ISSN: 2277-9655
Impact Factor: 1.852

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

A Survey on Intrusion Detection System in Mobile Ad-Hoc Networks

T. Ramesh[*1], S. Kavipriya[2]

[*1] Assistant Professor, Department of Information Technology, Bharathiar University, India, Coimbatore-641046India

[2] Research Scholar, Department of Information Technology, Bharathiar University, India, Coimbatore-641046, India

trcsebu@gmail.com

Abstract

Mobile Ad-hoc Network (MANET) is an Emerging Technology. MANET is a great strong point to be applied in dangerous situations like battlefields and commercial applications such as construction, traffic surveillance. Each device in a MANET is without free to move in any direction and its changes the connections to other devices frequently. Mobile Ad-hoc network is faces several challenges such as Energy, Routing, Security, Quality of services, Memory and etc... But the flexibility in such atmosphere has the challenged in risk of security. The main Intrusion Detection is one of the possible ways in recognizing possible attacks before the system could be penetrate. The encryption and authentication solution are consider as the first line of protection, are no longer enough to protect MANETs. This paper defines several MANET security threats and focuses on MANET intrusion detection methods.

Keywords: Mobile Ad-Hoc Network, Intrusion Detection System.

Introduction

Mobile Ad-Hoc Network (MANET) is a collection of mobile hosts with wireless network interfaces form a provisional network without the aid of any fixed communications or centralized organization [3].A MANET is an infrastructure less network because the mobile nodes in the network dynamically set up paths along with themselves to transmit packets temporarily.
The Mobile Ad-Hoc networking is gaining importance with the increasing number of extensive applications. There are several Applications used in Mobile Ad-Hoc Networks [5]. These are,

- Military battlefield,
- Commercial Environment,
- Location Aware Services,
- Personal Area Network
- Emergency Services.

There are several security threats and most important one is the node being Intrusion Detection. This paper defines Intrusion detection and discussed about different methods employed to detect the intruders.

MANET is an independent system in which nodes are connected by wireless links and send data to each other. This is no any centralized system subsequently routing is done by node itself. Due to its mobility and nature direction-finding capability, present be many weaknesses in this security. To solve the security issues and it need an Intrusion detection system [8].

Section 2 focuses on Several Challenges faced by the Mobile Ad-Hoc Network. Section 3 focuses on Security threats in Mobile Adhoc Networks. Section 4 focuses on intrusion detection methods. Finally all the conversation points are summed up in Section 5.

Challenges of Manets

Mobile Ad-Hoc Network (MANETs) is different from traditional networks and faces several challenges, these are

A. Routing

Routing is selecting paths in the network along without send network traffic. The topology of the network is constantly changing; the problem of routing packets between any pair of nodes becomes a difficult task. Most protocols must be based on reactive routing instead of proactive [2]. In reactive is routes are discovered on demand when pathway must be delivered to an anonymous destination. In proactive routes are computed automatically and separately of track arrivals. Multicast routing is also challenge; this multicast tree is no longer fixed outstanding to the random movement of nodes within the network [2].

ISSN: 2277-9655
Impact Factor: 1.852

B. Energy efficiency

Mobile Ad-Hoc Network has a limited battery power. In some areas such as surveillance of nature, armed forces etc. requires lengthy life time. So that it is very important to have Energy efficiency [8].

C. Quality of Services

Providing Quality of Service is another best effort, is a very complex problem in Mobile Ad-Hoc Networks and It making area challenging area of future MANET research [8]. Networks ability to provide Quality of Services depends on the fundamental characteristics of all the network mechanism, from communication links to the MAC and network layers.

Security Threats Faced By Manets

Securing Mobile Ad-hoc Network is highly challenging task. The attacks in MANETs are secure communication in MANETs and for that reason secure transmission of information is necessary. MANETs are more defenseless than that of wired network hence is more exposed by the security attacks [7]. These attacks are used in network security.

