Journal of Computer Applications ISSN: 0974 – 1925,
Volume-5, Issue EICA2012-4, February 10, 2012

An Efficient Leader Election Mechanism For Intrusion Detection in MANET

Shanmuga vadivu G
PG Student,
Department of CSE,
Paavai Engineering College ,
E-mail: vadivucs89@gmail.com

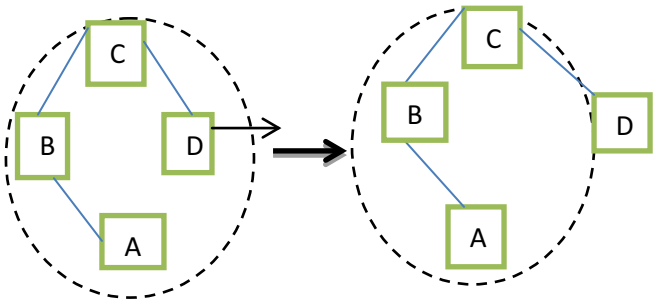
Umamaheswari A
Asst. Professor,
Department of CSE,
Paavai Engineering College,
E-mail: umamaheswarime2004@gmail.com

Abstract— The mobile ad hoc network (MANET) is highly vulnerable to security attacks compared to wired network and infrastructure based wireless network due to the dynamic changing and decentralized network topology. MANET has no clear line of defense, so, it is accessible to both legitimate network users and malicious attackers. In the presence of malicious nodes, one of the main challenges in MANET is to design the robust security solution that can protect MANET from various attacks. In this paper the cluster head is elected based on the clique and cluster head computation method to monitor the entire process in the cluster. The networks are particularly vulnerable to Distributed Denial of Service (DDoS) attacks launched through compromised nodes or intruders. The Hierarchical State Routing (HSR) protocol employs clustering at different levels with efficient membership management at every level of clustering. The use of clustering enhances resource allocation and reduces the size of the routing table.

Keywords : *Leader election, DDoS attacks, intrusion detection system, MANET security*.

I. INTRODUCTION

With the advances of wireless communication technology, low-cost and powerful wireless transceivers are widely used in mobile applications. Mobile networks have attracted significant interests in recent years because of their improved flexibility and reduced costs. A mobile ad hoc network (MANET) is a group of wireless nodes without the aid of any existing network infrastructure or centralized administration. Nodes within the same radio range communicate directly via wireless links, while those in different radio ranges use intermediate nodes for communication. The mobile ad hoc network have many salient characteristics such as dynamic topology, bandwidth constrained, variable link capacity, limited energy, limited physical security. Due to these features mobile ad hoc networks are particularly vulnerable to various types of attacks. Various intrusion detection methods are developed for detecting the intrusion in the wired networks. Due to the mobility of nodes, the intrusion detection methods of wired network cannot be used for MANETS. In figure 1 nodes A, B, C and D constitute an ad hoc network. The circle represents the radio range of node A. The network initially has the topology in (a), when node D moves out of the radio range of A, the network topology changes to the one in (b).



(a) (b)

Figure 1: Topology Change in Ad Hoc Networks

The nodes in the network are logically divided into clusters with a single cluster head for each cluster. Cluster heads of each cluster have more functionality than other nodes in the network. The cluster head is entrusted with responsibilities such as slot/frequency/code allocation, call admission control, scheduling of packet transmission, exchange of routing information and handling route breaks. The typical application scenarios [3] include the rescue missions, the law enforcement operations, the medical service, the cooperating industrial robots, the traffic management, and the educational operations in campus.

1. Attacks in MANET

In MANET security is done in five layers, such as Application layer, Transport layer, Network layer, Link layer, and Physical layer. This layers having various attack are Wormhole, Blackhole, Information disclosure, Routing attacks, etc. Other attacks also available in MANET that cannot strictly be associated with any specific layer in the protocol stack. Other attacks are Denial of Service (DoS) and Impersonation. In this paper the DDoS attack are prevented by the selected cluster leaders in the cluster.

Distributed DoS(DDoS) attack: A distributed denial-of-service (DDoS) [8] attack is more severe form of the DoS attack in which a multitude of compromised systems attack a single target, thereby causing denial of service for users of the targeted system. The flood of incoming messages to the target system essentially forces it to shut down, thereby denying service to the system to legitimate users.

II. ROUTING PROTOCOLS IN MANET

Routing protocols can be divided into **proactive, reactive** and **hybrid protocols**, depending on the routing topology [3] .In this paper HSR protocol is used for communication between the end nodes.

