Scientific Journal of Impact Factor (SJIF): 3.134

ISSN (Online): 2348-4470
ISSN (Print) : 2348-6406

International Journal of Advance Engineering and Research Development

Volume 1, Issue 11, November -2014

DISTRIBUTED INTRUSION DETECTION APPROACH FOR BYZANTINE ATTACK INVOLVING WORM HOLE IN AD HOC NETWORK

Bansi Aghera[1], Prof. Swati Sharma[2]

[1]*Computer Engineering, Darshan Institute of Engineering and Technology, Rajkot, Gujarat, India, bansiaghera@gmail.com*
[2]*Computer Engineering, Darshan Institute of Engineering and Technology, Rajkot, Gujarat, India, swati.sharma@darshan.ac.in*

Abstract: *To secure an ad hoc network is challenging problem. Feasibly detect and defined the internal attacks against the routing protocols, such as Byzantine behaviors in ad hoc network, is challenging problem. Where adversaries have full control on a number of authenticated devices and behave arbitrarily to disrupt the network, known as Byzantine wormhole attack. There are many forms of Byzantine attacks, including byzantine black hole, Byzantine flood rushing, and byzantine wormhole attack. Among all Byzantine attacks, Byzantine wormhole attack is considered one of the most complicated and severe attack in ad hoc networks. In this paper focus on Byzantine Wormhole attack that threatens the security of system and studying its effect on ad hoc network .The objective of work is to implement byzantine wormhole attack in AODVM enabled ad hoc network. Paper presents an approach to implement and analyze the effect of Byzantine Wormhole attack.*

Keyword: *Byzantine wormhole, AODVM, DIDS, Clustering, IDS, Central cluster-head.*

I. INTRODUCTION

Ad hoc network is decentralized wireless network. Its ad hoc because it does not have any preexisting infrastructure, such as routers in wired network or access points in managed wireless networks. Each node participates in routing process by forwarding data for other nodes, so determination of which nodes forward data is made dynamically on the basis of network connectivity. Because of Vulnerabilities in ad hoc network like dynamic topology, absence of infrastructure, vulnerability of nodes and channels, easily possible to compromised any node in routing process then intruder able drop packet or exchange the information.

MANET is one type of ad hoc network. In ad hoc network all nodes are mobile in nature that means its at some time its work with one topology and after some time its move to another topology. In MANET nodes can communicate via radio communication range and communicate directly. But those nodes which are not neighbor they depend on other nodes in network who relays their packets. In ad hoc network assume that all nodes are cooperative and helps to route packet from source to destination. Due to open nature and physical protection of nodes is not possible, any node within network can be compromised by intruder. Compromised node may behave maliciously and able to disturb normal operation in network. Other issue with MANET is routing protocol, which assumed that all nodes are cooperating. This create most vulnerable place which can be exploited by making attack on route discovery phase of the routing protocols. Some technique like authentication and encryption are defense to network but these techniques are inefficient to protect MANET. Above technique work well with wired network but in wireless network due to resource constraint and decentralization control over all nodes this technique can't work with MANET.

Other way to defense to network is IDS (Intrusion detection system). There are many solutions have been proposed and implemented in wired network. In wired network IDS can be defined two kind host based and network based. In network based IDS Installed on especially dedicated device or generally on gateway. But in MANET we don't have any centralized control or administration mechanism through which all packets will be passing. Main task of IDS is to audit data collection and analyze that collected data and make appropriate decision on it, but nature of MANET is dynamic. Because of nature raises two issues, how audit data collection is done and where our IDS agent resides. Many approaches are proposed for choosing architecture of IDS. Among all architecture distributed is most useful model. Nodes in MANET are resource constrained in terms of computation power and energy. Using cluster based IDS, IDS resides on all nodes but not active all at a time. One node chosen as cluster head and that perform intrusion detection. After some time again election algorithm initiated to choose another cluster head. This mechanism helps to save energy of nodes and improve life of MANET.

