A Novel Approach for Efficient Usage of Intrusion Detection System in Mobile Ad Hoc Networks

P. Bharathi Vikkiraman*, M. Lakshmi**, C. Madhumitha***, J. Nasrinbanu**** & R. Nivetha*****

*Assistant Professor, Department of Electronics and Communication Engineering, S.K.P Engineering College, Tamil Nadu, INDIA.
**UG Student, Department of Electronics and Communication Engineering, S.K.P Engineering College, Tamil Nadu, INDIA.
***UG Student, Department of Electronics and Communication Engineering, S.K.P Engineering College, Tamil Nadu, INDIA.
****UG Student, Department of Electronics and Communication Engineering, S.K.P Engineering College, Tamil Nadu, INDIA.
*****UG Student, Department of Electronics and Communication Engineering, S.K.P Engineering College, Tamil Nadu, INDIA.

***Abstract*—**Mobile Ad hoc Networks (MANET) are self-configuring, infra-structure 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 otherwise vulnerable network. In this paper, we present efficient schemes for analysing 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 neighbourhood nodes to reduce their individual active time. Usually, an IDS has to run all the time on every node to oversee the network behaviour. 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 IDSs without compromising on their effectiveness. To validate our proposed approach, we model the interactions between IDSs as a multi-player cooperative game in which the players have partially cooperative and partially conflicting goals. We theoretically analysis this game and support it with simulation results.

***Keywords*—**Intrusion Detection System; MANET; Protocol Description; Tool Command Language; Topology.

***Abbreviations*—**Computer Aided Design (CAD); Intrusion Detection Systems (IDS); Mobile Ad hoc Networks (MANET); Tool Command Language (TCL); Vehicular Ad hoc Network (VANET).

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 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.

MANETs 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. Besides being operable as a stand-alone network, ad hoc networks can also be attached to the Internet or other networks, thereby extending connectivity and coverage more importantly to areas where there are no fixed infrastructures. Present and future MANET applications cover a variety of areas. 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. Due to the inherent characteristics of a MANET, such as mobility, wireless communication links and lack of any centralized authority, providing security in a MANET is a challenging task. Moreover, security solutions for fixed wired networks are not easily adaptable to mobile wireless networks. 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 is 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 does not attempt to find a signature match but searches for anomalous events or behaviour. For instance, it could look out for anomalous behaviour such as dropping of data packets and events such as erratic changes in the routing table. IDSs can also be categorized based on the audit data used for analysis. Host-based IDSs 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 IDSs collect and analyse 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 IDSs, not much effort has been made on efficient employment of the IDSs. 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 MANETs, a detection system sits on every node, which runs all the time. One common mechanism used by such IDSs is monitoring traffic in the node's neighbourhood. Since 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 MANETs, 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 IDSs 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 setting in all the earlier game-theoretic work on IDS involves two sets of opposing players, the nodes/IDSs and the attacker/defaulters. In our work, we have set a game that involves players (IDSs sitting in neighbouring 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 IDSs (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 IDSs in a neighbourhood and used it to validate our proposed probabilistic scheme [Parker et al., 1].

The contributions of this paper are summarized as follows:

1. We present a novel technique, based on a probabilistic model, to optimize the active time duration of intrusion detection systems (IDSs) in a MANET. The scheme reduces the IDSs' active time as much as possible without compromising on its effectiveness.
2. To validate our proposed approach, we also present a multi-player cooperative game that analyses the effects of individual intrusion detection systems with reduced activity on the network.
3. Through simulation we show that a considerable saving in energy and computational cost is achieved using our proposed technique of optimizing the active time of the IDSs while maintaining the performance of the IDS.
4. The proposed scheme uses local information, thus making it distributed and scalable. Moreover, it works on both static and mobile networks. The rest of the paper is organized as follows. Section II reviews the work in the existing literature. We define a problem for optimizing the active time of the intrusion detection systems in a MANET in section III. In Section IV we give a multi-player cooperative game theoretic analysis to the problem. A distributed algorithm for efficient usage of IDS is presented in section V. In section VI, we present the performance evaluation and section VII concludes the paper along with directions on future research.