Hierarchical State Routing Protocol

The hierarchical state routing (HSR) protocol is a distributed multi-level hierarchical routing protocol that employs clustering at different levels with efficient membership management at every level of clustering [4]. The use of clustering enhances resource allocation and management. For example, the allocation of different frequencies or spreading codes to different clusters can improve the overall spectrum reuse. HSR operates by classifying different levels of cluster. Clustering algorithm is used for electing leaders at every level.

The first level of physical clustering is done among the nodes that are reachable in a single wireless hop. The next higher level of physical clustering is done among the nodes that are elected as leaders of each of these first-level clusters. It reduces the routing table size by making use of hierarchy information.

III. INTRUSION DETECTION SYSTEM (IDS)

Intrusion is defined as "any set of actions that attempt to compromise the integrity, confidentiality, or availability of a resource". The intrusion prevention techniques alone such as authentication and encryption, which are usually a first line of defense, are not sufficient. Intrusion detection can be used as a second wall of defense to protect the network from such problems [7]. If the intrusion is detected, a response can be initiated to prevent or minimize damage to the system.
Based on the detection techniques, IDS are classified into three types [8]:

1. **Misuse detection systems:** The system keeps patterns (or signatures) of known attacks and uses them to compare with the captured data. Any matched pattern is treated as an intrusion. Like a virus detection system, it cannot detect new kinds of attacks.
2. **Anomaly detection systems:** The normal profiles (or normal behaviors) of users are kept in the system. The system compares the captured data with these profiles, and then treats any activity that deviates from the baseline as a possible intrusion by informing system administrators or initializing a proper response.
3. **Specification-based detection:** The system defines a set of constraints that describe the correct operation of a program or protocol. Then, it monitors the execution of the program with respect to the defined constraints.

Dynamic Hierarchical Intrusion Detection

The nodes move arbitrarily across the network, a static hierarchy is not suitable for such dynamic network topology. The dynamic intrusion detection hierarchy is potentially scalable to large networks by using clustering method. However, it can be structured in more than two levels as shown in Figure 2. Nodes labeled \1" are the first level cluster leaders while nodes labeled \2" are the second level cluster leader and so on. Members of the first level of the cluster are called leaf nodes [10]. Every node has the responsibilities of monitoring, logging, analyzing, responding to intrusions detected if there is enough evidence, and alerting or reporting to cluster leader. Cluster leader in addition, must also perform:

1. **Data fusion/integration and data reduction:** Cluster leader aggregate and correlate reports from members of the cluster and data of their own. Data reduction may be involved to avoid conflicting data, bogus data and overlapping reports.
2. **Intrusion detection computations:** Since different attacks require different sets of detected data, data on a single node might not be able to detect the attack, e.g., DDoS attack, and thus cluster leader also analyze the consolidated data before passing to upper levels.
3. **Security Management:** The uppermost levels of the hierarchy have the authority and responsibility for managing the detection and response capabilities of the clusters and cluster leader below them. They may send the signatures update, or directives and policies to alter the configurations for intrusion detection and response. These update and directives will flow from the top of the hierarchy to the bottom.

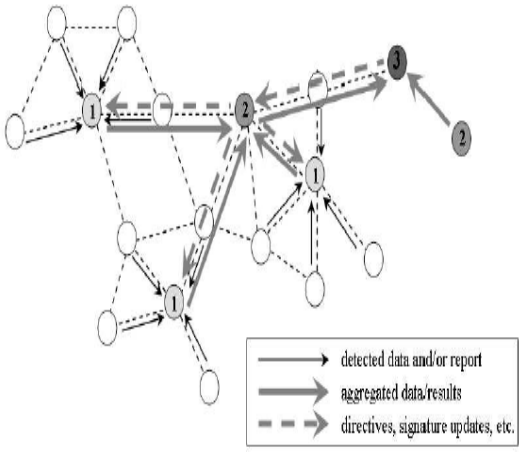


Figure 2: Dynamic Intrusion Detection Hierarchy

To form the hierarchical structure, every node uses clustering, which is typically used in MANETs to construct routes, to self-organize into local neighborhoods (first level clusters) and then select neighborhood representatives (cluster leader). These representatives then use clustering to organize themselves into the second level and select the representatives. This process continues until all nodes in the network are part of the hierarchy. Some of the criteria for selecting cluster leaders are:

1. **Connectivity:** the number of nodes within one hop.
2. **Proximity:** members should be within one hop of its cluster leader.
3. **Resistance to compromise (hardening):** the probability that the node will not be compromised. This is very important for the upper level cluster leaders.
4. Processing power, storage capacity, energy remaining, and bandwidth capabilities.

IV. CLUSTER BASED INTRUSION DETECTION

A MANET can be organized into a number of clusters in such a way that every node is a member of at least one cluster, and there will be only one node per cluster that will take care of the monitoring issue in a certain period of time, which is generally called cluster leader [2]. The cluster formation protocol is shown in Figure 3.

