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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

A Study on Homogeneous/Heterogeneous Intrusion Detection System in Mobile Ad Hoc Network

Kapil M. Patel[1], Sushant S. Bahekar[2]

PG Student, Dept. of Computer Engineering, SSBT'S COET, Bambhori, North Maharashtra University, Jalgaon, India[1]

Assistant Professor, Dept. of Computer Engineering, SSBT's COET, Bambhori, North Maharashtra University, Jalgaon, India[2]

ABSTRACT: Nowadays, Mobile Ad Hoc Networks (MANETs) are more vulnerable to various types of attacks due to the insecure communication medium and infrastructure-less environment. In this paper a system is proposed to detect misbehaving node in a homogeneous as well asa heterogeneous environment. In such networks, to monitor the behavior of nodes over a wide environment it is proposed to realize an intrusion detection system with only a single monitor node to be elected. This node will monitor the function of each node in the entire network. If there is any disruption in the normal behavior of a communication channel then the monitor node will identify the node, which is malicious node.

KEYWORDS: IDS, MANET, CBID, Malicious node.

I. INTRODUCTION

Mobile ad-hoc networks (MANETs) can be formed without any fixed infrastructure. A MANET is an infrastructure less network, since the nodes belonging to the network can easily move in the environment. It is due to this mobility of nodes, the network topology cannot be predicted. In this environment each node can have be a transceiver and receiver, so eachnode can also act as a router and the nodes communicate with each other without any fixed infrastructure. If both the sender and the receiver nodes are within their radio range, then they will communicate directly otherwise communication needs one or more intermediate node. This is called multihop communication. Therefore, there are normally situations when each node acts as a host and router at the same time.

MANETs are more vulnerable to attacks because of the open communication medium. The attacks can be classified into two categories: active attacks and passive attacks. Many methods have been proposed to detect active attacks, but passive attacks are more challenging in ad-hoc network environments. So, we observe numerous research efforts that have been made to secure ad-hoc networks from the attackers; but there are no sufficient methods for detection of an attacker and respond to an attacker. To solve this problem many Intrusion Detection systems (IDS) have been proposed. In Cluster Based Intrusion Detection (CBID) Systems, the mobile nodes are grouped together to form two or more clusters. Within the cluster, one node will be elected as a cluster head and this head node will monitor the behaviours of each and every node in that cluster. If there is any malicious activity identified by a cluster head then it will detect the intruder node and expel the misbehaving node from the cluster.

The rest of the paper is organized as follows: In Section II we review the literature survey. Various types of attacks are described in Section III. In Section IV we present the proposed mechanism. We conclude the paper in Section V.

II. LITERATURE SURVEY

Many intrusion detection systems have been proposed. In 2003, P.M.Mafra [1] proposed algorithms for a distributed intrusion detection system in MANETs. The aim of this paper is to employ fault tolerance techniques and cryptographic mechanisms to detect and deal with malicious or faulty nodes. This model focused only on hierarchical IDS model used

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

to detect the malicious activity in MANET environments. But this method did not focus on other malicious activity detection ideas.

Hasini.et.al [2] proposed the IDS applications that can be used in an environment with a set of mobile nodes. In which a leader node will be elected to monitor the behaviour of an entire network. This method reduces the energy consumption, network traffic and also leader election and also intrusion detection process. Ali. H. Afsari [3] proposed end to end communication between source and destination. The OLSR protocol mechanism was used to perform intrusion detection accurately and to isolate the misbehaving node.

Nisha Dang.et.al [4] proposed a clusterbased intrusion detection system and it analyse the involvement of overhead in cluster based intrusion detection systems and also explored some techniques for reduction of attacks. But this method has not provided any secure algorithm in terms of time consumption.

EjazAhmed.et.al[5] proposed a generalized clustering algorithm to detect intruders, which had high detection rate and low processing and memory overheads. But, CBID systemsrequire different routing protocolsto check the effectiveness and independence, which are not taken for consideration.

III. ATTACKS IN MANET

Attacks on mobile ad hoc networks can be divided in to two categories:

- Passive Attacks
- Active Attacks

Passive attacks will not perform any operation on the data.Instead it will just listen to the data which is being transmitted. But in active attacks the data will be modified by intruders, which include modifying the content or appending the new data which may disturb the normal operation of a network. Internal attack is the attack that comes from a compromised node inside the network. Whereas, as external attacks comes from outside of the network and also may cause congestion in the networks . Sometimes active attacks may be created by compromise nodes or selfish nodes that drop the packets.

A. *WORMHOLE ATTACK:*

In a wormhole attack, an attacker receives packets at one point in the network , “tunnels” them to another point in the network, and then replays them in to the network from that point.Routing can be disrupted when routing protocol message are tunnelled. This tunnel between two colluding attack is known as wormhole.

