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

A Security Scheme for Malicious Packet Dropping Attack in MANET

Utsav Singhi
M. Tech. Scholar Department of CSE
RKDF, University, Bhopal, M.P., India
singhiutsav@gmail.com

Prof. Gagan Sharma
HOD Department of CSE
RKDF, University, Bhopal, M.P. India
gagansharma.cs@gmail.com

***Abstract*—The MANET is the collection of mobile hosts that communicate with each other without any infrastructure. The security vulnerabilities of the routing protocols may be unprotected against attacks by the malicious nodes. The malicious attacks are maintained the integrity and absorbing all data packets in the network. Since the data packets do not reach the destination node on account of this attack, data loss will occur. The damage will be serious if malicious node in a network working as an attacker node absorbs all data packets delivered through them. In this research we proposed a novel Intrusion Detection System (IDS), neighbor based against malicious attack and measure the network performance after applying IDS scheme and malicious attack. The comparison of security scheme is applied on packet dropping attack and observe that the proposed security based scheme is providing better results in dynamic network. The routing misbehavior is evaluated negligible in dynamic network. The simulated scenario of normal, malicious and proposed security scheme against attacks is simulated in network simulator 2 (ns-2) and measured the packet loss in the presence of packet dropping attack and in presence of proposed IDS. The security scheme is improving the network performance and provides the reliable communication among the mobile nodes in the network.**

***Keywords*: -Security, Malicious Attack, Routing, IDS, NS-2.**

I. INTRODUCTION

All Mobile Ad-Hoc Network (MANET) is associate infrastructure less assortment of mobile nodes that may at random modification their geographic locations such these networks have dynamic topologies and random quality with forced resources. They even have capability of network partition [1]. A mobile ad-hoc network (MANET) could be a self-organized multi-hop system comprised of mobile wireless nodes. Two nodes out of direct communication want intermediate nodes to forward their messages. Because of multi-hop routing and open operating surroundings, MANETs area unit prone to attacks by stingy or malicious nodes, like packet dropping (black-hole) attacks and selective forwarding (gray-hole) attacks. All assure of MANET to resolve or disputing universe issues continues to hunt the eye from industrial and educational analysis comes. The foremost topographic point of analysis in mobile unintended networks is to produce sure surroundings and secure communication. There is a unit many applications of unintended network which require extremely protected communication. Common applications of MANET are: military or police networks, business operations like oil drilling platforms or mining operations and emergency response operation like when natural disaster sort of a flood, tornado, cyclone and earthquakes [2]. In black hole attack [2] the assailant records the packets (bits) at one location and tunnel them in another location in same network or in numerous networks. The assailant will transfer every bit directly, while not waiting the whole packet. It's terribly tough to search out the situation of region attack while not having the cytological key or while not well-known infrastructure of routing protocols. There is a unit essentially three forms of routing protocols: reactive routing protocol, proactive routing protocol and hybrid routing protocol [3, 4]. In proactive or table-driven routing protocols, every node unceasingly maintains up-to-date routes to each alternative node within the network. Routing info is sporadically transmitted throughout the network so as to take care of routing table consistency. Thus, if a route has already existed before traffic arrives, transmission happens at once. Proactive protocols suffer the disadvantage of further management traffic that's required to repeatedly update stale route entries. Since the topology is dynamic, once a link goes down, all methods that use that link area unit broken and need to be repaired. If no application is persecution these methods, then the hassle gone in to repair could also be thought of wasted. This wasted effort will cause scarce information measure resources to be wasted and may cause any congestion at intermediate network points. In distinction to proactive approach, in reactive or on demand protocols, a node initiates a route discovery throughout the network, only if it needs to send packets to its destination. For this purpose, a node initiates a route discovery method through the network. This method is completed once a route is decided or all potential permutations are examined. Once a route has been established, it's maintained by a route maintenance method till either the destination becomes inaccessible on each path from the supply or till the route isn't any longer desired. In reactive schemes, nodes maintain the routes to active destinations. A route search is required for each unknown destination. Finally, in hybrid protocols, every node maintains each the topology info among its zone and therefore the info relating to neighboring zones which means proactive behavior among a zone and reactive behavior among zones. Thus, a route to every destination among a zone is established at once, whereas a route discovery and a route maintenance procedure is needed for destinations that area unit in alternative zones.

