Journal of Theoretical and Applied Information Technology
10th July 2013. Vol. 53 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

EVALUATION OF INTRUSION DETECTION TECHNIQUES IN MOBILE AD-HOC NETWORKS

[1]ANUSHA.K ,[2]JAYALESHWARI.N

[1,2]School of Information Technology and Engineering, VIT University, Vellore, India

Email: [1]anusha.k@vit.ac.in , [2]jayaleshwari@gmail.com

ABSTRACT

Mobile ad-hoc networks are improvised wireless network increasingly appearing in recent years as portable wireless devices. Due to remarkable characteristics such as lack of central coordination, infrastructure less, dynamic topology and nature of wireless communication, Mobile ad-hoc networks are vulnerable to many security threats. Many Intrusion Detection Systems (IDS) have been introduced to identify the possible attacks in the MANET. In this paper, we review different methods of detection systems and evaluate the systems that have been proposed prominently.

Keywords: *Intrusion detection system, Mobile ad-hoc network, Routing protocols, Security threats.*

1. INTRODUCTION

1.1 Mobile Ad-Hoc Network

Mobile ad-hoc network [1] doesn't have a fixed infrastructure and exist with thousands of wireless machine nodes connected. In communication, mobile ad-hoc network does have a decentralized administration system. It is autonomous in deportment and is distinguished by rapid installation, short bandwidth, restricted processing capacity. The communication in MANET is made via neighbor nodes. When a source wants to send a message to destination nodes, which is not in the range, the mobile ad-hoc networks are capable of using multi-hop routing. An ad-hoc routing protocol can be used to organize routes and maintain them. Various protocols are available for mobile ad-hoc networks. The drive function of routing protocol is to find a route from source to destination in the network to forward the packets. Each node in the mobile ad-hoc network maintains a routing table to maintain a route and to forward the traffic to desired destination that is not bound for them.

1.2 Routing Protocols

There are two types of routing protocols - table driven or proactive routing protocols and reactive routing protocols [2-3] which route the packets to the destination and maintains the route. They follow different approach to maintain the route and forward the data packets. In table driven, the routing table stores the information about the route in advance and changes the route, accordingly and hence the topology will be changed. This is not preferable for large number of mobile nodes which are connected in a network. The disadvantage of proactive routing protocols such as OLSR (optimized link state routing), LSR (link state routing), DSDV (distance sequenced distance vector), DVRP (Distance vector routing protocol), GSR (Global state routing), HSR (Hierarchical state routing) is that it has to store all the relevant amount of information about the routes irrespective of data sent. In reactive routing protocols, the routing tables store information about active route at the time of route request i.e. only on-demand the protocol finds the route. Examples of reactive routing protocols are AODV (ad-hoc on demand distance vector), DSR (dynamic source routing), LAR (location aided routing), TORA (temporally ordered routing algorithm) and hybrid routing (combination of both pro-active and reactive protocols) such as ZRP (zone routing protocol). Both hybrid and reactive protocols are more appropriate with MANET characteristics.

1.3 Attacks

The distinguishable characteristic of mobile ad-hoc networks is their vulnerability to many possible attacks. Attacks can be classified into many types based on the behavior - Like passive and active attackers, external and internal attackers, mobile and wired attackers, single and multiple attackers. Passive attacks are difficult to detect as they do not involve alteration of data. Neither the sender nor the receiver will know about this. But can be prevented by means of encryption. Thus emphasis is on prevention rather than detection. Eavesdropping and traffic analysis attacks are passive attacks in mobile ad hoc network. The active attacks involve modification of data or creation of false stream. The attack launched outside of the domain i.e. not in the particular network is called external attacker where as an internal attack launched is by the one who lives in the legitimate area to secure its resources. The mobile attackers launch the attacks by the use of mobile node resources since all the nodes are having the same capacity, while wired attackers access the external resources for attacking. If the network is disrupted by single attacker then it is called single attacker. If the attacker colludes with group of attackers then it is called multiple attackers. The available routing attacks in MANET are classified into attacks through modification, interception, interruption, fabrication [14] etc. Table 1 shows the possible attacks.

