International Journal of Theoretical & Applied Sciences, **1**(1): 149-152(2009)

ISSN No. (Print): 0975-1718

Mobile Adhoc Networks: Architecture, Security, and Applications

Taran Singh Bharati
Department of Computer Science & Engineering,
ABES Engineering College, Ghaziabad,(U.P.), India.

ABSTRACT

Adhoc networks have become important in society in the situations like military and disaster because of their non dependency on any fixed. They may be sensor networks and mobile adhoc networks. Since these networks are more effective in special circumstances and therefore can pass very crucial and confidential information. There are many issues such as routing, cooperation, management, security, energy shortage, etc. but out those issues, security and privacy is of our concern. There are many ways to secure them like encryption, intrusion detection system, mobile agents and hybrid way. This paper on securing mobile adhoc networks using intrusion detection System.

Keywords: Adhoc networks, threats, intrusions, security, energy conservation, cooperation.

INTRODUCTION

Adhoc networks are temporary networks which are made for a fixed period of time in special situations. When its nodes are movable it becomes Mobile adhoc networks are the networks which are created by mobile nodes which have no additional extra infrastructure. There is no centralized authority for controlling its operations therefore all nodes have to work together in cooperative way. All important works such as routing, forwarding etc. have to be done by all nodes themselves. Every node works as a router for passing packets to and from it. Since it is a wireless network hence it has many security issues because of its vulnerabilities and open ports.

A. Intrusion Detection System

It is software that can be installed at many places depending on its types. It can be installed in Router/Gateway and it will be monitoring all those packets which coming into to the network or the packets which going outside from the network. Similarly, we have Host Based IDS that is installed in particular host machine and it will be checking intrusions upto host level. It inspects every packet and looks for the intrusions. If it suspects for the intrusions, it reports to the system administrator so that timely remedial action can be taken by the authorities. IDS must have been continuously monitoring the traffic without human intervention, fault tolerance, subversion resistant, incurring less overheads, looks for behavior deviations, easily configurable, and can adapt itself over the time[8], [10].

There are different types of IDS's like Anomaly based, Rule based and Statistical based intrusion detection. An IDS has three components Local data collection component: that collects local data about the behavior the user on the basis of activities performed by the user in his session. In order to detect whether the activity that is performed by the user is detection or not, we use misbehavior based, rule based and statistical methods on some parameters. Global data collection Component: It collects global data from all nodes in the network, and then it applies the algorithm to become assure whether not there is an intrusion into the network.

A number of Intrusion Detection System (IDS) techniques for MANETs have been proposed in the research literature. These techniques include trust building and cluster-based voting schemes, host-based watchdogs, and finite state machines for specifying correct routing behavior. Comparing and evaluating the effectiveness of these IDS techniques has been hindered by the limited number of large-scale MANET deployments, the lack of publicly available network traces of actual MANET traffic, and the difficulty in defining typical application and mobility scenarios. Network simulation tools have allowed researchers to study MANET IDSs without purchasing mobile nodes or conducting costly and time-consuming field trial tests. These simulations, however, have been conducted using widely varying assumptions on background network traffic, mobility, previous security associations, and the type of malicious network activity These network traces will allow a broader range of researchers to compare the effectiveness of different MANET IDS techniques on the same data set, and conduct cost-effective and time-saving offline

experiments with new IDS techniques without requiring expensive hardware.

Intrusion detection systems follow the following detection types [1]. The IDS keeps the three things, data collection, analyzing engine, and communications section. Detection engine can use for analyzing the intrusions, can used, statistical methods, Genetic algorithm, machine learning technique, soft computing, or artificial techniques.

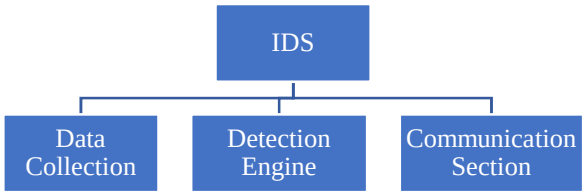

Fig. 1. Intrusion Detection System (IDS).

Signature Based Intrusions: For detecting the intrusion into the system these IDS checks for the signatures (special pattern).If that particular types of signature is found, then an intrusion is reported. It has the drawback that it can detect only those intrusions that keep particular types of signatures. Any other intrusion that has no signature cannot be detected by it.

Anomaly Based Intrusion Detection System: These are the system which watches the activities of the user and for noticing any suspicious activities, i.e., abnormal timing, trying the access beyond the assigned rights.

