Intrusion Detection for MANET to Detect Unknown Attacks Using Genetic Algorithm

M. Lalli
Department of Computer Science
Bharathidasan University
Trichy, India
Lalli_bdu@yahoo.co.in

V. Palanisamy
Department of Computer Science and Engineering
Alagappa University
Karaikudi, India
vpazhanisamy@yahoo.co.in

Abstract— **Traditional intrusion detection have a trouble dealing with lack of secure boundaries, threats from compromised nodes, lack of centralized management facility, restricted power supply and scalability. Due to these issues, we are motivated to propose efficient IDS, which involve a new technique to identify the anomalous activities in mobile ad-hoc networks. During this paper, we propose a Genetic based feature selection and rule evaluation process for anomaly detection. This process is effectively classified with new rules and also increases with high positive rate alarm. The new findings of our proposed work is effectively notice the anomalies with low false positive rate, high detection rate and attain the upper detection accuracy.**

Keywords—IDS, Genetic, MANET, Anomaly Detection, Feature Selection.

I. INTRODUCTION

A mobile ad-hoc network (MANET) may be a multi hop wireless network, wherever nodes communicate with one another with none pre-deployed infrastructure. With the absence of pre-established infrastructure, (e.g. no router, no access purpose, etc.) two nodes communicate with each other in a very peer-to-peer fashion. Whenever the two nodes communicate directly within the transmission, it will vary of every different node. Otherwise, nodes will communicate via a multi-hop route with the cooperation of different nodes. In Mobile Ad-hoc network, it has a self-creating, self-organizing and self-administrating capability. Examples embrace field of honor situations, disaster relief and short situations like public events [1]. The frequent changes in topology, scarce information measure, restricted storage and process capability of MANETs have spread out many challenges for network researchers. One in all the necessary challenges is to produce a support for time period multicast communication[2].

Mobile ad hoc networks have recently been the subject of in depth analysis. The interest in such networks stems from their ability to produce temporary and instant wireless networking solutions in particular time period, wherever cellular infrastructures area unit are lacking and it was impossible to deploy. Despite their fascinating characteristics, very important issues regarding their security should be solved so as to understand their full potential. In MANETs, the nodes themselves implement the network management in an exceedingly cooperative fashion and so, all of them area unit is accountable for this. MANET nodes have stringent resource constrains and they are typically mobile, forming a highly dynamic network topology, absence of any clear network boundaries. As a result, MANETs area unit prone to a range of attacks like eavesdropping, routing, packet modification, etc. And securing a MANET under such conditions is challenging. In various security controls, like the utilization of secret writing and authentication techniques, are projected to assist the risks of intrusion, but since such risks can't be fully eliminated there is a powerful need for intrusion detection systems for ad hoc network security. Whereas accuracy is that the essential demand of ad associate intrusion-detection system(IDS), its extensibility and flexibility are also important in today's network computing environment. Currently, building effective IDS is a massive engineering task.

The intrusion detection engines employed in MANETs are categorized into two main types (i) Signature based detection and (ii) Anomaly-based detection. Signature-based engines have a predefined set of patterns (signatures) to detect known attacks[3]. The signature is stored in a database and if the engine matches a monitored activity with a signature, then the activity is marked as malicious. This type of engines fails to detect novel attacks and requires always maintaining a signature database.

The anomaly-based engines are created a specific models of nodes' behaviors (normal profiles) and to detect that this nodes are deviated from these profiles which are known as malicious[4]. This type of engines can detect unknown attacks and does not require a, it database. However is prone to high rates of false alarms, since any legitimate behavior that deviates from normal profiles is also considered as malicious.

Taking into consideration the deployment environment of MANET and its limitation, it is evident that the process overhead is intercalary by the IDS architectures to the underlying network nodes should be kept minimum. However, almost all the cooperative IDS architectures, one or more additional detection engines (which are based on signature or anomaly detection) are used in each node, while not considering the restricted process capabilities. The hierarchical

978-1-4799-3972-5/14/$31.00 ©2014 IEEE

IDS architectures attempt to minimize the process overhead by comprehensive or multilayer detection engines only at some key nodes (i.e., cluster-heads), whereas the remaining nodes use light-weight engines[5]. However, the creation and maintenance of clustered/hierarchical structures adds additional process load to the network nodes. Moreover, in these architectures the relative high nodes' mobility, experienced in MANETs, can also increase the process loads of the nodes. In each cooperative and hierarchical IDS architectures[6], nodes need to exchange alerts, audit data, and detection results that impose additional communication overhead to the underlying network supported review, we tend to planned a unique intrusion detection framework for MANET.

