VOL. 11, NO. 7, APRIL 2016 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

EFFECTIVE INTRUSION DETECTION SYSTEM DESIGN USING GENETIC ALGORITHM FOR MANETs

R. Thanuja and A. Umamakeswari
Department of Computer Science Engineering, SASTRA University, SASTRA University, Thanjavur, India
E-Mail: thanuja.r@cse.sastra.edu

ABSTRACT

Wireless networks nowadays play an important role in day today's life. Every person wants to use the wireless networks for their daily routine work. The number of attacks seems to be increasing in nature day by day in Mobile Adhoc Networks (MANETs). In this paper we are going to design a three stage hybrid framework for IDS/IPS for MANETs. A new hybrid IDS/IPS is designed using evolutionary based scheme using genetic algorithm that is used to detect unknown types of attacks. The anomaly based technique will learn new patterns when abnormal traffic characteristics are observed in the network. This method is designed in such a way it can able to detect not only signature based attacks but also capable to detect unknown attacks in MANETs.

Keyword: security, MANETs, hybrid approach, IDS/IPS, genetic algorithm.

1. INTRODUCTION

Mobile Ad-Hoc Networks are stated as autonomous and decentralized wireless communication system. Any node in the network can join or leave at any time. Nodes may be mobile phone, laptop, PDA…etc which are in mobile in nature. The nodes can act as router or host machine at the same time in communication. They can form dynamic topology since the nodes are to be considered as moving in nature. The nodes have the capability of reconfiguring feature and they are able to configure depending upon the environment characteristics.

Security plays a vital role in Mobile Ad-Hoc Network since communication is done on open medium. The network is characterized by node availability, life time of node, confidentiality and integrity of the data can be achieved by using pro active measures. MANETs is pruned to attack since its feature like open medium, changing its topology dynamically, lack of central monitoring and management, cooperative algorithms and no clear defence mechanism. These factors are considered while designing the battle field situation for the MANETs against the security threats. The MANETs work on a decentralized zone since the nodes communicate with each other on the basis of mutual trust. This feature makes MANETs more vulnerable to be exploited by an intruder in the network. Wireless links signal leakage also makes the MANETs more vulnerable to attacks, which make it easier for the intruder to get access in the network in a easy manner.

Secure way of communication and transmission is a challenging task in MANETs since number of attacks goes on these two parameters. Security cannot be achieved to the core, but to a limited point where secure communication and transmission can be achieved in a effective manner. The designers must understand types of attacks and their damage on the network. List of attacks include Wormhole attack, Black hole attack, Sybil attack, flooding attack, routing table overflow attack, Denial of Service (DoS), selfish node misbehaving, impersonation attacks cause severe damage to networks. A MANET is more open to these kinds of attacks because communication is based on mutual trust between the nodes, there is no central point for network management, no authorization facility, dynamic changing topology and limited resources.

2. LITERATURE REVIEW

Vivek K. Kshirsagar, Sonali M. Tidke and Swati Vishnu [1] discussed a genetic based method to find the attacks in manets, but it is limited to signature based detection. Aarcha Anoop, Sreeja M. S [2] presented a genetic based system that perform detections mainly on classification of network based attacks but fail to detect any unknown attacks.

M.Crosbie and E. Spafford, [3] applied the multiple agent technology and GP to detect any unknown activities. Agent can monitor parameter of the network based on audit data received from the nodes. The agents are identified in the network by using GP that collectively determine anomalous network behaviors.

The advantage of using this method relays on many small autonomous agents, but the communication among them is still a problem. The training process of each node in the network can be time-consuming, since each node has to be trained in the initial stage setup of network.

Li [4] propose a genetic based method to detect anomalous network behaviors. The rules are derived using network behavioral model and parameters based on network attacks. This method is not suitable because of increases detection rates and false positives.

Xiao *et al*. [5] present an approach that uses Genetic algorithm to detect attacks in the network. The correlation relationship between network characteristics and intrusion types are used in a small number of networks to identify attacks. A linear rule is derived using both characteristic features and genetic algorithms are implemented in the node. The use of combined result reduces the complexity of GA, and the single resulting linear equation makes intrusion detection efficient in real-time environment.

Marti *et al* [6] uses a watchdog and pathrater mechanisms in network to monitor any abnormal behaviour. They identified the nodes which are not able to transfer packets to correct destinations. This method eliminates such nodes from routing in MANETs that will slowdown the network performance.

Changes were proposed to (DSR) protocol [7] to monitor the routing process in the watch dog and pathrater mechanisms. Number of packets dropped is calculated for each node that will be considered as a parameter to detect any attacks. The network is monitored based on threshold value and alters the manager if they found any attacks.

