Implementation of Genetic Algorithm Using of Intrusion Detection System in Mobile Ad Hoc Networks

G.Sureshkumar[1], Divya Haridass[2], T.K.P.Rajagopal[3]
[1, 2] Dept of Computer Science Engineering
[3]Associate Professor, Dept of Computer Science Engineering
[1, 2, 3] Kathir College of Engineering, Coimbatore – 641062, Tamil Nadu, India

Abstract- *Mobile Ad hoc Networks (MANET) are self-configuring, infra structureless, dynamic wireless networks in which the nodes are resource constrained. Intrusion Detection Systems (IDS) are used in MANET to monitor activities so as to detect any intrusion in the otherwise vulnerable network. In this paper, we present efficient schemes for analyzing and optimizing the time duration for which the intrusion detection systems need to remain active in a mobile ad hoc network. A probabilistic model is proposed that makes use of cooperation between IDS among neighborhood nodes to reduce their individual active time. Usually, an IDS has to run all the time on every node to oversee the network behavior. This can turn out to be a costly overhead for a battery-powered mobile device in terms of power and computational resources. Hence, in this work our aim is to reduce the duration of active time of the IDS without compromising on their effectiveness. To validate our proposed approach, we model the interactions between IDS as a multi-player cooperative game in which the players have partially cooperative and partially conflicting goals. We theoretically analyze this game and support it with simulation results.*

Keywords- Ad hoc networks, Energy efficiency, Intrusion detection.

I. INTRODUCTION

A mobile ad hoc network (MANET) collection of mobile nodes which communicate with each other without the help of any fixed infrastructure or central coordinator. A node can be any mobile device with the ability to communicate with other devices. In a MANET, a node behaves as a host as well as a router. A node intending to communicate with another node that is not within its communication range, takes help of intermediate nodes to relay its message. The topology of the network dynamically changes over time as nodes move about, some new nodes join the network or few other nodes disengage themselves from the network. MANET have distinct advantages over traditional networks in that they can easily be set up and dismantled, apart from providing flexibility as the nodes are not tethered. One important application scenario is vehicular ad hoc network (VANET). VANET is a self-configuring network of moving vehicles (i.e., a vehicle is a node) although the movement pattern of nodes are restricted by the road course, traffic regulations, etc. VANET is a promising technology that has tremendous potential to improve vehicle and road safety, traffic efficiency and convenience.

One way of providing security to a MANET is intrusion detection, a process of monitoring activities in the system so as to determine whether there has been any violation of security requirements. Intrusion Detection System (IDS) is the mechanism used by the nodes of a network for detection of intrusion and has been classified into two broad categories based on the techniques adopted, viz., (a) Signature-based intrusion detection and (b) Anomaly-based intrusion detection. In signature-based detection, knowledge about the signatures of attacks is incorporated in the detection system. At the occurrence of an attack, the characteristics of the attack are matched with the signatures included in the IDS. If there is a match, then an attack associated to that signature is said to have occurred. In anomaly-based detection, the IDS do not attempt to find a signature match but searches for anomalous events or behavior. For instance, it could look out for anomalous behavior such as dropping of data packets and events such as erratic changes in the routing table. IDS can also be categorized based on the audit data used for analysis. Host-based IDS make use of data obtained from the host for which it checks for intrusion detection. This kind of data could be operating system or application logs on the system. On the other hand, network-based IDS collect and analyze data from network traffic. In our work, we concentrate on network-based anomaly detection.

While a lot of research effort has been expended in Designing effective IDS, not much effort has been made on efficient employment of the IDS. In a resource-constrained environment, this is of utmost importance. We attempt to address this issue in our work. In most of the existing IDSs for

MANET, a detection system sits on every node, which runs all the time. One common mechanism used by such IDS is monitoring traffic in the node's neighbor hood. A node in a MANET may have limited battery power and computational resource, running an IDS all the time may turn out to be a costly overhead. Thus, the challenge is how to reduce the duration of time, an IDS needs to remain active without compromising on its effectiveness. This issue may not be much of a concern in a wired network, in which an IDS is deployed mainly in a stationary router or gateway, with virtually unlimited computational and battery power. But this is of significant concern in the case of MANET, where the mobile nodes themselves not only behave as hosts and routers, but also have to carry out other functions such as intrusion detection either collaboratively or individually. To this end, we propose a distributed scheme for efficient usage of IDS in a network based on probability theory.

Cooperative game theory can be used to model situations in which players coordinate their strategies and share the payoffs between them. The output of the game (individual payoffs that players receive) must be in equilibrium so that no player has incentive to break away from the coalition. The game settings in all the earlier game-theoretic work on IDS involve two sets of opposing players, the nodes/IDS and the attacker/defaulters. In our work, we have set a game that involves players (IDS sitting in neighboring nodes) cooperating to achieve a common goal (i.e., to monitor a single node). To the best of our knowledge, we have not come across any work on cooperating IDS (to get a security versus energy trade off) that models such a situation using game theory. We have presented such a cooperative multi-player game to model the interactions between the IDS in a neighborhood and used it to validate our proposed probabilistic scheme.

II. PROBLEM STATEMENT

We first present the minimization of the active duration of the intrusion detection system (IDS) in the nodes of a MANET as an optimization problem. The primary goal of the Intrusion Detection(IDS) is to monitor the nodes in its neighbor hood at a desired security level so as to detect any anomalous behavior, whereas, the secondary goal of the IDS is to conserve as much energy as possible. The main drawback of the existing system is more energy consumption and it is not possible in Heterogeneous Networks.