Active Attack

An **active attack is** the attacker try to bypass or break into secured systems. And it has done through worms, Trojan horses. Active attacks attempts to avoid or break protection features, to introduce malicious code, and take or modify information. Attacker gains the physical control link .It is detected to easily. The damage caused can be small or large depends on the condition [5].

LAYERS	ATTACKS
Application Layer	Repudiation, Data corruption
Transport Layer	Session hijacking, SYN Flooding
Network Layer	Warm hole, Block hole ,Flooding
Data Link Layer	Traffic Analysis, Monitoring, WEP weakness
Physical Layer	Jamming, interception
Multi Layer Attack	Dos , Replay, Man in the Middle, impersonation

Table 1: Active Attack on Layer in MANETs

Passive Attack

A **passive attack** is monitoring unencrypted traffic and clear-text passwords and sensitive information that can be used in other types of attacks. The attacker cannot directly cooperate with the parties occupied, so attacker attempts to crack the system by observing the data. Identification of attack is very hard. The damages caused by this attack are strict. A malicious node moreover ignores operations supposed to be accomplished by it in passive attack [5].

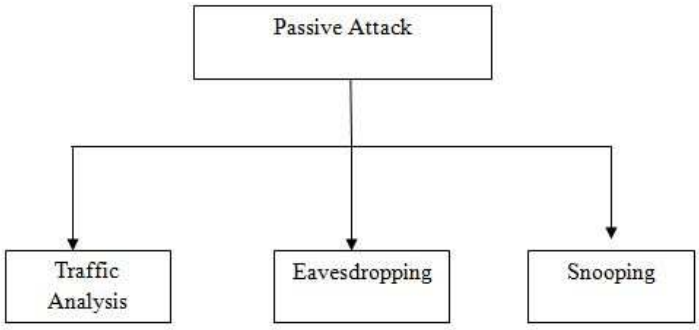

Fig.1: Passive Attack in MANETs

Intrusion Detection Methods

As Mobile Ad-Hoc Networks are placed in a hostile environment, it is subjected to several vulnerabilities. Detecting the intruder is not an easier assignment. Intrusion detection can generate inaccurate values and it can mislead other nodes. To handle this situation several approaches have been proposed. In this survey, 5 approaches are discussed in detail

Intrusion Detection Using a Cost Sensitive Classification in Manet

A cost sensitive classification algorithm is used to order to perform in intrusion detection in MANETs. This algorithm has basically computerized, it can be relatively accurate, and it is fixed in information. For with the purpose of motivation, it is prime candidates for use in cost-sensitive classification troubles. After preparation, it can be used for intrusion detection with random cost matrices [1]. A cost matrix has extensive applications including intrusion detection in wired networks, and both theoretically and experimentally, and it used in many applications with a high quantity of success.

The Intrusion Detection System is composed of the multiple local intrusion detection system agents, and it is responsible for detecting to possible intrusions locally. During the preparation phase, it collects data locally, join it and it is use to adjust the classifier models in offline. During the testing phase, the resulting classification rule is transmitted to the local intrusion detection system agents, and performs detection is independently.

All classification models are trained and so as to expect the probability of every class, and it specified an observation. The models are make decisions to types of mistaken classification decisions may be more important

ISSN: 2277-9655
Impact Factor: 1.852

to others. This can be modeled by specifying a set of cost for each type of error or mistake. This cost of matrix can be used within any classification and that has been trained to calculate class probabilities. Given a specification of expenses for correct and incorrect predictions, and the class decision should be the one that leads to the lowest expected cost [1].

Intrusion Detection Using Artificial Intelligence In Manet

The artificial intelligence is based to the number of knowledge, and it has been previously derivative to function. In the mobile ad hoc networks can be gathered information from the path selection through route detection performed during the analysis of the network earlier than transmission. It has been developed to an algorithm that can be integrated at every node of the network configuration [10]. The system is check for table and provides each node selected for relaying a sequence number and which direction sorter for each packet heading towards another destination. The sequence number is already present in Ad hoc On Demand Distance Vector routing protocol.

