International Journal of Scientific Research & Engineering Trends
Volume 6, Issue 1, Jan-Feb-2020, ISSN (Online): 2395-566X

A High Sequence Value and Packet Dropping based Security Scheme in MANET

M. Tech. Scholar Alok Gupta, Nikhil Ranjan
Dept. of ECE
RKDF Institute of Technology, Bhopal, India
alokguptadc@gmail.com,nikhilranjan101@gmail.com

Abstract **- The malicious nodes are always stump intermediate nodes in routing procedure because these nodes are only receive and forward respond of surrounding neighbour. The intermediate nodes work is very responsible in routing procedure with continuous movement. In this research we proposed Malicious Sequence Number Identification (MSNI) security algorithm against malicious blackhole attack in MANET. The blackhole 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 detect the attacker presence and also estimate total number of packets is dropped by Blackhole attacker in network. The packet dropping on link through node is detected and prevented by security system. The blackhole presence is makeable in different node density scenarios and the single as well as multiple presences is detected by MSNI scheme. This method not only identified the balckhole nodes but also prevent from routing misbehaviour of attacker nodes. security is less effective on attacker/s. The performance of existing security scheme is compare with proposed MSNI and the performance of existing scheme is pitiable. The proposed secure MSNI is securing the MANET and improves the network performance after blocking malicious nodes in network. The network performance in presence of attack and secure MSNI 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.**

Keywords- **MANET, Blackhole Attack, MSNI, Security, Routing, Nodes.**

I. INTRODUCTION

All 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 MANET [1] [2]. 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) [3]. Mobile ad-hoc networks are usually susceptible to different security threats and malicious node attack is one of these. In this attack, a 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 [2].

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. The sender S sends data to destination D mentioned in figure 1.

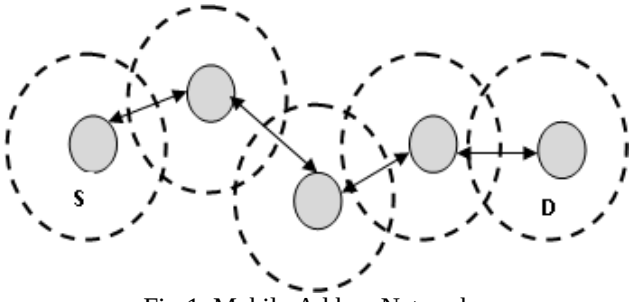

Fig.1. Mobile Ad hoc Network.

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 assemble [4]. 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.

II. LITERATURE SURVEY

The The previous work provides the information of security scheme that provides security in MANET. Some of the scheme is mention below:-

Taku Noguchi et al. [5] proposed a method in which intermediate nodes rebroadcast only the primary route request with the same request_id and not at all rebroadcast any subsequent request. After receiving a request, the destination node or an intermediate node that has a fresh enough entry for the destination in its routing table responds by unicasting a reply packet back to the source node. When an intermediate node receives a reply packet from its neighbors, unlike in AODV, it forwards multiple replies to its next hop nodes. In the proposed method, intermediate nodes maintain often multiple routing entries with different next hops for the source node of the request. An intermediate node makes copies of the received reply and forwards them to each next hop toward the source node.

Hussain et al [6] proposed Denial of Service Attack in AODV & Friend features Extraction to style Detection Engine for Intrusion Detection System in Mobile Adhoc Network. during this work Denial of Service attack is applied within the network, evidences are collected to style intrusion detection engine for MANET Intrusion Detection System (IDS). Feature extraction and rule inductions are applied to seek out out the accuracy of detection engine by exploitation support vector machine.

Jing-Wei Huang et al [7] proposed Multi-Path Trust-Based Secure AOMDV Routing in unexpected Networks. during this work uses a trust based mostly multipath AOMDV routing combined with soft encoding, yielding our so-called T-AOMDV scheme. a lot of exactly, this approach consists of 3 steps: (1) Message encoding – wherever at the supply node, the message is segmented into three components and these components are encrypted using one another using some XOR operations, (2) Message routing – wherever the message components are routed on an individual basis through totally different trust based mostly multiple ways using a novel node disjoint AOMDV protocol, and (3) Message coding – wherever the destination node decrypts the message components to recover the first message.