Ahmed *et al* [8] proposed a technique based on intrusion detection based on genetic algorithm. The leader in the network is elected using parameters that are used to monitor any abnormal behaviour. The messages that are to used to tell any type of attacks are passed through a encryption channel and it will create additional overload.
Rajaram and palaniswami [9] proposed a technique based on model created by trust based mechanism which uses Medium Access Control. Advantage of this technique includes packet authentication and security over routing protocols.

Su *et al* [10] proposed cooperative IDS to detect suspicious activity using neighbour nodes monitoring. It is identified by the number of such suspicious packets sent by a node exceeds a threshold; the monitoring node broadcasts an alert message to all nodes in the network used to alert the network. The alert message is first authenticated with the id of the monitoring node and carries information indicating the malicious node.

Overview of ids/ips techniques

The IDS system is an effective method to detect all types of attacks in a network. Intrusion detection systems can be run on each mobile node to check local traffic and detect local intrusions. These nodes can communicate local intrusion information to each other as and when needed. Figure-1 show the local model of intrusion detection system. Each node has local IDS that by this, node can connect to network and local IDS checking all send or receive data in/out node. Other technique is to run intrusion detection system for self and neighbour nodes to check for malicious neighbour. The global intrusion detection system can be deployed for clusters of mobile nodes where head node is responsible for global intrusion detection for its cluster.

Two types of attacks exist on the MANETs. They characterized attacks to passive and active. The passive attacks typically involve only eaves dropping of data, whereas the active attacks involve actions performed by adversaries such as replication, modification and deletion of exchanged data. In particular, Attacks in MANET can cause congestion, propagate incorrect routing information, prevent services from working properly or shutdown them completely.

The existing IDS architectures for MANETs fall under three basic categories (a) stand-alone, (b) cooperative, and (c) hierarchical.

(i) Stand-alone architectures have every node performs IDSs locally without collaborating and respond locally. This IDS architecture has a drawback for network attacks. There limitation is in terms of detection accuracy and the type of attacks that they detect.

(ii) In cooperative architecture all nodes in MANET have their own local IDS system. Nodes come to a decision in a distributed fashion cooperatively. Upon determination of an intrusion, nodes share this information, asset attack risk degree and take necessary actions to eliminate the intrusion using active or passive precautions. At the same time, all the nodes participate in a global detection decision making. This is more suitable to a flat MANET.

(iii) Hierarchical architectures use a multilayer approach, by dividing the network into clusters. Specific nodes are selected (based on specific criteria) to act as cluster-heads and undertake various responsibilities and roles in intrusion detection, which are usually different from those of the simple cluster members The main advantage of this architecture is effective use of constraint resources but has a drawback for highly mobile MANETs for establishing zones and detecting responsible nodes in clusters

3. IDS ENGINE

IDS engine is responsible for detecting local intrusions using local audit data. The local intrusion detection is performed using a classification algorithm. Firstly, it performs the appropriate transformations on the selected labeled audit data. Then, it computes the classifier using training data and finally applies the classifier to test local audit data in order to classify it as “normal” or “abnormal”.

Zone-based intrusion detection for mobile ad hoc networks

This method is based on Markov Chain based local anomaly detection model, including feature extraction, data pre-process, detection engine construction, and parameter tuning. The whole network is divided into non- overlapping zones. There are two categories of nodes in ZBIDS, if one node has a physical connection to a node in a different zone; this node is called a gateway node. Otherwise, it is called an intra-zone node. Only gateway nodes can generate alarms. They collect the local alerts broadcast from the intra-zone nodes and perform aggregation and correlation tasks to suppress many falsified alerts. For avoid of the single point of failure, if exist more than one gateway node in a single zone, all of which perform the alert aggregation task simultaneously. The functionality of Local Aggregation and Correlation Engine (LACE) is to locally aggregate and correlate the detection results of detection engines. Global Aggregation and Correlation Engine (GACE) in gateway nodes is to aggregate and correlate the detection results from local nodes in order to make final decisions. They can also cooperate with neighbour gateway nodes to further exchange information. After an attack is identified, based

on different attack types, the Intrusion Response Module (IRM) could take corresponding measures, such as identifying the intruders, reinitiating the communication channels, and excluding the compromised nodes from the networks.

Intrusion detection in mobile ad hoc networks using classification algorithms

In this approach intrusion detection models are designed and tested for MANETs using supervised classification algorithms that are used in advanced systems. The modern techniques uses this IDS architecture composed of multiple local IDS agents which are responsible for detecting possible intrusions in the network. The usage of Multilayer Perceptron (MLP), the linear model, the Gaussian Mixture model (GMM), the Naive Bayes model and the SVM model are used for classification of rules. All these models are to be trained for data set in the initialization stage. The trained data is given as input to the system. The data collected from multiple independent IDS agents forms the IDS system for the MANET. The local ID agent consists of the following items: Data Collector: Selection of local audit of network logs and data. Intrusion Detection Engine: is used for detection of attacks using audit data. The local intrusion detection is executed using a classification algorithm that act as a classifier. Response Engine is used to alter the network depending upon the event received from the attacks.

