Secure IDS against Sybil Attacker Routing Misbehavior in MANET

Akanksha Jain
MTech Scholar of Information Technology
Samrat Ashok Technical Institute, Vidisha
M.P, India

Abhishek Mathur
Dept. of Information Technology
Samrat Ashok Technical Institute, Vidisha
M.P, India

ABSTRACT

Sybil attacker is the routing layer active attacker that replies with multiple identification number (ID's) to nodes that forward request to attacker in a different time instant and drop the data forwarded to attacker after link establishment. The proposed research work is provides the novel secure Intrusion Detection System (IDS) against routing misbehavior of Sybil attack in MANET. The IDS are not determining whether the losses are caused by link errors. It determines the loss due to malicious nodes. In the especially interested in the insider Sybil attack case, whereby malicious nodes that are part of the route exploit their data of the communication context to drop an amount of packets critical to the network performance. The basic idea behind this method is that even though malicious dropping may result in a packet loss rate that is not comparable to normal channel losses. The attacker loss is more than the loss of channel. The proposed IDS is detecting attacker node that reply with multiple ID’s and broadcast the particular attacker original ID’s that generate fake ID’s. Therefore, by detecting the malicious or attacker loss % is decided whether the packet loss is purely due to a combined effect of fake ID’s for malicious drop. The routing performance is measured through performance metrics and detection through TPR and FPR. The simulation of attacker and proposed IDS is done in ns-2 simulator.

Keywords

Sybil attacker, MANET, IDS, Routing, Multiple Identities, performance metrics, ns-2

1. INTRODUCTION

In Mobile Ad hoc network is the collection of mobile nodes that moves freely in the dynamic environment. In this kind of network mobile nodes are freely moves in a particular limited region [1]. The range of mobile nodes is fixed and these anodes are sense the neighbors and sends request for transmission to neighbors in a limited distance. Those nodes are forming the dynamic link in between sender to receiver through intermediate nodes [2]. The intermediate nodes are play a very important role in communication because these nodes are retrieve data from sender and forwarded to next neighbor till the destination is not receives. The figure 1 is the example of MANET where S has sends data to R through intermediate nodes A, B and C. The routing protocol is required to established connection and data delivery. The security is the main concern in MANET [3] because of the absence of centralized authority. The main characteristics of MANET are open medium, dynamic behavior and limited range of communication. This network is easily deployed in any area and in any situation. The easily network deployment of MANET is also not so costly then wireless network i.e. the main advantage of MANET but security factor in wireless network is the very strong point to chose this network.

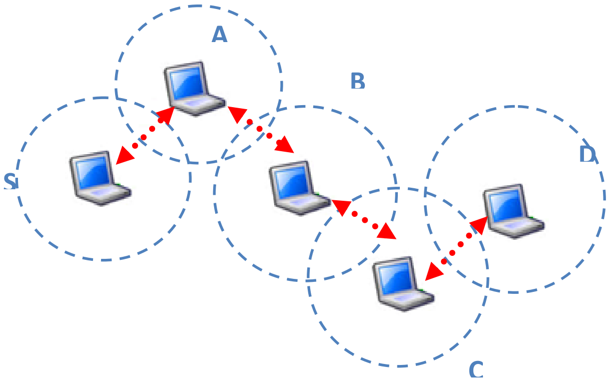

Fig. 1 Example of MANET

The security in MANET is a really a critical point of discussion. The MANET is vulnerable against attacks and the attackers are easily modified the original and normal performance of network by injecting the fake messages and dropping of valuable data of users. The attacks in MANET are classified in to two categories like active attack and passive attack [3]. The active attackers are very dangerous because they are actively participating in misbehavior activities for dumping the network performance at different layers of network. The examples of active attackers are well known Blackhole attack, Wormhole attack, DoS attack and Sybil attack. The passive attackers are not all time actively misbehaving or performing malicious activities but they active only for some time (at ant instants means at any time) but watches network activities all time. The active attacker misbehavior is limited and it drop only small amount of data. Although these attackers are more dangerous than active attackers because their bury monitoring are maintaining the record of network which is harmful for future heavy disaster. The identification or detection of passive attackers is not very easy. The active attackers are not observing are whole network activities. They are behaves like a normal nodes but after successful connection establishment perform malicious activities. The encryption decryption security scheme and IDS (Intrusion Detection System) against passive and active attackers is identified or detect the malicious actions done by attackers. The IDS are of many types [4, 5] that are detecting the malicious activities of attacker and provide the secure communication in MANET. The attacker detection is not only necessary but prevention is also required. The prevention system is protect the network by disable the communication capability of attacker and this attacker malicious record is maintained some time to recognizes the attacker attacks in future is easily identified and prevent.

