Cluster Based Intrusion Detection System for MANETS

Nisha Dang
M.Tech. Student
DCSA, MDU
Rohtak

Pooja Mittal
Assistant Professor
DCSA, MDU
Rohtak

ABSTRACT

Manets are the ad hoc networks that are build on demand or instantly when some mobile nodes come in the mobility range of each other and decide to cooperate for data transfer and communication. Therefore there is no defined topology for Manets. They communicate in dynamic topology which continuously changes as nodes are not stable. Due to this lack of infrastructure and distributed nature they are more vulnerable for attacks and provide a good scope to malicious users to become part of the network. To prevent the security of mobile ad hoc networks many security measures are designed such as encryption algorithms, firewalls etc. But still there is some scope of malicious actions. So, Intrusion detection systems are proposed to detect any intruder in the network and its malicious activities. Cluster based intrusion detection system is also designed to restrict the intruders activities in clusters of mobile nodes. In clusters each node run some intrusion detection code to detect local as well as global intrusion. In this paper we have taken insight of intrusion detection systems and different attacks on Manet security. Then we proposed how overhead involved in cluster based intrusion detection system can be reduced.

Keywords

Wireless Network, Mobile ad hoc Network, MANET, Intrusion Detection System, IDS

1. INTRODUCTION

Mobile ad hoc networks are so widely used in present mobile world where every one wants to get information instantly and rapid growth in wireless devices such as mobile, laptop, PDAs and wireless telephones. Mobile ad hoc network is formed by a group of wireless mobile nodes that cooperate by performing routing functions to provide end to end communication without any fixed network infrastructure. These nodes coordinate with each other by forwarding packets so that far away nodes can communicate on the network.Manets find their applications in many areas like battlefield and rescue operations, mobile conferencing, home based networking, virtual classrooms etc.Mobile ad hoc networks are easily created as some nodes come nearby and communicate in their radio range. But these networks are more vulnerable to different types of attacks than wired networks due to distributed processing and lack of infrastructure, changing network topology and cooperative algorithms. Many research efforts have been made to secure ad hoc networks and this have been analyzed that prevention methods are not sufficient and there is a need for detection and response mechanisms. For this many Intrusion detection systems have been proposed.

2. INTRUSION DETECTION SYSTEM

The intrusion detection system analyzes the system and network activities and uses the patterns of well known attacks and normal profile to detect potential attacks. Intrusion detection systems can be run on each mobile node to check local traffic and detect local intrusions. These nodes can communicate local intrusion information to each other as and when needed. This technique of local intrusion detection is easy to implement but malicious node can make fake measurements and communicate with others.

Other technique is to run intrusion detection system for self and neighbor nodes to check for malicious neighbor. The global intrusion detection system can be deployed for clusters of mobile nodes where head node is responsible for global intrusion detection for its cluster. In clusters a head node is employed which keep record of member nodes as well as communicates with other clusters for cooperate detection and response. In this paper intrusion detection for clusters of mobile nodes is proposed which will reduce the overhead of head node involved in detecting intrusions.

3. TYPES OF ATTACKS IN MANET

Types of attacks produced by the malicious nodes are of Rushing attack, Black hole attack, Neighbor attack, Jellyfish attack and Denial of service (DoS).

Black hole attack is the type of attack where the attacker first needs to invade into the multicast forwarding group and then drops some or all data packets it receives instead of forwarding them to the next node on the routing path.

Rushing attack is that, when source nodes flood the network with route discovery packets in order to find routes to the destinations, each intermediate node processes only the first non duplicate packet and discards any duplicate packets that arrive at a later time. A rushing attacker exploits this duplicate suppression mechanism by quickly forwarding route discovery packets in order to gain access to the forwarding group.

Jellyfish attack is that the attacker first needs to intrude into the forwarding group. It then delays data packets unnecessarily for some amount of time before forwarding them. This results in significantly high end-to-end delay and thus degrades the performance of real-time applications.

Neighbor attack is that, upon receiving a packet, an intermediate node records its ID in the packet before forwarding the packet to the next node. An attacker, however, simply forwards the packet without recording its ID in the packet to make two nodes that are not within the communication range of each other believe that they are neighbors.

Selfishness attack is that the node is not serving as a relay to other nodes.

Sleep Deprivation attack is that the node is forced to exhaust its battery power.

Denial-of-Service attack is that the node is prevented from receiving and sending data packets to its destinations.

3. RELATED WORK

Mobile Ad hoc Network security is addressed by various researches and has been a major research area. Intrusion detection in Ad hoc networks by using modular approach is proposed by Zhang et al. [8]. In this proposed solution every node is responsible to detect the intrusion independently. The nodes can collaborate in scenarios where an individual node can not conclude about the intrusive behavior. In this architecture each node runs various modules including local, global detection engine and response. A complex multilayer integration approach is used to analyze the intrusion which results in storing lot of information on each node thus making it storage and processing intensive.

Using mobile agents (MA) in intrusion detection is a new dimension in Ad hoc Network Security research. Li et al.[9] proposed a coordinated approach of intrusion detection in ad-hoc networks using MA technology. The Manager, assistant and response mobile agents are used for detection and notification of intrusion within a network. The proposed architecture floods the network with intrusion information thus resulting in processing and storage overhead on each individual node.