All the existing IDS techniques are failed to detect any unknown type of attacks that can occur in Manets.

Disadvantage of existing IDS

(i) High false positive rate (good packets are treated as bad ones)

(ii) Fail to detect multiple attacks at the same time

(iii) Detection rate is not very fast.

(iv) IDS algorithms run on specified routing protocols only.

4. MATERIALS AND METHODS

Evolutionary algorithms are based on computational models of fundamental evolutionary processes such as selection, recombination and mutation. Individuals, or current approximations, are encoded as strings composed over some alphabet(s), e.g. binary, integer, real- valued etc., and an initial population is produced by randomly sampling these strings. Once a population has been produced it may be evaluated using an objective function which characterizes an individual's performance in the problem domain.

The objective function is also used as the basis for selection and determines how well an individual performs in its environment. A fitness value is then derived from the raw performance measure given by the objective function and is used to bias the selection process. Highly fit individuals will be assigned a higher probability of being selected for reproduction than individuals with a lower fitness value. Therefore, the average performance of individuals can be expected to increase as the fitter individuals are more likely to be selected for reproduction and the lower fitness individuals get discarded.

Selected individuals are then reproduced, usually in pairs, through the application of genetic operators. These operators are applied to pairs of individuals with a given probability and result in new offspring that contain material exchanged from their parents. The offspring from reproduction are then further perturbed by mutation. These new individuals then make up the next generation. These processes of selection, reproduction and evaluation are then repeated until some termination criteria are satisfied, e.g. a certain number of generations completed, a mean deviation in the performance of individuals in the population or when a particular point in the search space is reached.

```
Procedure GA
{
        y = 0;
    Initialize P(y);
    Evaluate P(y);
  While not finished do
{
        y = y + 1;
 Select P(y) from P(y-1);
 Reproduce pairs in P(y);
    Mutate P(y);
    Evaluate P(y);
        }
    }
```

Figure-1. Overview of GA procedure.

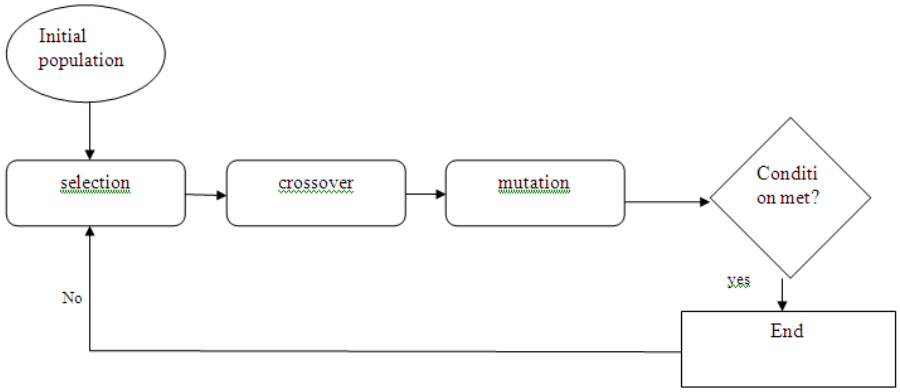

Figure-2. Genetic algorithm initial operation.

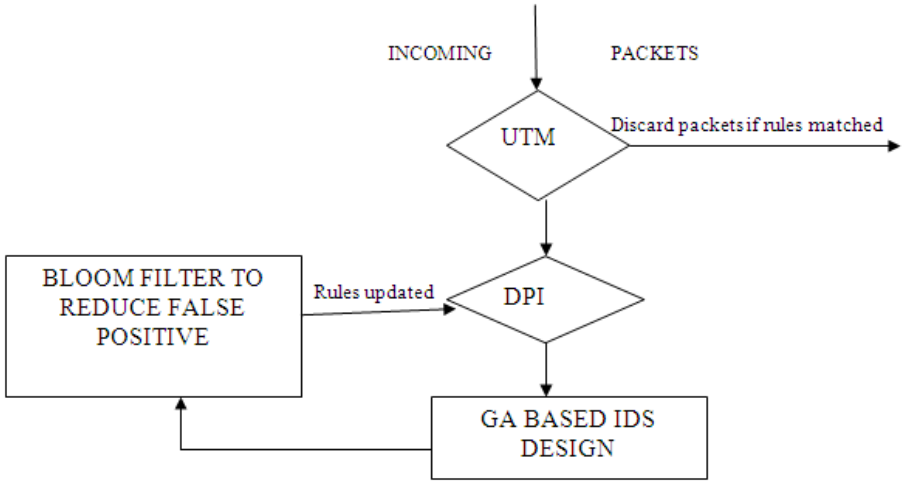

Figure-3. Proposed GA based IDS/IPS.