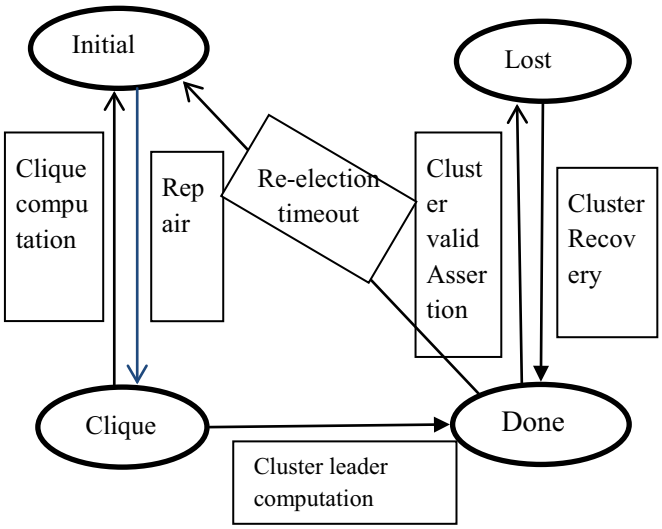


Figure 3: Cluster Formation Protocol

Basically there are four states in the cluster formation protocol: initial, clique, done and lost. All the nodes in the network will be in the initial state at first, which means that they will monitor their own traffic and detect intrusion behaviors independently.

There are two steps to get the cluster leader of the network: clique computation and cluster leader computation. A clique is defined as a group of nodes where every pair of members can communicate via a direct wireless link [3]. The cluster formation algorithm is used to compute cliques, the members of which are named citizens here in the paper. Once the protocol is finished, every node is aware of its fellow clique members. Then a node will be randomly selected from the clique to act as the cluster leader. There are two other protocols that assist the cluster doing some validation and recovery issues, which are respectively called Cluster Valid Assertion Protocol and Cluster Recovery Protocol.

The Cluster Recovery Protocol is mainly used in the case that a citizen loses its connection with previous cluster leader or a cluster leader loses all its citizens, when it enters LOST state and initiates Cluster Recovery Protocol to re-discover a new cluster leader.

V. CONCLUSION

This paper analyzed an ad hoc network faces security threats and presented the security objectives that need to be achieved. By making use of the hierarchy information, routing table size also reduced. Ad hoc networking is still a raw area of research as can be seen with the problems that exist in these networks and the emerging solutions.

REFERENCES

1. S. Basagni, "Distributed and Mobility-Adaptive Clustering for Multimedia Support in Multi-Hop Wireless Networks," Proc. IEEE Int'l Vehicular Technology Conf. (VTC), 1999.
2. S. Basagni, "Distributed Clustering for Ad Hoc Networks," Proc. IEEE Int'l Symp. Parallel Architectures, Algorithms, and Networks (ISPAN), 1999.
3. M. Bechler, H. Hof, D. Kraft, F. Pahlke, and L. Wolf, "A Cluster-Based Security Architecture for Ad Hoc Networks," Proc. IEEE INFOCOM, 2004.
4. S. Vasudevan, J. Kurose, and D. Towsley, "Design and Analysis of a Leader Election Algorithm for Mobile Ad Hoc Networks," Proc. IEEE Int'l Conf. Network Protocols (ICNP), 2004.
5. P. Brutch and C. Ko, "Challenges in Intrusion Detection for Wireless Ad-Hoc Networks," Proc. IEEE Symp. Applications and the Internet (SAINT) Workshop, 2003.
6. S. Gwalani, K. Srinivasan, G. Vigna, E.M. Beding-Royer, and R. Kemmerer, "An Intrusion Detection Tool for AODV-Based Ad Hoc Wireless Networks," Proc. IEEE Computer Security Applications Conf. (CSAC), 2004.
7. K. Chen and K. Nahrstedt, "iPass: An Incentive Compatible Auction Scheme to Enable Packet Forwarding Service in MANET," Proc. Int'l Conf. Distributed Computing Systems, 2004.
8. Y. Huang and W. Lee, "A Cooperative Intrusion Detection System for Ad Hoc Networks," Proc. ACM Workshop Security of Ad Hoc and Sensor Networks, 2003.
9. Y. Zhang and W. Lee, "Intrusion Detection in Wireless Ad-Hoc Networks," Proc. ACM MobiCom, 2000.
10. T. Anantvalee and J. Wu, "A Survey on Intrusion Detection in Mobile Ad Hoc Networks," Wireless/Mobile Network Security, Springer, 2006.