II. RELATED WORK

Mohammad Sazzadul Hoque[7] by applying genetic algorithm (GA) to efficiently detect various types of network intrusions. Parameters and evolution processes for GA are discussed in detailed manner was implemented. This approach uses evolution theory to information evolution in order to filter the traffic data and thus reduce the complexity.

R.H. Gong[8] discuss about GA primarily based approach for network intrusion detection, that comes a collection of classification rules and it support-confidence framework to evaluate the fitness function.

T. Xia[9] explained the GA to detection the anomalous behaviors based on the information theory. B. Abdullah [10] used a GA based performance evaluation function for network intrusion detection. This method utilizes information theory for filtering the traffic data. GA based formula used to classify all kinds of attacks exploitation by trained dataset with terribly low false positive rate and to convey correct detection rate [11].

This paper is structured as follows; Section II provides the review of a background work. In Section III, we tend to discuss regarding the Genetic based feature selection and evaluation process. The simulation results are discussed in Section IV. Section V provides the outline of our work.

III. PROPOSED WORK

Our proposed detection method was to classify the packets[12], and evaluated with rule based process and Genetic algorithm for unknown attack detection and making alarm units.

A. Genetic based Feature selection and Rule Evaluation

In different ways in which Genetic Algorithm rule will be employed in Intrusion Detection System, the IDS will be illustrated as rule based and to generate knowledge for the RBS GA is used as tools. Feature selection is that the method of choosing vital options from the big data set. The chosen features are relevant to the detection method. GA-based Feature selection algorithm rule relies is on the wrapper model. The purpose of applying GA to intrusion detection was to develop a knowledge base and define rule for detection of intrusion.

B. Features Definition in IPv6 support packets

Evaluation of intrusion detection approaches for finding new attacks is a vital and multi-faceted problem. Following steps are concerned in GA application:

- At the beginning of a run of a GA, a large population of random genes is made. Everyone represents a dissimilar solution to the problem. Within the initial population there are N chromosomes, and then the subsequent steps are repeated until a solution is found.
- Each and every chromosome is examining for the betterment, and allots a fitness score consequently.
- From this population two members are selected. The possibility of being selected is proportional to the chromosomes fitness. Normally Roulette wheel selection method is used.
- According to the crossover rate, the bits from every opted chromosome are crossover randomly at chosen point.
- Step through the selected chromosomes bits and flip reliant on the mutation rate.

Features for GA

- land Flag to spot whether connection is from/to the similar host/port
- wrong fragment Number of wrong fragments within the connection.
- synflood Connections that have "SYN" errors.
- num compromised Number of compromised constraints.
- same srv rate Percentage of connections to the similar services.
- diff srv rate Percentage of connections to dissimilar services.
- count Number of connections from the similar source host to the similar destination host.
- srv count Number of connections from the similar source service to the similar destination service.
- dst host count Number of connections from the similar destination host to the similar source host.
- dst host srv count Number of connections from the similar destination service to the similar source service.

C. Algorithm for our System

Our system is divided into two main sections: the pre-calculation section and also the detection section. In that pre-calculation section, collection of chromosome is created by set of training data. That chromosome sets are utilized in the next section for the purpose of comparison. The primary steps in pre-calculation as,

Algorithm : Initialize chromosomes for evaluation
Input : Network audit information (for training)
Output : A collection of chromosomes

1. Range = 0.125
2. For every training information
3. If it has any nearest neighbor chromosome within Range
4. Combine it with the adjacent chromosome
5. Else
6. Generate a new chromosome
7. End if
8. End for

The second one is a detection section, where a population is generated for a test data and going through some analysis process (selection, crossover, mutation) and also the type of test data is predicted. The pre-calculated set of chromosome is employed during this section and finds the fitness of each chromosome of entire population.