Table 1: Security Attacks In Each Layer

Application layer	Repudiation, data corruption
Transport layer	Session hijacking, Sync flooding
Network layer	Worm hole , Black hole, byzantine, Flooding, Location disclosure
Data link layer	Traffic Analysis Monitoring, Disruption, Web weakness
Physical layer	Jamming, interceptions, Eavesdropping
Multilayer attacks	Dos, Impersonation, Replay, Man-in-the-middle attack

In attacks through modification the opponent will make some changes to the routing messages to misroute the packets. The types of message modification attacks are impersonate attack and packet misrouting. Interception type of attackers drives the attack to get an illegitimate access to the forwarding messages and stop that node to involve in the network operation. Examples of this type of attack are black hole attacks, wormhole attacks and routing packets analysis attack. In fabrication method the attacker dispatch its own large packets to fabricate the networks. sleep deprivation attacks and route salvaging attack are examples of this attack. In interruption type the attack will be launched the attack by accessing the routing messages or mobile nodes. Examples of this type of attack are flooding attacks, packet dropping attacks and lack of operation attacks.

2. INTRUSION DETECTION SYSTEM IN MOBILE AD HOC NETWORK

Due to the lack of suitable security system a malicious node might join the network freely and act as a legitimate node i.e.an intermediary node which is a threat to salvation of data which is exchanged. Several intrusion detection systems (IDS) have been developed for detecting malicious node in the network. The system which monitors the traffic of network and detect the malicious or selfish node in the network can be defined as intrusion detection system. Due to dynamic topology, the task of IDS is very difficult and challenging to say the least. Generally IDS can be categorized into two types (Fig.1) i.e., data collection and data analysis techniques [4-5]. The data collection techniques are further classified into network based and host based. In network based technique, IDS runs on a portal of a network and capture survey data from network traffic that flows over it, and it analyzes the collected data. In host based technique, IDS access the audit data from system log files that runs on the node. Data analysis technique can also be classified into three major types namely - signature based, specification based and anomaly based. In the signature based technique, the set of predefined rules or patterns which will be compared to match the attack. Several techniques are available for signature based method such as genetic algorithm, expert system, rule based, state transition analysis and pattern matching. In the specification based method, it has the set of predefined constraint which defines the appropriate operation of a protocol which monitors the execution of a protocol in respect of defined constraints. If it is deviated from that then the node will be reported as malicious or selfish node. In anomaly based method, the IDS have the normal behavior system that will be constructed according to the target system. Based on this, threshold value will be defined which shows end point between normal and abnormal behavior of the system. Then the captured profile is compared with the defined profile. The available methods of anomaly based technique are data mining, file checking, statistical, immune system and neural network [4-5].

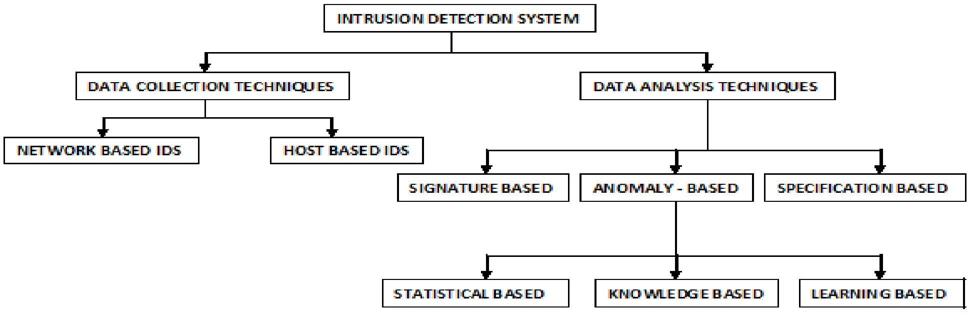

Fig. 1: Classification of IDS

2.1 Fuzzy Based Approach To Detect Black Hole Attack

Fuzzy logic is a mathematical paradigm to deal with uncertainty about the data that intricate in the human interpretation. It expresses any statement in linguistic way which makes fuzzy rule based systems stunning for application. Poonam et al. [6] have proposed intrusion detection system which is fuzzy logic based system to detect black hole attack on AODV protocol in mobile ad-hoc network and it addresses various detection techniques based on only one factor for detection purpose and there are also some detection systems which uses centralized approach to detect the malicious node. But the proposed system detects the malicious node through two factors such as destination sequence number, and forward packet ratio which will find all the intermediary nodes to reach the destination and send packets to intermediate nodes at the beginning of transmission. If the intermediary node fails to send packets then it sends probe message to next node since MANET is multi hop in nature. Then the system fuzzifies the delivery ratio on each neighbor hop. It audits the response time or acknowledgement time for each intermediary node and based on which the node will be detected as attacked node or otherwise [6]. The probe messages will not be sent by unresponsive nodes. The drawback of this method is that it detects only black hole attack.

