Intrusion Detection in Mobile Ad hoc Network

Pooja Chhabra
Lecturer,Department of Computer Science
Guru Nanak Khalsa College,Karnal , Haryana,india

Abstract- In recent years, many wireless devices are available and tend to make life more convenient. e.g., mobile laptop computers, PDAs, and wireless phones. A mobile ad-hoc network (MANET) is composed by a group of mobile wireless nodes without a fixed network infrastructure. This paper presents Architectures for Intrusion Detection in a Mobile Ad hoc Network which includes an overview of its structure and operation.

Keywords –Cluster head, Intrusion detection system

I. INTRODUCTION

Mobile ad hoc networks are IP networks made up of a collection of wireless and mobile nodes communicating via radio links. They do not depend on any predefined infrastructure or centralized administration to operate [2] and could, for example, find applications in the case of networks created for the needs of participants to a conference or meeting [3], students and teachers in a classroom, rescuers in a search and rescue operation, soldiers on a battlefield.

Due to the lack of an underlying infrastructure, basic functionalities, such as routing, configuration of the hosts or security management cannot rely on predefined or centralized entities to operate, and must be carried out in a distributed manner. For instance, in the case of security, the nodes cannot rely on network architecture based defense techniques such as centralized firewalls. Each node thus becomes a point of vulnerability and must assume, by itself, it's own security.

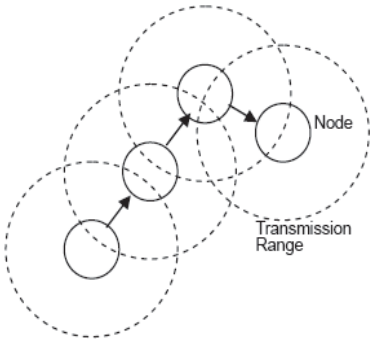

Figure.1. Mobile ad hoc network

The rest of the paper is organized as follows. Methods of IDS are explained in section II. IDS architecture for cluster based MANET is presented in section III. Concluding remarks are given in section IV.

II. METHODS OF IDS IN MANET

A. Method 1(M1)-

Method 1 is efficient and bandwidth-conscious. It targets intrusion at multiple levels and fits the distributed nature of IDS for MANET. The method has clusters and the IDS on cluster head employs independent detection decision-making after gathering information from other nodes. It utilizes mobile agent for the communications among nodes.

B. Method 2(M2)-

Method 2 implements local and collaborative decision making in anomaly detection. In this approach, individual IDS agent works by itself and collaborate in decision making. Each IDS agent runs on a node and monitors local activities. If a node detects locally intrusion with strong evidence, then the node can conclude intrusion happens and then initiate an alarm response. However, if the evidence is not strong enough but needs investigation in a wider area in the network, then the IDS agent can start a collaborate procedure which is a distributed consensus algorithm.

C. Method 3(M3)-

In Method 3,a cluster-based scheme is used in which a cluster head is elected by a group of nodes in a neighborhood (citizen nodes) and the head node monitor the citizen nodes. Once the cluster head is elected, then other nodes need to transmit the features it obtains locally to the cluster head. This IDS uses anomaly detection implemented with data mining as its detection technique.

D. Method 4((M4)-

In Method 4 each node runs a local IDS. Each node detects intrusion locally and uses the external data to confirm the detection. The nodes use mobile agents to communicate and collaborate.

E. Method 5(M5)-

Method 5 implements an IDS which use collaboration mechanism in anomaly detection. In this model, a network is divided into logical zones. Each zone has a gateway node and individual nodes. Individual nodes has IDS agent working and detect intrusion activities individually. Once an individual node detects intrusion, it generates an alert message. Gateway node aggregate and correlate the alerts generated by the nodes in its zone. An algorithm is used in aggregate the alerts based on the similarities in the attributes of the alert. Only gateway nodes can utilize alert to init alarm.

F. Method 6(M6)-

Method 6 also utilize cluster and cluster head employs the independent decision making. It also utilizes the mobile agent for communications among nodes. The intrusion detection engine is a case-based agent designed with the principle of artificial intelligence.

G. Method 7(M7)-

Method 7 mainly introduces a detection algorithm which uses the statistics of packets, namely the relations between different features, such as the correlation between the number of packet dropped and the percentage of change in routing table. This algorithm can be used as an intrusion detection engine in other IDS architecture.