Algorithm : Envisage the data or intrusion type (using Genetic Algorithm)
Input : Review Network auditing data (for testing), Pre-calculated set of chromosomes
Output : Various type of informations.

1. Set the overall population
2. CrossoverRate equal to the range of 0.15, MutationRate equal to the range of 0.35
3. While the number of generation is not attained
4. For every chromosome in overall population
5. For every pre-calculated chromosome
6. Get the fitness
7. End for
8. Assign optimum fitness. The fitness of that chromosome
9. End for
10. Eradicate some chromosomes with worse fitness
11. Apply crossover to the chosen pair of chromosomes of the population
12. Apply mutation to each and every chromosome of the population
13. End while

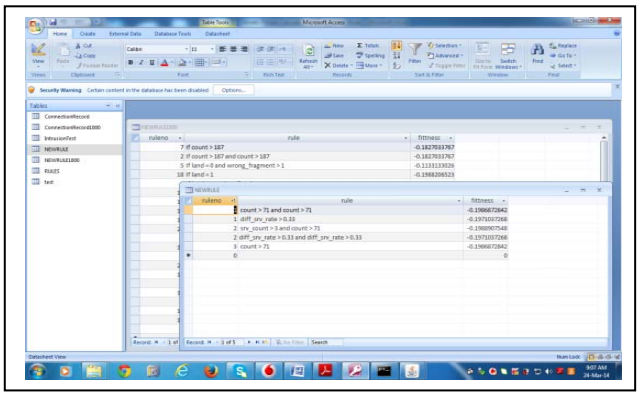

Fig. 1 New Rules Generated from Genetic

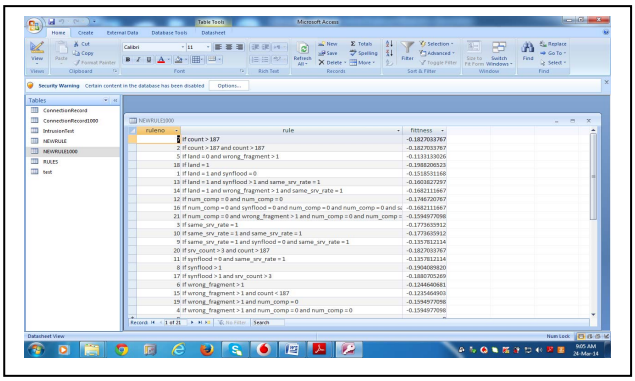

Fig. 2 Overall Rules from Expects

After funding the fitness function, a new rule evaluated via genetic process[13]. GP is used to find the unknown attacks, which is predicted on some assumptions based new rules in Fig. 1. It gives a healthier performance than initial ones, based on known attacks. The new rules are not only covering the known attacks, but also it finds the novel ones which is shown in Fig. 2. According to the Fitness calculation we use GP to get the new Rules for IDS in Fig. 3.

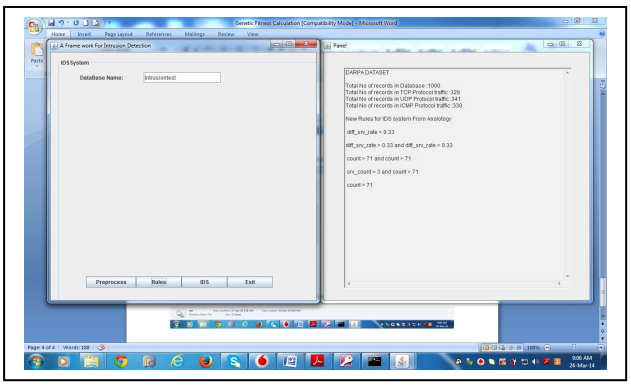

Fig. 3. Fitness Calculation and New Rules Generated from Genetic

IV. Simulation Results and Discussions

Simulators measure the foremost common tools used for validating MANET intrusion detection systems [14,15]. We use Ad hoc On Demand Distance Vector (AODV) [16], one amongst the popular MANET routing algorithms, which is a network routing protocol. The simulation nodes having identical transmission range of 200 meters with channel capacity of 2000 bps. Distributed Co-ordination Function (DCF) of IEEE 802.11 for wireless LAN as a MAC layer protocol. During the simulation period, 30 mobile nodes are set to be in motion, with in the space of 500 x 500 meters. To simulate the mobility of a node, we utilize the Random Waypoint model (RW). All the nodes are set to travel autonomously with similar average speed.

