ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 4, April 2014

A Novel Protection Scheme against Byzantine Attack in Mobile Ad hoc Network

Varsha Shrivastava, Prof. Pradeep Mishra

M.Tech. Scholar, Dept. of CSE, Oriental Institute of Science & Technology, Bhopal, India

Dept. of CSE, Oriental Institute of Science & Technology, Bhopal, India

ABSTRACT: Nodes In Mobile Ad hoc Network (MANET) nodes are communicates with each other in the absence of any centralized authority by that the Security is the one of the major problem in MANET. Due to unique characteristics of MANETS, it creates a number of consequential challenges to its security design. To overcome the challenges, there is a need to build a security scheme that achieves both extensive protection and desirable network performance from attacks. In mobile ad hoc networks where the network topology animatedly changes, straight methods cannot be used efficiently. The different security schemes against attack are improves the network performance in presence of attacker to disable misbehavior activity.In this paper we examine the behaviour of Byzantine attack effect in network that throw out infected packets in network that are beyond the capacity of network and apply proposed Intrusion Detection Scheme (IDS) scheme to secure the network from attacker. The proposed IDS scheme is detect the attacker behaviour by matching the profile of attacker to normal nodes in network if the profile of nodes are normal in the foam of proper data delivery in network then the IDS are declare the network has no attack but if the attack is identified then IDS has aware about the attacker node in network and also maintained the profile of attacker and count the infection percentage that infected the network performance. The IDS scheme is 100% recover the network performance as equal to normal routing.

KEYWORDS: Byzantine Attacker, MANET, Security, AODV, IDS

I. Introduction

Wireless communications offer organizations and users many benefits such as portability and flexibility, increased productivity, and lower installation costs. Wireless local area network (WLAN) devices, for instance, allow users to move their laptops from place to place within their offices without the need for wires and without losing network connectivity. Less wiring means greater flexibility, increased efficiency, and reduced wiring costs. Ad hoc networks, such as those enabled by Bluetooth, allow data synchronization with network systems and application sharing between devices. Handheld devices such as personal digital assistants (PDA) and cell phones allow remote users to synchronize personal databases and provide access to network services such as wireless e-mail, Web browsing, and Internet access. However, risks are inherent in any wireless technology. Some of these risks are similar to those of wired networks; some are exacerbated by wireless connectivity; some are new.

The loss of confidentiality and integrity and the threat of attacks [1] are risks typically associated with wireless communications. Unauthorized users may gain access to agency systems and information, corrupt the agency's data, consume network bandwidth, degrade network performance, and launch attacks that prevent authorized users from accessing the network, or use agency resources to launch attacks on other networks. Network traffic can be monitored on a wired network segment, but ad hoc nodes can only monitor network traffic within their observable radio transmission range [2].

MANET [3] has come into prominence due to potentially rapid infrastructure-less deployment in military and emergency situations. However, the unreliability of wireless links between nodes, possibility of mobile nodes being captured or compromised, break down of cooperative algorithms, all lead to increased vulnerability [4]. Unrelenting attackers will eventually infiltrate any system. It is important to monitor what is taking place in a system and look for intrusions. Intrusion Detection Systems (IDS) do precisely that. An IDS forms the second wall of defence in a high-survivability network.

Intrusion prevention measures such as authentication and encryption are not guaranteed to work all the time, which brings out the need to complement them with efficient intrusion detection and response. If an intrusion is detected quickly enough, the intruder can be ejected before any damage is done or any data is compromised. Effective IDS can not only serve as a deterrent acting to prevent intrusions but also provide information about intrusions to strengthen intrusion prevention measures.

II. RELATED WORK

In byzantine attack only some work is done that is mentioned here.

This paper [5] proposes a novel attack detection and defense 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. The route-discovery messages are protected by pair wise secret keys between a source and destination and some intermediate nodes along a route established by using public key cryptographic mechanisms. We also propose an optimal routing algorithm with routing metric combining both requirements on a node's trustworthiness and performance.

The main drawback of this paper not mentioned the infection from attack and using the already implemented cryptographic technique to identified attack.

In this paper [6] a detailed description of several Byzantine attacks (black hole, flood rushing, and wormhole and overlay network wormhole), analyze their mechanisms and describe the major mitigation techniques. Through simulation, we perform a quantitative evaluation of the impact of these attacks on an insecure on-demand routing protocol. The relative strength of the attacks is analyzed in terms of the magnitude of disruption caused per adversary. An implementation of the On-Demand Secure Byzantine Routing protocol (ODSBR) was created in order to quantify its ability to mitigate the considered attacks. We present a detailed description of several Byzantine attacks (black hole, flood rushing, wormhole and overlay network wormhole), analyze their mechanisms and describe mitigation techniques.