II. ATTACK ASPECTS

The property of mobile nodes over a wireless link in MANETS that is multi hop in nature powerfully depends on the actual fact that ensures cooperation among the nodes within the network. Since network layer protocols forms property from one hop neighbors to any or all alternative nodes in MANET, the peace of mind of cooperation among nodes is needed. The attacks in MANETS area unit classified into two major classes, particularly passive attacks and active attacks, consistent with the attack suggests that [5]. Passive attacks area unit those, launched by the adversaries exclusively to snoop the info changed within the network. These adversaries in any manner don't disturb the operation of the network. Such attacks identification becomes terribly tough since network itself doesn't affect and that they will reduced by persecution powerful encoding techniques. However, an energetic attack tries to change or destroy the knowledge that's being changed, thereby distressing the conventional practicality of the network. Passive attacks are often listed as eavesdropping, traffic analysis, and traffic observance. Active attacks embrace hole, black hole, gray hole, info revelation, resource consumption, routing attacks et al embrace electronic jamming, impersonating, modification, denial of service (DoS), and message replay. Such attacks are often prevented by persecution powerful encoding techniques and firewalls. Internal attacks area unit launched by the compromised nodes among the network. This node tries to gather security info and may access the protected rights of the network. Since the compromised node is a licensed one within the network, it's terribly tough to spot the inner attacks.

III. LITERATURE SURVEY

The previous work in field of security in MANET is discussed in this section. Each and every author is providing their valuable contribution.

Tao Shu and Marwan Krunz [6], we develop an accurate algorithm for detecting selective packet drops made by insider attackers. This algorithm also provides a truthful and publicly verifiable decision statistics as a proof to support the detection decision. The basic approach behind this method is that even though malicious dropping may result in a packet loss rate that is comparable to normal channel losses, the stochastic processes that characterize the two phenomena exhibit different correlation structures (equivalently, different patterns of packet losses). Therefore, by detecting the correlations between lost packets, one can decide whether the packet loss is purely due to regular link errors, or is a combined effect of link error and malicious drop. This algorithm takes into account the cross-statistics between lost packets to make a more informative decision, and thus is in sharp contrast to the conventional methods that rely only on the distribution of the number of lost packets.

Hussain et al [7] planned Denial of Service Attack in AODV &amp; Friend options Extraction to style Detection Engine for Intrusion Detection System in Mobile Ad-hoc Network. During this work Denial of Service attack is applied within the network, evidences square measure collected to style intrusion detection engine for painter Intrusion Detection System (IDS). Feature extraction and rule inductions square measure applied to search out the accuracy of detection engine by exploitation support vector machine. True Positive generated by the detection engine is incredibly high and False Positive is suppressed to negligible. True positive are going to be according in no time in Lids &amp; Friend list generated by Lids are going to be sent to the Grids module for more investigation. world Detection Engine can generate the friend list in line with trust level, higher the trust level of the node is also used for different completely different processes like routing, and deciding the cluster head for ascendible ad-hoc networks. Feature extracted for Routing parameters and painter Traffic generation parameters may be used for various routing protocols. For detection engine machine learning algorithmic rule Support Vector Machine is employed that is lightweight weighted and regarded best among the supervised learning algorithms, prediction (accuracy) generated by the SVM for input options and completely different values of C &amp; λ to established the system for given coaching and testing information sets square measure satisfactory.