Shreenath et al [8] planned Countermeasures against Multicast Attacks on Enhanced-On Demand Multicast Routing Protocol in MANETs. This work concentrate on rising the Secure Enhanced-On Demand Multicast Routing Protocol (EODMRP) to safeguard it against flooding and blackhole attacks. The planned mechanism is for flooding attack works even once the identity of the malicious nodes is unknown and doesn't use any extra network bandwidth. The performance of alittle multicast cluster can degrade seriously below these kinds of attacks even the answer is obtainable. The planned algorithm provides protection against region attack in MANET.

Sujatha et al. [9] planned style of Genetic algorithmic program based mostly IDS for painter. during this work a method to research the exposure to attacks in AODV, specifically the foremost common network layer hazard, region attack and to develop a specification based Intrusion Detection System (IDS) exploitation Genetic algorithm approach. The planned system relies on Genetic algorithm, that analyzes the behaviors of each node and provides details regarding the attack.Genetic algorithm control (GAC) may be a set of varied rules supported the important options of AODV like Request Forwarding Rate, Reply Receive Rate and then on.

Konate et al [10] proposed AN Attacks Analysis in mobile unexpected networks: Modeling and Simulation. in this paper present work is devoted to review attacks and countermeasures in MANET. when a brief introduction to what MANETs are and network security we tend to gift a survey of varied attacks in MANETs relating fail routing protocols. we tend to additionally gift the various tools employed by these attacks and also the mechanisms utilized by the secured routing protocols to counter them. during this outlined the conception of DoS like its varied varieties.

Gandhewar et al [11] planned Detection and prevention of sinkhole Attack on AODV Protocol in Mobile Adhoc Network. This work in the main focuses on sinkhole

problem, its consequences & presents mechanism for detection & prevention of it on the context of AODV protocol. depression is one among severe quite attack that makes an attempt to draw in most of network traffic towards it & degrade the performance of network. AODV is principally analyzed below blakhole, wormhole & flooding attack, that must analyze below other forms of attack additionally.

P.K Singh et al [12] proposed an efficient prevention of black hole problem in AODV Routing Protocol in MANET. in this work a solution to the region attack in one among the foremost outstanding routing algorithmic program, ad-hoc on demand distance vector (AODV) routing, for the MANETs. The region attack is one among such security risks. during this attack, a malicious node incorrectly advertise shortest path to the destination node with an meaning to disrupt the communication. The proposed methodology uses promiscuous mode to discover malicious node (black hole) and propagates the knowledge of malicious node to any or all the opposite nodes within the network.

Sanjay Ramaswamy et al. [13] "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 et al. [14] "BlackHole 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 BlackHole 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.

III. PROBLEM STATEMENT

Mobile ad-hoc communication is a growing field of latest research but it's vulnerable due to decentralized routing strategies. Defence of any network is one of the important parts of communication. In the existing research many researcher provide the methodology to secure the mobile ad-hoc communication from various attacks. In the mobile ad-hoc network, routing attack is more harmful as compare to other attack, from the past research studies shows and conclude that the network layer attack such as black hole attack is a more challenging task to controlled and completely remove from the network. From the existing security mechanism we identifies that no one can fully prevent the black hole node in dynamic environment, that's why our aim to decide the work under field of black hole attack defence mechanism through fake sequence number detection and trust based routing based communication in MANET.

IV. PROPOSED APPROACH

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

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**
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. RESULT ANALYSIS

The result analysis of previous wok and proposed work is mentioned in this section. The simulation of both the protocols are done in NS-2 simulator [15].

1. 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 blackhole attack, previous security scheme and Malicious Sequence Number Identification (MSNI) is evaluated. The normal routing performance is only evaluated to stint the network performance after applying proposed security scheme. The effect of blackhole 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 MSNI 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.