An Artificial Intelligence is fetched this component in network simulator and integrated and it with the algorithm as a basic element and then coded for collection of relaying node on basis of sequence number provided to every node through the route detection. Also, this progression number is generated on the time of routing and selection of next relaying node and it can't be affected by intruders. But, the one important factor came that if intruder node generates the hello message containing a sequence number analogous to relaying node. This caused the serious issue.

A technique is termed as tell your source. This technique asks the source for that generated a sequence number for the node is to operate in an exacting network. This is solved the problem of false sequence numbers. On application of this algorithm in path selection and communication, decreased the delays and improved the fault tolerance to high-quality extent [10].

Mobile Agents-Based Intrusion Detection System for Mobile Ad-hoc networks

Intrusion Detection System is divided into the clusters head by using appropriate algorithm and it is detecting a unit based on agent to runs on the cluster head. Cluster head is identifies disturbing activity by local data to gathering and characteristics comparison and then the isolates to intrusion detection nodes. If a cluster head is unable to gather sufficient verification to declare a node malicious, it can be generate to joint decision with each other cluster heads to determine disturbing activity of a node by using partial determination. Partial determination instead of collective determination effectively reduces energy consumption of nodes.

An agent is activated to the cluster head node and gathers the data from all other nodes in the cluster to investigate the performance of the nodes; if the intrusion is detected, it will notify the other nodes in the cluster head by propagation [6]. If agent is not capable to make a decision, it will be select an ordinary number of hops as radius and send joint decision request to all cluster head nodes in range of its hop radius.

Cluster head nodes are after analyzing for the abnormal data, it will be determine whether intrusion has occurred or not. Agent is making a decision based on the decision of majority of cluster head nodes inform the all nodes. If cluster head node itself is compromised to an agent will notify this to all other cluster heads and exclude it from routing elect a new cluster head by clustering algorithm. The main drawbacks are Intrusion detection technique used that issues pertaining to security of mobile agents.

Grammatical Evolutions in Intrusion Detection On Manets

Evolutionary calculation mimics the processes of usual development to find a fit solution to posed problems. A population of individual candidate solutions for the target problem is generated. Each individual is evaluated and assigned to fitness value that indicates to candidate solves. Grammatical Evolution is problem is defined with the syntax and the fitness function.

The grammar used evolves the programs to detecting the attacks on Manet and increase an alarm is defined library is used for the growth process. It uses both mobility-related features as well as packet related features as input to the development system. While some features give information about mobility in directly, some result is mobility. Packet-related features include routing protocol manage packets and transfer protocol packets [9]. Some features are used only for particular attacks such as data packets not forwarded by the next node for dropping in attacks, and average step count feature for route disturbance attacks. All features are gathered every time interval by each node.

The fitness function is the mainly important parameters in evolutionary calculation, since it evaluates to good solution. In the experiment, use fitness function based on the detection rate and false positive rate to evaluate efficiency of proposed system. The detection rate ratio is appropriately detected to intrusions on the network. The false positive rate ratio is normal activities are incorrectly marked as intrusions behavior on the network. A low false positive rate is as important as high detection rate for good intrusion detection system.

ISSN: 2277-9655
Impact Factor: 1.852

Cross-Layer Based Intrusion Detection Technique in Manet

A measure of energy is observed in physical layer at the antenna of the receiver is called as received signal strength. In IEEE 802.11 networks, though performing Medium Access Control dimension and roaming operations, the received signal strength indication value is used. The Radio Frequency signal strength is measured or relative manner. It is clear that it is not possible for an attacker to assume the received signal strength exactly for a sender by a receiver. The attacker not exactly at same location as the receiver it uses the same radio equipment and receives the radio signal with the same level of intrusion, reflections and refractions. Even if the sender is fixed, received signal strength value seems to vary little and it proved. This restricts the attacker from using the radio equipment to spoof the received signal strength clearly by the receiver.

