ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 5, Issue 11, May 2016

A Unique Identification based IDS security Scheme for Byzantine Attack in MANET

[1]Nidhi Pandey, [2]Neetesh Gupta
[1]M-tech pursuing, Dept of computer science, [2]Professor, Dept. of computer science
Rajiv Gandhi Proudyogiki Vishwavidyalaya Bhopal, India

Abstract*—The absence of decentralized administration is the main cause of attacks in Mobile Ad hoc Network (MANET). The attacker is disrupting the proper communication in network by that the lot of data is drop or corrupted by attacker. Many of the attackers are in MANET and each and every attacker is the different technique to do misbehavior in network. The Byzantine attacker flooded the huge number of packets in an every time interval. The packets are not directly lot of injected in network but gradually. In this research we proposed a novel security scheme for Byzantine attacker in network. The attacker is consumes the whole bandwidth, so that problem is created for proper communication. The proposed scheme is identified the attacker in network and obstruct the attacker misbehavior in network. The attacker is identified by node identification or number that flood the packets in beyond the capacity in network. The proposed IDS scheme is first to identify the node that only flooded the duplicate packets in network, on the basis of that IDS authenticate the Byzantine attacker misbehavior to other normal nodes that receives the broadcasted duplicate packets and identified which malicious node is responsible for it and captures the node_id of attacker in network. The whole performance in measured through performance metrics and removes the drop percentage due to Byzantine attacker in network.

***Index Terms*—Security, MANET, IDS, Routing, Byzantine attacker.**

I. INTRODUCTION

A mobile ad hoc network (MANET) is a collection of mobile devices that can communicate with each other without the use of a predefined infrastructure or centralized administration [1] [2]. In addition to freedom of mobility, a MANET can be constructed quickly at a low cost, as it does not rely on existing network infrastructure. Mobile nodes in MANET operational with both a wireless transmitter and a receiver that communicate with each other via bidirectional wireless links either directly or indirectly. One of the major advantages of wireless networks is its ability to allow data communication between different parties and still maintain their mobility. However, this communication is limited to the range of transmitters. This means that two nodes cannot communicate with each other when the distance between the two nodes is beyond the communication range of their own. MANET solves this problem by allowing intermediate parties to relay data transmissions. This is achieved by dividing MANET into two types of networks, namely, single-hop and multihop. In a single-hop network, all nodes within the same radio range communicate directly with each other. On the other hand, in a multihop network, nodes rely on other intermediate nodes to transmit if the destination node is out of their radio range. In contrary to the traditional wireless network, MANET has a decentralized network infrastructure. MANET does not require a fixed infrastructure; thus, all nodes are free to move randomly [1] [2] [3]. MANET is capable of creating a self-configuring and self-maintaining network without the help of a centralized infrastructure, which is often infeasible in critical mission applications like military conflict or emergency recovery. Minimal configuration and quick deployment make MANET ready to be used in emergency circumstances, where an infrastructure is unavailable or unfeasible to install in scenarios like natural or human-induced disasters, military conflicts, and medical emergency situations.

Owing to these unique characteristics, MANET is becoming more and more widely implemented in the industry [4]. However, considering the fact that MANET is popular among critical mission applications, network security is of vital importance. Unfortunately, the open medium and remote distribution of MANET make it vulnerable to various types of attacks. For example, due to the nodes' lack of physical protection, malicious attackers can easily capture and compromise nodes to achieve attacks. In particular, considering the fact that most routing protocols in MANET assume that every node in the network behaves cooperatively with other nodes and presumably these are not malicious [5], but the chances of malicious actions are always be positive at any time in network. Attackers [5] in MANET can easily compromise MANET by inserting malicious or non-cooperative nodes into the network. Furthermore, because of MANET's distributed architecture and changing topology, a traditional centralized monitoring technique is no longer feasible in MANETs. In such case, it is crucial to develop an Intrusion Detection System (IDS). The IDS scheme is identified and block the attacker misbehavior procedures to affect routing performance in dynamic self established MANET.

In this paper we proposed a security scheme to achieve the complete control on routing misbehavior through Byzantine attacker. The proposed scheme is identified the attacker on the basis of particular identification (ID) and this ID (node_id) of the attacker is present in every node in network which received the unwanted or untruthful packets. The IDS scheme is broadcast the network ID after identification and block this attacker action.