In our proposed work, 10 source nodes and 10 destination nodes are selected randomly, to come up with Constant Bit Rate (CBR) traffic as background traffic. The broadcast rate is

2 packets per second, and the packet size is 512 bytes. In our simulation, so as to provide the nodes enough time to complete the warm up time of 400 seconds. During this time period, the data is validated in three sampling periods: 10 seconds, 30 seconds, and 60 seconds. Select the proper set of features is essential, when formulating the classification process. The features are designated as a sensitive feature and it is supported in the confidence measure of our proposed work. Even though some features provide high confidence for ordinary prediction or for abnormality prediction. The proposed work, evaluate the network performance of Black Hole Attack and Dropping Routing Traffic Attack according to the following metrics'.

***Packet delivery ratio*:** It is defined that the ratio between the number of packets transmitted by a traffic source and the number of packets received by traffic sink is shown in Fig. 4.

$$PDR = N1 / N2 \quad (1)$$

Where, N1 is the sum of data packets received by each destination and N2 is the sum of data packets generated by each source.

End-to-end delay: Delay is the distinction between the time at which the sender generated the packet and the time at which the receiver received the packet is shown in Fig. 5.

$$EED = T / N \quad (2)$$

Where, T is the average time spent to deliver the packets for every destination and N is the number of packets received by all the destination nodes.

Control overhead: Control overhead is defined as the total number of routing packets transmitted over the network in terms of packets/second. High control overhead may adversely affect delivery ratio.

Authentication delay: The average request processing and verification delay for security.

Detection rate (DR) is outlined as the ratio between the number of appropriately detected intrusions and the total number of intrusions.

$$DR = TP / (TP + FN) \quad (3)$$

False positive rate (FPR) is deliberate as the ratio between the numbers of normal connections that are incorrectly classifies as intrusions and the total number of normal connections.

$$FPR = FP / (FP + TN) \quad (4)$$

The value of the delivery in our detection rate is increasing, even once when the maximum node request is increases. According to the categorization with GA, 95% of the packets are reach the destination perfectly. The delivery ratio decreases drastically. Packet delivery ratio variation is between 5% - 7%, at higher requests the slit in packet delivery ratio starts widening.