H. Method 8(M8)-

In method 8, the normal behavior of critical objects in the Network is constructed into normal specification first. Then the actual behavior is compared to the normal specification. It uses distributed network monitor to trace the request-reply flow in the routing protocol. The network monitor runs a specification based detection algorithm to make decisions.

I. Method 9(M9)-

In method 9, the two neighbouring nodes of one node are used to ensure that the packets are not modified when traveling in the network. This is done by comparing the information in each packet at each hop. It has two modes: passive mode-to protect a single host and active mode-to collaboratively protect the nodes in a cluster. In active mode, a cluster head starts a voting algorithm to determine whether intrusion really happens.

J. Method 10(M10)-

In method 10, information in the management information base (MIB) is used as input data. It also uses mobile agent and a collaborative decision making mechanism.

Comparison

Table 1.comparison of different methods

S.NO.	CHARACTERISTICS	M1	M2	M3	M4	M5	M6	M7	M8	M9	M10
1.	**INPUTS**										
(a)	Packet related information						√			√	
(b)	Network related information								√		
(c)	Statistical data							√			
(d)	Different types of audit data	√	√	√							
2.	**OUTPUTS**										
(a)	Intrusion happen	√	√	√	√	√	√	√	√	√	√
(b)	Type of attack		√			√			√		
(c)	Location of intruder		√			√					
3.(a)	Cluster-head nodes	√		√			√			√	
(b)	Gateway nodes					√					
4.(a)	Anomaly detection		√			√					
(b)	Misuse detection						√				
5.	**COMMUNICATION MECHANISM**										
(a)	Mobile agent	√			√		√				√
(b)	Network protocol		√	√		√		√	√	√	
6.	**ARCHITECTURE**										
(a)	Distributed		√		√	√		√	√		√
(b)	Hierarchical	√		√			√			√	
7.	**DETECTION DECISION MAKING MODEL**										
(a)	Collaborative		√		√					√	√
(b)	Independent	√		√			√				
8.	**SECURITY**										

(a)	Low										√
(b)	Medium	√		√	√		√				
(c)	High		√			√		√	√	√	
9.	**EFFICIENCY**										
(a)	Low								√		
(b)	Medium		√			√		√		√	
(c)	High	√		√	√		√				√

Drawback of Current IDS and Requirement Of New IDS

Intrusion detection in MANETs, however, is challenging for a number of reasons [9-11]. These networks change their topologies dynamically due to node mobility; lack of concentration points where traffic can be analyzed for intrusions; utilize self configuring multi-party infrastructure protocols that are susceptible to malicious manipulation; and rely on wireless communication channels that provide limited bandwidth and are subject to noise and intermittent connectivity. To overcome these constraints, a number of decentralized intrusion detection approaches tailored specifically for MANETs have been proposed. These approaches, however, have focused almost exclusively on detecting malicious behavior with respect to MANET routing protocols and have provided little evidence that they are applicable to a broader range of threats, including attacks on conventional protocols, which also pose new problems in MANETs. This paper describes a generalized, cooperative intrusion detection architecture proposed as the foundation for all intrusion detection and supporting activities in mobile ad hoc wireless networks.

As a backdrop for discussion below, I list the general requirements that should be met and services that should be provided by an ideal intrusion detection architecture for this domain. Some are not explicitly addressed.

The architecture should:

• *Address the broad spectrum of attacks* that may target the MANET, including both MANET-specific and conventional attacks, especially those having distributed sources or distributed targets;

• *Provide intrusion detection coverage for all traffic, all of the time,* regardless of changes in topology and routing that occur because of node mobility and other dynamic environmental factors.

• *Support layered defense* by imposing independent, overlapping intrusion detection mechanisms across potential attack paths.

• *Support a broad spectrum of detection techniques*, including signature-based, statistical anomaly, specification-based detection techniques, techniques that utilize promiscuous eavesdropping of wireless transmissions, and cooperative detection techniques involving exchange of data among detectors.

• *Provide access to intrusion detection data* from multiple protocol layers, operating system logs, and application logs, since some attacks and attack patterns may be detectable only via multi-source sensing.

• *Minimize consumption of bandwidth by communications among intrusion detection components,* e.g., avoid unnecessary flooding.