The rest of paper is organized as follows. In section 2 related works on existing DIDS and IDS and attack study. Section 3 byzantine wormhole attack creation and proposed detection and recovery technique. In section 4 routing protocol AODVM (ad hoc on demand distance vector multipath routing). In Section 5 evolutionary parameter and in section 6 conclusion and future work.

II. RELATED WORKS

2.1 Attack in Ad hoc Network

Attacks on networks, in many varieties and they can be classified into main two way.

1. *Passive attacks*: which not involve disruption of information but they are merely intended to get information and to spy on the communication within the network. For example eavesdropping.
.
2. *Active attacks*: In which data are altered by attacker which involves overloading of network or preventing nodes from using the networks services effectively anymore. It involves specific actions performed by adversaries, for instance modification and deletion of exchanged data among the nodes.

Also we can classify attacks on a MANET into two categories external and internal attack. In case of external attack origin of attacks lies within node that is external to victim node network while internal attack launched by compromised node or nodes within network. Impact of internal attack is more severe than that of external attack because internal compromised nodes have valuable information like network topology and he also possesses adequate access privileges.

Table 1 : Attacks on Protocol Stack

Layer	**Attack**
Application Layer	Repudiation, data corruption
Transport Layer	Session hijacking, SYN flooding
Network layer	Wormhole, black hole, Byzantine, flooding, resource consumption, location disclosure attacks
Data link layer	Traffic analysis, monitoring, disruption MAC (802.11), WEP weakness
Physical layer	Jamming, interceptions, eavesdropping
Multi-layer attacks	DoS, impersonation, replay, man-in-the-middle

Table1. Lists some attacks related to corresponding protocol layer. There are some attacks which can be launched at multiple layers.

2.2 Byzantine Attack

Because of much vulnerability in network protocols (including wireless ad hoc routing protocols) are caused by the lack of message integrity and authentication mechanisms, which allow an attacker to alter or drop the packets. Much research is done to secure ad hoc wireless routing protocols and wired routing protocols focused on this issue. Authentication and integrity mechanism is required to protect a network protocol, they ensure that a packet was generated by an authenticated node and it is not altered or modified packet. However, they do not provide any guarantee about the legitimacy of actions taken by authenticated nodes. Protect a network protocol, since they ensure that a packet was generated by an authenticated node and has not been tampered with. However, they do not provide any guarantee about the legitimacy of actions taken by authenticated nodes.

Attacks where the adversary has full control of an authenticated device and can perform arbitrary behavior to disrupt the system are referred to as Byzantine1 attacks. Research addressing this category of attacks is quite scarce below we outline several Byzantine attacks that are considered in this work [2].

There are several Byzantine attacks.

Black Hole Attack: In black hole attack adversary node stops forwarding data packets and still participates correctly in routing process. As result when source node chooses a route involve adversary node, it prevents communication on that path. Most of routing protocols are disrupted by black hole attacks.
Flood Rushing Attack: In this attack, its take place during the propagation of a legitimate flood and the adversarial variant of it. If an adversary successfully reaches some of its neighbors with its own version of the flood packet before they receive a version through a legitimate route, then those nodes will ignore the legitimate version and will propagate the adversarial version. This may result in the continual inability to establish an adversarial-free route, even when authentication techniques are used.

Byzantine Wormhole Attack: In this attack the adversary perform a more effective attack. One such attack is a Byzantine wormhole, where two adversaries collude by tunneling packets between each other in order to create a shortcut in the network. This tunnel can be created either using a private communication channel, such as radios and directional antennas, or by using the existing ad hoc network infrastructure. The adversary node can send a route request and discover a route across the ad hoc network, and then tunnel packets through the honest nodes to execute the attack. The adversaries can use the low cost appearance of the wormhole links in order to increase the probability of being selected as part of the route, and then attempt to disrupt the network by dropping all of the data packets. The Byzantine wormhole attack is strong attack that can be performed even if only two nodes have been compromised.