Jing-Wei Huang et al [8] planned Multi-Path Trust-Based Secure AOMDV Routing in mobile ad-hoc Network s. During this work uses a trust based mostly multipath AOMDV routing combined with soft cryptography, yielding our supposed T-AOMDV theme. a lot of exactly, this approach consists of 3 steps: (1) Message cryptography – wherever at the supply node, the message is metameric into 3 elements and these elements square measure encrypted exploitation each other exploitation some XOR operations, (2) Message routing – wherever the message elements square measure routed severally through completely different trust based mostly multiple ways employing a novel node disjoint AOMDV protocol, and (3) Message coding – wherever the destination node decrypts the message elements to recover the first message.

Shreenath et al [9] planned Countermeasures against Multicast Attacks on Enhanced-On Demand Multicast Routing Protocol in MANETs. This work concentrates on raising the Secure Enhanced-On Demand Multicast Routing Protocol (EODMRP) to safeguard it against flooding and region 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 information measure. The performance of a tiny low multicast cluster can degrade seriously beneath these sorts of attacks even the answer is accessible. The planned algorithmic rule provides protection against region attack in painter.

Sujatha et al. [10] planned style of Genetic algorithmic rule based mostly IDS for painter. during this work a way to research the exposure to attacks in AODV, specifically the foremost common network layer hazard, region attack and to develop a specification based mostly Intrusion Detection System (IDS) exploitation Genetic algorithmic rule approach. The planned system is predicated on Genetic algorithmic rule that analyzes the behaviors of each node and provides details concerning the attack. Genetic algorithmic rule management (GAC) could 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 [11] planned AN Attacks Analysis in mobile ad-hoc networks: Modeling and Simulation. During this title gift work is devoted to check attacks and countermeasures in painter. Once a brief introduction to what MANETs square measure and network security we tend to gift a survey of varied attacks in MANETs touching on fail routing protocols. We tend to additionally gift the various tools employed by these attacks and also the mechanisms employed by the secured routing protocols to counter them. During this outlined the idea of DoS like its numerous sorts. They conferred many alternatives of DoS attacks met in MANETs, there in operation method so the mechanisms used and also the protocols that implement them to counter these attacks.

IV. PROPOSED SECURITY METHOD

In general, MANET routing protocols fall into two categories: proactive routing protocols that rely on periodic transmission of routing updates, and on-demand routing protocols that search for routes only when necessary. It should be nodded that malicious are dangerous by themselves, even if attackers are diligently forwarding all packets without any disruptions, on some level, providing a communication service to the network. Number is an increasing value, i.e., the next packet must have higher value that the current packet sequence number. The node in regular routing protocols keeps the last packet sequence number that it has received and uses it to check if the received packet was received before from the same originating source or not. In Intrusion detection system (IDS), every node needs to have two additional small-sized tables; one to keep last-packet-sequence-numbers for the last packet sent to every node and the other to keep last-packet-sequence-numbers for the last packet received from every node (from node through node). These tables are updated when any packet arrived or transmitted. The sender broadcasts the RREQ packet to its neighbors. Once this RREQ reach the destination, it will initiate a RREP to the source, and this RREP will contain the last- packet-sequence-numbers received from this source. When an intermediate node has a route to the destination and receives this RREQ, it will reply to the sender with a RREP contains the last- packet-sequence-numbers received from the source by this intermediate node. This solution provides a fast and reliable way to identify the suspicious reply. No overhead will be added to the channel because the sequence number itself is included in every packet in the base protocol.

Proposed Security Algorithm

```
Create mobile Node = N;            //Mobile Nodes
Sender Nodes = S;                  // S € N;
Destination Nodes = D;             // D € N;
Routing Protocol = AODV;
Set Simulation Time = T
While (S send RREQ_B)
 {   rtable -> insert(rtable->rt_nexthop);
     Add extra filed to rtable (next_hop, Through) //both value 1, 0 format
  If ((next_hop = true) && (through == true) && (send_D_pkt==true))
   {
        True route;
   }
     Else if (next_hop = false) && (through == false)
   {
     In previous No data and route through that hop;
     Insert into ->rtable;         // for route to destination if shortest path
       }
Else if ((next_hop = true) && (through == false) && (send_D_pkt==true)) // identified Probability factor based on data receiving
   {
   In previous No data through that hop;
   But exist in rtable entry; //Check reliability
   if next hop (next_hop is unreliable);
     {
     Block that Hop;
            }
 else
```

```
            {
              Send RREQ_B till the Destination}
                        }
      else
      {
            Send_RREQ_B to next other hop;
            Search destination D;
      }
      }
```

