ISSN: 2277-3754
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 1, Issue 4, April 2012

INTRUSION-TOLERANT ARCHITECTURE FOR MOBILE ADHOC NETWORKS

G.M.Padmaja, Ch.Rajya Lakshmi

Abstract -- Now a Days, the use of mobile ad hoc networks (MANETs) has become very important communication medium through which several users communicate, large amount of information exchange including some mission critical applications, and as such security has become one of the major concerns in MANETs. Due to some unique characteristics of MANETs, prevention methods have been insufficient to make them secure; therefore, in our architecture intrusion detection and tolerant mechanism is added .Ingeneral, the intrusion detection techniques for traditional wireless networks are not well suited for MANETs. This Architecture mainly depends on dependability and diversification principle in order to maintain system consistency, and it is constructed for static as well as fully dynamic systems.

Index Terms: **Dependability, Diversification, Intrusion Detection, Tolerance, Security.**

I. INTRODUCTION

A mobile ad hoc network (MANET) is a self-configuring network that is formed automatically by a collection of mobile nodes without the help of a fixed infrastructure or centralized management. Each node is equipped with a wireless transmitter and receiver, which allows it to communicate with other nodes in its radio communication range. In order for a node to forward a packet to a node that is out of its radio range, the cooperation of other nodes in the network is needed; this is known as multi-hop communication. Therefore, each node must act as both a host and a router at the same time. The network topology frequently changes due to the mobility of mobile nodes as they move within, move into, or move out of the network.

In recent years, MANETs have been developing rapidly and are increasingly being used in many applications, ranging from military to civilian and commercial uses, since setting up such network scan be done without the help of any infrastructure or interaction with a human. Some examples are: search-and-rescue missions, data collection, and virtual classrooms and conferences where laptops, PDA or other mobile devices share wireless medium and communicate to each other. As MANETs become widely used, the security issue has become one of the primary concerns. For example, most of the routing protocols proposed for MANETs assume that every node in the network is cooperative and not malicious. Therefore, only one compromised node can cause the failure of the entire network. For passive attacks, packets containing secret information might be eavesdropped, which violates confidentiality. Active attacks, including injecting packets to invalid destinations into the network, deleting packets, modifying the contents of packets, and impersonating other nodes violate availability, integrity, authentication, and non-repudiation. Proactive approaches such as cryptography and authentication were first brought into consideration, and many techniques have been proposed and implemented. However, these applications are not sufficient. If we have the ability to detect the attack once it comes into the network, we can stop it from doing any damage to the system or any data. Here is where the intrusion detection system comes in.

II.PRINCIPLE OF INTRUSION DETECTION

Intrusion detection can be defined as a process of monitoring activities in a system, which can be a computer or network system. The mechanism by which this is achieved is called an intrusion detection system (IDS). An IDS collects activity information and then analyzes it to determine whether there are any activities that violate the security rules. Once an IDS determines that an unusual activity or an activity that is known to be an attack occurs, it then generates an alarm to alert the security administrator. In addition, IDS can also initiate a proper response to the malicious activity. Although there are several intrusion detection techniques developed for wired networks today, they are not suitable for wireless networks due to the differences in their characteristics. Therefore those techniques must be modified or new techniques must be developed to make intrusion detection work effectively in MANETs. IDS monitor but are otherwise ordinary platforms running diverse COTS software. Attacks, vulnerabilities, and intrusions are defined as three types of interrelated faults:

- **Attack:** This is a malicious interaction fault through which an attacker aims at deliberately violating one or more security properties or an intrusion attempt.
- **Vulnerability:** This is a fault created during the development of the system or during operation, which could be exploited to create an intrusion.
- **Intrusion:** This is a malicious externally induced fault resulting from an attack that has been successful in exploiting vulnerability.

A. Intrusion-DetectionArchitecture:

Intrusion detection can be classified based on audit data as either host-based or network-based. A network-based IDS captures and analyzes packets from network traffic while a host-based IDS uses operating system or application logs in its analysis. Based on detection techniques, IDS can also be classified into two categories as follows.

1. Stand-alone IntrusionDetectionSystems
2. Distributed and Cooperative Intrusion Detection Systems Intrusion detection in mobile ad-hoc networks is shown in Fig 1.