Byzantine wormhole is different from traditional worm hole. In the traditional wormhole attack, an adversary or multiple adversaries trick two honest nodes into believing that there exists a direct link between the honest nodes. The difference is that in the Byzantine case, the wormhole link exists between the adversarial nodes, not between the honest nodes

*Byzantine Overlay Network Wormhole Attack***:** A more general variant of the previous attack occurs when several nodes are compromised and form an overlay network. By tunneling packets through the overlay network, the adversaries make it appear to the routing protocol that they are all neighbors, which considerably increases their chances of being selected on routes. This is the strongest attack considered in this work.

2.3 Distributed Intrusion Detection Technique

IDS for traditional wired systems are not well suited to Ad hoc network, many researchers have proposed several distributed IDS especially for ad hoc network, out of which some of them will be reviewed in this section.

Distributed IDS using mobile agents: This approach is combination of distribution and cooperative scheme, in which malicious node is detected with the help of the mobile agent. Fast randomized algorithm is used for key distribution and security is increased by encrypting the packets. The time taken to find the malicious node is reduced when compared to the other scheme [3].

Cluster based distributed detection scheme: In order to address the run-time resource constraint problem, a cluster-based detection approach is used. The idea is to elect a node, the cluster head, to perform IDS functions for all nodes within a cluster [4].

Agent based cooperative and distributive: In anomaly detection system comprises of detection modules for detecting anomalies in each layer. This system is cooperative and distributive; it considers the anomaly detection result from the neighbor node(s) and sends the current working node's result to its neighbor node(s) [5].

Neural network based distributed detection: In this distributed IDS for mobile ad hoc networks using eSOM. By exploiting the visualization of network traffic our approach detects selective packet dropping attack by classifying malicious and normal behavior. This approach uses the MAC layer feature set as audit data. This audit data are used as input a type of neural networks known as Emergent SOM in order to perform intrusion detection [6].

Cluster based distributed IDS: This approach use of FSM makes possible to analyze in depth, the messages exchanged between nodes. In this apply a backward checking algorithm to detect violations on the specification. This approach provides significant benefit on the quickness of the verification process, what is crucial in the context of run-time verification [7].

III. BYZANTINE WORMHOLE ATTACK

In byzantine attack, black hole attack needs a large number of attacker or intruder to disrupt the network. Intuition would lead us to believe that if intruder or adversary was capable to compromise some set of nodes, then exist a more effective

attack which would involve cooperation of the adversary nodes. One such that type of attack is Byzantine wormhole attack. Traditional wormhole and Byzantine worm hole both are different, in the traditional wormhole attack an adversary or multiple adversaries trick two honest nodes into believing that there exists a direct link between honest nodes. Difference is that in Byzantine case, wormhole link exists between adversarial nodes, not between honest nodes.

This attack occurs when two adversaries cooperate to tunnel packet between each other in order to create a shortcut (or wormhole) in the network. Two adversary nodes create a tunnel by using private communication channel such as wired communication or pair of radios and directional antennas or by using existing ad hoc infrastructure in network. In this attack adversary have complete control on authenticated devices, so that have complete access to use the ad hoc network and as a result, the adversaries can send a route request and discover a route across the ad hoc network. Adversaries can then tunnel packets through non adversarial nodes to execute attack. When adversaries tunnel a route request between one another, they are able two to make a route that actually appear shorter than it actually is. Because of short path, adversaries have high probability of being selected by routing protocol. Once that route selected, adversaries perform a black hole attack, by dropping actual packet data. Also, as it allows an adversary to jump several hops ahead of the legitimate flood at once, a wormhole serve as an effective tool for conducting flood rushing attacks.

