Energy Efficient unauthorized Intrusion Detection in mobile Ad-Hoc Neworks

Ms.P.Rajeswari,M.E.
PG Student,CSE Department
Muthayammal Engineering College
Rasipuram, India
rajeswariit09@gmail.com

Prof.R.Vijayalakshmi,M.E.,(Ph.D.)
Professor and Head, CSE Department
Muthayammal Engineering College
Rasipuram, India
viji21076@gmail.com

***Abstract*—**Mobile Ad hoc Networks (MANET) are self-configuring, infrastructure-less, dynamic wireless networks in which the nodes are resource constrained. Intrusion Detection Systems (IDS) are used in MANETs to monitor activities so as to detect any intrusion in the network. The proposed system present efficient scheme 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 IDSs 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, this project aim is to reduce the duration of active time of the IDSs without compromising on their effectiveness. To validate this proposed approach, it models the interactions between IDSs as a multi-player cooperative game in which the players have partially cooperative and partially conflicting goals.

Keywords*-MANET, IDS, Active Time***

*****

I. INTRODUCTION

A Mobile ad hoc network (MANET) is a self-organized 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 MANET, a node behaves as a host as well as a router. A node intending to communicate with another node (i.e.) 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 [1]. MANETs have distinct advantages over traditional networks in that they can easily be set up and dismantled. Mobile Ad Hoc Networks (MANETs) is an emerging type of wireless networking, in which mobile nodes associate on an extemporaneous or ad hoc basis. MANETs are self-forming and self-healing, enabling peer-level communications between mobile nodes without reliance on centralized resources or fixed infrastructure [4].These attributes enable MANETs to deliver significant benefits in virtually any scenario that includes a cadre of highly mobile users or platforms, a strong need to share IP-based information and an environment in which fixed network infrastructure is impractical, impaired or impossible. Key applications include disaster recovery, heavy construction, mining, transportation, defense, and special event management. It should be noted that a key characteristic of such applications is that nearby sensor nodes monitoring an environmental feature typically register similar values. This kind of data redundancy due to the spatial correlation between sensor observations inspires the techniques for in-network data aggregation and mining. By measuring the spatial correlation between data sampled by different sensors, a wide class of specialized algorithms can be developed to develop more efficient spatial data mining algorithms as well as more efficient routing strategies. Also, researchers have developed performance models for MANET by applying queuing theory. All researchers have two categories of attacks on the MANETs. They are 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. General MANET attack categories are routing, multipart and performance. Example of routing attacks is Routing loop attack, Black hole attack, Link Withholding attack, Link Spoofing attack, Wormhole attack, Replay attack and Packet Modification/Insertion. Multipart attacks consist of Neighbor attack, Jellyfish attack. Example of performance attacks are DoS attacks, Sleep deprivation and Resource consumption attack. Numerous schemes have been proposed for secure routing and intrusion detection for ad hoc networks.

Intrusion Detection Systems Intrusion detection system (IDS) is an indispensable second line of defense since traditional prevention mechanisms are not strong enough to protect MANET. There are three main components of IDS: data collection, detection, and response [5]. The data collection component is responsible for collection and pre-processing data tasks, transferring data to a common format, data storage and sending data to the detection module. IDS have several highlight parts such as architecture, engine and watermarking techniques that are discussed below

IDS Architecture -The existing IDS architectures for MANETs fall under three basic categories (a) Stand-alone (b) Cooperative and (c) Hierarchical [6].

(a)Stand-alone: In stand-alone architectures, 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.

(b)Cooperative: In this 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.

(c)Hierarchical: The hierarchical architectures amount to 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 simplecluster 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.

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 labelled 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”.

IDS Watermarking Technique-Watermarking is the method for protecting the related data that should exchange between nodes or is imperceptible added to the cover-signal in order to convey the hidden data. Watermarking techniques are then applied in order to prevent the possible modification of the produced map.