2.2 Energy Based Trust Solution For Detecting Selfish Nodes In MANET Using Fuzzy Logic

This system will determine whether the distrusted node is strictly a malicious node or not. The proposed system has four modules to detect the malicious node which are supervisor, aggregator, trust calculator and disseminator. In supervisor module, neighbors will be monitored with the help of PACK (passive acknowledgement) system that analyze whether the nodes really forward the packets or not through keenly listening to their communication. If there is any deviation from normal behavior it invokes an aggregate module. This module calculates the number of packets dropped by nodes. And then the fuzzy based trust value will be calculated for nodes in fuzzy trust module. It has three components to calculate the trust value of each node - Direct trust value calculated by direct trust agent (DTA), indirect trust value calculated by indirect trust agent (IDTA), aggregator which uses DTA and IDAT to calculate the total trust value. Since fuzzy logic gives accurate result, the proposed system uses fuzzy logic to calculate the trust value of the target node. It also decides the trust value based on one single membership function [7]. The drawback of this system is the complexity of computation and it finds only the selfish nodes in the network. This method is not applicable to predict the type of attack.

2.3 Detection Of Black Hole Attack On AODV In MANET Using Fuzzy Logic

The proposed system consists of two major modules fuzzy parameter extraction and fuzzy computation. This system detects the black hole attack using two factors as forward packet ratio and destination sequence number. In the first module it monitors the network traffic and collects the data about forward packet ratio and average destination sequence number. Here the Forward packet ratio is defined as number of packets forwarded divided by number of packets received. In the second module fidelity level is computed. The Fidelity level is used to assure the malicious behavior of the node which ranges between zero and one. The fuzzy rule is applied for calculating the fidelity level. If forward packet ratio is low and average destination sequence ratio is low then fidelity level is low. The fidelity value zero shows that the node has malicious behavior and it will be compared with threshold value and the model decides the black hole attack [8]. This method doesn't finds more attacks which are available in the MANET network.

Forward Packet Ratio = Number of Packets forwarded / number of packets received

2.4 Intelligent Agent-Based Intrusion Detection System Using Enhanced Multiclass SVM

An intelligent agent is a self-determining entity which senses the environment continuously. Here the environment is Mobile Ad hoc Network and so that it can recognize the considerable amount of change in the environment. It will be used to detect the abnormal behavior of the node in network with the help of Support Vector Machine (SVM) classification technique and outlier detection. The proposed system is called as intelligent agent based feature selected hybrid classifier. And the valuable attributes will be selected by intelligent agent used in preprocessing of data. The classification is made by enhanced multicast support vector machine and distance between two classes will be calculated by Minkowski distance. In the module of intelligent agent based weighted outlier detection, it used to make the result more accurate. It can also give the result to the other possible attacks in MANET. The complication here is computational part [9].

2.5 Intrusion Detection In MANET Using Fuzzy Logic

The proposed system has two approaches to detect the black hole attack and gray hole attack towards destination, on AODV protocol in mobile ad-hoc network using threshold value and fuzzy logic methods. Both the methods detect the intruded node in network based on the number of packets dropped. In the first part of the authors work, IDS in each node monitors the network and make the data structure to store the details about the traffic. It will call the drive function to consequently update the data structure. Then two other data structures maintain the details about number of packets dropped towards source and destination. The number of dropped packets will be compared with threshold value. The selection of threshold value is the essential part of detection for intrusion in MANET. The author uses two threshold values to detect the intrusion in the network namely- threshold and DestThreshold values. If the total number of dropped packets and the node which drops the packet is greater than threshold value then the node will be invaded by black hole attack. In gray hole attack towards source, number of packets dropped by node which traverses from source and the total number of dropped packets should be greater than threshold value. The total number of dropped packets which traverses from source should be greater than DestThreshold value. In gray hole attack towards destination, number of packets dropped by node which traverses from source and the total number of dropped packets should be greater than threshold value. And the total number of dropped packets which is destined to particular destination should be greater than DestThreshold value. In fuzzy based approach it makes the same rules as symptoms [10] for different nodes which will determine the types of attack. Based on the set of symptoms, attacks and nodes, the system generates four types of indications

1. The occurrence indication
2. Conformability indication
3. Non-occurrence indication
4. Non –symptom indication

The comparative study of those indication matrices shows the node character and the type of attack in each node. The disadvantage of this method is it decides the attack on the node based on single membership function value. The result will be accurate when it is based on fuzzy. To make a proper detection and more accurate we use intuitionistic fuzzy [11] which uses at least two or more functions such as membership function, non-membership function and hesitation degree to decide the result.

