An Active Usage of Intrusion Detection System in Mobile Ad Hoc Networks

Jeyalakshmi.PR[1],Yogalakshmi.S[2], Rupa Kesavan[3], P.Veeralakshmi[4]
[1, 2] Dept of Information Technology
[3]Assistant Professor, Dept of Information Technology
[4]Associate Professor, Dept of Information Technology
[1, 2, 3, 4] Prince Shri VenkateshwaraPadmavathy Engineering College

Abstract- *An efficient usage of Intrusion Detection System in Mobile Ad Hoc Networks is of practical interest in many applications such as detecting an intruder in battlefield. The intrusion detection is defined as a mechanism for WSN to detect the existence of inappropriate, incorrect, or anomalous moving attackers. In this paper, we consider this issue according to heterogeneous WSN models. Furthermore, we consider two sensing detection models: single-sensing detection and multiple-sensing detection. Our simulation results show the advantage of multiple sensor heterogeneous WSNs. A Mobile Ad Hoc Network also known as wireless ad hoc network is a continuously self-configuring, infrastructure-less network of mobile devices connected wirelessly. Our aim is to decrease the duration of active time of the Intrusion Detection System without compromising their performance. This can turn out to be costly overhead for a battery powered mobile device in terms of power and computational resources.*

Keywords- Wireless sensor Network, Intrusion detection, Heterogeneous, Multiple-sensing.

I. INTRODUCTION

A Wireless Sensor Network (WSN) is a collection of spatially deployed wireless sensors by which to monitor various changes of environmental conditions (e.g., forest fire, air pollutant concentration, and object moving) in a collaborative manner without relying on any underlying infrastructure support .Recently, a number of research efforts have been made to develop sensor hardware and network architectures in order to effectively deploy WSNs for a variety of applications. Due to a wide diversity of WSN application requirements, however, a general-purpose WSN design cannot fulfill the needs of all applications. Many network parameters such as sensing range, transmission range, and node density have to be carefully considered at the network design stage, according to specific applications. To achieve this, it is critical to capture the impacts of network parameters on network performance with respect to application specifications. Intrusion detection (i.e., object tracking) in a WSN can be regarded as a monitoring system for detecting the intruder that is invading the network domain.

The intrusion detection application concerns how fast the intruder can be detected by the WSN. If sensors are deployed with a high density so that the union of all sensing ranges covers the entire network area, the intruder can be immediately detected once it approaches the network area. However, such a high-density deployment policy increases the network investment and may be even unaffordable for a large area. In fact, it is not necessary to deploy so many sensors to cover the entire WSN area in many applications, since a network with small and scattered void areas will also be able to detect a moving intruder within a certain intrusion distance. In this case, the application can specify a required intrusion distance within which the intruder should be detected. The intrusion distance is referred as D and defined as the distance between the points the intruder enters the WSN, and the point the intruder is detected by the WSN system. This distance is of central interest to a WSN used for intrusion detection. In this paper, we derive the expected intrusion distance and evaluate the detection probability in different application scenarios.. For example, given an expected detection distance, we can derive the node density with respect to sensors' sensing range, thereby knowing the total number of sensors required for WSN deployment.

In a WSN, there are two ways to detect an object (i.e., an intruder): single-sensing detection and multiple-sensing detection. In the single-sensing detection, the intruder can be successfully detected by a single sensor. On the contrary, in the multiple-sensing detection, the intruder can only be detected by multiple collaborating sensors .In some applications, the sensed information provided by a single sensor might be inadequate for recognizing the intruder. It is because individual sensors can only sense a portion of the intruder. For example, the location of an intruder can only be determined from at least three sensors' sensing.

In view of this, we analyze the intrusion detection problem under two application scenarios: single-sensing detection and multiple-sensing detection. According to the capability of sensors, we consider two network types: homogeneous and heterogeneous WSNs We define the sensor capability in terms of the sensing range and the transmission range. In a heterogeneous WSN some sensors have a larger sensing range and more power to achieve a longer transmission range. In this paper, we show that the heterogeneous WSN increases the detection probability for a given intrusion detection distance. This motivates us to analyze the network connectivity in this paper. Furthermore, in a heterogeneous WSN, high capability sensors usually undertake more important tasks (i.e., broadcasting power management information or synchronization information to all the sensors in the network), it is also desirable to define and examine the broadcast reachability from high-capability sensors. The network connectivity and broadcast reachability are important conditions to ensure the detection probability in WSNs. They are formally defined and analyzed in this paper. To the best of our knowledge, our effect is the first to address this issue in a heterogeneous WSN.