V. SIMULATOR OVERVIEW & PARAMETERS

We simulate our work using network simulator -2 generally known as NS-2 [12]. The entire simulations were carried out using ns 2.31 network simulator which is a discrete event driven simulator developed at UC Berkeley as a part of the VINT project. The goal of NS2 is to support research and education in networking. It is suitable for designing new protocols, comparing different protocols and traffic evaluations. NS2 is developed as a collaborative environment. It is distributed as open source software. A large number of institutes and researchers use, maintain and develop NS2. NS2 Versions are available for Linux, Solaris, Windows and Mac OS X. The simulator is written in C++ and a script language called OTcl2. Ns uses 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.

A. Simulation Parameter

Let's get Evaluation Parameter like Number of nodes, Dimension, Routing protocol, transport layer protocol, application layer data and maximum speed of mobile nodes etc. According to below table 1 we simulate our network.

B. Performance Evaluation Metrics

1) Malicious Loss

The malicious loss is measured in network by evaluate the number of dropping packets percentage by attacker nodes in network.

2) Packets dropped

Some of the packets generated by the source will get dropped in the network due to high mobility of the nodes, congestion of the network etc.

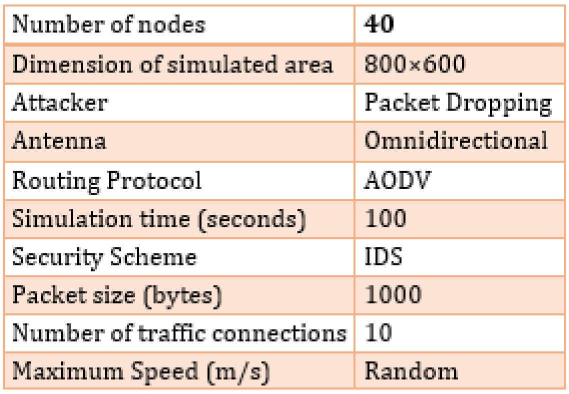
3) Packet delivery ratio

The ratio of the data packets delivered to the destinations to those generated by the CBR (Constant bit Rate) and FTP (File Transfer Protocol) sources.

4) Normalized routing overhead

The number of routing packets transmitted per data packet delivered at the destination. Each hop-wise transmission of a routing packet is counted as one transmission. The simulation is also measures on the basis of probability factor of routing packets and data packets. Less probability is shows better if the performance of network is better as for maximization.

Table 1 Simulation Parameters Consider for Simulation



Number of nodes	40
Dimension of simulated area	800×600
Attacker	Packet Dropping
Antenna	Omnidirectional
Routing Protocol	AODV
Simulation time (seconds)	100
Security Scheme	IDS
Packet size (bytes)	1000
Number of traffic connections	10
Maximum Speed (m/s)	Random

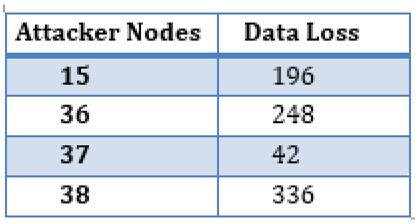
VI. RESULTS DESCRIPTION

The simulation results analysis is measured on the basis of existing proposed IDS (Intrusion Detection System) applied on packet dropping attack and compare their performance with normal routing.

A. Attacker Nodes Identification and Loss Analysis

The enhancement of packet loss is also enhancing the degradation in network performance in MANET. The attacker is easily affected the performance of decentralized network because of that network actual performance is affected. The attacker nodes loss is mentioned in table 2. The proposed IDS scheme is identified the four attackers and block their misbehavior activities in network.