Yi-an et al. [10] proposed a cooperative intrusion detection system for MANETS. The run-time resource constraint problem was addressed using a cluster-based intrusion detection scheme. The cluster formation and cluster head selection for cooperative intrusion detection is done through clique computation and cluster head computation protocols. The requirement of having bi-directional links for clique computation protocol causes an overhead in terms of number of elections and number of HELLO messages exchanged to maintain connectivity.

Apart from the secure architectures various clustering algorithms have been proposed for Mobile Ad hoc Networks for efficient routing, as their dynamic nature makes routing a difficult task.

4. PROPOSED WORK

A generalized clustering algorithm has been proposed that can run on top of any routing protocol and can monitor the intrusions constantly irrespective of the routes. The proposed simplified clustering scheme has been used to detect intrusions, resulting in high detection rates and low processing and memory overhead irrespective of the routes, connections, traffic types and mobility of nodes in the network. And implementation of the system is done in OS-LINUX using NS-2 (NETWORK SIMULATOR-2) TOOL. The proposed works involves

- Cluster formation
- Intrusion Detection Architecture

5. CONCLUSION

Mobile ad hoc networking (MANET) has become an exciting and important technology in recent years, because of the rapid proliferation of wireless devices. Mobile ad hoc networks is highly vulnerable to attacks due to the open medium, dynamically changing network topology, cooperative algorithms, lack of centralized monitoring and management point. Hence a need arises for a wall of defense, an Intrusion Detection System. This Intrusion Detection System is used to detect Intrusion, identify the malicious nodes and isolate them from the rest of the network. The presence of a detection system will discourage malicious nodes from attempting intrusion in future. So the low-overhead clustering algorithm is proposed for the benefit of detecting intrusion rather than efficient routing and the performance metrics of the system are analyzed based on the particular types of attacks.

In future the target is to make this algorithm more effective and less time consuming. Also memory and processing overhead should be minimum. Cluster formation and division of head and member nodes responsibilities should be instantaneous. It is also a major research task to make the IDS so powerful to detect any new type of attack.

6. REFERENCES

[1] Kashan Samad, Ejaz Ahmed, Waqar Mehmood: MultiLayer Cluster-based Intrusion Detection Architecture for Mobile Ad Hoc Networks using Mobile Agents , Hi Optical Networks and Enabling Technology (HONET), Islamabad, Pakistan, Dec 28-31, 2004.

[2] A. Patwardhan, J. Parker, M. Iorga, A. Joshi, T. Karygiannis and Y. Yesha "Threshold-based intrusion detection in ad hoc networks and secure AODV," Ad Hoc Networks, Vol. 6, Issue No. 4, pp. 578-599. June 2008.

[3] Yi-an Huang, Wenke Lee, "A Cooperative Intrusion Detection System for Ad Hoc Networks", inProceedings of the 1st ACM workshop on Security of ad hoc and sensor networks (SASN), Fairfax, Virginia,October 31, 2003.

[4] Yu Liuy, Yang Liy, Hong Many, "MAC Layer Anomaly Detection in Ad Hoc Networks", 6th IEEE Information Assurance Workshop, USA, 15-17 June 2005.

[5] Kashan Samad, Ejaz Ahmed, Waqar Mahmood, "Simplified Clustering Scheme for Intrusion Detection in Mobile Ad Hoc Networks", 13th International Conference on Software, Telecommunications and Computer Networks (SoftCOM), Split, Croatia, September 15-17, 2005.

[6] S.Bansal, M.Baker, "Observation based cooperation enforcement in ad hoc networks," Research Report cs. NI/0307012, StanfordUniversity.

[7] Ningrinla Marchang, Raja Datta, "Collaborative techniques for intrusion detection in mobile ad-hoc networks," Ad Hoc Networks, Vol. 6, Issue No. 4, pp. 508-523. June 2008.

[8] Yongguang Zhang, Wenke Lee, "Intrusion Detection in Wireless Ad-Hoc Networks" , Proceedings of the Sixth Annual International Conference on Mobile Computing and Networking, MobiCom 2000, Boston, Massachusetts, Aug 6 11, 2000, pp 275-283.

[9] Chunsheng Li, Qingfeng Song, Chengqi Zhang: "MA-IDS Architecture for Distributed Intrusion Detection using Mobile Agents", Proceedings of the 2nd International Conference on Information Technology for Application (ICITA), 2004.

[10] Yi-an Huang, Wenke Lee, "A Cooperative Intrusion Detection System for AdHoc Networks", in Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks (SASN), Fairfax, Virginia, October 31, 2003.

[11] Mingliang Jiang, Jinyang Li, Y.C. Tay: “Cluster Based Routing Protocol (CBRP)”, Internet Draft, Jul, 1999.

[12] Yunjung Yi, Mario Gerla, Taek-Jin Kwon: Efficient Flooding in Ad-Hoc Networks using On Demand (passive) Cluster Formation , Proceedings of Mobihoc, Jun 2003.