In this paper the security against Sybil attack in MANET is proposed. In this scheme it’s proposed the secure IDS against Sybil attack. The attacker is has replies to requester node through multiple replies and these replies are IDS identified to match with node number. The whole attacker malicious record is maintained in a communication procedure in routing table and the attacker misbehavior performance is recognizes by IDS. The IDS is block the attacker and improves network performance.

2. ROUTING PROTOCOLS OVERVIEW

Routing is the procedure to finding the destination by source in network. The routing is playing the important role network because in absence of routing the connection in and route existence in network is not possible. The sender is created the request for destination then at network layer the routing procedure is initiated [6]. The network layer function is to complete the routing procedure through routing protocols. In wired and wireless network the routing protocols are different because here the route is forming in between the stationary hosts and if the communication devices or hosts are movable then in rage of centralized authority. In MANET the link in between sender and receiver is created in an open and dynamic environment. The nodes are incessantly modifying their present location. The efficient routing is the main challenge in MANET and the routing protocols in MANET and also are not same as traditional protocols that are used in wired network. There are many types of attacks in MANET that are affected the actual performance of network. In this research **the** proposed the secure routing scheme against Sybil attacker at network layer. The routing misbehavior of Sybil attacker is degrades the whole network performance by dropping the data packets. The routing protocols are not able to recognize the actual misbehavior of attacker because attacker is behaves like that the normal node in network. The MANET is the one type of wireless network but this network is totally different. There are three types of routing protocols [6, 7] in MANET

2.1 Proactive Routing Protocols

The proactive routing protocols routing procedure is slightly same as like wired routing protocols. In this routing technique the routing protocols are maintained the routing table on each node or router. The mobile nodes in MANET are creating the routing record to reduce the overhead of maintaining the same record repeatedly. But in dynamic network the topology is frequently changes and the table record of new incoming nodes in route establishment is not easy by that storage overhead is increased. The example of such type of protocol is DSDV (Dynamic Source Distance Vector) protocol.

2.2 The Reactive Routing Protocol

The reactive routing protocols are the second category of routing protocols in MANET. In reactive routing approach the nodes is established the connection in on-demand manner. The connection is only established if it is required. The nodes in MANET are not maintained the routing table or route information of nodes. The table is only maintained at the time of connection establishment and after complete data delivery connection is refuse and also the table record is refused. The AODV (Ad hoc On demand Distance Vector) Routing protocol is the example of reactive routing protocol.

2.3 The Hybrid Routing

The hybrid routing protocol is the combination of both the routing techniques like proactive and reactive. The hybrid routing protocol is marinating the table of information and also able to established the connection in an On demand manner. The routing procedure is called in a different zone or part of network. The example of hybrid routing protocol is ZRP (Zonal Routing Protocol).

In this research it consider the AODV routing protocol for route establishment and data delivery. The routing performance is measures in normal AODV, AODV with Sybil attack and AODV with Sybil attack and Secure IDS.

3. PREVIOUS WORK DISCUSSED

In this paper [8], the proposed system works considering the Certification Authority as one parameter and RSSI as the other parameter. The RSSI is used to form the cluster and to elect the cluster head. The CA's responsibility is given to the CH. Whenever huge variations occur in RSSI on neighbour's entry and exit behavior, the Certification Authority comes into play. The CA checks the certification of a node. If it is not valid, its certificate is revoked otherwise it is free to communicate in the network. RSSI (Received signal strength Indicator) as a parameter to detect the Sybil node because of its lightweight but it has failed to detect the fast moving Sybil nodes. The work is done in cluster based approach and used the concept of digital signature to identified attacker.

The RSSI value is measured through low and high energy value. The results are evaluated only on the basis of False positive Ratio (TPR) and True Positive Ratio (TPR).