B. *EAVESDROPPING ATTACK:*

In this type of attacks, the intruder silently listens to the communication by tapping the wireless link.

C. *FLOODING ATTACK:*

In a flooding attack, attacker exhausts the network resources, such as bandwidth and to consumes a nodes resources, such as computational and battery power or to disrupt the routing operation to cause server degradation in network performance.

D. *BLACK-HOLE ATTACK:*

In this type of attack, a malicious node acts like a Black hole, dropping all data packets passing through it as like matter and energy disappears from our universe in a black hole. If the attacking node is a connecting node of two connecting componentsof that network, then it effectively separates the network in to two disconnected components.

E. *GRAY-HOLE ATTACK:*

In this attack, instead of dropping all packets the intruder node will randomly drop the packets.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

F. ***JELLYFISH ATTACK:***

Jellyfish attack is somewhat different from Black-Hole & Gray-Hole attack. Instead of blindly dropping the data packets, it delays them before finally delivering them. It may even scramble the order of packets in which they are received and sends it in random order. This disrupts the normal flow control mechanism used by nodes for reliable transmission. This attack can result in significant end to end delay and thereby degrading QoS.

G. ***ROUTELOOP ATTACK:***

The malicious node may advertise wrong routes to the source node, due to which, the source node may send packets through wrong route. So the packet may not reach the destination within the stipulated time.

H. ***IGNORING THE MAC PROTOCOL ATTACK:***

In an ad-hoc network environment only two nodes can communicate with each other at a time. But this rule may not be known by malicious node. The malicious node may initiates sending a packet to a node when it already has communication with some other node.

I. ***CLONING NODE ATTACK:***

In a clone node attack, the malicious node captures the credentials of the original node by extracting its feature and replicates it in the network.

IV. PROPOSED SYSTEM

In this paper it is proposed that a cluster based intrusion detection system with a single master cluster-head will monitor the behavior of nodes both in inter-cluster and intra-cluster. In this method, one cluster head will be elected from each cluster, and then one master cluster-head will be elected from among the different cluster-heads. This master cluster-head node will collect the information from the different cluster-heads, analyses the presence of intrusion and then eliminates the malicious node or malicious nodes from the network. This system is being implemented using NS2 tool.

V. CONCLUSION

Currently MANET plays a vital role in information sharing era, due to the rapidadvancement in wireless technology. MANET is vulnerable to intrusion because of the dynamic change in network topology and the lack of security measures. So, this type of network requires security incorporation into the environment. The intrusion detection system will monitor the behaviour of nodes in the network and detect and isolate the malicious node(s). The conventional detection mechanisms will slow down the process of creating harmful event in a mobile environment with several issues, which harness the quality of the MANET. So the proposed cluster based intrusion detection system will protect the mobile network with minimized overheads.

REFERENCES

1. P. M. Mafra, J.S. Fraga, A.O. Santin, “Algorithms for a Distributed IDS in MANET” Journal of computer and system sciences 80 (2014).
2. Saravana Kumarasamy, Hemlatha B. and Hasini,“Cluster Based Cost Efficient Intrusion Detection System for MANET” Crptography and Security, Networking and Internet Architecture.
3. Ahamed M. Abdalla, Imane A. Saroit, Amira Kotab, Ali. H. Afsari,“Misbehaviour nodes Detection and Isolation for MANETs OLSR Protocol”, Procedia Computer Science(2011)
4. Nisha Dang,“Cluster Based Intrusion Detcetion Systems for MANETs” International Journal of Computer Applications & Information Technology.
5. Ejaz Ahmed Kashan Samad,“Cluster_Based Intrusion Detection (CBID) Architecture for MANETS”, 5th Conference, AusCERT2006 Gold Coast, Australia, May 2006 Prceedings.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

6. Abhijit Deodhar,"A Cluster Based Intrusion Detection System For Mobile Ad Hoc Networks", 2013.
7. Mingliang Jiang Li, Y. C. Tay,"Cluster Based Routing Protocol (CBRP)", Internet Draft, Jul, 1999.
8. Yunjung Yi, Mario Gerla, Tack-Jin Kwon, "Efficient Flooding in Ad-Hoc Networks using On demand (Passive) Cluster Formation", Proceedings of Mobihoc , Jun 2003.
9. Manjeet Singh and Gaganpreet Kaur,"A Surveys of Attacks in MANET", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3, pp. 1631-1636, June 2013.
10. Mr. P. Ramkumar, Ms. V. Vimala and Ms. G. Sivakama Sundari," Heterogeneous and Homogeneous IDS in MANETS", International Conference on omputing Technologies and intelligent data engineering, 2016