II. RELATED WORK

This section presents existing related work on energy efficient usage of intrusion detection systems in a MANET. In, the authors provided a formal study on optimizing network topology for edge-self monitoring in sensor networks with the objective of maximizing the lifetime of the network. The focus is on optimized selection of monitor nodes that monitor communication links so as to reduce the number of monitor nodes. Though the objective is the same, i.e., energy conservation, our work focuses on reducing the active time of the monitor nodes instead of reducing the number of monitor nodes. The existing work focus on reducing the number of monitor nodes that monitor a communication link. Hence, the active nodes bear the whole burden of monitoring communication links while the sleeping nodes sleep. While the overall energy consumption may be reduced, some nodes' energy may be depleted sooner than that of the others. In our network, instead of placing the burden of monitoring on a few selected nodes, every neighbour node chips in so that each node fairly shares the profit (energy saving) as will be illustrated in the simulation results in section VI. The protocol SLAM makes use of special nodes called guard nodes for local monitoring in sensor networks. Usually the guard nodes remain in sleep mode in the network. Before communicating on a link, a node awakens the guard nodes responsible for local monitoring on

its next hop. The main aim of the protocol is to reduce the time a guard node remains awake for the purpose of monitoring malicious activities. We find that there is an inter dependence between the nodes while carrying out network monitoring. However, in our proposed work, a node determines the probability with which its own IDS monitors and schedules its monitoring time independent of the other nodes. Moreover, when a large number of communication links are in use, almost all the guard nodes in SLAM might be awake, which is also a downside of the protocol. In a protocol for optimal selection and activation of intrusion detection agents for wireless sensor networks is presented. Only nodes which have the trust value above the trust requirement can activate the intrusion agent which is to monitor the packet and send the alert packet to cluster heads. The main requirement of the protocol for each sensor node to maintain a small trust database of its neighbours and the clustering of sensor nodes. A game theoretic framework for distributed intrusion detection in ad hoc networks which maximizes the network lifetime while ensuring probabilistic guarantees for the achieved security level is presented in. The authors assume that the network in divided into clusters of nodes among which some are trusted. A trusted node is equipped with a perfect IDS so that when it performs intrusion detection, it is effective for the whole cluster and no other node is involved in the monitoring process. In comparison, in our proposed approach we neither assume that some nodes are trusted nor that an IDS is perfect. The existence of the energy security trade-off that is shown in is also observed in our simulation results. More importantly, all the above work assume the network to be static while our approach works even when the nodes are mobile. In a technique is presented which optimally selects a subset of nodes in a dynamic network, each of which manages/monitors a subset of nodes with the aim of reducing monitoring traffic or choosing nodes predicted to be long-lived. Optimal selection of m out of M sniffers and assignment of each sniffer to one of the K channels to maximize the total amount of information gathered in a multi-channel wireless network is done. However, our work does not share the same goal as the above two. Reduction of energy consumption by intrusion detection systems is being researched in the context of wired networks too. In an architecture (LEONIDS) is presented for network-level intrusion detection system which resolves the energy-latency trade-off by providing both low power consumption and low detection latency at the same time. Packet-based selective encryption is used in for reducing the energy consumption during intrusion detection for networked control systems security. Game theory is widely used for modelling intrusion detection in wireless network. Several other game-theoretic solutions are also found in the literature that take care of issues like cooperation and selfishness of the nodes in the network [Li Ling & Constantine Manikopoulos, 2; Ketan Nadkarni & Amitabh Mishra, 3].

2.1. Existing Work

We first present the minimization of the active duration of the intrusion detection system (IDSs) in the nodes of a MANET as an optimization problem. The primary goal of the Intrusion Detection (IDSs) is to monitor the nodes in its neighbourhood at a desired security level so as to detect any anomalous behaviour, whereas, the secondary goal of the IDSs 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 [Zhang & Lee, 4].