In this paper [9] the attacker detection threshold based on the maximum speed of the network; assuming that no node can move faster than this maximum speed. This threshold will make the distinction because the first RSSs from newcomers, if greater than the threshold imply abnormal entry into the neighborhood. It also showed the various factors affecting the detection accuracy, such as network connections, packet transmission rates, node density, and node speed. This detection scheme can work as a standalone scheme, but could equally be deployed as an add-on to existing schemes, for example it could be incorporated into a reputation-based system, i.e., the detected Sybil identities from the MAC layer will be plugged into the reputation-based system on network layer. In our scheme, nodes share and manage identities of Sybil and non-Sybil nodes in distributed manner. The detection accuracy will be improved when nodes move with low speeds.

In this paper [10] the enhanced the lightweight Sybil attack detection technique. In enhanced technique, the use three more parameters i.e. energy, frequency and latency. In Enhanced Sybil Attack Detection Technique, throughput of network is increased; number of Sybil nodes and bit error rate is decreased as compared to Lightweight Sybil Attack Detection technique. In this, first network is created consisting of nodes and their parameters value i.e. Speed, Energy, Frequency and Latency are initialized. Then Id's of each node, address per Id and IP address per id is generated. Set threshold value of each parameter i.e. for speed it is set to 10m/s and for energy, frequency and latency parameters it is set to average energy of network, average frequency of network and average latency of network respectively. When new node enters in network, first its address is checked with address of nodes present in the network. If the address of new node does not match with any node's address present in the network, then it's all parameters are checked i.e. Speed, energy, frequency and latency.

Athichart Tangpong, George Kesidis, Hung-yuan Hsu, and Ali Hurson [11] Robust Sybil Detection for MANETs In propose a robust Sybil attack detection framework for MANETs based on reputation-based system, monitoring of network activities. It does not require designated and honest monitors to perform the Sybil attack detection. Each mobile node in the network observes packets passing through it and periodically exchanges its observations in order to determine the presence of an attack. Malicious nodes fabricating false observations will be detected and rendered ineffective. Our framework requires no centralized authority and, thus, is scalable in expanding network size. Privacy of each mobile node is also a consideration of our framework. Our preliminary experimental results yield above 80% accuracy (true positives) and about 10% error rate (false positives).

Sohail Abbas, Madjid Merabti, and David Llewellyn-Jones [12] "Deterring Whitewashing Attacks in Reputation Based Schemes for Mobile Ad hoc Networks" in this title it's describe a reputation based scheme for MANETs that acts as a deterrent for whitewashing attacks. Rather than trying to detect whitewashing attacks, In this approach the problem in a novel way by removing the advantages that whitewashing can provide. In our proposed scheme, each node must pay an entry fee to consume network services. As monetary fees are not suitable for MANETs due to fee management complications, instead of a monetary fee it use a fee in the form of cooperation. A node will receive services from the network after it cooperates until its reputation is increased to a certain level *Y*. For a normal selfish node, it is no longer beneficial to perform a whitewash because it will be required to pay the entry fee each time it enters into the network. Simulation results show that our scheme performs well in reducing evil throughput and evil nodes' utility as compared to the CONFIDANT scheme in the presence of whitewashing nodes.

Yingying Chen, Member, IEEE, Jie Yang, Student Member, IEEE, Wade Trappe, Member, IEEE, and Richard P. Martin, Member, IEEE [13] "Detecting and Localizing Identity-Based Attacks in Wireless and Sensor Networks" in this title it describe how it integrated this attack detector into a real-time indoor localization system, which can also localize the positions of the attackers. It show that the positions of the attackers can be localized using either area- or point-based localization algorithms with the same relative errors as in the normal case. In further evaluated our methods through experimentation in two real office buildings using both an IEEE 802.11 (WiFi) network and an IEEE 802.15.4 (ZigBee) network. This results show that it is possible to detect wireless identity-based attacks with both a high detection rate and a low false-positive rate, thereby providing strong evidence of the effectiveness of the attack detector utilizing the spatial correlation of RSS and the attack localizer.