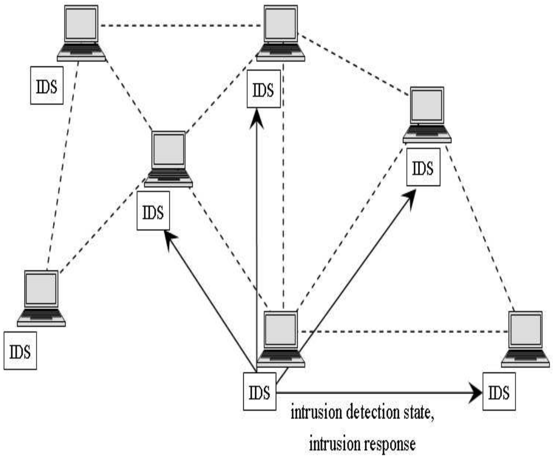


Fig.1: Intrusion Detection in MANETs

B. Stand-alone Intrusion DetectionSystems:

In this architecture, an intrusion detection system is run on each node independently to determine intrusions. Every decision made is based only on information collected at its own node, since there is no cooperation among nodes in the network. Therefore, no data is exchanged. Besides, nodes in the same network do not know anything about the situation on other nodes in the network as no alert information is passed. Although this architecture is not effective due to its limitations, it may be suitable in a network where not all nodes are capable of running IDS or have IDS installed. This architecture is also more suitable for flat network infrastructure than for multi-layered network infrastructure. Since information on each individual node might not be enough to detect intrusions, this architecture has not been chosen in most of the IDS for MANETs.

C: *Distributed and Cooperative Intrusion Detection Systems:*

Since the nature of MANETs is distributed and requires cooperation of other nodes, the intrusion detection and response system in MANETs should also be both distributed and cooperative as shown in Figure 1. Every node participates in intrusion detection and response by having an IDS agent running on them. An IDS agent is responsible for detecting and collecting local events and data to identify possible intrusions, as well as initiating a response independently. However, neighboring IDS agents cooperatively participate in global intrusion detection.

III.MOBILE AGENT FOR INTRUSION DETECTION SYSTEMS

A concept of mobile agents has been used in several techniques for intrusion detection systems in MANETs. Due to its ability to move through the large network, each mobile agent is assigned to perform only one specific task, and then one or more mobile agents are distributed into each node in the network. This allows the distribution of the intrusion detection tasks. There are several advantages for using mobile agents. Some functions are not assigned to every node; thus, it helps to reduce the consumption of power, which is scarce in mobile ad hoc networks. It also provides fault tolerance such that if the network is partitioned or some agents are destroyed, they are still able to work. Moreover, they are scalable in large and varied system environments, as mobile agents tend to be independent of platform architectures. However, these systems would require a secure module where mobile agents can be stationed to. Additionally, mobile agents must be able to protect themselves from the secure modules on remote hosts as well.

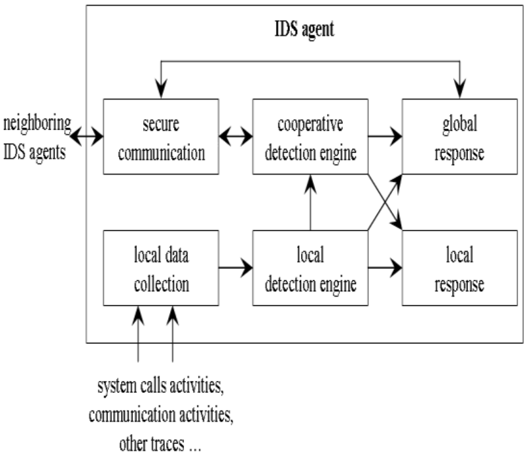


Fig. 2: A Model for an IDS Agent

IV. DYNAMIC HIERARCHICAL INTRUSION DETECTION AND TOLERANT ARCHITECTURE

In this every node has the responsibilities of monitoring (by accumulating counts and statistics), logging, analyzing (i.e., attack signature matching or checking on packet headers and payloads), responding to intrusions detected if thereis enough evidence, and alerting or reporting to cluster heads. Cluster heads, in addition, must also perform data fusion/integration and data reduction: Cluster heads 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. Besides, cluster heads may send the requests to their children for additional information in order to correlate reports correctly.

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 heads 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. 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 heads). 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. The authors also suggested criteria on selecting cluster heads. Some of these criteria are:

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

Additionally, this proposed architecture does not rely solely on promiscuous node monitoring like many proposed architectures, due to its unreliability as described in .Therefore, this architecture also supports direct periodic reporting where packet counts and statistics are sent to monitoring nodes periodically.

A. Intrusion-tolerance Architecture:

Whenever the IDS identify a node misusing resources in the network, it will be tolerated or denied access of the resources according to the context. The intrusion tolerance is done with the help of membership and proactive reaction measures which will reduce the response time of detection. The response time of detection can be improved in such architecture since the node can detect the intrusion directly. The problem in placing the IDS in each node is that in MANET, the resources are limited and thereby, each node may need more memory for placing the IDS. To reduce the consumption of memory at each node in the network monitor can be selected among the nodes .The monitor is an intelligent one which learns an updates the database with the details about the nodes that have sent invalid data to the network. This information will be used for tolerating the nodes in the network.