II. RELATED WORK

Secure Routing and Intrusion Detection in Ad Hoc Networks Numerous schemes have been proposed for secure routing and Intrusion Detection for ad hoc networks[4]. In this technique, they present a proof-of-concept implementation of a secure routing protocol based on AODV over IPv6, further reinforced by a routing protocol independent Intrusion Detection System (IDS) for ad hoc networks. Security features in the routing protocol include mechanisms for non-repudiation and authentication, without relying on the availability of a Certificate Authority (CA) or a Key Distribution Center (KDC). They present the design and implementation details of our system, the practical considerations involved, and how these mechanisms can be used to detect and thwart malicious attacks[5]. They discuss several scenarios where the secure routing and intrusion detection mechanisms isolate and deny network resources to nodes deemed malicious. A Game-Theoretic Approach for Optimizing Intrusion Detection Strategy in WSNs-Due to the limited capabilities of sensor nodes in Wireless Sensor Networks (WSNs) in terms of computation, communication and energy, selecting the profitable detection strategy for lowering resources consumption determines whether the IDS can be used practically. The signaling game is used to set up an intrusion detection game modeling the interactions between a malicious sensor node and an IDS agent and its equilibriums are found for optimal detection strategy. The stage intrusion-detection game at each individual time slot is showed in aspects of its player’s utilities and the mixed-strategy Bayesian Nash equilibrium (BNE). As the game evolves, the stage intrusion detection game is developed into a multi-stage dynamic intrusion detection game in which the beliefs on malicious sensor node can be updated based on Bayesian rules. Depending on the current belief, the best response strategy for the IDS agent can be gained based on the Perfect Bayesian equilibrium (PBE). The simulation results have shown the effectiveness of the proposed games, thus, the IDS agents are able to select optimal strategy to defend the malicious sensor node’s actions. This method uses the signaling game to capture and analyze the interactions between a malicious sensor node and an IDS agent in WSNs. The stage intrusion detection game is considered at individual time slot and the mixed-strategy BNE is explored. As the game evolves, author study the mixed-strategy PBE of the multi-stage dynamic intrusion detection game where the IDS agent can dynamically update its beliefs based on the new actions of its opponent, and then adjust its strategy accordingly. Finally, author provides simulations to support the efficiency of the multi-stage dynamic intrusion detection game[4].

III.FRAMEWORK STRUCTURE

A. System Architecture

System architecture defines the overall component used in the system. It also describes the overall functionality of each component. The main component used in this system is MANET Creation, IDS implementation, Cooperation among IDS nodes, Multiplayer cooperative game approach and Network monitoring[5].

 ISSN: 2321-8169
188 – 191

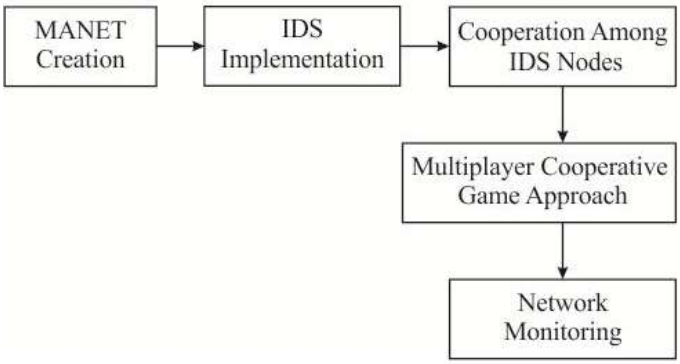

Figure 1.System Architecture.

B. Description of Proposed Algorithm

Fixing the nodes in network region and showing the deployed nodes sensible range. Constructing the network by the nodes. Neighbor table construction and sharing information with neighbors takes place. Each node is equipped with an IDS component. The IDS monitors the traffic of its neighbors all thetime.Each player's (IDS's) objective is to monitor the nodes in its neighborhood at the desired security level in order to detect any malicious activity. Another objective is to conserve its energy. Here, we would like to consider the first objective as the primary goal and the second one as the secondary goal. If the second objective, i.e., saving battery power, were the main objective, each node would independently decide to sleep all the time resulting in totally inactive IDS. Since the nodes are independent, they have to cooperate to achieve the above goals.Routing is the process of selecting a path for traffic in a network or between or across multiple networks. Routing is performed for many types of networks, including circuit-switched networks, such as the public switched telephone network, computer networks, such as the Internet, as well as in networks used in public and private transportation. Several routing protocols are available Data routing between source and destination. Performance analysis takes place.

IV.ALGORITHM AND RESULTS

Genetic Algorithm

Genetic algorithms can be used to evolve simple rules for network traffic (Sinclair, Pierce, and Matzner 1999). These rules are used to differentiate normal network connections from anomalous connections. These anomalous connections refer to events with probability of intrusions. The rules stored in the rule base are usually in the following form (Sinclair, Pierce, and Matzner 1999): if {condition } then { act } For the problems we presented above, the condition usually refers to a match between current network connection and the rules in IDS, such as source and destination IP addresses and port numbers (used in TCP/IP network protocols), duration of the connection, protocol used, etc., indicating the probability of an intrusion. The act field usually refers to an action defined by the security policies within an organization, such as reporting an alert to the system administrator, stopping the connection, logging a message into system audit files, or all of the above. For example, a rule can be defined as: if {the connection has following information: source IP address 124.12.5.18; destination IP address: 130.18.206.55; destination port number: 21; connection time: 10.1 seconds } then {stop the connection} This rule can be explained as follows: if there exists a network connection request with the source IP address 124.12.5.18, destination IP address 130.18.206.55, destination port number 21, and connection time 10.1 seconds, then stop this connection establishment. This is because the IP address 124.12.5.18 is recognized by the IDS as one ofthe blacklisted IP addresses; therefore, any service requestinitiated from it is rejected. 3 The final goal of applying GA is to generate rules that match only the anomalous connections. These rules are tested on historical connections and are used to filter new connections to find suspicious network traffic. In this implementation, the network traffic used for GA is a pre-classified data set that differentiates normal network connections from anomalous ones. This data set is gathered using network sniffers (a program used to record network traffic without doing something harmful) such as Tcpdump The data set is manually classified based on experts' knowledge. It is used for the fitness evaluation during the execution of GA. By starting GA with only a small set of randomly generated rules, we can generate a larger data set that contains rules for IDS. These rules are "good enough" solutions for GA and can be used for filtering new network traffic.