A.Rajaram. Dr. S. Palaniswami "Malicious Node Detection System for Mobile Ad hoc Networks" [14] in this title, it 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, this design a trust based packet forwarding scheme for detecting and isolating the malicious nodes using the routing layer information. It uses trust values to favor 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, **found of** provide link-layer security using the CBC-X mode of authentication and encryption. By simulation results, it show that the proposed MAC-layer security protocol achieves high packet delivery ratio while attaining low delay, high speed and overhead.

4. PROBLEM IDENTIFICATION

Mobile ad hoc networks are becoming popular in the resent past due to the nature of functionality and application in critical areas of domain due to which secure information delivery in MANET is a major concern. Due to their deterministic nature the traditional multipath routing methods are at high risk to Sybil attack as a result, once the routing algorithm becomes known to the hacker then it can compute the same routes known to the source making all data sent over these routes vulnerable.

Sybil attack has caused too much intimidate to ad hoc network in routing, voting system, fair resource allocation, data aggregation and misbehavior detection. Hence many methods are being proposed to detect and prevent Sybil attack in wireless sensor network.

This think it necessary to find out how this can judge if a mobile ad hoc network is secure or not, or in other words, what should be covered in the security criteria for the mobile ad hoc network when **found** want to inspect the security state of the mobile ad hoc network.

5. PROPOSED IDS AGAINST SYBIL ATTACK

In this research, the note that the behavior of attackers behind initiation either packet dropping or routing misbehavior is to achieve a certain goal such as sybil attack (i.e. making certain resources or services, such as applications, web access, printing, or routing, unavailable to the intended users). In addition, other goals of attackers might include partitioning the network, creating routing loops or generating multipile identies discovering valuable information, or theft of resources.

It's assume that the attacker joins the network with its single identity, and that malicious nodes do not collide with one another. It also assume that nodes do not increase or decrease their transmit power because power consumption issue of attack is in different catageory. The attackers can get identities by two ways. First, they are able to fabricate their identification (Second, they can use stolen identities, i.e., satire the identities of genuine nodes (concealed) in the network. It assume the first case where nodes can create random identities because in MANET, there are no restrictions on identity creation.

After attack module it generate profile table during simulation and apply node Identity (ID) with node number checking base technique through abstract window tool kit and detect misleading node and number of packet captured by the Sybil attacker node in both scenario. And lastly this design cooperative protection system in that system check all neighbor node routing entries and if any node adversely sends different identification into more than two different sender so protector nodes is identify that particular node and more than one protector node collaboratively make decision for blocking that path and true information all sender node so they cannot sends any data through that attacker node. The proposed secure Intrusion and Detection system (IDS) is not only protect the routing misbehavior but also prevent from Sybil attacker infection. The attacker is detected also from TPR and FPR where the nodes are detected behaves as an attacker and normal routing behaviour.

1.1 Algorithm for Detection and Prevention Sybil Attack:

Here the algorithm is design for Sybil attacker node detection and prevention for providing security in the system. The Sybil attacker detection is based on the same identity identification in different time instance and the data dropping is highest through that node in network.

```
Nodes consider for Simulation = $N_s$ // Simulation is done in 20, 40, 60 nodes.
Number of attacker nodes =$A_n$  // An € $N_s$
Intermediate Nodes consider = $I_n$    // $I_n$€ $N_s$
Secure Nodes =  IDS
Range of communication of mobile nodes= 250m // meters
Step1 Sender ($S_c$) is ready for sending data to Receiver ($R_c$)
Step2 If (($S_c$ sends RREQ to rest $N_s \leq$ 250m) && (Next_Neighbour==Ready) && (Next_Neighbour !== $R_c$))
{
Forward RREQ to Next_Neighbour;
Receive RREP from Next_Neighbour
Store the hop count value (HP) ;
Forward RREQ to Next_Neighbours and Receives RREP till $R_c$ Found;
}
Else
{
  $R_c$ Confirms connection from $S_c$;
  $S_c$ starts data sending to $R_c$ ;
}
// Identified Attacker Existence and Prevention //
Step3: IDS Create Behavior files for identification of attacker in Network.
Step4: if ((Intermediate Node_no == True) && (Intermediate Node_id count==1))
        {
        Store Node _ID for further Prevention through that node;
        }
        Else
        {
        Check the possibility of attacker
        }
Step 5: if ((Intermediate Node_no == True) || (Intermediate Node_id count >1) && (Time instance = Variant))
        {       If (Data forwarding to Node_id != True)
                {
                Confirm Attack Type = "Sybil";
                Capture route information;
                Attacker infection inject in network;
                }
        }
        Else
        { go to step 2}
Step 6: IDS or secure node number is the Preventer Node block the communication capability of attacker    // disable attacker identity
Step 7 :  if (IDS capture the attacker identity == attacker Node multiple ID's with Node_no.)
          {
               RREQ=Block;      // means inactive that mode of operation by assign value=0 by 1,
             RREP=Block;
             Disable routing participation;
          }
Step 8: Secure IDS check Neighbor for updating the ID's received and sends by other Nodes
Step 9: IDS broadcast attacker node information to sender and all nearby nodes to convey about the attacker.
Step 10: Analyze the network behavior for further analysis.
 Step 11: IDS Retrieve Destination Node ID and Actual ID of all Nodes from abstract window tool kit (AWK) programming
Step12    End
```