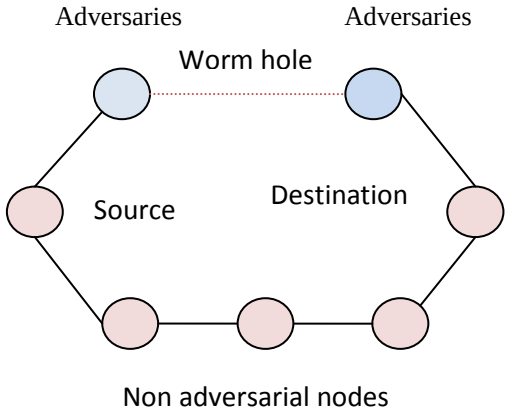

Figure 1 : Byzantine wormhole configuration

3.1 Model for Byzantine Wormhole Attack

In this paper approach can be abstractly classified into three categories as follows
1. Implementation of Byzantine attack (i.e. Wormhole Attack)
2. Analyze the effect of Attack on ad hoc network
3. Adoption of efficient recovery techniques

It is difficult to detect such dangerous attacks and no one can predict what the wormhole nodes can do. The wormhole attack is not visible at the higher layer and therefore, two end points which create the wormhole are not visible in the route in which detection becomes much more complex. Wormhole can be classified into further five categories as proposed,

- Wormhole using Encapsulation.
- Wormhole using out of band channel.
- Open wormhole attack.
- Closed wormhole attack.
- Half open wormhole attack.
- Wormhole with high power transmission.

Wormhole Using Encapsulation: When Destination node broadcast for the RREQ to its neighbor's node, where as some neighbor is an attacker. Attacker node records the RREQ request. Then tunnel to other adversary node. Via adversary route request is transmit quicker than other route, as a result source route a packet through adversary nodes.

Open wormhole attack: In this attack malicious node keep examine the wireless medium to process the discovering RREQ packets, in the presence of adversary node in the network other node on the network suppose that malicious node are present on path and they are their direct neighbors.

*Closed wormhole attack***:** The attacker does not modify the capture packet nor did it modify the packet field head. The attacker take the advantage when the packets are in the process to find a route know as route discovery. At route discovery process attacker tunnel the packet from one side of the network to another side of the network and re-broadcast packets.

*Half open wormhole attack***:** In this attack only one side of the packet is modify from the malicious node and the other side of the malicious node do not modify the packet subsequently route discovery procedure.

Wormhole with high power transmission In this attack malicious node use maximum level of energy transmission to broadcast a packet, When malicious node received a Route Request (RREQ) by using route discovery process, it broadcast the Route Request (RREQ) at a maximum level of energy of it power so the other node on the network which are on the normal power transmission and lack of high power capability hears the maximum energy power broadcast they rebroadcast the packet towards the destination. By doing this malicious node get more chances to create a route between source and destination without using colluding node.

3.2 Cluster Based Distributed Intrusion Detection Scheme

3.2.1 Cluster Formation and Maintenance

In a clustering scheme a mobile nodes in MANET are divided into different group based on certain rules. Cluster is formed based on COMBINED HIGHER CONNECTIVITY LOWER ID (CONID) clustering algorithm. It is an extension of the lowest ID algorithm; lowest ID algorithm does not take into account the connectivity (degree) of nodes, therefore may pro-duce more number of clusters than necessary. The pure connectivity based clustering algorithm modified version the lowest ID algorithm, in which ID is replaced by node degree, but it does not work properly because of numerous ties between nodes. On base both algorithm k-CONID (k- hop connectivity) algorithms used, in which each node assigned with cluster head priority. A pair is denoted by did = (d, ID), where d is its connectivity and ID is its IP address.