In view of this, we analyze the intrusion detection problem under two application scenarios: single-sensing detection and multiple-sensing detection. According to the capability of sensors, we consider two network types: homogeneous and heterogeneous WSNs We define the sensor capability in terms of the sensing range and the transmission range. In a heterogeneous WSN some sensors have a larger sensing range and more power to achieve a longer transmission range. In this paper, we show that the heterogeneous WSN increases the detection probability for a given intrusion detection distance. This motivates us to analyze the network connectivity in this paper. Furthermore, in a heterogeneous WSN, high capability sensors usually undertake more important tasks (i.e., broadcasting power management information or synchronization information to all the sensors in the network),it is also desirable to define and examine the broadcast reachability from high-capability sensors. The network connectivity and broadcast reachability are important conditions to ensure the detection probability in WSNs. They are formally defined and analyzed in this paper. To the best of our knowledge, our effect is the first to address this issue in a heterogeneous WSN.

The contributions of this paper are summarized as follows.

1) We present a novel technique, which is based on a probabilistic model, to optimize the active time duration of IDSs in a MANET. The scheme reduces the IDSs' active time as much as possible without compromising its effectiveness.
2) To validate our proposed approach, we also present a multiplayer cooperative game that analyzes the effects of individual IDSs with reduced activity on the network.
3) Through simulation, we show that considerable savings 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.

II. RELATED WORKS

This section presents existing related work on the energy efficient usage of IDSs in a MANET. In Dong et al. provided a formal study on optimizing the network topology for edge-self monitoring in sensor networks with the objective of maximizing the life time 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. Although 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. The protocol SLAM makes use of special nodes called guard nodes for local monitoring in sensor networks. Typically, 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 interdependence 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 that have the trust value above the trust requirement can activate the intrusion agent to monitor packets and send an alert packet to cluster heads. It is a requirement in the protocol for each sensor node to maintain a small trust database of its neighbors and the clustering of sensor nodes. 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 tradeoff is also observed in our simulation results.

III. SYSTEM ARCHITECTURE FOR INTRUSION DETECTION SYSTEM

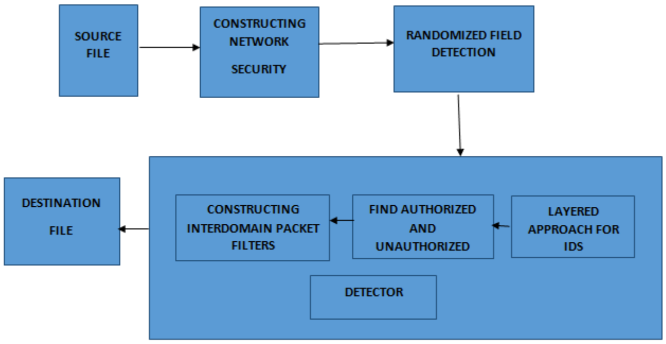
SOURCE FILE
CONSTRUCTING NETWORK SECURITY
RANDOMIZED FIELD DETECTION
LAYERED APPROACH FOR IDS
FIND AUTHORIZED AND UNAUTHORIZED
CONSTRUCTING INTERDOMAIN PACKET FILTERS
DETECTOR
DESTINATION FILE