III. PROPOSED WORK

We attempt to solve the problem of efficient usage of IDS in two phases: First, we look at the problem from the point of view of a node being monitored by its one-hop neighbours. We present an optimization problem for the same and analyse it using game theory. Second, we view the problem from the point of view of a node which monitors its neighbours. Using the solution to the optimization problem, we arrive at an efficient distributed algorithm which every node in the network employs. Let us consider a network of wireless nodes, each having an intrusion detection system (IDS) that is responsible for detecting malicious activities within its neighbourhood. We assume that a mobile node is watched for malicious activities by all its neighbours (nodes within its radio range) using these IDSs. The main advantage of the proposed system is reduction of energy consumption in each node and it is possible in Heterogeneous Network [Yongguang Zhang & Wake Lee, 5].

3.1. Modules Name

- Creating Topologies
- Protocol description
- Tool Command Language (TCL) script development
- Configure nodes

3.1.1. Creating Topology

- Nodes
  - Set properties like queue length, location.
  - Protocols, routing algorithms.
- Links
  - Set types of link – Simplex, Duplex, Wireless, Satellite.
  - Set bandwidth, latency etc.
- Done through TCL Scripts.

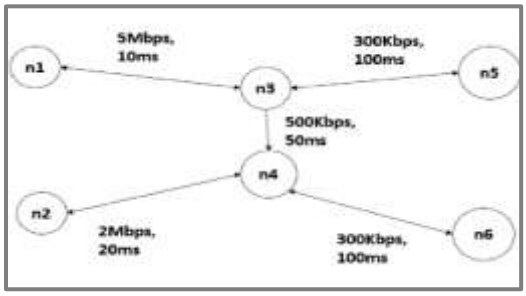

Figure 1: Topology

3.1.2. Protocol Description

Ad Hoc On-Demand Distance Vector, a routing protocol for ad hoc mobile networks with large numbers of mobile nodes. The protocol's algorithm creates routes between nodes only when the routes are requested by the source nodes, giving the network the flexibility to allow nodes to enter and leave the network. An ad hoc routing protocol is a convention, or standard, that controls how nodes decide which way to route packets between computing devices in a mobile ad hoc network. In ad hoc networks, nodes are not familiar with the topology of their networks. Instead, they have to discover it: typically, a new node announces its presence and listens for announcements broadcast by its neighbors [Hu et al., 6].

3.1.3. Tool Command Language (TCL) Script Development

The name TCL is derived from "Tool Command Language" and is pronounced "tickle". TCL is a radically simple open-source interpreted programming language that provides common facilities such as variables, procedures, and control structures as well as many useful features that are not found in any other major language. While TCL is flexible enough to be used in almost any application imaginable, it does excel in a few key areas, including: automated interaction with external programs, embedding as a library into application programs, language design, and general scripting. TCL was originally developed as a reusable command language for experimental computer aided design (CAD) tools. The interpreter is implemented as a C library that could be linked into any application [Saha et al., 7].

3.1.4. Configure Nodes

Node configuration essentially consists of defining the different node characteristics before creating them. They may consist of the type of addressing structure used in the simulation. Defining the network components for mobile nodes, turning on or off the trace options at Agent/Router/MAC levels, selecting the type of ad hoc routing protocol for wireless nodes or defining their energy model. All node instances created after a given node-configuration command will have the same property unless a part or all of the node configuration command is executed with different parameter values. And all parameter values remain unchanged unless they are explicitly changed [Zhakhary & Radenkovic, 8; Tamilselvan & Sankaranarayanan, 9].

IV. SIMULATION

4.1. Environment Algorithm

Step 1: Each node M broadcasts a message of type Send-Degree to its neighbours asking them to send their degree.

$$M -> broadcast: (SendDegree)$$

Step 2: On receipt of the SendDegree message in Step 1, each neighbour node, B of M replies to M a ReplyDegree message.

$$B-> M: (ReplyDegree)$$

Step 3: On receipt of each ReplyDegree message in Step 2, M does the following: For each message do

$$degree = ReplyDegree:$$
$$k = Minimum\ (degree):$$

If $l > k$ then $= 1$ otherwise, is assigned the minimum value of p (where l is the desired security level of the neighbour, $T + € = 1$, € is a very small positive number) such that

$$\sum_{=1}( ) (1 -)^{-1} \geq T$$

V. SIMULATION RESULT

5.1. Case: 1

Intermediate Nodes

The client is not within the network coverage so the Base Station uses the intermediate nodes to transfer information's to the client.