II. TYPES OF ATTACK IN MANET

Attacks on Mobile Ad hoc Networks can be classified as active and passive attacks, depending on whether the normal operation of the network is disrupted or not [4] [5].

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 5, Issue 11, May 2016

A. Passive Attack

In passive attacks, an intruder the data exchanged without altering it. The attacker does not actively initiate malicious actions to cheat other hosts. The goal of the attacker is to obtain information that is being transmitted, thus violating the message confidentiality. Since the activity of the network is not disrupted, these attackers are difficult to detect.

B. Active Attack:

In active attacks, an attacker actively participates in disrupting the normal operation of the network services. A malicious host can create an active attack by modifying packets or by introducing false information in the ad hoc network. It confuses routing procedures and degrades network performance. Active attacks can be divided into internal and external attacks.

C. External Attack

External Attacks are carried by nodes that are not legitimate part of the network. In external attacks, it is possible to disrupt the communication of an organization from the parking lot in front of the company office.

D. Internal Attack

Internal Attacks are from compromised nodes that were once legitimate part of the network. In ad hoc wireless network as authorized nodes, they are much more severe and difficult to detect when compared to external attacks.

The most of the attackers [6] [7] are affecting the ad hoc network performance and execute malicious activities at the time of sending and receiving the data. The attackers are categorized according to different layer of network like Eavesdropping, jamming attacker, black hole attack, gray hole attack, byzantine attack [8], wormhole attack, DoS attack and so on [6] [7], because the different attacker is clash the network performance at different layer.

III. ROUTING PROTOCOLS DESCRIPTION

In MANET currently, there are mainly two types of routing protocols in MANETs, namely, topological routing and geographic routing [2] [9]. In topological routing, mobile nodes utilize topological information to construct routing tables or search routes directly. In geographic routing, each node knows its own position and makes routing decisions based on the position of the destination and the positions of its local neighbors.

The investigation of topological routing has lasted for decades, and a variety of topological routing protocols have been developed. Generally, the topological routing protocols can be further divided into two categories, namely, proactive routing and reactive routing. In proactive routing, route information is propagated periodically in the network.

Thus, each node can maintain a routing table containing route entries to other nodes. When packets arrive at an intermediate node, the next hop can be selected by looking up the routing table. Destination-sequenced distance-vector (DSDV) [10] routing is referred to as a well-known example of proactive routing. In reactive routing, no routing table is maintained at the nodes. When needed, the source node triggers a route search procedure to discover the routing path to the destination. Both ad hoc on-demand distance vector (AODV) [11] routing and dynamic source routing (DSR) [12] are referred to as representative examples of reactive routing. By exploiting the strength and avoiding the weakness of each type, hybrid topological routing protocols are proposed, for example, Zone Routing Protocol (ZRP) [13], which maintains a k-hop routing zone proactively and triggers the inter-zone route discovery reactively.

IV. LITERATURE SURVEY

Many of the researchers have proposed the security schemes against attacks. The latest research in field of byzantine attack is discussed in this section.

The latest research by Henrique Moniz, Nuno F. Neves, and Miguel Cor in [14] presented Turquois, an Byzantine fault-tolerant binary consensus protocol specifically designed for ad hoc networks. Its design takes into account the typically constrained resources of wireless ad hoc environments, while aiming for optimal resilience parameters. This paper aims at conciliating Byzantine fault tolerance with the unreliable and resource-constrained nature of ad hoc networks. To achieve this, this paper focuses on the problem of Byzantine fault-tolerant binary consensus for single-hop wireless ad hoc networks, while assuming a system model that closely matches the reality of wireless environments. In particular, it is assumed that nodes are subject to transitory disconnection (due to mobility or unreliable communication) and permanent corruption by a malicious entity. The focus on the single-hop scenario is directly related to the fact that nodes within direct communication range of each other frequently have to synchronize their actions due to their physical proximity.

The drawback of this research is the work is done on key exchange method based on the logical mathematical values and calculates the average latency on different scenarios like node density, group size and time variations. The network performance is not evaluated at network layer in term of packets send, receive and loss in a particular simulation of time in network. The whole research is divided in to authenticity validation and semantic validation, this validation is based on the correct message passing from the nodes.