III. METHODOLOGY

For solving both constrained and un constrained optimization problems based on natural selection that genetic algorithm is proposed. For an each node finding a fitness value based on the network parameters are Data rate, Bandwidth and Overhead. If the fitness value is below the threshold value the performance of network is degrade. The high fitness value achieves a better network performance.

IV. ALGORITHM

4.1. Genetic Algorithm

The Genetic algorithm is a random selection of chromosomes which are representations of the problem to be solved. According to the attributes of the problem different positions of each chromosome are encoded as bits, characters or numbers. Genetic Algorithm is used to evolve rules for network traffic. The rules are used to normal network connections from anomalous connections. It refers to events with probability of intrusion.

if {Condition} then {act}

The current network connection is intrusion detection as source and destination IP addresses and port numbers used in are TCP/IP protocols duration. The connection protocol is indicating the probability of an intrusion. For the above condition we require source IP address, destination IP address, port number connection time and stop the connection. The final goal of genetic algorithm is match only to network intrusion connections. In genetic algorithm, the evaluation function is one of the most important parameters. The overall outcome is calculated based on whether a field of the connection matches the object in dataset and then multiply the weight of that field. Matched value is either 0 or 1.

$$\text{Outcome} = \sum \text{Matched} * \text{Weight}$$

All objects are representing destination IP address field have same weight. Destination IP address is the target of an intrusion while the source IP address is the originator of the intrusion.

V. CONCLUSION

In this paper we have proposed an efficient way of using intrusion detection systems (IDS) that sits on every node of a mobile ad hoc network (MANET). We first present the minimization of the active duration of the IDS in the nodes of a MANET as an optimization problem. We then described a cooperative game model to represent the interactions between the IDS in a neighbor hood of nodes. The game is defined in such a way that the primary goal of the IDS is to monitor the nodes in its neighborhood at a desired security level so as to detect any anomalous behavior, whereas, the secondary goal of the IDS is to conserve as much energy as possible. To achieve these goals, each of the nodes has to participate cooperatively in monitoring its neighbor nodes with a minimum probability. We then develop a distributed scheme to determine the ideal probability with which each node has to remain active (or switched on) so that all the nodes of the network are monitored with a desired security level. The evaluation of the proposed scheme is done by comparing the performances of the IDSs under two scenarios: (a) keeping IDS running throughout the simulation time and (b) using our proposed scheme to reduce the IDS active time at each node in the network. From the simulation results we observe that the effectiveness of the IDS in the network is not compromised while using the proposed scheme, rather, there is considerable reduction of energy consumption in each of the nodes that increases the network lifetime significantly. Here we have assumed a homogeneous network in a way that all the nodes have the same capacities in terms of their computational and energy resources. In future we wish to extend our model to accommodate a heterogeneous network.

REFERENCE

[1] N. Marchang and R. Datta, ”Collaborative Techniques for Intrusion Detection in Mobile Ad-hoc Networks,” Elsevier Ad Hoc Networks, vol. 6, no. 4, pp. 508-523, June 2008.

[2] T. Hoang Hai and E-N. Huh, ”Optimal Selection and Activation of Intrusion Detection Agents for Wireless Sensor Networks,” Proc. Future Generation Communication and Networking (FGCN 2007),vol.1, no., pp.350-355, 6-8 Dec. 2007.

[3] C. Manikopoulos and L. Ling, ”Architecture of the Mobile Ad-hoc Network Security (MANS) System,” Proc. IEEE International Conference on Systems, Man and Cybernetics, vol. 4, pp. 3122- 3127, October 2003.

[4] K. Nadkarni and A. Mishra, ”Intrusion Detection in MANETs - The Second Wall of Defense,” Proc. IEEE Industrial Electronics Society Conference ’2003, pp. 1235-1239, Roanoke, Virginia, USA, Nov. 2-6, 2003.

[5] S. M. Fitaci, K. Jaffres-Runser and C. Comaniciu, ”On modeling energy- security trade-offs for distributed monitoring in wireless ad hoc networks,” Proc. Military Communications Conference, 2008. MILCOM 2008. IEEE , vol., no., pp.1-7, 16-19 Nov. 2008.

[6] A. Afgah and S. K. Das and K. Basu, ”A Non-cooperative Game Approach for Intrusion Detection in Sensor Networks,” Proc. VTC 2004, Fall 2004.

[7] A. Partwardan, J. Parker, A. Joshi, M. Iorga and T. Karygiannis, ”Secure Routing and Intrusion Detection in Ad-hoc Networks,” Proc. 3rd IEEE International Conference on Pervasive Computing and Communications, Hawaii Island, Hawaii, March 8-12, 2005.

[8] I. Khalil, S. Bagchi and N. B. Shroff, ”SLAM: Sleep-Wake Aware Local Monitoring in Sensor Networks,” Proc. 37th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, 2007
(DSN 2007), 565-574.

[9] N. Marchang and R. Datta, ”Lightweight Trust-based Routing Protocol for Mobile Ad Hoc Networks,” IET Information Security, vol. 6, no. 4, pp. 77-83, 2012.

[10] S. Marti, T. J. Giuli, K. La and M. Baker, “Mitigating Routing Misbehavior in a Mobile Ad-hoc Environment,” Proc. 6th Annual ACM/IEEE International Conference on Mobile Computing and Networking, pp. 255-265, August 2000.