The main drawback of this scheme is to categorize behavior of byzantine attack to different attacks and proposed the security scheme for that.

The LIDS is distributed in nature and utilizes mobile agents on each of the nodes of the ad hoc network. In order to make local intrusions a global concern for the entire network, the LIDS existing on different nodes collaborate [7]. Collaboration among the nodes is achieved using two types of data: security data to obtain complementary information from collaborating hosts, and intrusion alerts to inform others of a locally detected intrusion.

SPRITE is the acronym for "a Simple cheat-Proof, RedIT-based system for Mobile Ad hoc networks with selfish nodes" system proposed by [8]. This scheme uses credits to provide incentives to selfish nodes. The charges and credit are determined by the system from a game-theoretic perspective, motivating each node to report its action honestly, even when a collection of the selfish nodes collude. The novel feature of this scheme is that it does not require the use of any tamper-proof hardware at any node.

In this paper [9], has proposed the source node to wait until the arrival of a RREP packet from more than two nodes. On receiving multiple RREPs, the source node checks about a shared hop. If at least one hop is shared, the source node judges that the route is safe. The drawback here is the introduction of a time delay due to the wait till the arrival of multiple RREPs.

In this paper [10] authors analyzed the blackhole attack and propounded that the destination sequence number must sufficiently be increased by the attacker node in order to convince the source node that the route provided is optimum. Based on differences between the destination sequence numbers of the received RREPs, the authors propose a statistical based anomaly detection approach to detect the blackhole attack. This approach has a merit that the attack can be detected at a low cost without introducing extra routing traffic without modification of the existing protocol, albeit false positives is a demerit.

In this paper [11], has shown that a malicious node can isolate a specific node and prevent it from receiving data packets from other nodes by withholding a TC message in OLSR protocol. A detection technique based on observation of both a TC message and a HELLO message generated by the MPR nodes is proposed. If a node does not hear a TC message from its MPR node regularly but hears only a HELLO message, a node judges that the MPR node is suspicious and can avoid the attack by selecting one or more extra MPR nodes.

III. PROBLEM STATEMENT

In Byzantine attack the compromised or malicious nodes tries to deliver huge amount of routing packets or routing of the data packets on the non optimal routes or selectively drop packets. Byzantine attacks can also be defined as attacks against routing protocols, in which two or more routers collude to drop, fabricate heavy data flooding, modify, or misroute packets in an attempt to disrupt the routing services since the network seems to be operating very normally in the view of the user but after some time other nodes are also affected from same behaviour. Proposed scheme is the detection of any suspicious behavior in a network performed by the network members. In that case we use AODV routing protocols and analyzed those results.

IV. Proposed Scheme against Byzantine Attack

An IDS is shown below in figure 1 which have three different modules namely Normal Profile, Worm node and Intrusion information. It contains the path of packet flow in the network this information is before the worm node enters in the network. After that worm node enter the network in place of Byzantine attack, it captures the information of normal profile and infect the vulnerable node in network through message passing (probing packets) between abstract network and detailed network and then worm node set the scan rate, scan port, percentage of vulnerability and infection parameters. If probing port of detailed network and abstract network are same then worm node sends the infected packets to all the vulnerable nodes and infects the network. Intrusion Information takes the information from both normal profile and worm node and detects the intrusion by comparing both the information's. It checks for fields like worm node number, port number, time of intrusion and type of attack.

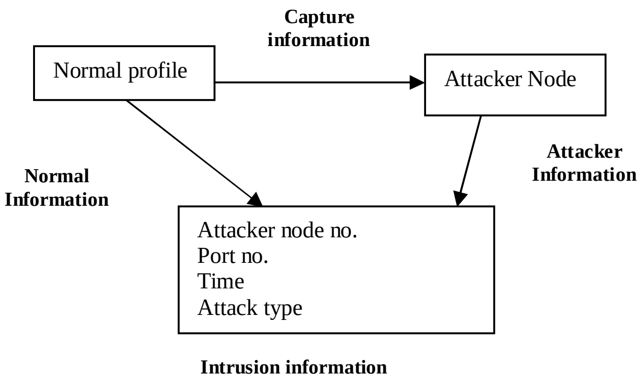

Fig. 1 Model of Intrusion Detection System

A. *An IDS (Intrusion Detection System) Algorithm of detecting the Byzantine Attack*

i. Byzantine attack Misbehavior of nodes may cause serve damage, even fails whole of the network. In proposed work we create a new protection scheme against byzantine attack misbehaviour of nodes. The IDS node identified the attacker on the basis of profile of nodes in network. The attacker profile is not match with normal nodes and in case of attacker only infection is found.