The second one by Ming Yu, Mengchu Zhou, and Wei Su in [15] proposes a novel attack detection and defence algorithm to solve the preceding problems for MANETs. It also develops a secure routing protocol called secure routing against collusion (SRAC) to defend Byzantine attacks as well as other internal attacks against routing protocols for MANETs in adversarial environments. There are two basic key management approaches, i.e., public and secret key-based schemes. The public key-based scheme uses a pair of public/private keys and an asymmetric algorithm such as RSA to establish session keys and authenticate nodes. In the latter scheme, a secret key is a symmetric key shared by two nodes, which is used to verify the data integrity.

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 5, Issue 11, May 2016

The main drawback of this paper not mentioned the infection from attack and using the already implemented cryptographic technique to identified attack. Public key infrastructure (PKI) and certificate authority (CA) is to achieve the security requirements including confidentiality, integrity, authentication, and non-repudiation services. The key exchange is started at the time of message delivery; it implies every exchange is verified by CA but why it is necessary because every node has unique identification number in network already present.

In this paper [16], proposed new secure system called Audit based Misbehavior Detection, (AMD) which achieves per-packet behavior evaluation without incurring a per-packet per-hop cost. AMD is a comprehensive solution that integrates identification of misbehaving nodes, reputation management, and trustworthy route discovery in a distributed and resource-efficient manner. We show that AMD can construct paths consisting of highly trusted nodes, subject to a desired path length constraint. When paths contain misbehaving nodes, a behavioral audit process efficiently locates these nodes.

Borran and Schiper in [17] introduced a protocol that, like ours, is leader-free, tolerates Byzantine nodes, and is always safe regardless of the number of omission faults. To circumvent the Santoro-Widmayer impossibility result, their model assumes the existence of a Global Stabilization Round (GSR), after which communication between correct nodes is assumed to be reliable. In other words, there are no omission faults in the system involving correct nodes after a specific, but unknown, point in time (i.e., the GSR).

G. Chockler, M. Demirbas, S. Gilbert, C. Newport, and T. Nolte, in [18] described a consensus algorithm for a system where nodes can fail by crashing and messages can be lost due to collisions. Their protocol can solve consensus due to the additional power offered by collision detectors, which allow nodes to take measures to recover from message losses. Message omissions other than those due to collisions, however, are not covered by their model.

V. PROPOSED SCHEME FOR BYZANTINE ATTACKER

The goal of this work is to provide routing survivability under an adversarial model where any intermediate node or group of colluding nodes perform Byzantine attacks. While some existing work provides protection against specific attacks that may be conducted by a single Byzantine node against different routing components, no other existing work provides an ad hoc wireless routing protocol for coping with a large set of attacks available to a set of colluding Byzantine attackers and targeting both route discovery and data forwarding.

Number of nodes = N;
Set Preventer node = Q ϵ N; // IDS node
Byzantine Attacker = A // A ϵ N
Range of Communication= RC
Routing Protocol = AODV
If ((N_RC< 500) && (next hop !=Null)) // Attacker Detection
{
Capture load of all nodes
Maintain the normal profile
Maintain abnormal profile
}
If ((load < = max_limit) && (new_profile = = normal_profile))
{
Confirm no attack in network;
}
Else
{
Found Attack in network;
}

AODV sends RREQ (Q, (N+Q-A), Range) // broadcast for communication and send request packets to all (N-Q) nodes via Q node // Attacker Prevention
{
If ((N_RC < 500) && (Next Node Availability = True))
{
If (P_n = = message)
{
IDS Consumes false Packets (message) = (packets P_1 at time T_1, packets P_2 at time T_2.....packets P_n at time T_n); // false packet detection
Forward Node_id of Attacker to all (N-A) nodes;
Find number of pkt accepted nodes;
Node_id= A is Disable for communication; // by change their id =0
Block attacker Node;
Node infection removes via Block node_id
}
Else
Byzantine Attacker not found
}
Else
Forward RREQ for Connection Establishment or Destination Unreachable
}
}

The proposed IDS module that protect through the byzantine attacker, if Byzantine attacker node in the range of IDS. First IDS check which node update the routing table and send higher sequence number to the sender node, if find out so IDS sends the message to the sender node for elimination of that particular path where belongs byzantine attacker node and search new route according to IDS instruction. The IDS grasp the particular attacker node_id that circulates unnecessary control packets. Here IDS internal module provides only protection of misbehave and provide trust communication between sender and destination. After prevention we detect byzantine attacker node via trace analysis and provide secure communication in MANET.

