing security scheme and in FSND proposed scheme. The performance is measured in all different node density scenarios. The main reason of delay is to re-establishment of connection again and again due to link breakage or successful not receiving the data at destination. The End to End delay in presence of attacker is high and the delay is minimizing by applying existing security scheme but proposed security scheme is minimizing the delay and provides strong connection establishment. The delay in network is degrades the routing performance due to the presence of attacker.

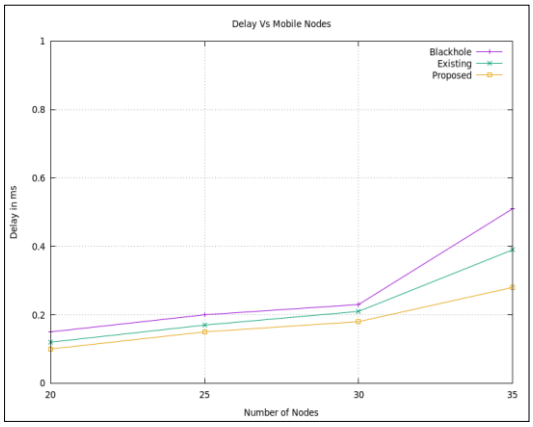

Figure 3: End to End Delay Analysis

D. Throughput Analysis

The better throughput performance is also representing the better data receiving in network. In this graph the throughput performance measurement of Exiting Scheme, Black hole attack and proposed FSND is measured. The noticeable thing is that the in case of existing approach the throughput percentage is about maximum 90 % per second in network but in case of black hole attack the throughput performance is 40% in network in 35 node density, means up to end of simulation it is about only 40% of packets received from total sending. but after applying proposed FSND scheme the throughput is enhance up to 96% packets/ sec. It means the proposed FSND scheme are definitely improves the network performance and providing the attacker free background of communication in between sender and receiver through intermediate nodes.

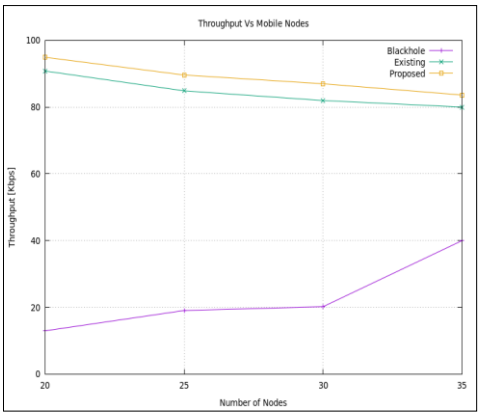

Figure 4: Throughput Analysis

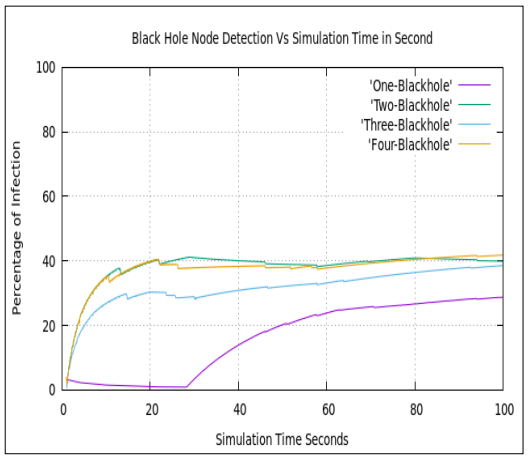

Figure 5: Black Hole Attack Percentage

E. Black Hole Attack Percentage Analysis

The black hole attacker is very harmful for the network because those nodes that are in range of attacker then attacker are definitely sending the fake message to sender or sending the wrong information of path to sender. The fake path is actually directly connected to attacker and attacker is actually receiving the packets from sender and drops the whole packets. The performance of attacker loss percentage is mentioned in this graph in all node density scenarios. The numbers of attacker nodes in network are in different quantity in different node density scenario. The loss percentage is minimum in one black hole node about 20% and loss percentage is more in 3 or 4 attacker nodes about 40%. That means the attacker consumes 40% of data in network and rest of the data us drop due to nor receive packets means receive incomplete data.