All the nodes in the network other than the monitor will be having a minimum level of filtering which will contain the minimum set of data to validate the messages, the membership details of the nodes and the details about the member nodes that are found to be working maliciously. The IDS proposed will try to minimize both the issues i.e., the response time and the utilization of the memory.

B. Principle of Intrusion detection and tolerance:

An intrusion-tolerant system is a system that is capable of self diagnosis, repair, and reconfiguration while continuing to provide a correct service to legitimate users in the presence of intrusions. The mechanisms that can be used to make a system intrusion tolerant are directly inherited from the usual fault-tolerant mechanisms:

1. Error detection techniques,
2. Error handling techniques to avoid errors from propagating into a security failure observed by the users, and Fault handling techniques to eliminate the causes of the detected errors.

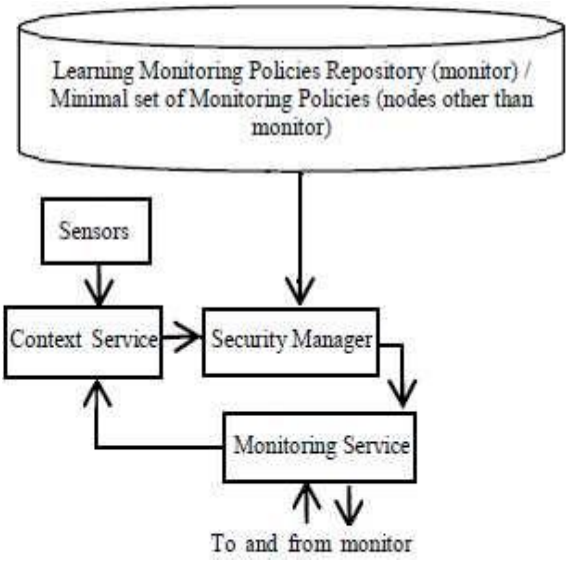
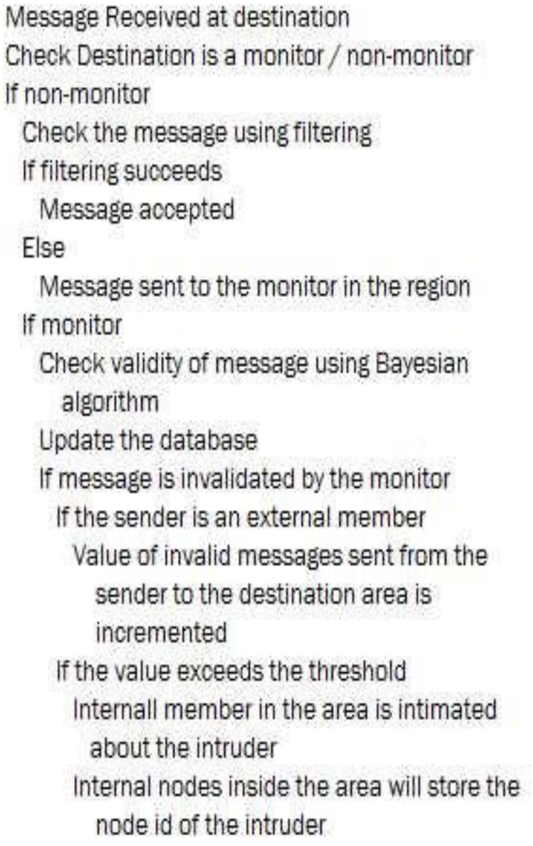

Learning Monitoring Policies Repository (monitor) / Minimal set of Monitoring Policies (nodes other than monitor)
Sensors
Context Service
Security Manager
Monitoring Service
To and from monitor

Fig 3: intrusion detection and tolerance architecture

The data flow in the architecture is as follows. The sensors will check the nodes present in the network and will send the information to the context service. The context service will analyze the data and will decide the context. The monitoring service will check the validity of the message by considering the policy specified for the context in the policy repository and will raise alerts in the case when it is not able to distinguish the validity of the message. The security manager manages the data flow between the repository, context service and the monitoring policy The entire network is divided into small areas and one of the nodes in the area is selected as the monitor. All the nodes other than the monitor will be having a minimum level of intrusion detection. Each of the nodes will be having a node membership database in it. If the sender is not a member, the data will be ignored. Otherwise, the data will be analyzed for the basic pattern which might be found in the message with the filtering in the destination. If the filtering fails, the message will be sent to the monitor.

C. Algorithm for Intrusion Detection:

The algorithm for intrusion detection is given in Figure 4[4].