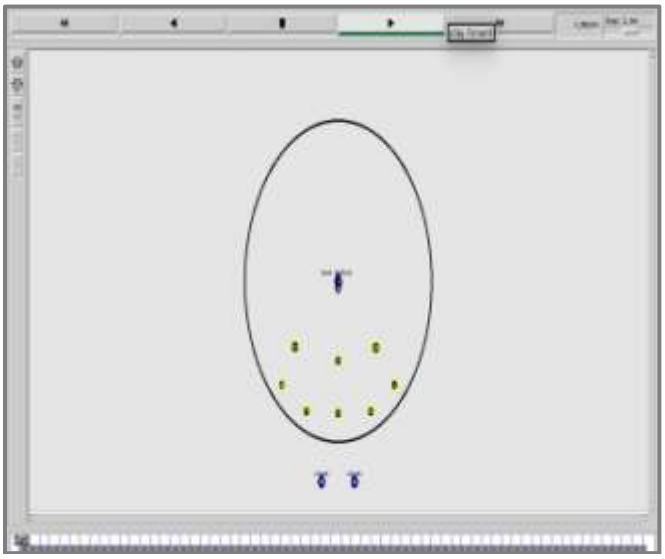

Figure 2: Case 1

5.2. Case: 2

The Base Station starts transferring, the information to the intermediate nodes.

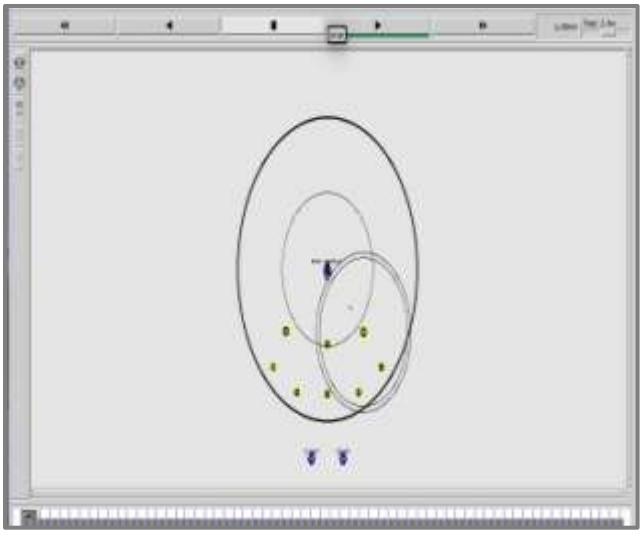

Figure 3: Case 2

5.3. Case: 3

IDS

IDS occurs due to some anomalous behaviour.

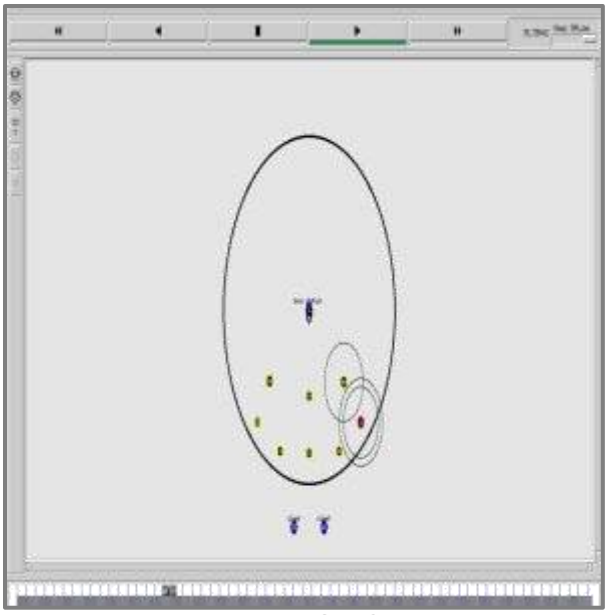

Figure 4: Case 3

5.4. Case: 4

Finally the information reaches the client through the intermediate nodes.