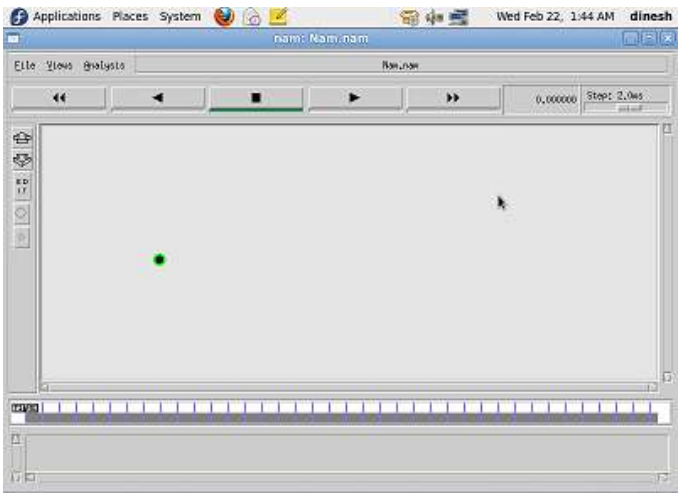

Figure 2.Node Creation.

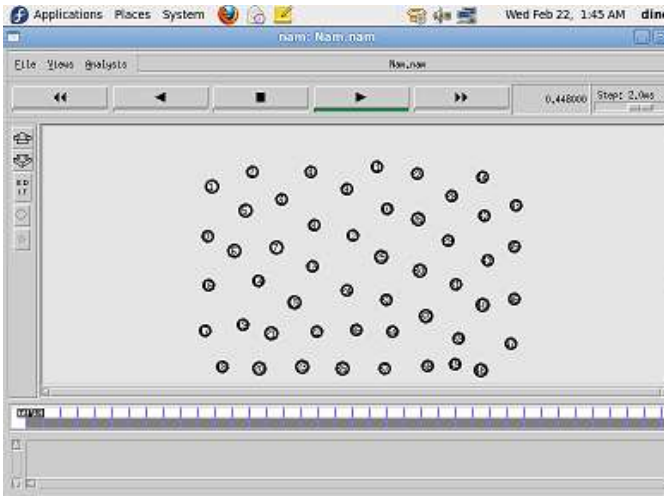

Figure 3.Intrusion Detection System.

V. CONCLUSION

An efficient way of using intrusion detection systems (IDSs) that sits on every node of a mobile ad hoc network (MANET) is proposed. First present the minimization of the active duration of the IDSs in the nodes of a MANET as an optimization problem. Then described a cooperative game model to represent the interactions between the IDSs in a neighborhood of nodes. The game is defined in such a way that the primary goal of the IDSs 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 IDSs 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. Also developed a distributed scheme to determine the ideal probability with which each node has to remain active (or switched on) 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 IDSs running throughout the simulation time and (b) using proposed scheme to reduce the IDS's active time at each node in the network. From the simulation results, one can observe that the effectiveness of the IDSs 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. 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 wish to extend this model to accommodate a heterogeneous network.

REFERENCES

[1] Baker M., Giuli T.J., La K. and Marti S., (2000), "Mitigating routing misbehavior in a Mobile Ad-hoc Environment," Proc. 6th Annual ACM/IEEE International Conference on Mobile Computing and Networking, pp. 255- 26.

[2] Bhoi S.K. and Khilar P.M. (2014), "Vehicular communication: a survey", IET Networks, vol. 3, no. 3, pp. 204 - 217

[3] Chen Y.S., Hassan A., Hunt R., Irwin A. and Zeadally S. (2012), "Vehicular Ad Hoc Networks (VANETS): status, results, and challenges," Telecommunication Systems, vol. 50, no. 4, pp. 217-241.

[4] Datta R. and Marchang N. (2008), "Collaborative techniques for intrusion detection in Mobile Ad-hoc Networks," Elsevier Ad Hoc Networks, vol. 6, no. 4, pp. 508-523.

[5] Iorga M., Partwardan A., Parker J., Joshi A., and Karygiannis T. (2005), "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.

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

[7] Mishra A., andNadkarni K. (2003) "Intrusion dsetection in MANETs – The Second Wall of Defense," Proc. IEEE Industrial Electronics Society Conference, pp. 1235-1239, Roanoke, Virginia, USA, Nov. 2-6.

[8] Web Reference:www.monstercrawler.com

[9] Mobile Ad-Hoc Network by Louis Hourticq