6. SIMULATION TOOL OVERVIEW AND PERFORMANCE PARAMETERS WITH METRICS

The simulation of Sybil attacker and proposed IDS is done in Network Simulator (NS-2) version 2.31 (NS-2.31) [15]. This simulator is open source code and due to that the modification in internal modules are possible. It is discrete event simulator (timing of events is maintained in a scheduler). This simulator is developed by Start 1989 as a variant of REAL (network simulator for studying the dynamic behavior of flow and congestion control schemes in packet-switched data networks)

After 1995, Funding from DARPA through many projects (VINT project at LBL, Xerox PARC, UCB, USC/ISI. SAMAN and NSF with CONSER). Table 1 are represents the following simulation parameters to make the scenario of routing protocols. The detailed simulation model is based on network simulator-2 is used in the evaluation.

Table 1 Simulation parameters will uses for simulation

Simulator Used	NS-2.31
Number of nodes	20, 40 and 60
Radio Range (meters)	250m
Attacker	Sybil (4)
Routing Security	IDS
Dimension of simulated area	800m×600m
Routing Protocol	AODV
Simulation time	100 sec.
Traffic type (TCP & UDP)	FTP, CBR (2pkts/s)
Packet size	1024 bytes

Number of traffic connections	4, 2
Node movement at MAX Speed	random (20 m/s)

6.1 Performance Metrics

It’s computed the following metrics for after the simulation of Sybil attacker and proposed IDS.

6.1.1 Packet overhead.

The number of transmitted routing packets; for example, a HELLO or RREP and RREQ message sends by all senders in network.

6.1.2 Attacker Loss Percentage

This metrics is calculated the data packets that is drop by attacker in network.

6.1.3 Detection Accuracy

To identify the attacker loss malicious actions, in use two main metrics in order to determine the detection accuracy of in scheme in different environments, i.e., true positive rate (TPR) and false positive rate (FPR).

a) True positive Ratio (TPR) means a malicious node is correctly detected.

b) False Positive Ratio (FPR) means a good or legitimate node is incorrectly detected as a maliciou.s

7. RESULTS EVALUATION AND DISCUSSION

In this section the simulation results are discussed in presence of Sybil attacker and proposed IDS scheme. The proposed IDS is provides secure routing and blocks malicious attacker routing misbehavior.

7.1 Sybil Attacker Drop Percentage Analysis

The Sybil attacker is the routing layer attack their active presence is continuously showing the routing misbehavior by dropping the data packets through generating the multiple phony identities in dynamic network. The routing attacker is only diverted or drops the data packets to next unrecognized node or dropped at attacker node by that data receiving is affected. The Sybil attacker drop percentage analysis in presence of attacker and IDS is mentioned in this table. Here the attacker drop percentage is about 40 % at time 5 seconds but after that, this drop percentage is maintained at 25% up to end of simulation. This drop is only evaluated through attacker but that drop is also affected the normal routing performance that is recognized through higher TPR and lower FPR. But after applying IDS security system attacker drop percentage is completely removes from network and their no existence is presence in MANET.