Let did'= (d', ID') and did"= (d", ID"). Then did'>did' if d'> d" or d'=d" and ID' < ID". That is, a node has cluster head priority over the other node if it has higher connectivity or in case of equal connectivity and has lower ID. After applying clustering algorithm the network is shown Figure 2. After running CONID, each cluster head finds its all neighbor cluster heads

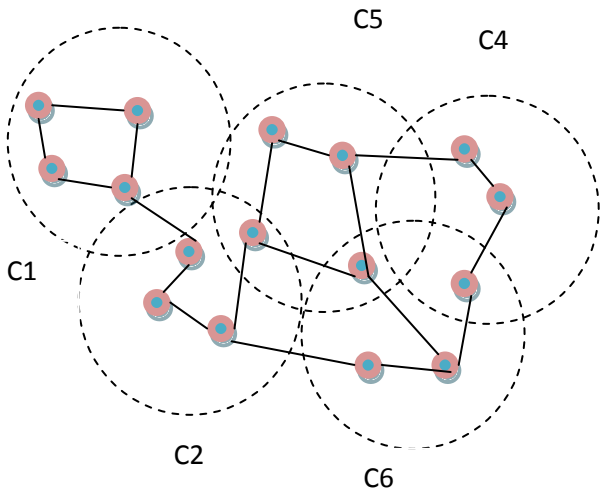

Figure 2 : Network with clusters

After deciding cluster head all communication takes place between cluster head. Using AODVM routing algorithm

Step: 1 route request to cluster-head
Exits, sends packets
Else
Route request to neighbor cluster-head;
Step: 2 Start timers (Record (Hop Count, Delay)

Step: 3 Worm-hole Detection
Hop-count<threshold (average hop-count)
Then
Check delay;
Step: 4 Check Delay of all previous routes which involve any on node of the suspicious route Now the node not encounter previously should be malicious let there are N such nodes.

Step: 5 if (N==1)
Then it is attacker
Else
Send route query to neighbor
If neighbor detect similar node and with malfunctioning
Then
Mark it malicious;
Else
Repeat process;
Step: 6 Cluster-head send info to guard node, guard node broadcast to other cluster-head to delete that route.

IV. AODV-MULTIPAT RROUTING PROTOCOL

The AODV-Multi-path (AODVM) routing protocol (Ye *et al.*, 2003) is an extension of the AODV protocol to determine node-disjoint routes. In AODVM route selection is based on the route discovery. In order to facilitate the computation of multiple node disjoint paths from the source to destination, we choose the Ad hoc On-Demand Distance Vector Multipath (AODVM) protocol as a candidate protocol and make modifications to it to enable the discovery of node disjoint paths via cluster heads [11].

In the AODVM, when the source node wants to send packets to a destination, it looks up its route cache to determine if it already contains a route to the destination. If it finds that an unexpired route to the destination exists, then it uses this route to send the packet. But if the node does not have such a route, then it initiates the route discovery process by broadcasting a RREQ packet.

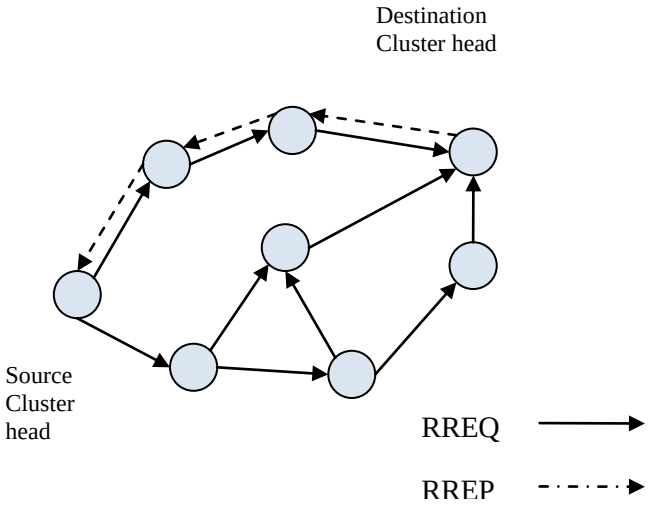

Figure 3 : Route Discovery Process of AODV Routing Protocol

When a RREQ packet is received to a destination cluster head, it generates a RREP packet and sent back to its neighbor cluster head (last hop) from which the RREQ packet has been received. When an intermediate cluster-head receives the RREP packet, it checks its RREQ table to find its neighbor cluster head (next hop in reverse path) through which shortest path back to the source cluster-head and sends the RREP packet to it by deleting corresponding entry in the RREQ table.