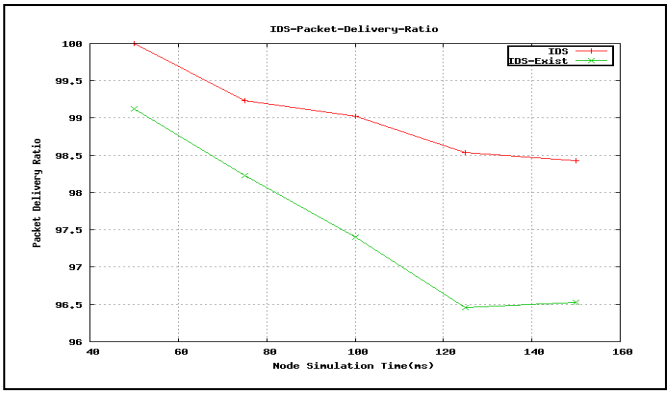

Fig. 4 IDS- Packet-Delivery Ratio

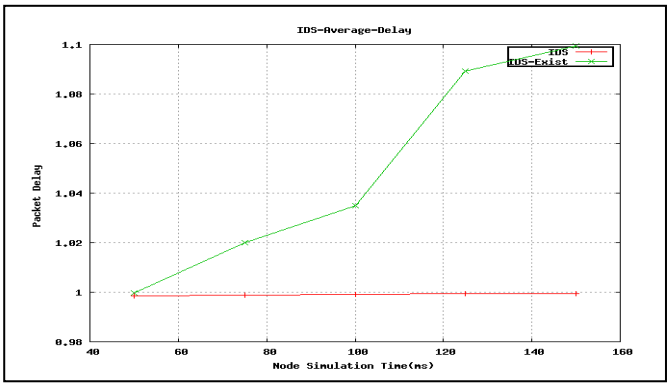

Fig. 5 IDS- Average Delay Ratio

V. CONCLUSION

In this paper, a Genetic based feature selection and rule evaluation process is used to achieve effective intrusion detection. The proposed algorithm have a new detection approach for two common attacks, Dropping routing traffic attack, Black hole attack to evaluate the performance of our IDS. The experimental results for the proposed model can effectively detect anomaly with low false positive rate, high detection rate with higher detection accuracy.

REFERENCES

[1] Farhan Abdel-Fattah," Distributed and cooperative hierarchical intrusion detection on MANETs" International Journal of Computer Applications (0975 – 8887) Volume 12– No.5, December 2010

[2] Christoforos Panos,"A Novel intrusion detection system for MANETS", International Conference on Security and Cryptography, July 2010.

[3] Marianne A. Azer, Sherif M. E1-Kassas, Magdy S. E1-Soudani, " A survey on anomaly detection methods for ad-hoc networks", Ubiquitous Computing and Communication Journal, Volume 2, Number 3, Page 42.

[4] Yongguang Zhang and Wenke Lee, " Intrusion detection in wireless adhoc networks", In Proceedings of the 6th annual international conference on Mobile computing and networking, MobiCom '00, pages 275–283, New York, NY, USA, 2000. ACM.

[5] Patrick Albers, Olivier Camp, Jean marc Percher, Bernard Jouga, and Ricardo Puttini, "Security in ad hoc networks: a general intrusion detection architecture enhancing trust based approaches", In Proceedings of the First International Workshop on Wireless Information Systems (WIS-2002, pages 1–12, 2002.

[6] Yi-an Huang and Wenke Lee, " A cooperative intrusion detection system for ad hoc networks", In Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks, SASN '03, pages 135–147, New York, NY, USA, 2003. ACM

[7] Mohammad Sazzadul Hoque, Md. Abdul Mukit, Md. Abu Naser Bikas, " An implementation of intrusion detection system using genetic algorithm", International Journal of Network Security & Its Applications, Vol.4, No.2, March 2012.

[8] R. H. Gong, M. Zulkernine, P. Abolmaesumi, "A software implementation of a genetic algorithm based approach to network intrusiond etection", 2005.

[9] T. Xia, G. Qu, S. Hariri, M. Yousif, "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, 2005.

[10] B.Abdullah, I. Abd-alghafar, Gouda I. Salama, A. Abd-alhafez, "Performance evaluation of a genetic algorithm based approach to network intrusion detection sSystem", 2009.

[11] Anup Goyal, Chetan Kumar, "GA-NIDS: A Genetic Algorithm based Network Intrusion Detection System", 2008.

[12] M. Lalli, V. Palanisamy, "A novel intrusion detection model for mobile ad-hoc networks using CP-KNN", International Journal of Computer Networks & Communications (IJCNC) Vol.6, No.5, September 2014

[13] Dr.M.V.Siva Prasad," An intrusion detection system architecture based on neural networks and genetic algorithms" International Journal of Computer Science and Management Research

[14] D. Sterne, P. Balasubramanyam, D. Carman, B. Wilson, R. Talpade, C. Ko, R. Balupari, C y. Tseng, T. Bowen, K.Levitt, and J. Rowe. "A general cooperative intrusion detection architecture for manets", In IWIA 05: Proceedings of the Third IEEE International Workshop on Information Assurance (IWIA05, pages 57–70. IEEE Computer Society, 2005.

[15] W J Ulivla. Evaluation of intrusion detection system. J. J. Res. Natl. Inst. Stand. Technol., 108(6):453–473, 2003.

[16] Chin-Yang Tseng, Poornima Balasubramanyam, Calvin Ko, Rattapon Limprasittiporn, Jeff Rowe, and Karl Levitt, " Aspecification-based intrusion detection system for aodv", In Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks, SASN '03, pages 125–134, New York, NY, USA, 2003. ACM.