VI. NETWORK SIMULATOR

We use the NS2 Network Simulator. This is an object oriented simulator, written in C++, with an OTCL interpreter

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 5, Issue 11, May 2016

as a front-end. The simulator supports a class hierarchy in C++ (also called the compiled hierarchy) and a similar class hierarchy within the OTCL interpreter (also called the interpreted hierarchy). The two hierarchies are closely related to each other; there is a one-to-one correspondence between a class in the interpreted hierarchy and one in the compiled hierarchy. The root of this hierarchy is the class TCL Object. Users create new simulator objects through the interpreter; these objects are instantiated within the interpreter and are closely mirrored by a corresponding object in the compiled hierarchy. The interpreted class hierarchy is automatically established through methods defined in the class TCL Class. User instantiated objects are mirrored through methods defined in the class TCL Object.

A. Performances Metrics

The performance of network is evaluated in case of AODV, Byzantine attack and secure IDS scheme.

1) Routing Load

The number of routing packets (RREQ, RREP, and RERR) transmitted per data packet delivered at the destination.

2) Packet delivery ratio

The ratio between the numbers of packets originated by the application layer to those delivered to the final destination.

3) Average end to end delay

This is the average of the time taken by the packets to reach the destination in the network. The average time to packets sends by sender and received by receiver is network.

4) contamination Packets Percentage

The contamination packets percentage is calculated by how much percentage of data in network are infected by Byzantine attacker in network.

5) Packet loss

The calculation of number of data packets in network are drop by Byzantine attacker.

B. Simulation Parameters

The simulation parameters like area of simulation is 800m *600m in transmission range of 550m. Rest of them that are consider for simulation is mentioned in table 1.

Table I Simulation Parameter

Area of Simulation	800m x 600m
Mobile Nodes	50
Radio Range (meters)	550
Transferring Mode	Unicast through Unipath
Maximum Speed (ms)	40
Routing Protocol	AODV
Transport Layer	TCP , UDP
Traffic	CBR, TTP
Application Layer	FTP
Simulation Time (sec)	50
Packet Size	512 bytes

VII. SIMULATION RESULTS

The simulation results are evaluated to measure the performance of protocols. An important contribution of this work is the comparison of the performance of AODV routing protocol with and without Byzantine malicious node and applying proposed security scheme on it.

A. Attacker Data Drop Percentage Analysis

The drop percentage due to attacker is more than 35 % in network but on the other hand the drop percentage of proposed IDS is zero that shows the network is definitely secure from the byzantine malicious actions. The misbehaving nodes could cause the damage to the network without being identified during the data transferring operation of the network. When an attacker node floods an uncertain packet it will notice that attacker consumes the whole bandwidth of the link. Now the sender nodes can choose to cooperate and forward packets for a limited time (until the link is free) and then continue to drop packets. It is obvious that the number of attacker nodes has a significant effect on the rate of packets that are successfully delivered in the network. These packets are degrades the network performance and improves the drop percentage of data that is completely block by proposed IDS in MANET