Table 2 Attacker Loss Analysis



Attacker Nodes	Data Loss
15	196
36	248
37	42
38	336

B. Malicious Attackers Data Loss Percenatge Analysis

The malicious nodes or attacker in network is continuously dropping the packets by that the whole network performance is affected. The attacker detection and prevention in MANET is necessary for removing routing misbehavior, executed by attacker in network. In this graph the performance analysis of attacker misbehavior is evaluated in terms of loss percentage. The attacker loss percentage is continuously degrading with respect of time and lowest is 14% at the end of simulation. The attacker or malicious nodes are also mobile in dynamic network due to that misbehavior is also possible to reduced but not removed in network.

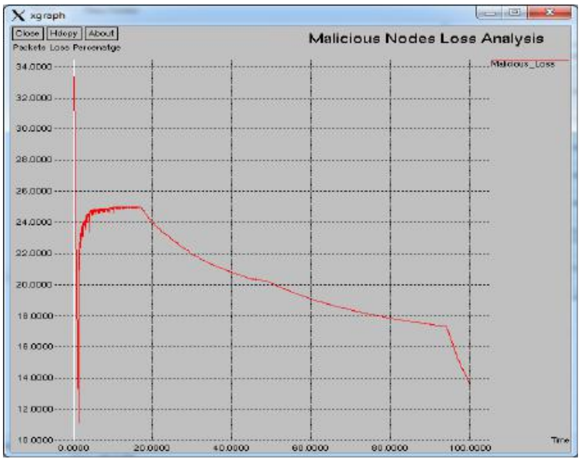


Fig.1 Malicious nodes Loss Analysis

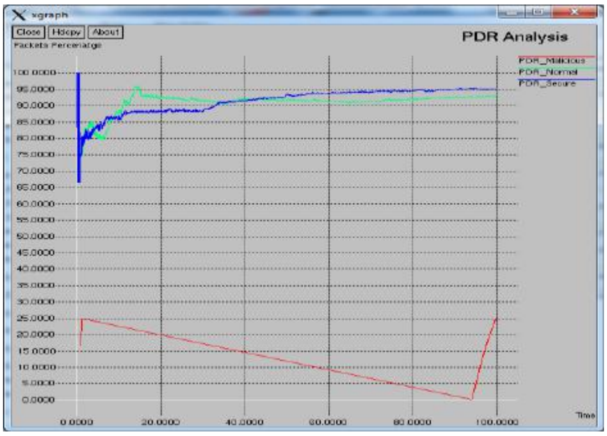


Fig.2 PDR Performance Analysis

C. PDR Analysis

The performance is measured by PDR metrics. The number of packets incoming to receiver and outgoing by sender performance in term of percentage is evaluated through Packets Delivery Ratio (PDR). In this scheme the packets percentage is counted of genuine packets sends by sender at current time to receiver. If packet delivery ratio is higher that means our performance is best, here in this result the PDR performance of normal routing scheme, Malicious attacker and proposed security scheme is measured and observe that the PDR of proposed scheme maximum about 95 %, normal is 93% and the attacker is only 25% and at time 90 second counts negligible the IDS improves routing performance.

D. Routing Packets Flooding Analysis

The number of routing packets flooded by sender for maintains the connection in between sender and receiver. In this simulation results analysis, we analyze same three cases of security scheme performance in routing packet analysis and we find that misbehaver nodes degrade the routing performance in network but also degrades the packets receiving. The attacker loss number of packets and also nodes are not instantly flooded routing packets The overhead performance of normal scheme is worst but data packets receiving is more in proposed security scheme in minimum overhead of packets.