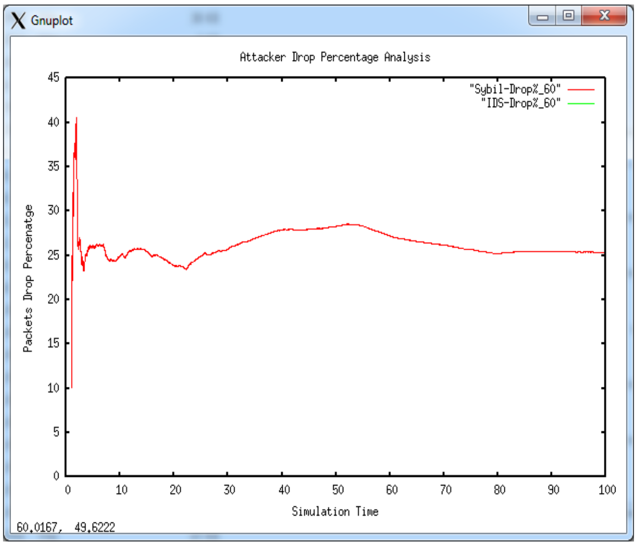

Fig. 2 Malicious Drop Percentage

7.2 Sybil Attacker Multiple Identity Drop Analysis

The attacker aim in network to degrades and dumps the whole network performance. The better routing performance are shows the enthusiastic network performance. The routing protocols are established connection in between sender and receiver. In MANET multi-hop connection is established, the chances of receiver possibility in single hop is abot negligible in network. The request packets are sending by sender to receiver through intermediate nodes and attacker’s nodes are one or more than one are conduct itself as intermediate nodes. They receive and forward the request packets to nest nodes. The Sybil attacker nodes identification in 60 nodes scenario is mentioned in this graph. Here the node number 4 is generating the five fake values like 7, 12, 19 24 and 29. Through these fake identities the attacker is communicate to destination and after confirmation, sender starts data deliver and attacker is drop the all packets. The attacker nodes existence in IDS presence is completely zero. It implies that no attacker is active in network for malicious deeds and routing degradation.

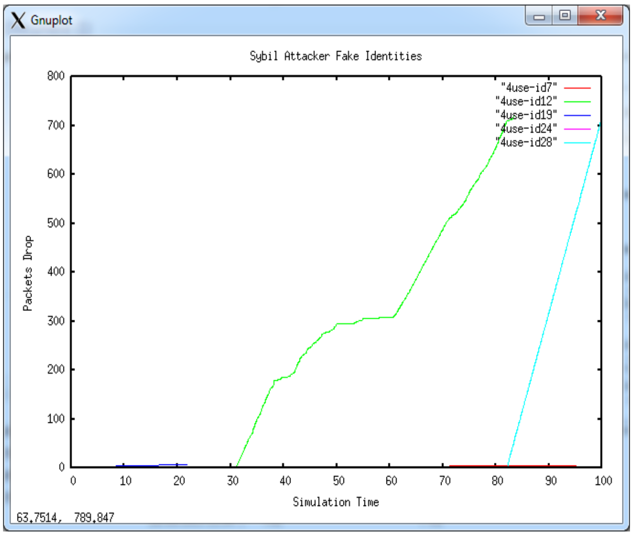

Fig. 3 Fake Identity Analysis

7.3 Abbreviated or Recapitulated Performance Analysis of Sybil attacker and Proposed Secure IDS.

The routing performance of Sybil attacker in 20, 40, 60 nodes and proposed secure IDS is mentioned in table 1. In this table it scrutinized that in attacker scenario, due to retransmission sending of data is more in 20 and 60 nodes but in 40 nodes routing load (NRL) is more, that is more than normal routing performance. The proposed secure IDS against Sybil attacker is improves the packets receiving t5hat shows the better routing performance. The security system is identified the attacker and obstruct their malicious activities in network.