In our proposed techniques incoming packets from networks are sent through a Unified threat model (UTM), which checks for any malicious activity based on header sections of packets. If there is any malicious packet found then it discarded the bad packets and sends to second level of security measures.

The following steps will be followed to detect any unknown type of attacks that can occur in Manets.

Step 1: In first level security, the incoming packets are checked under UTM. The UTM check the packets only by its header format. If it is malicious it will discard the packet and pass the original packets to the second level.

Step 2: Since the first level will discard the packets only by header format. So there is chance of malicious packets travelling through the next level, so in DPI the byte wise operation of packet checking is done.

Step 3: Then the packets are send to the Bloom filtering, here the concept of Genetic Algorithm is implemented. The UTM or DPI would discard the packet that only matches the training set in Bloom filter. The updating the training set is main concept of discarding the malicious packets.

Step 4: The affected packet are sent to the process of genetic algorithm. Then the affected packet is checked with the parent packets that are already stored in training set. In comparing process bit pattern analysis is done, it checks over bit by bit. The next process is tolerance input which was set by user that used for comparing process. Then the last process ends with decision for selecting packets. The genetic algorithm will run the above process for k-iterations.

Step 5: Then the result will be added with the training data which then updates the UTM for first level of checking.

5. RESULTS AND DISCUSSIONS

1. False positive rate is reduced: Genetic algorithm help us to reduce false positive rate. This is achieved by usage of bloom filters that will be used to design the training set of IDS. Training set will contain

patterns of attacks that are compared with incoming ones. Tuning of training set will be updated by comparing with parent packets received from the UTM.

2. Multiple attacks can be detected at the same time: In our proposed technique, IDS engine can be able to detect simultaneous attack that can occur in the network. Traditional IDS are able to detect only single at a time.

3. Detection of unknown attacks: Proposed IDS is able to detect unknown attacks with a fast detection rate. GA is used to identify the new type of attacks which is updated as new training set in the bloom filters techniques.

4. Ga Based IDS can be run on all type of routing protocols: Traditional algorithms are able to run on specific type of routing protocols such as AODV, DSR etc.. Our new design of IDS/IPS algorithm will be able to run on all type of routing protocols such as static, dynamic or hybrid mode.

6. CONCLUSIONS

In this paper we are to design a GA based IDS/IPS which will be helpful for MANETs to detect any unknown type of attacks. This method also has the advantage over traditional IDS mechanism such as fast detection rate, reducing false positive rate, multiple attack detection at the same time and able to run on any type of routing strategy. In our future work a test bed will be created and IDS algorithm is implemented for which results are to be compared with traditional IDS mechanisms.

REFERENCES

[1] Vivek K. Kshirsagar, Sonali M. Tidke and Swati Vishnu. 2012. Intrusion Detection System using Genetic Algorithm and Data Mining: An Overview. International Journal of Computer Science and Informatics. 1(4).

[2] Aarcha Anoop, Sreeja M. S. 2013. New Genetic Algorithm Based Intrusion Detection System for SCADA. International Journal of Engineering Innovation and Research. 2(2).

[3] M.Crosbie and E. Spafford. 2012. An implementation of intrusion detection system using genetic algorithm. International Journal of Network Security and Its Applications (IJNSA). 4(2).

[4] W. Li. 2004. A Genetic Algorithm Approach to Network Intrusion Detection. SANS Institute, USA.

[5] T. Xia, G. Qu, S. Hariri, M. Yousif. 2005. An Efficient Network Intrusion Detection Method Based on Information Theory and Genetic Algorithm. Proceedings of the 24th IEEE International Performance Computing and Communications Conference (IPCCC '05). Phoenix, AZ, USA.

[6] S.Marti, T.J. Giuli, K.Lai, M. Baker. 2000. Mitigating routing misbehaviour in mobile adhoc networks. The 6th ICMCN. pp. 255-265.

[7] D.B. Johnson, D.A. Maltz, J. Broch. 2001. DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks, Addison-Wesley.

[8] S. Ahmed. 2012. An Effective Intrusion Detection System for Detection and Correction of Gray Hole Attack in MANETs. IJNS.

[9] A. Rajaram, S. Palaniswami. 2010. Malicious node detection system for mobile adhoc networks. JCSIT International Journal of Computer Science and Information Technologies. 21): 77-85.

[10] Y.Su. 2011. Prevention of selective black hole attacks on mobile adhoc networks through intrusion detection systems. Computer Communications. 34(1): 107-117.