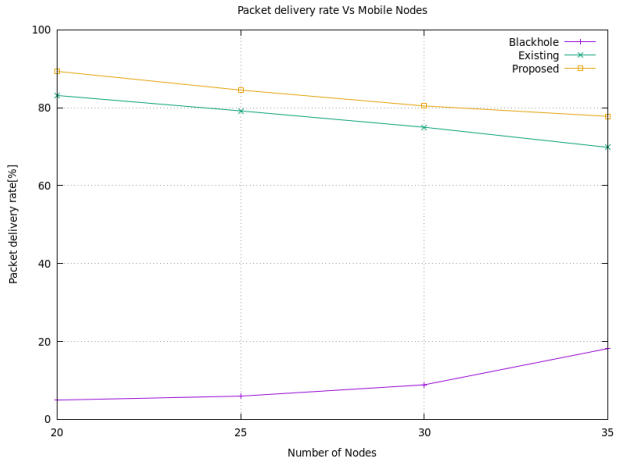

Fig.2. PDR Analysis.

2. 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 improves the control overhead performance because of retransmission of control packets. The number of attacker nodes presence are enhance 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 MSNI is improves the performance that's why the overhead is minimum. The 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 are showing the degrades in packets receiving.

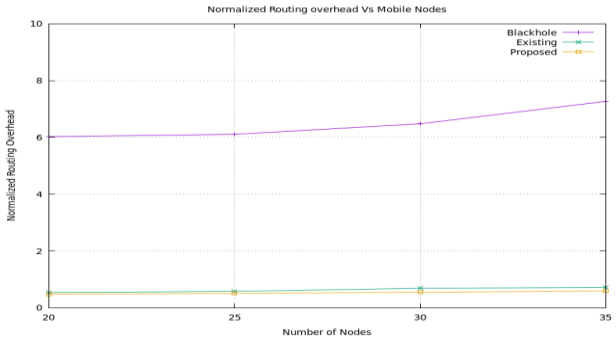

Fig.3. Overhead Analysis.

3. End to End Delay Analysis

The End to End delay analysis is measures in presence of attacker, in existing security scheme and in MSNI 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 minimizes by applying existing security scheme but proposed security scheme is minimizes the delay and provides strong connection establishment. The delay in network is degrades the routing performance due to the presence of attacker.

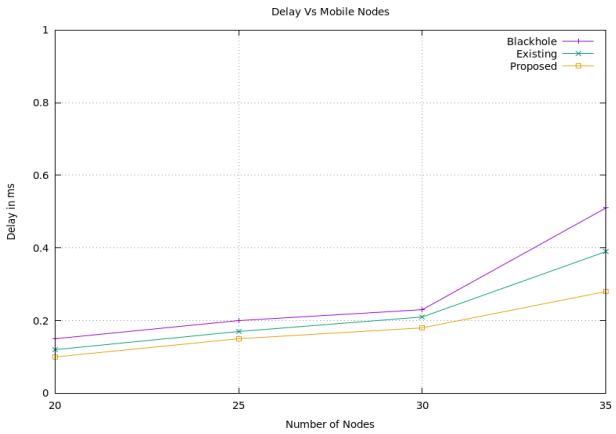

Fig.4. End to End Delay Analysis.

4. Throughput Analysis

The better throughput performance is also represents the better data receiving in network. In this graph the throughput performance measurement of Exiting Scheme, Blackhole attack and proposed Malicious Sequence Number Identification (MSNI) 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 blackhole 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 MSNI scheme the throughput is enhance up to 96% packets/ sec. It means the proposed MSNI scheme are definitely improves the network performance and providing the attacker free background of communication in between sender and receiver through intermediate nodes.

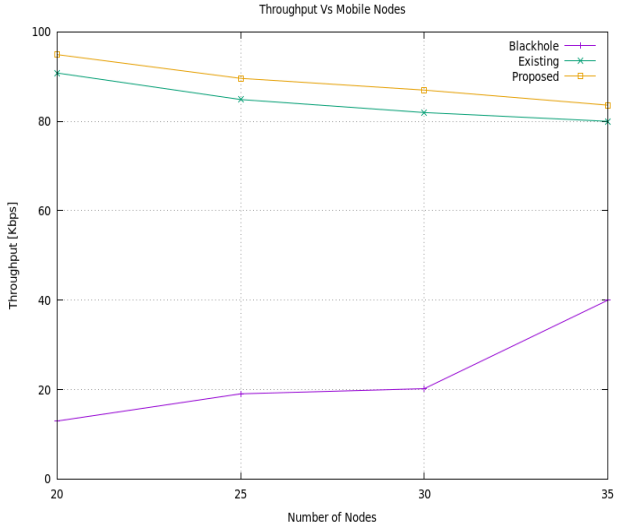

Fig.5. Throughput Analysis.