• *Adapt its behavior* in the event of failure or compromise of nodes and communications links, to *degrade gracefully.*

• *Provide autonomy of intrusion detection* capabilities when the MANET is partitioned or disconnected from the reach-back network or other fixed infrastructure.

Required Services-

The architecture should provide efficient services for transferring data from widely distributed sources so that data can be collected, interpreted, and correlated locally, regionally, and "globally", as appropriate, and exchanged among pairs or groups of peer nodes for correlation or trace back. It should provide services for querying data sources for additional related data as needed. It should provide services to support data fusion/integration and data reduction including support for correlating distributed events to a single attack, reconciling conflicting data and compensating for possibly bogus data, and avoiding or compensating for overlapping reports. The architecture should provide services for relaying intrusion detection management and intrusion response directives. It should provide a tailored interface to key-sharing services provided by underlying cryptographic components to enable designated nodes to decrypt and inspect packet headers and payloads.

These services should be integrated with policy and configuration mechanisms that dynamically assign and reassign intrusion detection, correlation, response, and security management responsibilities to nodes based on their topological placement, capabilities, trustworthiness, and other factors, including desired tradeoffs among detection coverage and accuracy, bandwidth utilization, session key exposure, redundancy, survivability, and other factors.

III. IDS ARCHITECTURE FOR CLUSTER BASED MANET

Each node implements a trained , pre-installed IDS (Anomaly & Signature) in a passive state. It will be activated only if the particular node is elected as either cluster-head or backup. The elected cluster head will perform signature detection on all the member nodes along with running anomaly detection only on the backup node. Similarly the backup will be running anomaly detection on all nodes along with signature detection only on the master.

A. *Signature Detection by Cluster Head-*

Signature detection requires maintenance of an extensive database of attack signatures, which in the case of ad hoc network would have to be replicated among all the hosts. Every packet in a signature based approach needs to be compared with the attack signature database. This operation requires O (n) time where n is the number of signatures in the database. The signature database would generally have hundreds of attack patterns. Anomaly detection, on the other hand has fewer comparisons, typically less than twenty parameters are used. Thus it can be concluded that signature detection requires greater computational power as compared to anomaly detection. This election algorithm favors a node that has a better computational power and a better battery power as compared to other nodes in the cluster. So it is decided to run signature detection on the cluster head. For a pre-decided window of time, the cluster head will monitor each node for potential attack signatures. This is done in a round robin manner for all nodes in the cluster. The database of signatures does not need frequent updates. An update is needed only when a new attack has been discovered and its signature needs to be added to the database. The probability of update during a particular ad-hoc session is very rare.

B. *Anomaly Detection by Cluster Backup-:*

Anomaly detection model is built on a long-term monitoring and classifying of what is a normal or abnormal system behavior. Ad hoc wireless networks are very dynamic in structure, giving rise to apparently random communication patterns, thus making it challenging to build a reliable behavioral model and it is possible that the anomaly detection model will give a lot of false positives. Thus in such a highly dynamic environment, the simplest and the most reliable technique of anomaly detection is threshold based detection. Initial thresholds are set on the preinstalled IDS for local and network parameters which are to be monitored. The required network audit data can be obtained through SNMP (Simple network management protocol) and local data can be obtained using the operating system kernel logs. The thresholds can be modified in joint consensus with all the member nodes of the cluster. A malicious node may go unnoticed if it drops a few packets intermittently. However, if the threshold has been set

appropriately, the potential damage caused by such intermittent packet drops will be acceptable and will not significantly affect the MANET. If a node exceeds a small threshold of such allowed "misbehavior" it will be detected and classified as intrusive.

C. *Detection between Cluster Head (CH) and Cluster Backup (CB)-*

Cluster head performs signature detection on all nodes including itself. Similarly cluster backup performs anomaly detection on all nodes including itself. But a compromised cluster head or cluster backup might have its own IDS disabled. So a second degree of reliability and fault tolerance is added to this system by allowing the cluster backup to perform signature detection on cluster head and cluster head to perform anomaly detection on cluster backup. The backup can perform signature detection for a pre-defined window of time but at a higher frequency than the detection performed by master on the member nodes. The master in turn can monitor the parameters of backup on a random basis for detecting anomalies.