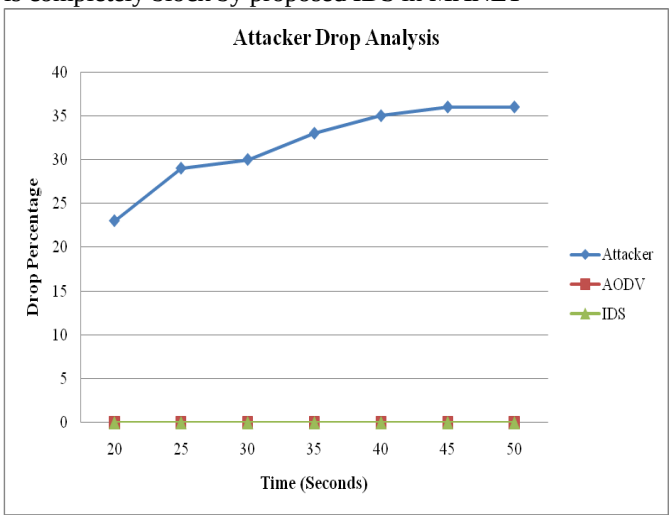

Fig. 1 Attacker Drop Percentage Analysis

B. Routing Overhead Performance Analysis

When the source node receives the RREP packet by sending the next node or neighbor, which receives the RREQ packets from sender, the control packets or routing overhead is evaluated. The attacker has easily modified or changes the network performance by injecting the unnecessary number of control packets in decentralized dynamic network. The detection of such routing misbehavior is achieved through a system called proposed IDS. However, proposed detection scheme is manipulate the attacker information and provides the normal routing performance in presence of attacker. The load of packets that is sending by attacker is more than 2, 00,000 in network. These packets are dumping the network performance by squeeze the network bandwidth. The proposed IDS are blocking the attacker misbehavior and provide normal performance as equal to normal AODV routing module.

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 5, Issue 11, May 2016

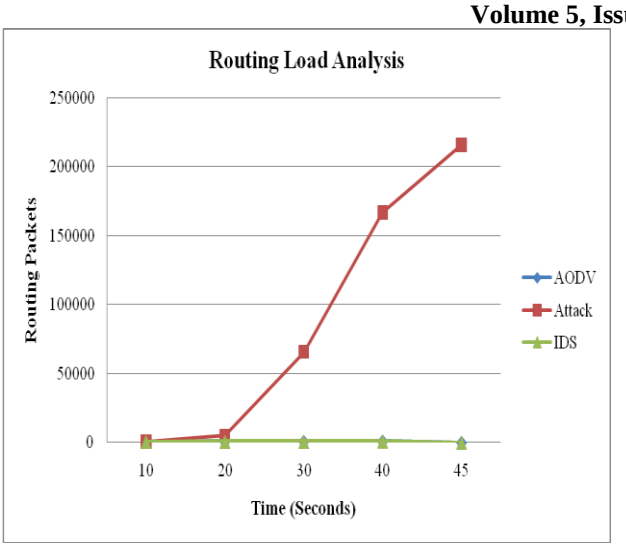

Fig. 2 Routing Overhead Analysis

C. Throughput Performance Analysis

The throughput achieved of AODV routing protocols due to byzantine infection is substantially less than as compare to normal performance and IDS performance. The proposed IDS are deal for the honest majority cooperates. Under the assumption of an honest majority, detection of misbehaving nodes becomes the primary goal in dealing with misbehavior. The byzantine attacker is degrades the network per unit of time data receiving and only up to 40 seconds the communication among the nodes is possible including sender and receiver. The throughput of IDS is as equal to normal performance of AODV protocol which is about more than 1100 packets in a unit time and provides the secure communication in dynamic network. The proposed IDS authentication is necessary with normal performance to measure the difference in performance measurement.