ii. In this scheme first analyze the routing behaviour of malicious nodes against the behaviour of byzantine attack and flooding attack, then apply the proper well planned security scheme on it that block the whole misbehaviour of malicious nodes and enhance the network performance.

```
Create node =IDS ; //  Node as a IDS
Set routing Protocol = AODV;
If ((node in radio range) && (next hop !=Null))
{
        Capture load (all_node)
        Create normal_profile();
        Create abnormal_table();
If ((load < = max_limit) && (new_profile == normal_profile()))
```

```
 {        No attack found;
 }
Else
{    Attack in network;
If (new_attack == abnormal_table())
{
Block the infected node ;
Find_attack_info(node_number, pkt_type,time)
Captute infection type ;
Infect percentage ;
Port_number ;
}
}
Else
{
"Node out of range or destination unreachable"
}
}
```

V. Simulation Environment

NS2 is an open-source event-driven simulator designed specifically for research in computer communication networks. The simulator we have used to simulate the ad-hoc routing protocols in is the Network Simulator 2 (ns-2) [14] from Berkeley. To simulate the mobile wireless radio environment we have used a mobility extension to ns that is developed by the CMU Monarch project at Carnegie Mellon University. Since its inception in 1989, NS2 has continuously gained tremendous interest from industry, academia, and government.

A. *Simulation Parameters*

Table 5.1 shows simulation parameter here we use two different type of routing protocol AODV [12, 13] and analyze effects of byzantine effect (Intrusion) and recovery through IDS Module.

Table 5.1 Simulation Parameter

Simulation Environment	Area 800m x 600m
Simulation Time (sec)	50
Mobile Nodes	50
Radio Range (meters)	250
Transferring Mode	Unicast
Maximum Speed (ms)	30
Routing Protocol	AODV
Transport Layer	TCP , UDP
Traffic	CBR
Application Layer	FTP
Simulation Time (sec)	50
Packet Size	512 byte
MAC layer	802.11

VI. Simulation Results

In this section the analysis of simulation results are mentioned with the scenario of normal routing, in case of attack and with protection IDS scheme.

A. *Infection Analysis*

This graph represents the infection percentage analysis in case of attack. Here we clearly visualized about 29% network are only infected from attack. The infection in network is started at time 19 sec. But after applying IDS

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 4, April 2014

scheme the infection are zero in presence of attack it means, the security scheme are completely block the misbehavior activity of attacker.

B. *UDP Packets Receiving Analysis*

User datagram protocol (UDP) is the connection less unreliable protocol for data delivery because no Acknowledgement is received by sender after deliver data. In this graph the UDP packet analysis is observed in case in case of normal AODV routing, in case of attack and in case of IDS. Here we clearly visualized the packet loss in case of attack. In case of attack negligible packets are delivering in network but after applying IDS scheme the performance of network are same as normal AODV routing.