Figure 1.1

IV .INTRUSION DETECTION SYSTEM USAGE ALGORITHM

Thus far, it looked at the problem of efficient usage of an IDS from the perspective of a node monitored by its neighbors. Next, use is the optimization problem of (2) as a building block and develop a distributed scheme for the IDSs. Every node employs this scheme to determine the ideal probability with which is IDS has to remain active so that all nodes in the network are monitored with the desired security level. Let pmini be the optimal (minimum) probability with which node i has to monitor so that its neighbors are monitored with the desired security level. It refers to pmini as the minimum monitoring probability of node i. For instance, in Fig. 2, node 5 has three neighbors (1, 4, and 6). Suppose l = 1. Here, 4, 1, and 6 have to be monitored by their respective neighbors with a probability of 0.85, 0.97, and 0.90 (solutions of problem (2) when T = 0.995), respectively. Since node 5 is a neighbor of nodes 1, 4, and 6, pmin5 = max(0.85,0.97,0.90)=0.97. Here it defines the degree of a node to be the number of its neighbors at any instant of time. Let mi denote the minimum degree of the neighbors of node i. It assign to k in the optimization problem of (2) to obtain the following optimization problem whose solution is pmini :
Minimize p subject to
The term T as previously explained denotes a threshold value, which is the minimum probability with which the desired security level (l) is maintained, albeit for the whole network.m5 = 2 since 2 is the least of all the degrees of node 5's neighbors, viz., 1, 4, and 6. Consequently, pmin 5 = 0.97. Similarly, the corresponding (mi,pmini) pairs for other nodes are also shown. The minimum monitoring probability obtained as the solution to the optimization problem of ensures that every node in the network is monitored at the desired security level. The proof follows. Theorem: Each node in the network is monitored with the desired security level when pmini of each node i is calculated using the minimum degree of its neighbors (mi) in the optimization problem.

Proof:

Assumption: For every node i, pmini is calculated using a positive integer x such that x>m and yet, every node in the network is monitored with security level l. Let p(mi) be the solution to the optimization problem of (4). Hence, p(x) denotes the corresponding solution when mi is replaced by x. Without loss of generality, let node 1 be the neighbor of node i with a minimum degree among all its neighbors. Since the left-handside of the constraint of the optimization problem is the probability that at least l neighbors are monitoring out of all the x neighbors, the value of p(x) decreases as the value of x increases. Hence, p(x) <p (mi) since x>m i. Here, mi is the degree of node 1. Hence, p(mi) is the minimum probability with which node 1 has to be monitored by its neighbors so that security level l is achieved [see the optimization problem of (2)]. Since p(x) <p (mi),node1isnotmonitoredwithsecuritylevel.This contradicts our assumption and, hence, provesthe theorem. The mechanism employed by each node in the network to determine the minimum monitoring probability is best presented by the simple algorithm, called LDK, which stands for Least Degree fork. Each node (e.g., M) initiates this algorithm to determine the probability with which it has to monitor its neighborhood.

ALGORITHM:

Step 1: M broadcasts the message send Degree. This message is limited to only one hop.
Step 2: The neighbors of M reply back with their respective degrees.
Step 3: The least of these degrees is assigned to k in the formula, and the minimum monitoring probability of M is calculated.
Step 4: The new epoch for the composition is defined.
Step 5: While updating rounds decisions are depend upon the agreement of f+1.
Step 6: The ratios of this periods is illustrated at the end.

V. FUTURE ENHANCEMENT

This paper analyzes the intrusion detection problem by characterizing intrusion detection probability with respect to the intrusion distance and the network parameters (i.e., node density, sensing range, and transmission range).The analytical model for intrusion detection allows us to analytically formulate intrusion detection probability within a certain intrusion distance under various application scenarios. 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 in energy consumption in each of the nodes that increases the network lifetime significantly.

REFERENCES

[1] S. Zeadally, R. Hunt, Y.-S. Chen, A. Irwin, and A. Hassan, "Vehicular ad hoc networks (VANETS): Status, results, and challenges," Telecommun. Syst., vol. 50, no. 4, pp. 217–241, 2012.

[2] S. K. Bhoi and P. M. Khilar, "Vehicular communication: A survey," IET Netw., vol. 3, no. 3, pp. 204–217, 2014.

[3] S.Marti,T.J.Giuli,K.La,andM.Baker,"Mitigatingroutingmisbehaviorinamobilead-hoc environment," inProc.6thAnnu.ACM/IEEEInt.Conf. Mobile Comput. Netw., Aug. 2000, pp. 255–265.

[4] C. Manikopoulos and L. Ling, "Architecture of the Mobile Ad-hoc Network Security (MANS) system," in Proc. IEEE Int. Conf. Syst., Man Cybern., Oct. 2003, vol. 4, pp. 3122–3127.

[5] K. Nadkarni and A. Mishra, "Intrusion detection in MANETs—The second wall of defense," in Proc. IEEE Ind. Electron. Soc. Conf., Roanoke, VA, USA, Nov. 2–6, 2003, pp. 1235–1239.

[6] NingrinlaMarchang,RajaDatta and SajalK.Das,"An Novel Approach for Efficient Usage of Intrusion Detection System in Mobile Ad Hoc Networks",IEEE Transactions on vehicular technology,VOL.66,NO.2