Both approaches have their own advantages and disadvantages. Signature based detection can do fast detection, the intrusion whose signature is matched to the available data base. For new intrusions having unknown pattern, it is difficult to be detected because its signatures are not found in the database.

Agents Based IDS: They are the programs that get installed on the hosts without their permissions, collect spy data and send it to their masters. Master analyzes the data for detecting the intrusion. They overcome network delay, reduce the network load, can execute autonomously, can adapt themselves automatically, robust and scalable. Agents have drawbacks that they impose vulnerabilities into the network.

MANET$_S$ ARCHITECTURE

MANETs' architecture has three layers [7]:

i) **Enabling Technology:** It becomes possible because of these facilities, i.e., Bluetooth, 802.11, HiperLAN, medium access control, antennas, and power control.

ii) **Networking:** Communication in MANETs becomes possible because of transport and network protocols, TCP, IP Routing, Addressing, Multicasting, and interconnection.

iii) **Applications and Middleware:** It provides the services like location, group communications shared memory.

Apart from the above, there are several cross-layer services also such as security and cooperation, energy conservation, simulation, quality of services.

TOP FREE NIDS FOR ENTERPRISE

Snort: It is the pioneer of the open-source NIDS software. It uses both signature-based and anomaly-based intrusion detections. It doesn't have its own GUI but many front ends are created to address the GUI for snot.

Suricata: It similar to snot therefore it also supports both signature-based and anomaly- based detections. It is better than snort because of multi threading, GPU, and statistical anomaly modeling, etc.

Bro IDS: It is used with snot and it is a kind of anomaly intrusion detection system. It is good for traffics analysis.

OpenWIPS-ng: It is signature-based IDS and provides solutions for wireless security, traffics analysis, and good GUI.

SECURITY OF MANETs

Security gives the feeling of being a secure in the form of its services such accessibility, confidentiality, authentication, availability, and non repudiation. Particularly for MNAETs because it's distributive nature and no fixed infrastructure its security can be thought of [2, 4, 5, 6, 9]:

i) Routing Level Security
ii) Data f Security
iii) Link state Security
iv) Security via Key Management
v) Security via Intrusion Detection System(IDSs)

Any activity which breaches or compromises the security of the system is called attack. The attacks can be of any kinds depending on whether they are able read the messages only (passive attacks) or they capable enough to modify and replay the messages to the destination also (active attacks).Attacks on MANETs challenge the mobile infrastructure in which nodes can join and leave easily with dynamics requests without a static path of routing. There is a trusted third party (TTP) which handles authentication of sender, destination. Schematics of various attacks as described on individual layer are as under [1]:

i) **Application Layer**: Malicious code, Repudiation.
ii) **Transport Layer**: Session hijacking, Flooding
iii) **Network Layer:** Sybil, Flooding, Black Hole, Grey Hole. Worm Hole, Link Spoofing, Link Withholding, Location disclosure etc.
iv) **Data Link/MAC**: Malicious Behavior, Selfish Behavior, Active, Passive, Internal External

v) **Physical:** Interference, Traffic Jamming, Eavesdropping.

Intrusion Detection: It is used to check whether or not an intrusion has taken place in your system or not by seeing the performance of the system. It is of two types [3].

Audit Based Intrusion Detection

i) **Naïve Audit Base:** These audits are prepared by operations system and these can be analyzed to monitor the users' activities.

ii) Detection Specific Audit Records: This gathered information may be required for intrusion detection.

Statistical Anomaly Detection: It checks the behavior of the user by using statistical parameters. Some of the statistical parameters are as counter of logins, logouts, session, number of times password failures, number of times logical connections to application, number of time outgoing message queued up a process, interval time, resource utilization, etc. They are categorized into two ways as:

i) **Threshold Based**: It monitors the numbers of times the activities happen over the time period. If that count goes beyond, it is suspected intrusion.

ii) **Profile Based**: Past behavior of the user is taken into consideration to know the deviation from users' normal behavior.

Proposed Model for Detection: In the data analysis sense, data sets are available and can be downloaded from the web sites and the data sets are analyzed with the help of data mining or machine learning techniques using the above discussed methods for intrusions if any, occurred into the system. The proposed schematics steps may be as below [11]:

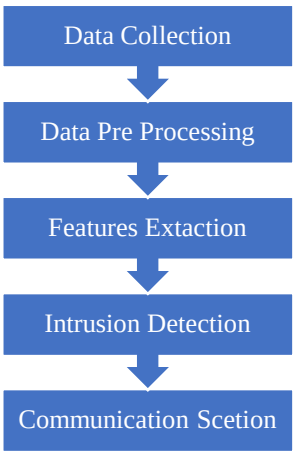

Fig. 2. Proposed Intrusion Detection Process.

i) **Data Collection:** Data sets about the users' behavior can be downloaded online.

ii) **Data Pre-Processing:** Data downloaded may not be suitable for the system to be processed, it is tunned by pre-processing techniques i.e., noise removal, normalizing, missing substitutions, etc.