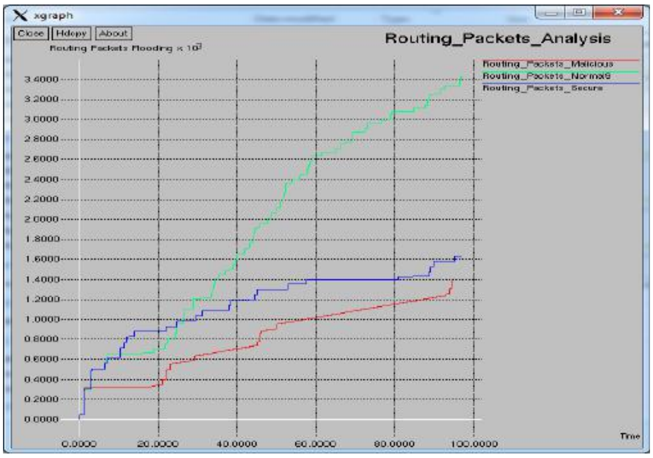


Fig.3 Routing Packets Flooding Analysis

VII. CONCLUSION & FUTURE SCOPE

Mobile Ad-hoc networks are a collection of mobile hosts that communicate with each other without any infrastructure. Due to security vulnerabilities of the routing protocols, wireless ad hoc networks may be unprotected against attacks by the malicious nodes. In this research we have gone through the routing security issues of MANETs, described the cooperative Malicious nodes attack that can be mounted against a MANET and proposed a feasible solution for it in the AODV protocol. The proposed solution can be applied to a) Identify malicious nodes in a MANET; and b) Discover secure paths from source to destination by avoiding malicious nodes acting routing misbehavior. The ML security scheme is better than the existing security scheme in MANET but the proposed hop based security scheme is better than the ML scheme and provides secure communication among mobile nodes. Also we showed that the effect of packet delivery ratio and throughput has been detected in case of attack. There is reduction in Packet Delivery Ratio and Throughput. In Malicious nodes attack all network traffics are redirected to a specific node or from the malicious node causing serious damage to network and nodes as shown in the result of the simulation. The energy efficient utilization of node is also the important issue in MANET. In Future we also work out on effect of attack on Node Energy, location based routing and Multicast routing protocols.

REFERENCES

[1]. C.R Dow, P J Lin, S .C Chen, J. H Lin, S. F Hwang "A Study of Recent Research Trends and Experimental

Guidelines in Mobile Ad-hoc Networks", Paper presented at the IEEE 19th International Conference on Advanced Information. Networking and Applications, Tamkang University, Taiwan, 28-30 March 2005.

[2]. Yibeltal Fantahun Alem, Zhao Cheng Xuan "Preventing Black Hole Attack in Mobile Ad-hoc Networks Using Anomaly Detection", 2nd International Conference on Future Computer and Communication (ICFCC), volume -3, pp. 672 – 676, 2010.

[3]. W.R. S. Jeyaseelan and Sh. Hariharan, "Investigation on routing protocols in MANET", International Journal of Research and Reviews in Information Sciences (IJRRIS), Vol. 1, No. 2, June 2011, ISSN: 2046-6439.

[4]. S. Shah, A. Khandre, M. Shirole and G. Bhole, "Performance evaluation of Ad hoc routing protocols using NS2 simulation", National Conference on Mobile and Pervasive Computing (CoMPC-2008).

[5]. Rashid Hafeez Khokhar, Md Asri Ngadi & Satria Mandala, "A Review of Current Routing Attacks in Mobile Ad Hoc Networks", International Journal of Computer Science and Security, volume 2, 2008.

[6]. Tao Shu and Marwan Krunz, "Privacy-Preserving and Truthful Detection of Packet Dropping Attacks in Wireless Ad Hoc Networks" IEEE Transactions On Mobile Computing, Vol. 14, No. 4, April 2015, pp. 813-828.

[7]. Husain. Shah Nawaz, 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.

[8]. 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.

[9]. 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* -2012), pp. 1-7, 2012.

[10]. 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.

[11]. 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.

[12]. http://www.isi.edu/nsnam/ns/