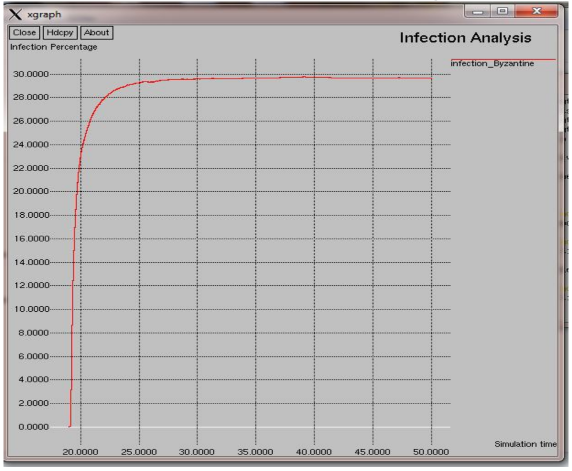

Fig. 3 Infection Analysis in Case of Attack

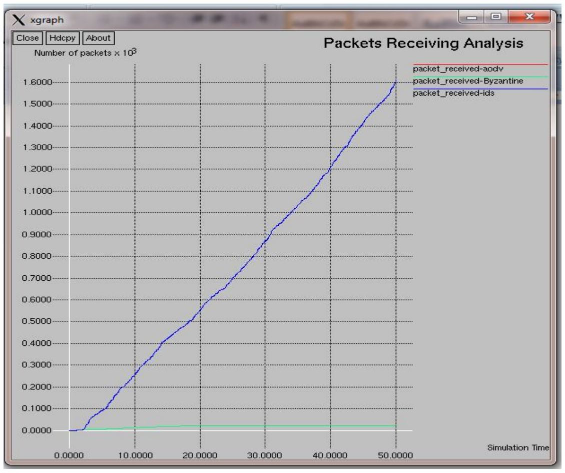

Fig. 3 UDP Receiving Analyses

C. *PDR Analysis*

PDF is the ratio of packets received by send. The PDF in case of attack are only evaluated at time 20 seconds but after applying security scheme PDF is improved and equal to normal. The security scheme are improved the performance and providing the efficient PDR in network. In case of attack the PDF is about 85% at time about 20 seconds but in case of IDS scheme the PDF performance is 90% up to end of simulation.

D. *Routing Packets Analysis*

The DDOS attacker are continuously flooding the huge number of packets in network (About more than 200000) it means to consume the bandwidth in network by that the nodes are not confirm with each other about such kind of misbehaviour. This graph represents the routing load in case of attack is very high, this is the main reason of congestion occur in the network. After applying IDS routing load is in under control and equal to normal routing behaviour.

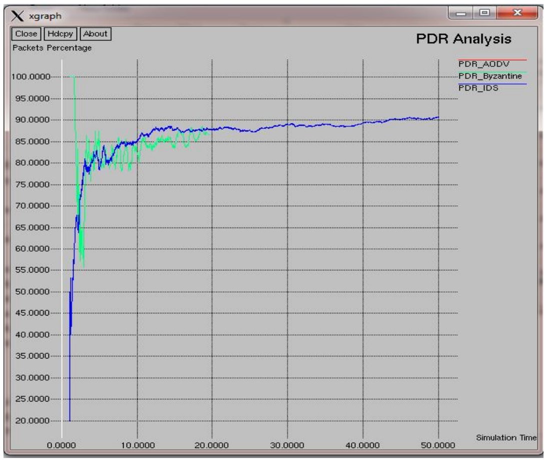

Fig. 5 PDR Analysis

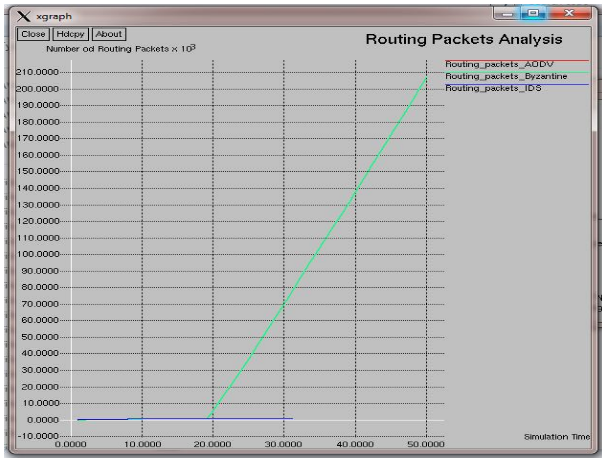

Fig. 6 Routing Packets Analysis

E. *Throughput analysis*

This graph represents the throughput analysis in case of normal routing, Byzantine attack and IDS. The throughput has measure on number of data packets are received at destination in per second. At the time of attack throughput decreases due to heavy routing packets flooding in network. It is measurable only up to 30 seconds in network. But after applying IDS scheme the throughput is equal to normal routing about 1400 packets /sec.

F. *Overall Analysis*

The overall performance of network is shown in table 3. This table represents the whole summery of performance metrics in exact figure foam means how many packets are send, receive and loss so on in network in case of normal routing, attack and IDS.

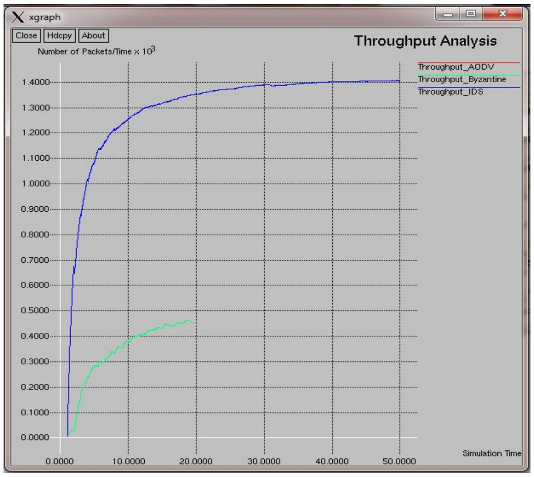

Fig. 7 Throughput Analysis

Table 2 Overall performance of network

Parameters	AODV	Byzantine Attack	IDS
SEND	5150	728.00	5150
RECV	4666	517	4666
ROUTING PKTS	716	206933	716
PDF	90.60	71.02	90.6
NRL	0.15	400.26	0.15
dropped data (packets)	478	152	478