D. *Intrusion response-*

The ideal intrusion response for a wireless ad-hoc network is to isolate compromised node from the rest of the network [4]. Fixed networks implement this using the "electronic quarantine" method by updating the firewalls to block the entry of particular compromised node into the network. In a dynamically changing wireless ad-hoc topology, the centralized solution proposed by the electronic quarantine would not be effective, since the implementation of firewalls may not be feasible. In a cooperative IDS architecture for MANETs, one approach suggests "secret isolation" where all other nodes are informed about the malicious node through their 1 hop neighbors, who then delete all the paths to the malicious node from their routing tables, thus secretly isolating the malicious node. It has been proposed to use dirty / counter certificate method, in which the cluster head / backup can isolate a suspected node from the rest of the network by broadcasting a counter certificate for that node.

E. *Sharing of data-*

To have a synchronized database of rules (Signature) and parameters (Anomaly) it is proposed to broadcast table updates at the end of election period by master and backup to all member nodes. This is under the assumption that an update to the signature database is needed only when a new attack has been discovered, and the probability of such an update during a particular ad hoc session is very rare. Similarly for an anomaly database the update might be just a revision of threshold for a particular parameter which may also be not that often considering that we are using trained pre-installed IDS for each node and even if it happens, it will not be energy consuming.

IV.CONCLUSION

Intrusion detection in MANETs is challenging because these networks change their topologies dynamically due to node mobility; lack of concentration points where traffic can be analyzed for intrusions; utilize self-configuring multi-party infrastructure protocols that are susceptible to malicious manipulation; and rely on wireless communications channels that provide limited bandwidth and are subject to noise and intermittent connectivity. I have proposed an Architecture for Intrusion Detection in Mobile Ad hoc Network for MANETs that is intended to address these challenges.

The architecture is organized as a dynamic hierarchy in which data acquisition occurs at the leaves, with intrusion detection data being incrementally aggregated, reduced, analyzed, and correlated as it flows upward toward the root. A key principle is that detection and correlation should occur at the lowest level in the hierarchy at which the

aggregated data is sufficient to enable an accurate detection or correlation decision; this strategy can reduce detection latency and bandwidth consumption.

REFERENCES

[1] Gartner Group, 2000**.** "Gartner unveils the shape of the wireless economy", Gartner Press Release, September 11 2000 Gillick, Kevin and Randy Vanderhoof, 2000**,** "Mobile e-Commerce: market place enablers and inhibitors." Smartcard Forum Annual Meeting

[2] Mishra, Amitabh and Ketan Nadkarni, 2004, "Intrusion Detection in wireless Ad Hoc Networks." IEEE Wireless Communications, February 2004, pp. 48-60

[3] Wei, J., L. Liu, and K. Koong, 2003, "A Framework for Delivering Mobile Commerce Security System." Proceedings of International Conference for Pacific RIM Management: ACME Transaction

[4] Zhang, Yongguan and Wenke Lee, 2000, "Intrusion detection in wireless ad-hoc networks." Proceedings of the 6th annual international conference on Mobile computing and networking , pp.275**–**283.

[5] H Yang, H Y. Luo, F Ye, S W. Lu, and L Zhang, Security in mobile ad hoc networks: Challenges and solutions, IEEE Wireless Communications. 11 (1), pp. 38-47**.** 2004**.**

[6] R. Rao and G. Kesidis, "Detection of malicious packet dropping using statistically regular traffic patterns in multihop wireless networks that are not bandwidth limited," Brazilian Journal of Telecommunications,2003**.**

[7] Benoit Garbinato and Philippe Rupp, "From Ad Hoc Networks to Ad Hoc Applications", 7th International Conference on Telecommunications (ConTel), Zagreb, Croatia, June 2003.

[8] Yian Huang, Wenke Le "A Cooperative Intrusion Detection System for Ad Hoc Networks " Georgia Institute of Technology

[9] Yian Huang and Wenke Lee, "A Cooperative Intrusion Detection System for Ad Hoc Networks" , In Proceedings of the ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN '03), Fairfax VA, October 2003.

[10] Yi-an Huang and Wenke Lee. "A Cooperative Intrusion Detection System for Ad Hoc Networks." Proceedings of the ACM Workshop on Security in Ad Hoc and Sensor Networks (SASN'03), October 2003.

[11] R. Rao and G. Kesidis, "Detection of malicious packet dropping using statistically regular traffic patterns in multihop wireless networks that are not bandwidth limited," Brazilian Journal of Telecommunications, 2003.