5. Black Hole Attack Percentage Analysis

The blackhole 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 blackhole 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.

Figure 6 Attacker Loss Percentage Analysis.

VI. CONCLUSION AND FUTURE WORK

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 Malicious Sequence Number Identification (MSNI) security algorithm against blackhole attack, that is always tried to be a part of fake path established by attacker for loss data packets.

The blackhole attacker are degrades 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 MSNI 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 19% 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 confirm by detection the loss of data and fake route information in dynamic network. The proposed scheme is minimizes overhead and delay i.e. the main cause to degrades the routing performance because more 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]. Amitabh Mishra, “Security and Quality of Service in Ad Hoc Wireless Networks” (chapter 1, 3), ISBN- 13 978-0-521-87824-1 Handbook, 2008.

[2]. Magnus Frodigh, Per Johansson and Peter Larsson "Wireless ad hoc networking-The art of networking without a network," Ericsson Review No. 4, 2005.
[3]. Charles Perkins and Elizabeth Royer "Ad hoc on-demand distance vector routing", In Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, pages 90–100, Feb-2008.
[4]. Irshad Ullah and Shahzad Anwar "Effects of Black Hole Attack on MANET Using Reactive and Proactive Protocols" IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 3, No 1, May 2013.
[5]. Taku Noguchi, Mayuko Hayakawa, "Black Hole Attack Prevention Method Using Multiple RREPs in Mobile Ad Hoc Networks", 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering, 2018.
[6]. Husain. Shahnawaz, Gupta S.C., Chand Mukesh "Denial of Service Attack in AODV & Friend Features Extraction to Design Detection Engine for Intrusion Detection System in Mobile Adhoc Network", International Conference on Computer & Communication Technology (ICCCT-2011), pp. 292-297, 2011.
[7]. Jing-Wei Huang, Isaac Woungang, Han-Chieh Chao, Mohammad S. Obaidat, Ting-Yun Chi, Sanjay K. Dhurandher "Multi-Path Trust-Based Secure AOMDV Routing in Ad Hoc Networks", proceedings of IEEE Global Telecommunications Conference (GLOBECOM 2011), pp. 1-5, 2011.
[8]. Dr. N. Sreenath, A. Amuthan, & P. Selvigirija "Countermeasures against Multicast Attacks on Enhanced-On Demand Multicast Routing Protocol in MANETs", International Conference on Computer Communication and Informatics (ICCCI), pp. 1-7, 2012.
[9]. K. S. Sujatha, Vydeki Dharmar, R. S. Bhuvaneswaran "Design of Genetic Algorithm based IDS for MANET", International Conference on Recent Trends in Information Technology (ICRTIT), pp. 28-33, 2012.
[10]. Dr Karim Konate, Gaye Abdourahime "Attacks Analysis in mobile ad hoc networks: Modeling and Simulation", 2011 Second International Conference on Intelligent Systems, Modelling and Simulation, pp. 367 – 372, 2011.
[11]. Gandhewar, N., Patel, R. "Detection and Prevention of Sinkhole Attack on AODV Protocol in Mobile Adhoc Network", Fourth International Conference on Computational Intelligence and Communication Networks (CICN), pp. 714 – 718, 2012.
[12]. P.K Singh, G. Sharma, "An Efficient Prevention of Black Hole Problem in AODV Routing Protocol in MANET", IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), pp. 902 – 906, 2012.
[13]. Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon and Kendall Nygard "Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks," Conference: Proceedings of the International Conference on Wireless Networks, (ICWN), 2003.
[14]. Vipin Khandelwal, Dinesh Goyal "BlackHole Attack and Detection Method for AODV Routing Protocol in MANETs" International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 4, 2013.
[15]. "NS2Tutorials," http://www.isi.edu/nsnam/ns, visit on October 2018.