Let A be the intuitionistic fuzzy set, x is a non empty set, Membership function and Non-membership function can be defined as

$$A = \{(x, \mu_A(X), v_A(X)) \mid x \text{ belong to } X)\}$$

Where degree of membership $\mu_{A:}$ X $\longrightarrow$[0, 1] and non membership $v_{A:}$ X $\longrightarrow$ [0, 1], element x belongs to the set A with $0 \leq \mu_A + v_A \leq 1$ for each x belongs to X

Hesitation Degree of x belongs to A is given by,

$\pi_{A\,=}\, 1\text{-}\, \mu_{A\,-}\, v_A$

3. SUMMARY OF REVIEWED INTRUSION DETECTION METHODS

Due to the remarkable characteristics of mobile ad-hoc network it is not possible to concentrate on all possible attacks since the attacks not only occur on single layer, it occurs in other layers such as network layer, transport layer and MAC layer. The IDS which have been discussed above focus on attack on particular protocol and decide the malicious behavior of nodes based on single parameter.

4. CONCLUSION

Recently many intrusion detection systems have been developed for mobile ad-hoc networks, Since MANET are used in many of the application like military operation, civil sectors, sensor network and metro scale broad band city network in the city of Cerritos. Considering the parameters with more valuable attributes which reduces the complexity of detection methods in terms of computational paradigm makes use of intuitionistic fuzzy which gives better result.

5. REFERENCES

[1] Aniruddha Chandra: "Ontology for MANET Security Threats", PROC. NCON, Krishnankoil, Tamil Nadu, Mar. 2005, pp. 171 -17 6.

[2] Abolhasan, Tadeusz Wysocki and Eryk Dutkiewicz: "A review of routing protocols for mobile ad hoc networks"

[3] Sunil Taneja & Ashwani Kush: "A survey of routing protocols in mobile ad hoc networks", International Journal of Innovation Management and Technology, Vol. 1, No. 3, August 2010.

[4] Davood Kheyri & Mojtaba Karami: "A comprehensive survey on anomaly based intrusion detection in MANET", Computer and Information science: Vol. 5, No. 4; 2012.

[5] Sandip Sonawane, Shailendra Pardeshi and Ganesh Prasad: "A survey on intrusion detection techniques", World Journal of Science and Technology 2012, 2(3): 127-133.

[6] Poonam Yadav, Rakesh Kumar Gill and Naveen Kumar: "A fuzzy based approach to detect black hole attack", International Journal of soft computing and Engineering, ISSN: 2231-2307, volume-2, Issue -3, July 2012.

[7] Vijayan R, Mareeswari V and Ramakrishna K: "Energy based trust solution for detecting selfish nodes in MANET using fuzzy logic", International journal of research and review in computer science, vol.2 No.3, June 2011.

[8] Ekta Kamboj: "Detection of black hole on AODV in MANET using fuzzy", Journal of current computer science and technology, vol.1 Issue 6[2011]316-318.

[9] S.Ganapathy, P. Yogesh, and A.Kannan: "Intelligent agent based intrusion detection system using enhanced multiclass SVM", Computational Intelligence and Neuroscience, volume 2012, article ID 850259.

[10] Monita Wahengbam, Ningrinla Marchang: "Intrusion detection in MANET using fuzzy logic", 2012 IEEE.

[11] Atanassov K. (1986): "Intuitionistic fuzzy sets, Fuzzy Sets and Systems", 20 (1986) 87-96.

[12] Eulalia Szmidt, Janusz acprzyk:"Intuitionistic Fuzzy Sets in Some Medical Applications", Fifth International conference on IFSs, Sofia, 22-23 Sept. 2001.

[13] John A. Clark, John Murdoch, John A. McDermid, Sevil Sen, Howard R. Chivers, Olwen Worthington, and Pankaj Rohatgi:"Threat Modelling for Mobile Ad Hoc and Sensor Networks.", in Annual Conference of ITA *(2007).*

[14] Ashwani Garg and Vikas Beniwal:"A review on security issues of routing protocols in mobile ad-hoc network.", International Journal of Advanced Research in Computer Science and Software Engineering 2.9 (2012): 171-176.