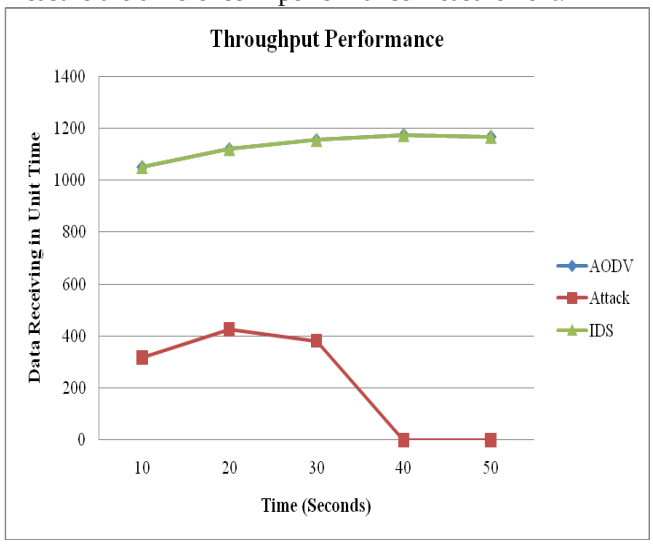

Fig. 3 Throughput Analysis

D. Packet Delivery Ratio (PDR) Performance Analysis

The PDR performance is evaluated through the percentage of data receiving and sending in network. The PDR poor performance is clearly visualized if the difference in receiving and sending packets is more. In this graph the PDR is almost equal up to 30 seconds in all three cases but after that the link is squeeze due to that the few packets receiving is also affected. The PDR performance of IDS tries to get the detection effectiveness as high as possible. Having a number of good nodes being misclassified has a negative effect on the overall performance of the network. An interesting phenomenon is that the probability of perfect detection decreases as the percentage of misbehavior is increases through byzantine attacker. The performance of IDS is really effective to provide as equal percentage of data without any delay and loss in network.

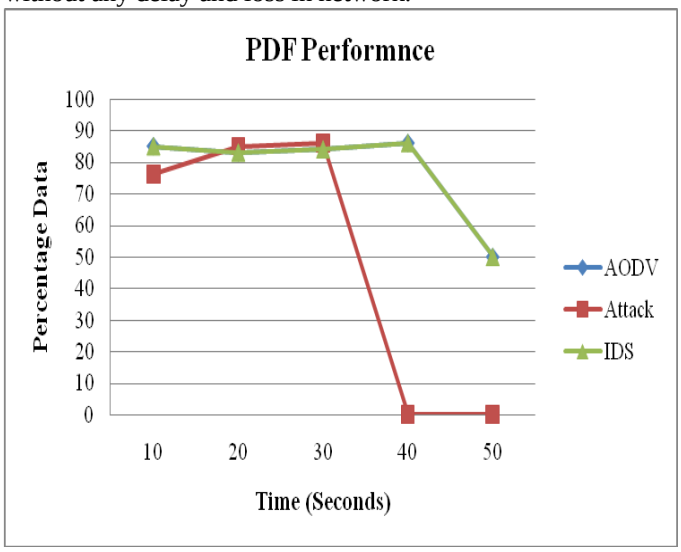

Fig. 4 PDR Analysis

E. Actual Packets Analysis of AODV, Byzantine Attack and IDS

The communication in dynamic network is very critical due to continuous change of network topology and if the attacker is existing then the performance is really unpredictable because the attacker is also change their position. The actual performance of data in term of routing packets and data packets are mention in table 2.The IDS is really works effective that provides the complete secure communication in existence of attacker. The average delay in presence of attacker is more but receives about 9 times less packets as compare to IDS and normal AODV, which is the sigh of poor performance.

Table 2 Actual Performance of Packets

Metrics	AODV	Byzantine Attack	IDS
SEND	5032	790	5032
RECV	4355	561	4355
No. of dropped data (packets) =	677	229	677
Routing Pkt	924	303864	924
Average e-e delay(ms)=	1116.64	1022.74	1116.64

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 5, Issue 11, May 2016

VIII. CONCLUSION & FUTURE WORK

Mobile Ad hoc NETwork (MANET) is a gathering of mobile stations that moves freely and forming a dynamic connection without any authorized administration. The nodes are self-organize in capricious and temporary network topologies. Due to the mobility of the nodes and the continuously changing topology in the ad hoc network, it is sometimes relatively hard to collect the enough evidences for a attacker node in network. The AODV On demand routing protocol is better for dynamic network but also vulnerable for attacks. The Byzantine attacker is not sends the limited number of packets at equal number of time but it sends always enhance inconsistent amount of packets to nodes, because of it not easy to recognize the routing misbehavior of that kind of attack. In this research the proposed IDS scheme is identified the first information of packets that is not contain the routing information and also identified the node_id (NID) of node that is deliver that kind of packets in network. In proposed scheme each of the nodes in the mobile ad hoc network should be equipped with an particular IDS, and all of the IDS can work independently and locally as well as cooperative with each other to detect some intrusion behaviors in a larger range. The IDS nodes continuous scrutinized the misbehavior of Byzantine attacker identified the atypical and not evocative route information. The IDS identified the attacker on the evidence of atypical and not evocative route information and also aware about the others to not narrate with attacker NID. Because of that the attacker is absolutely immobilized and the network performance is usual as original AODV routing.