VII. Conclusion & Future Work

The malicious nodes or attacker is only aim to agitate actual performance of network. The MANET is completely dynamic and, in this network, attackers are easily modified actual performance. The malicious attacker is considered in

this research is actually affected the original routing performance of dynamic network. The nodes in dynamic network are mobile and forming a temporary connection in between sender and receiver through intermediate nodes or sometime directly. The routing protocol is transferring the data in between sender and receiver through intermediate nodes. The connection establishment up to destination through source having a combination of normal nodes and malicious node and attacker aim is to drop data packets sending by sender to destination after connection establishment. we proposed Fake Sequence Number Detection (FSND) security algorithm against black hole attack, that is always tried to be a part of fake path established by attacker for loss data packets. The black hole attacker is degrading the routing performance of network and the attacker infection is measure in four node density scenarios. After detecting the malicious nodes the proposed secure mechanism is also prevent from attacker by deny the possibility of routing through malicious nodes. The performance metrics shows the difference in performance of attacker and proposed FSND and clearly conclude that performance of proposed scheme is proving the secure communication. The PDF is about 85% in proposed security scheme and about 5% less in existing security scheme. The presence of attacker is very poor, about less than 18% maximum in 35 nodes density. The packet dropping is reduced and enhance receiving of data packets. The performance of transport layer protocol is also satisfactory. The rest of the performance like delay, throughput and overhead in existing is better but very good in proposed security scheme. The attacker presence is confirming by detection the loss of data and fake route information in dynamic network. The proposed scheme is minimizing overhead and delay i.e. the main cause to degrades the routing performance because a greater number of packets are drooping are enhancing the delay and overhead. In future also the simulation is performing through different routing protocol like OLSR and multipath routing protocols. Apply the same detection and prevention scheme to secure routing protocol. The network is dynamic that's why also applying Location Tracker System to trace attacker easily and also aware forwarding massage to nearby nodes of network about malicious activities and apply proper Location based security scheme.

REFERENCES

[1]. Taku Noguchi, Mayuko Hayakawa "Black Hole Attack Prevention Method Using Multiple RREPs in Mobile Ad-Hoc Network" 2018 17th International Conference on Trust, Security And Privacy In Computing And Communication /12th IEEE International Conference On Big Data Science And Engineering.

[2]. 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.

[3]. 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.

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

[5]. 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.

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

[7]. Ei Khin and Thandar Phyu "Impact Of Black Hole Attack On Aodv Routing Protocol" International Journal of Information Technology, Modeling and Computing (IJITMC) Vol. 2, No.2, May 2014.

[8]. Rupinder Kaur and Parminder Singh "Review Of Black Hole And Grey Hole Attack" The International Journal of Multimedia & Its Applications (IJMA) Vol.6, No.6, December 2014.

[9]. Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon and Kendall Nygard "Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks" North Dakota State University, Fargo,

[10]. Vipin Khandelwal, Dinesh Goyal "Black Hole Attack and Detection Method for AODV Routing Protocol in MANETs" International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 4, April 2013.

[11]. Jaspal Kumar, M. Kulkarni, Daya Gupta "Effect of Black Hole Attack on MANET Routing Protocols" I. J. Computer Network and Information Security, 2013, 5, 64-72 Published Online April 2013 in MECS.

[12]. Ashish Sharma, Dinesh Bhuriya , Upendra Singh , Sushma Singh "Prevention of Black Hole Attack in AODV Routing Algorithm of MANET Using Trust Based Computing" Ashish Sharma et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (4) , 2014

[13]. SUSHIL KUMAR CHAMOLI, SANTOSH KUMAR, DEEPAK SINGH RANA, "Performance of AODV against Black Hole Attacks in Mobile ad-hoc Networks" Sushil Kumar Chamoli et al ,Int. J. Computer Technology & Applications, 1395-1399

[14]. Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method" International Journal of Network Security, Vol.5, No.3, PP.338–346, Nov. 2007.