Feature Extraction: in data sets there could many features, important features are chosen for further processing.

iii) **Intrusion Detection:** it is done with the help defining threshold as:

Threshold = $\sum w_i x_i$

Where x represents a feature and w a represents weight assigned to feature (in some range). The intrusion may be detected as:

Intrusion if $\sum_{i=1}^{i=n} w_i x_i \leq$ Threshold

iv) **Communication Section:** An alert message is sent to all nodes in the network once intrusion I s detected by the detection unit so that other nodes can measures accordingly.

MANETS APPLICATIONS FUTURE SCOPE

Because of nature of MANETs there are several applications of them in special situation such as military communication or operations, they can used in home appliances in the form of sensors, emergency situations like disaster, shared home/office applications, to set up virtual classrooms, games, follow-on services, and location-based services.

Because they are emerging technologies and they are very much useful in some special circumstances. Therefore, there are several areas where they need much attention of the researchers for better performance such as; secure routing; data security; energy consumption saving; other quality of service parameters.

CONCLUSIONS

This paper discusses a state-of-the-art research topic, mobile adhoc networks. This network is very powerful specially in the disastrous situations when already existing networks stop operating. These networks are setup by the mobile devices available to common people with less hurdles and no extra additional infrastructure. How they exchange their information securely and how they detect intrusions if any, their remedies, architecture, etc. are addressed. Since it is new type of research field hence bears a lot of difficulties. This paper explained it and its difficulties, security aspects, working, protocols, etc, and proposed a model for analysis for intrusion detection.

REFERENCES

[1]. Jabas, A., Garimella, R.M., Ramachandram, S. (2008). Proposing an enhanced mobile ad hoc network framework to the open-source simulator ns2. In 2008 Mosharaka International Conference on Communications, Computers and Applications 2008 Aug 8 (pp. 14-19). IEEE. Doi: 10.1109/MICCCA.2008.4669843

[2]. Zhang, Q., Wang, X., Gong, Z. (2008). A Role-Based Automated Trust Negotiation and Authentication Design in Mobile Ad Hoc Networks. In 2008 International Conference on Computer Science and Software Engineering Dec, 2008 (Vol. **3**, pp. 688-691). IEEE.
[3]. Soungalo, T., Dong, W., Yulan, L. (2009). Performance evaluation of campus mobility model in mobile ad hoc networks. In2009 International Conference on New Trends in Information and Service Science, June, 2009 (pp. 743-748). IEEE.
[4]. Min, Z. and Jiliu, Z. (2009). Cooperative black hole attack prevention for mobile ad hoc networks. In 2009 International Symposium on Information Engineering and Electronic Commerce May, 2009 (pp. 26-30). IEEE.
[5]. Djenouri, D., Khelladi, L., Badache, A.N. (2005). A survey of security issues in mobile ad hoc and sensor networks. IEEE Communications surveys & tutorials. **7**(4): 2-8.
[6]. de Morais Cordeiro, C., Agrawal, D.P. (2002). Mobile ad hoc networking. Center for Distributed and Mobile Computing, ECECS, University of Cincinnati. 2002: 1-63.
[7]. Chlamtac, I., Conti, M., Liu, J.J. (2003). Mobile ad hoc networking: imperatives and challenges. *Ad hoc networks*, **1**(1): 13-64.
[8]. Jansen, W., Jansen, W., Karygiannis, T., Marks, D. (1999). Applying mobile agents to intrusion detection and response. US Department of Commerce, National Institute of Standards and Technology; 1999 Oct 1.
[9]. Irshad, A., Noshairwan, W., Shafiq, M., Khurram, S., Irshad, E., Usman, M. (2008). Security Enhancement in MANET Authentication by checking the CRL Status of Servers. *Int J Adv Sci Technol.*, **1**: 91-8.
[10]. Stallings W. (2006). Cryptography and network security, 4/E. Pearson Education India; 2006.
[11]. Mining, W.I. (2006). Data mining: Concepts and techniques. Morgan Kaufinann, **10**: 559-569.