VII. CONCLUSION

In Mobile Ad hoc Network (MANET) the nodes are continuously interchanging the information in network. But the information is in the foam of large number of packets flooded in network then in that case the network is affected from Byzantine attack. The simulation has been done with AODV routing protocol. The proposed mechanism eliminates the need for a centralized authority which is not practically in Mobile Ad hoc network due to their self organizing nature. The byzantine attacker has degrades the network performance but he security scheme has improves the network performance as equal to normal AODV routing. The results demonstrate that the presence of a Byzantine increases the packet loss and routing load in the network considerably. The proposed IDS or Profile based Protection Scheme (PPS) mechanism protects the network through a self organized, fully distributed and localized procedure. The attacker has infected the 29% network performance in network but due to that remaining performance of network is also affected. The proposed security scheme showing the better results in presence of Byzantine attacker.

REFERENCES

1. Sudhir Agrawal, Sanjeev Jain, Sanjeev Sharma, "A Survey of Routing Attacks and Security Measures in Mobile Ad-Hoc Networks", Journal of Computing, Volume 3, Issue 1, pp. 41-48, January 2011
2. http://library.uws.edu.au/adt-NUWS/uploads/approved/adt NUWS20060125.131604/public/12Chapter11.pdf.
3. G. S. Mamatha1 and Dr. S. C. Sharma "Analyzing the MANET Variations, Challenges, Capacity and Protocol Issues" International Journal of Computer Science & Engineering Survey (IJCSES) Vol.1, No.1, August 2010.
4. Ketan Nadkarni, Amitabh Mishra,"A Novel Intrusion Detection Approach for Wireless Ad hoc Networks IEEE Wireless Communications and Networking Conference (WCNC), pp. 831-836, Atlanta, Georgia, USA, 21-25 March 2004.
5. Ming Yu, Mengchu Zhou and Wei Su, "A Secure Routing Protocol Against Byzantine Atacks for MANETs in Adversarial Environments" IEEE Transactions on Vehicular Technology, Vol. 58, No. 1,pp. 449-460, January 2009.
6. www.etd.unipi.it/theses/available/etd05182005122420/unrestricted/ LVMM.pdf
7. Amitabh mishra, Ketan nadkarni, and Animesh patcha "Intrusion Detection in wireless Ad-hoc networks IEEE Wireless Communication, 48–60, 2004.
8. S. Capkun, J.-P. Hubaux, and L. Buttyan, "Mobility helps security in ad hoc networks," Proceedings of the 4th ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC 2003), pp. 46–56, Annapolis, Maryland, USA, 2003.
9. [47] M.A.Shurman, S.M.Yoo, and S.Park, "Black Hole Attack in Mobile Ad Hoc Networks," ACM Southeast Regional Conference, pp. 96-97, 2004.
10. [48] S.Kurosawa, H.Nakayama, N.Kato, A.Jamalipour, and Y.Nemoto, "Detecting Blackhole Attack on AODV-Based Mobile Ad Hoc Networks by Dynamic Learning Method," International Journal of Network Security, vol. 5, no. 3, pp. 338-346, November 2007.
11. B. Kannhavong, H. Nakayama, N.Kato, Y.Nemoto and A.Jamalipour, "Analysis of the Node Isolation Attack Against OLSR-based Mobile Ad Hoc Networks," Proceedings of the Seventh IEEE International Symposium on Computer Networks (ISCN' 06), pp. 30-35, June 2006.
12. C. Perkins, E. B. Royer, S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing - Internet Draft", RFC 3561, IETF Network Working Group, July 2003.
13. Humayun Bakht,"Survey of Routing Protocols for Mobile Ad-hoc Network" International Journal of Information and Communication Technology Research (IJICT) Volume-1 No. 6, pp 258-270, October 2011.
14. K Fall and K. Varadhan, The NS Manual, November 18, 2005, http://www.isi.edu/nsnam/ns/doc/ns_doc.pdf. 25 July 2005.