It is develop a dynamic profile for the communicating nodes based on their received signal strength values through monitoring values sometimes for a specific Mobile Station or a Base Station from a server. Any unexpected or unusual changes marked as uncertain activity which indicates the possible session of hijacking attack [4]. The received signal strength profile is called dynamic because it rebuilt the session between two nodes and it is continuously updated with new observed received signal strength values for each node per session. Any unexpected changes in the received signal strength dynamic profile can be marked as doubtful activity with a higher confidence level because Base Station are generally immobile. If the Mobile Station is individual received signal strength values vary quickly which can be observed by the server.

If an attacker mobile station1 hijacks mobile station2 through isolating from the network and spoofing it Medium Access Control address server is pick up suddenly changes in the received signal strength profile of mobile station2's Medium Access Control give an alert signal. Since it depends on the mobile station1's real place, radio tools and surrounding environment received signal strength values for the mobile station2's Medium Access Control address will be change. In another, if attacker mobile station1 spoofs the base station base station then it also gets detected the dynamic received signal strength profile for the base station undergoes sudden variations. Therefore this mechanism gives intrusion detection for both session hijacking and man-in-the-middle attacks which is targeted at either mobile stations or base stations.

Conclusion

The Intrusion detection is the primary security problem in mobile ad hoc network. Intrusion detection are major detection in MANET, probably that need to be addressed in mobile ad hoc networks. Many approaches are used to Intrusion Detection. In this paper, we have discussed five different approaches to temperate the intrusion detection issues faced in MANET. In each method we have seen about how Intrusion detection are identified and detected and handled effectively by different methodologies that are employed.

References

[1] Aikaterini Mitrokotsa a, Christos Dimitrakakis b, "Intrusion detection in MANET using classification algorithms: The effects of cost and model selection", Journal of Elsevier, Aug-2012.

[2] Imrich Chlamtac, Marco Conti, Jennifer J.N. Liu," Mobile ad hoc networking: imperatives and challenges", Journal of Elsevier, Sep-2003.

[3] Jacob Abraham, V.Arun Prasath, G.Michael," A Survey of Intrusion Detection for Ad-Hoc Network ", Journal of Global Research in Computer Science, Volume 4, No. 4, April 2013.

[4] Jatinder Singh, Lakhwinder Kaur, and Savita Gupta," A Cross-Layer Based Intrusion Detection Technique for Wireless Networks", The International Arab Journal of Information Technology, Vol. 9, No. 3, May 2012.

[5] Md Tanzilur Rahman, Kunal Gupta," MANET: Security Aspects and Challenges", International Journal of Computer Trends and Technology, volume 4 Issue 6–June 2013.

[6] Monika Darji, Bhushan Trivedi, "Survey of Intrusion Detection and Prevention System in MANETs based on Data Gathering Techniques", International Journal of Applied Information Systems, Volume 1– No.3, February 2012.

[7] Pradip M. Jawandhiya, Mangesh M. Ghonge, Prof. J.S. Deshpande," A Survey of Mobile Ad Hoc Network Attacks", International Journal of Engineering Science and Technology ,Vol. 2(9), 2010.

[8] Priyanka Goyal, Vinti Parmar, Rahul Rishi," MANET: Vulnerabilities, Challenges, Attacks, Application", IJCEM International Journal of Computational Engineering & Management, Vol. 11, January 2011.

ISSN: 2277-9655
Impact Factor: 1.852

[9] Sevil ¸ Sen, John A. Clark, "A Grammatical Evolution Approach to Intrusion Detection on Mobile Ad Hoc Networks"march-2009.
[10] Vishal Sharma, Takshi Gupta," An Artificial Intelligence Approach towards Intrusion Detection in Soft Systems", International Journal of Advanced Research in Computer Science and Software Engineering, volume 2, issue 2, February 2012.