REFERENCES

[1] S. Ci et al., "Self-Regulating Network Utilization in Mobile Ad-Hoc Wireless Networks," IEEE Trans. Vehic. Tech., vol. 55, no. 4, pp. 1302–1310, July 2006.

[2] C. S. R. Murthy and B. S. Manoj, Ad Hoc Wireless Networks: Architectures and Protocols, Prentice Hall PTR, 2004.

[3] F K. Kuladinith, A. S. Timm-Giel, and C. Görg, "Mobile ad-hoc communications in AEC industry," J. Inf. Technol. Const., vol. 9, pp. 313–323, 2004.

[4] M. Zapata and N. Asokan, "Securing Ad Hoc Routing Protocols," in Proceeding of ACM Workshop on Wireless Security, pp. 1–10, 2002.

[5] L. Buttyan and J. P. Hubaux, Security and Cooperation in Wireless Networks. Cambridge, U.K.: Cambridge Univ. Press, Aug. 2007.

[6] Pradip M. Jawandhiya, Mangesh M. Ghonge, Dr. M.S.Ali, Prof. J.S. Deshpande, " A Survey of Mobile Ad Hoc Network Attacks", International Journal of Engineering Science and Technology, Vol. 2(9), pp. 4063-4071, 2010.

[7] Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei, "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks,"Wireless/Mobile Network Security, Y. Xiao, X. Shen, and D.-Z. Du (Eds.) pp. 1-38, @ 2006 Springer.

[8] B. Awerbuch, D. Holmer, C. Nita-Rotaru, and H. Rubens, An On-demand Secure Routing Protocol Resilient to Byzantine Failures. Proceedings of the ACM Workshop on Wireless Security, pp. 21-30, 2002.

[9] 6G. Jayakumar and G. Gopinath, "Ad Hoc Mobile Wireless Networks Routing Protocol—A Review," Journal of Computer. Science, Vol. 3, No. 8, pp. 574–582, 2007.

[10] C. E. Perkins and P. Bhagwat, "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers," Proc. ACM SIGCOMM, 1994.

[11] C. Perkins, E. Belding-Royer, and S. Das, "Ad Hoc On demand Distance Vector (AODV) Routing," IETF RFC 3561, July 2003.

[12] D. B. Johnson and D. A. Maltz, "Dynamic Source Routing in Ad-Hoc Wireless Networks," T. Imielinski and H. Korth, ed., Mobile Computing, Kluwer Academic Publishers, 1996, pp. 153–81.

[13] Z. J. Haas and M. R. Pearlman, "The Performance of Query Control Schemes for the Zone Routing Protocol," IEEE/ACM Trans. Net., vol. 9, no. 4, 2001, pp. 427–38.

[14] Henrique Moniz, Nuno F. Neves, Miguel Correia, "Byzantine Fault-Tolerant Consensus in Wireless Ad Hoc Networks", IEEE Transactions on Mobile Computing, Vol. 12, No. 12, pp. 2441-2454, December 2013.

[15] Ming Yu, Mengchu Zhou, and Wei Su, "A Secure Routing Protocol Against Byzantine attacks for MANETs in Adversarial Environments", IEEE Transactions on Vehicular Technology, Vol. 58, No. 1, pp. 449-460, January 2009.

[16] Yu Zhang, Loukas Lazos and William Jr. Kozma, "AMD: Audit-based Misbehavior Detection in Wireless Ad Hoc Networks", IEEE Transactions on Mobile Computing (Article in Press), pp1-14, 2012.

[17] F. Borran and A. Schiper, "A Leader-Free Byzantine Consensus Algorithm," Proc. 11th Int'l Conf. Distributed Computing and Networking, pp. 67-78, 2010.

[18] G. Chockler, M. Demirbas, S. Gilbert, C. Newport, and T. Nolte, "Consensus and Collision Detectors in Wireless Ad Hoc Networks," Proc. 24th ACM Symp. Principles Distributed Computing, 2005.

[19] Network Simulator-ns-2 Tutorial Available on link, http://www.isi.edu/nsnam/ns/tutorial/index.html.