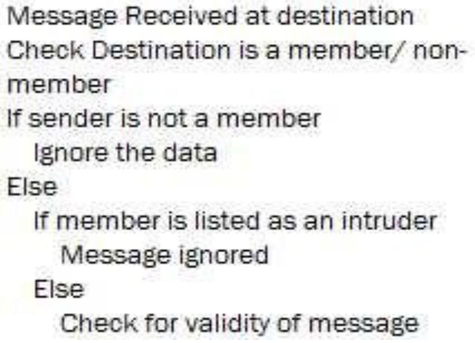


```
Message Received at destination
Check Destination is a monitor / non-monitor
If non-monitor
  Check the message using filtering
  If filtering succeeds
    Message accepted
  Else
    Message sent to the monitor in the region
  If monitor
    Check validity of message using Bayesian
      algorithm
    Update the database
    If message is invalidated by the monitor
      If the sender is an external member
        Value of invalid messages sent from the
          sender to the destination area is
          incremented
      If the value exceeds the threshold
        Internall member in the area is intimated
          about the intruder
        Internal nodes inside the area will store the
          node id of the intruder
```

Fig 4: Algorithm For intrusion detection

The area for the monitor is considered by dividing the network as square areas and the node which is at the least distance from the centre of the square is considered as the monitor. So, the selected monitor will be the one which will be probably staying in the area for the maximum time. If the current monitor moves out of the area, a new monitor is selected using the same algorithm. The technique will reduce the average response time of the nodes using the minimum filter where as it will also reduce the total memory usage by placing the major IDS part in the monitor. The monitor will be having the same information as a normal node at the beginning. When the node is selected as a monitor, it will start learning and check the validity of messages.

D. ***Algorithm for Intrusion Tolerance:*** The algorithm for intrusion tolerance is given in Figure 5.



```
Message Received at destination
Check Destination is a member/ non-
member
If sender is not a member
  Ignore the data
Else
  If member is listed as an intruder
    Message ignored
  Else
    Check for validity of message
```

Fig 5: Algorithm For intrusion tolerance

Whenever a member node sends an invalid message to the monitor, (either for validating the message or for the monitor itself) the information in the message and the information about the sender node is saved in the monitor. If the sender member node is an external node, i.e., the location of the node is not in the similar service area as the receiver node, it will be tolerated to send message up to a threshold limit. When it exceeds the limit, then onwards, it will be considered as an intruder and the data send from that member node is ignored. If the sender member node is an internal node, i.e. it is located in the same service area as the receiver node, it will not be blocked. The main modules of the intrusion detection and tolerance system are as follows.

A. Monitor Placement:

Selecting the monitor is done by checking the node's respective position in the network. Let "n" be the node and "nx" and "ny" be the x and y position of node. Let "X" and "Y" be the x and y coordinates of the centre position of the area considered. Then position of monitor node is calculated as: min [abs (X-nx) + abs(Y-ny)]

B. Node Types

There are mainly two types of nodes in an area.

1. Filtering Node
2. Monitoring Node

Each region will have one monitor node and the rest of the nodes are filtering nodes.

C. Membership

All the nodes will have a list of nodes from which it will accept data. When a node which is not a member sends a message, the message will be ignored. The node which is a member can be an internal member or an external member. An internal member is a member that has the similar context data as of the current node (eg: if the current node is having the context of a university, the internal member will also have the same context). An external member is a member that is not in the similar context as of the current node.

V. CONCLUSION

This study has been supported by an intrusion detection and tolerant architecture for Mobile ad hoc networks. This Architecture mainly depends on dependability and diversification principle in order to maintain system consistency, and it is constructed for static as well as fully dynamic systems.

REFERENCES

[1] Zhang Y, Lee W, Huang Y "Intrusion detection techniques for mobile wireless networks", 2003, A CM MONET Journal pages 3.

[2] Zhou B, Shi Q, Merabti M "Intrusion Detection in Pervasive Networks Based on a Chi-Square Statistic Test" In: Computer Software and Applications Conference, 2006, COMPSAC 2006.

[3] S. Jacobs and M. S. Corson. MANET authentication architecture. Internet draft- jacobs-imep-auth-arch-01.txt expired 2000, February 1999.

[4] T. Joachims. Making large-scale SVM learning practical, chapter 11. MIT-Press, 1999.

AUTHOR BIOGRAPHY

G.M.Padmaja received the Master of Technology in Information Technology from Sathyabama University, in 2010. Currently, she is a Senior Assistant Professor at Padmasri Dr.B.V.Raju Institute of Technology, Narsapur. Her interests are in networks, image processing and data mining.

CH.Rajyalakshmi received the Master of Technology in Computer Science & Engineering from Avanthi Institute of Engineering & Technology, Narsipatnam, in 2011. Currently, she is an Assistant Professor at Padmasri Dr.B.V.Raju Institute of Technology, Narsapur. Her interests are in mobile wireless networks, image processing and data warehousing.