In order to ensure that a cluster head does not participate in multiple paths, If it receives another RREP packet from different neighbor cluster head, it is dropped (i.e., RREQ table is already empty), it generates a Route Discovery Error (RDER) packet and sends it back to the neighbor cluster head through which another the RREP packet has been received. The neighbor clustered upon receiving the Route Discovery Error (RDER) packet will try to forward the RREP packet to another neighbor cluster head through which shortest path back to the source cluster head and sends the RREP packet to it by deleting corresponding entries in the RREQ table.

V. EVOLUTION PARAMETER

Basic parameters used for experimentation. Some of the experimentation done for checking the behavior of AODV protocol under wormhole attacks are given below:

Table 2: Parameters

Parameters	Value
Simulator	Ns2
No of nodes	50 or more
Routing protocol	AODVM
Traffic model	CBR

VI. CONCLUSION

In previous study Worm hole detection using optimized multipath algorithm shows result based on three parameter hop count, delay and throughput. In this paper proposed work define a distributed intrusion detection approach based on cluster. In which all cluster-head have mechanism to detect wormhole attack. In previous work detection scheme used on node while in proposed scheme used at head of cluster this idea helps to save energy of nodes and improve life of MANET. Member of cluster, all members able to perform IDS but at time elected cluster head perform. If any reason clusters head not able to perform IDS, then lower ID and higher connectivity node choose as a cluster-head based on k-hop CONID.

VII. FUTURE WORK

Future work is to implement proposed scenario and analyze the performance of AODVM under normal environment, under byzantine wormhole attack and performance after elimination of byzantine wormhole attack in term of throughput, number of hops per route and delay. Further work to show a result, how much disturbance occurs in network when cluster-head behaves as intruder.

REFERENCES

[1].”Deng, Hongmei, Wei Li, and Dharma P. Agrawal. "Routing security in wireless ad hoc networks." *Communications Magazine, IEEE* 40, no. 10 (2002): 70-75.
[2]. “Mitigating Byzantine Attacks in Ad Hoc Wireless Networks Technical Report Version 1 March 2004”.
[3].”Intrusion detection scheme using mobile agent in MANET”. Research journal’s Journal of Computer Science Vol. 1 | No. 2 March | 2014.
[4].” A Cooperative Intrusion Detection System for Ad Hoc Networks” SANS ’03 Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks New York, NY, USA ©2003.
[5]” Agent Based Efficient Anomaly Intrusion Detection System in Ad hoc networks” IACSIT International Journal of Engineering and Technology Vol. 2, No.1, February, 2010 ISSN: 1793-8236.
[6].” Intrusion Detection of Packet Dropping Attacks in Mobile Ad Hoc Networks” International Conference on Intelligent Systems And Computing: Theory And Applications.
[7].” An EFSM-based intrusion detection system for ad hoc networks”.
[8]. Saurabh Upadhyay ” Impact of Wormhole Attacks on MANETs” , International Journal of Computer Science & Emerging Technologies (E-ISSN: 2044-6004) 77 Volume 2, Issue 1, February 2011.
[9]. J. Han and M. Kamber. Data Mining, Concepts and Technique. Morgan Kaufmann, San Francisco, 2001.
[10]. YU-FANG ZHANG, DISTRIBUTED INTRUSION DETECTION BASED ON CLUSTERING” Proceedings of the Fourth International Conference on Machine Learning and Cybernetics, Guangzhou, 18-21 August 2005.

[11]. M. BHEEMALINGAIAH" Energy Aware Clustered Based Multipath Routing in Mobile Ad Hoc Networks" I. J. Communications, Network and System Sciences, 2009, 2, 91-168 Published Online May 2009 in SciRes (http://www.SciRP.org/journal/ijcns/).