Table 2 Performance Analysis

Performance Metrics	Sybil 20	Sybil 40	Sybil 60	Proposed IDS_60
SEND	11408	2621	14469	6100
RECV	3035	8	667	5592
Routing Pks	960	1239	6490	5135
PDF	26.6	0.31	4.61	91.67
NRL	0.32	154.88	9.73	0.92
No. of dropped data (packets)	10448	2613	13802	500

7.4 Sybil Attacker Detection through TPR

The True Positive Ratio (TPR) is the percentage ratio of the nodes that has act as the malicious node/s. It means that how many activities of normal nodes are approximately same as attacker i.e. drops data packets in network. The TPR percentage ratio is evaluated to detect the attacker malicious activities in network. In this figure the observe the Sybil attacker malicious actions in three different scenarios. The malicious TPR percentage is observed in 20 nodes, 30 nodes and 40 nodes in presence of Sybil attacker. The normal TPR percentage is not greater than 88% in network. The large number of data packets dropping is shows the emaciated routing performance. The proposed IDS scheme is improve the routing performance by blocking the malicious activities in network.

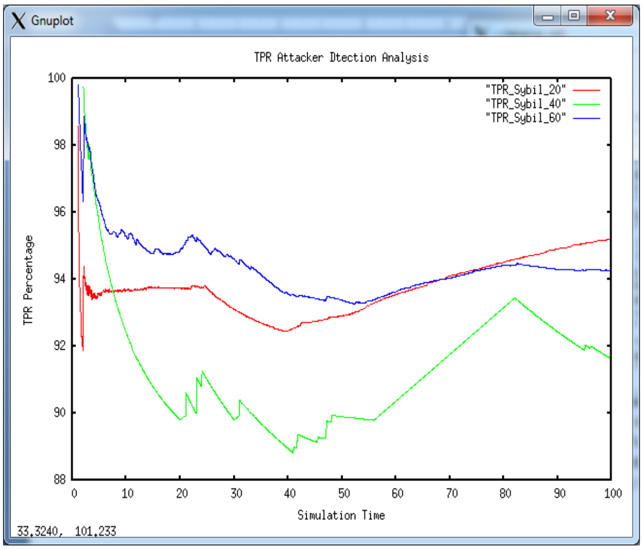

Fig. 4 FPR Performance Analysis

7.5 Sybil Attacker Detection through FPR

The False Positive Ratio (FPR) in network is evaluated to observe the normal routing performance in presence of Sybil attacker. The FPR is observing how much number of nodes in network are maintained the normal performance, means perform normal data packets forwarding. The better FPR ratio is shows the better routing performance in network. The attacker detection is possible by observing less FPR value in network. In this figure also same scenarios like 20, 30 and 40 nodes are considered for simulation in presence of Sybil attacker. The FPR percentage is not more than 18 % that shows the abnormal performance in network. The proposed secure IDS is provides the reliable routing performance in presence of attacker and enhance the data packets receiving in network.