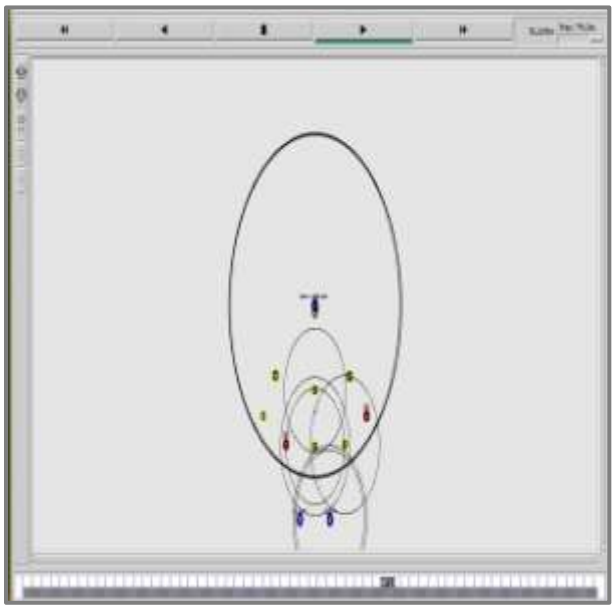

Figure 5: Case 4

VI. CONCLUSION

In this paper we have proposed an efficient way of using intrusion detection systems (IDSs) that sits on every node of a mobile ad hoc network (MANET). We first present the minimization of the active duration of the IDSs in the nodes of a MANET as an optimization problem. We then described a cooperative game model to represent the interactions between the IDSs in a neighbourhood of nodes. The game is defined in such a way that the primary goal of the IDSs is to monitor the nodes in its neighbourhood at a desired security level so as to detect any anomalous behaviour, 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 neighbour 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 IDSs running throughout the simulation time and (b) using our proposed scheme to reduce the IDS's active time at each node in the network. From the simulation results we 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. 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.

REFERENCES

[1] J. Parker, J.L. Undercoffer, J. Pinkston & A. Joshi (2004), "On Intrusion Detection in Mobile Ad Hoc Networks", *23rd IEEE International Performance Computing and Communication Conference- Workshop on Information Assurance*.

[2] Li Ling & Constantine Manikopoulos (2006), "Architecture of the Mobile Ad-hoc Network Security (MANET) System", *CONEX Laboratory*, *NJWINS Center*.

[3] Ketan Nadkarni & Amitabh Mishra (2004), "Intrusion Detection in MANETs", *The Second Wall of Defense*.

[4] Y. Zhang & W. Lee (2000), "Intrusion Detection in Wireless Ad-hoc Networks", *Proceedings of the 6th International Conference on Mobile Computing and Networking (MobiCom 2000)*, Pp. 275–283.

[5] Yongguang Zhang & Wake Lee (2000), "Intrusion Detection in Wireless Ad-hoc Networks", *Sixth Annual International Conference on Mobile Computing and Networking*, Pp. 275–283.

[6] Y. Hu, D. Johnson & A. Perrig (2002), "SEAD Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks", *Proceedings of the 4th IEEE Workshop on Mobile Computing Systems & Applications (WMCSA 2002)*, *IEEE*, Calicoon, NY.

[7] H.N. Saha, D. Bhattacharyya & P.K. Banerjee (2011), "A Distributed Administration based Approach for Detecting and Preventing Attacks on Mobile Ad Hoc Networks", *International Journal of Engineering Science*.

[8] S.R. Zhakhary & M. Radenkovic (2010), "Reputation-based Security Protocol for MANETs in Highly Mobile Disconnection-Prone Environments", *Proc. IEEE/IFIP WONS 2010 –Seventh International Conference on Wireless On-Demand Network Systems and Services*, Pp.161–167.

[9] L. Tamilselvan & V. Sankaranarayanan (2007), "Prevention of Black Hole Attack in MANET", *Proceedings of Wireless Broadband and Ultra Wideband Communications*, Pp. 21–26.

