An Approach to Intrusion Detection System in Mobile Ad Hoc Networks

Satyam Singh¹, Rishabh Goyal², Mohd Arif³, Mr. Rishabh Jain⁴
B.Tech Students¹²³, Assistant Professor⁴
Department of Computer Science Engineering
Galgotias College of Engineering and Technology, Greater Noida, India

Abstract:
Mobile Adhoc Network (MANET) is a collection of wireless mobile computers (nodes) in which each node communicate with the other nodes in the network through radio waves. Here each node in the network is independent and thus it does not rely on each other for moving across the network. Intrusion Detection Systems (IDS) are used in MANETs to monitor activities so as to detect any intrusion in the otherwise vulnerable network. A probabilistic model is suggested that makes utilization of participation between IDSs among neighborhood nodes to diminish their individual dynamic time. For the most part, an IDS needs to run all the time on each hub to regulate the system conduct. This can end up being an expensive overhead for battery-powered mobile devices as far as power and computational assets. 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 analyze this game and support it with simulation results.

Keywords: Ad hoc networks, intrusion detection, energy efficiency.

I. INTRODUCTION

The term MANET (Mobile Ad hoc Network) refers to a multihop packet based wireless network composed of a set of mobile nodes that can communicate and move at the same time, without using any kind of fixed wired infrastructure. MANET is actually self-organizing and adaptive networks that can be formed and deformed on-the-fly without the need of any centralized administration. Otherwise, a stand for “Mobile Ad Hoc Network” A MANET is a type of ad hoc network that can change locations and configure itself on the fly. Because MANETS are mobile, they use wireless connections to connect to various networks. This can be a standard Wi-Fi connection, or another medium, such as a cellular or satellite transmission. MANET applications cover a variety of areas. One important application scenario is vehicular ad hoc network (VANET).

![Figure 1. Structure of MANET](image)

The purpose of the MANET working group is to standardize IP routing protocol functionality suitable for wireless routing application within both static and dynamic topologies with increased dynamics due to node motion and other factors. Because of the inborn attributes of a MANET, such as portability, remote correspondence connections and absence of any incorporated specialist, giving security in a MANET is a challenging task. Additionally, security answers for settled wired systems are not effectively versatile to portable remote systems 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. An ad-hoc network is the cooperative engagement of a collection of mobile nodes without the required intervention of any centralized access point or existing infrastructure. In this paper we present Ad-hoc On Demand Distance Vector Routing (AODV), a novel algorithm for the operation of such ad-hoc networks. Each Mobile Host operates as a specialized router, and routes are obtained as needed (i.e., on-demand) with little or no reliance on periodic advertisements. Our new routing algorithm is quite suitable for a dynamic self starting network, as required by users wishing to utilize ad-hoc networks. AODV provides loop-free routes even while repairing broken links.

II. EXISTING SYSTEM

The Existing 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. 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. Some disadvantages associated with existing systems are -
• 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.
• More energy consumption
• Less network lifetime
• High computational cost

III. PROPOSED SYSTEM

We present a 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’ working time as much as possible. To validate our proposed approach, we also present a multi-player cooperative game that analyzes the effects of individual intrusion detection systems with reduced activity on the network. 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 IDS while maintaining the performance of the IDS. The proposed scheme uses local information, thus making it distributed and scalable. Moreover, it works on both static and mobile networks.

![Sequence Diagram of an IDS](Image)

Figure 2. Sequence Diagram of an IDS

Advantages of the proposed system are as follows –
• Increase network lifetime
• Decrease energy consumption
• Low computational cost

IV. MODULES

A. Network Topology

The sensor nodes are randomly distributed in a sensing field. We are using mobile ad hoc network (MANET). This is the infrastructure less network and a node can move independently. In a MANET, each node not only works as a host and also acts as a router. We can find the communication range for all nodes. Every node communicates only within the range. If suppose any node out of the range, node will not communicate those nodes or drop the packets.

B. Usage of IDS

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 neighbors. We present an optimization problem for the same and analyze it. Second, we view the problem from the point of view of a node which monitors its neighbors. 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 neighborhood. We assume that a mobile node is watched for malicious activities by all its neighbors (nodes within its radio range) using these IDSs. Hence, by neighbor, we mean 1-hop neighbor throughout the rest of the paper. Some level of redundancy can be observed here. At any instant of time, all or some of the k neighbors may detect the malicious activity of node a depending upon the detection rate of the IDS components on them. More importantly, the neighbors spend their valuable computational resources and energy while monitoring node a all the time. However, it may not be required to keep the IDS running on each node all the time. We attempt to reduce this redundancy, thereby saving the afore-mentioned resources.

C. Algorithm:

The mechanism employed by each node in the network to determine the minimum monitoring probability is best presented by the simple algorithm. Each node (say M) initiates this algorithm to determine the probability with which it has to monitor its neighborhood. In step 1, M broadcasts the message To-Degree. This message is limited to only one hop. In step 2, the neighbors of M reply back with their respective degrees. In step 3, the least of these degrees is assigned to k in the formula, and the minimum monitoring probability of M is calculated. In step 2 of Algorithm, a malicious neighbor may send false degree information to M and try to disrupt the algorithm. However, Algorithm is versatile to such an attack under the following assumption. We assume that a malicious neighbor of M to be as less as possible so that the chance of being detected is reduced. It cannot change its security level and thus to be monitored with a low monitoring probability, it can only send a high degree to M.

D. Performance Evaluation

In this section, we can evaluate the performance of simulation. We are using the xgraph for evaluate the performance. The focus is not on the design of the cooperative IDS but on how integrating Algorithm in it helps reduce the active time of individual IDSs while attempting to maintain its effectiveness. The performance metrics are detection rate, false detection rate, and the saving of energy and computational resource. We compare these metrics when Algorithm is in use as compared to when it is not. Additionally, we show the comparison of energy depletion of the individual nodes in the network.

V. PERFORMANCE ANALYSIS

The system is completely implemented on basis of NS2.28 version and system is tested for various metric analysis which include:
1. Detection Rate
2. Energy Saved
3. Computational Time
For the analysis the proposed system is compared with existing IDS. Figure 3. Denotes the comparison between the detection rate of the existing system and the proposed system. Here red line is used for the existing system and green line for the proposed system.

![Figure 3. Detection Rate Comparison](image)

The next aspect is the Energy Saved which has to be high. The figure 4 depicts the comparisons of Energy Saved.

![Figure 4. Energy Saved Comparison](image)

The another metric is the computational time which indicates the processing time. Figure 5 depicts the comparison of computational time.

![Figure 5. Computational Time Comparison](image)

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 present the minimization of the active duration of the IDSs in the nodes of a MANET as an optimization problem. Each of the hubs has to take an interest agreeably in checking its neighbor hubs with a base likelihood. We then build up an appropriated plan to decide the perfect likelihood with which each hub needs to stay dynamic (or exchanged on) so that every one of the hubs of the system are checked with a coveted security level. Here we assumed our system to be homogeneous and we would like to extend for heterogeneous system in future.

VII. ACKNOWLEDGEMENT
The authors would like to thank the teachers and students of Galgotias College of Engineering and Technology (GCET) particularly, Mr. Rishabh Jain (Professor, GCET) and Mr.Manish Kumar Sharma (Professor, GCET) for the constant support and guidance.

VIII. REFERENCES


[5]. B.Sai Srujana and Mrs. S. Nasrath,” A NOVEL APPROACH TO INTRUSION DETECTION SYSTEM IN MANETS,” International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE) ISSN: 0976-1353 Volume 17 Issue 2 – SEPTEMBER 2015