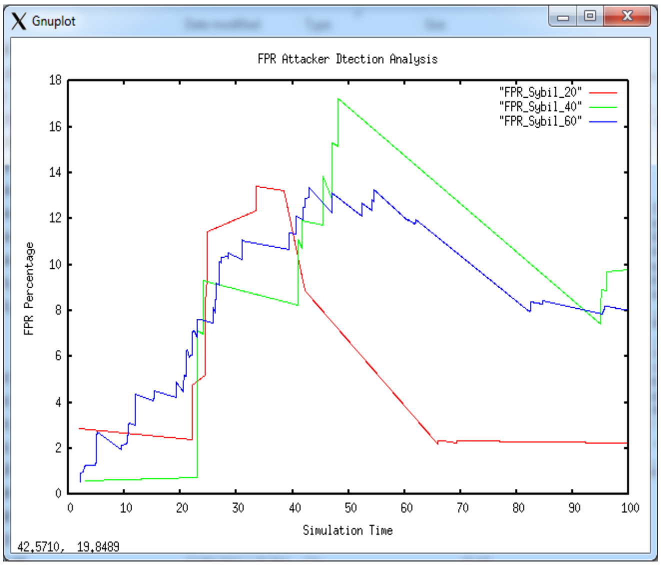

Fig. 5 TPR Performance Analysis

8. CONCLUSION WITH FUTURE EXTENTION

MANET security composed of challenging and complex area, in which further research is still being performed and will results in finding of new threats. In Sybil attack, an attacker node behaves as if it were a group of nodes by showing multiple Identification (ID's) number in network. There are, basically two ways by which a Sybil node can get an identity; abducting other node's identity or constructing false identities. In this research it use the second way to identify the Sybil attacker in network. Routing protocol independent attacks are not prone to occur for specific routing protocol this attack can take place irrespective of the routing protocol. The routing protocol dependent attacker identification is basically limited and for other routing protocol identification is not possible. The main advantage of proposed security scheme is it is protocol independent .The proposed IDS identified the false identity information of attacker and improves the routing performance of network in presence of attacker. The following IDS improve the throughput, PDF, FPR and reduces routing load, packet dropping, reduces TPR value in presence of attacker and IDS nodes. The proposed IDS scheme produces zero (0) % malicious drop percentage that confirm the 100% attacker contamination free secure routing in MANET.

In future it 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. This scheme it observe higher mobility of mobile nodes and forward the message to control their mobility to reduces the chances of link in network.

9. REFERENCES

[1] G. Mobile Ad-hoc Networks (MANET). URL:http://www.ietf.org/html.charters/manet

[2] Charles E.Perkins. Ad hoc Networking, Addison-Wesley, 2001

[3] Mohammad O. Pervaiz, Mihaela Cardei, and Jie Wu, "Routing Security in Ad Hoc Wireless Networks", Mohammad O. Pervaiz, Mihaela Cardei, and Jie Wu Springer pp.1-32, 2005

[4] B. Sun, L. Osborne, Y. Xiao, and S. Guizani, "Intrusion Detection Techniques in Mobile Ad Hoc and Wireless Sensor Networks," IEEE Wireless Communications Magazine, special issue on Security in Wireless Mobile Ad Hoc and Sensor Networks, Vol.14, No.5, pp. 56-63, October 2007.

[5] Adnan Nadeem and Michael P. Howarth, " A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks" IEEE Communications Surveys & Tutorials, Accepted for Publication, pp.1-19, 2013.

[6] Elizabeth M. Royer, Chai-Keong Toh, "A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks", IEEE Personal Communications, Vol. 6, No. 2, pp. 46-55,April 1999.

[7] Anuj K. Gupta, Harsh Sadawarti, and Anil K. Verma, "Review of Various Routing Protocols for MANETs", International Journal of Information and Electronics Engineering, Vol. 1, No. 3, pp. 251-259, November 2011.

[8] R. Vintoh kumar, Mr. P. Ramesh,Dr. H. Abdul Rauf, "Cluster Based Enhanced Sybil Attack Detection in MANET through Integration of RSSI and CRL", IEEE International Conference on Recent Trends in Information Technology, pp. 1-7, 10-12 April 2014.

[9] Sohail Abbas, Madjid Merabti, David Llewellyn-Jones, and Kashif Kifayat, “Lightweight Sybil Attack Detection in MANETs” IEEE Systems Journal, Vol. 7, No. 2, pp. 236 -248, June 2013. .

[10] Himika Sharma and Roopali Garg, “Enhanced Lightweight Sybil Attack Detection Technique”, IEEE 2014 5th International Conference on The Next Generation Information Technology Summit (Confluence), 476 – 481, 25-26 September 2014.

[11] Athichart Tangpong, George Kesidis, Hung-yuan Hsu, Ali Hurson, “Robust Sybil Detection for MANETs”, IEEE Proceedings of 18th International Conference on Computer Communications and Networks (ICCCN), pp. 1-6, 3-6 August 2009.

[12] Sohail Abbas, Madjid Merabti, and David Llewellyn-Jones “Deterring Whitewashing Attacks in Reputation Based Schemes for Mobile Ad hoc Networks”, IEEE Conference Wireless Days (WD), 2010 IFIP, pp. 1 – 6, 20-22 October 2010

[13] [5] Yingying Chen, Jie Yang, Wade Trappe, and Richard P. Martin, “Detecting and Localizing Identity-Based Attacks in Wireless and Sensor Networks” IEEE Transactions on Vehicular Technology, Vol. 59, No. 5, June 2010.

[14] A.Rajaram. Dr. S. Palaniswami “Malicious Node Detection System for Mobile Ad hoc Networks” International Journal of Computer Science and Information Technologies (IJCSIT), Vol. 1, Issue 2 , pp.77-85, 2010.

[15] www.isi.edu/nsnam/ns/