INTERNATIONAL JOURNAL · ENGINEERING RESEARCH

International Journal for Innovative Engineering and Management Research

A Peer Revieved Open Access International Journal

www.ijiemr.org

IJIEMR Transactions, online available on 17 April 2019.

Link : http://www.ijiemr.org

Title:- Design of Energy Efficient Intrusion Detection Technique In Homogeneous And Heterogeneous Wireless Sensor Networks.

Volume 08, Issue 04, Pages: 211 - 217.

Paper Authors

CHOLLANGI NAGA DURGA PRASAD, M.TILAK.

Department of MCA, SKBR PG College.

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

DESIGN OF ENERGY EFFICIENT INTRUSION DETECTION TECHNIQUE IN HOMOGENEOUS AND HETEROGENEOUS WIRELESS SENSOR NETWORKS

[1]CHOLLANGI NAGA DURGA PRASAD, [2]M.TILAK
[1]PG Scholar, Department of MCA, SKBR PG College, Amalapuram
[2]Assistant Professor, Department of MCA, SKBR PG College, Amalapuram

ABSTRACT: Intrusion detection in Wireless Sensor Network (WSN) is of practical interest in many applications such as detecting an intruder in a battlefield. The intrusion detection is defined as a mechanism for a WSN to detect the existence of inappropriate, incorrect, or anomalous moving attackers. For this purpose, it is a fundamental issue to characterize the WSN parameters such as node density and sensing range in terms of a desirable detection probability. In this paper, we consider this issue according to two WSN models: homogeneous and heterogeneous WSN. Furthermore, we derive the detection probability by considering two sensing models: single-sensing detection and multiple-sensing detection. In addition, we discuss the network connectivity and broadcast reachability, which are necessary conditions to ensure the corresponding detection probability in a WSN. Our simulation results validate the analytical values for both homogeneous and heterogeneous WSNs.

KEY WORDS: Intrusion detection, node density, node heterogeneity, sensing range, Wireless Sensor Network (WSN).

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 [1]. 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. Fig. 1 gives an example that sensors are deployed in a square area for detecting the presence of a moving intruder. Note that in Fig. 1, as well as in Figs. 3 and 4, the illustration of sensors and an intruder is based on a slide for paper [2]. 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 [3], 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 withinNwhich the intruder should be detected. As shown in Fig. 1, the intrusion distance is referred as D and defined as then distance between the point 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. Given a maximal allowable intrusion distance Dmax ¼ , we theoretically capture the impact on the detection probability in terms of different network parameters, including node density, sensing range, and transmission range. For example, given an expected detection distance EðDÞ, 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 [4]. 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 data [5], [6], [7], [8]. In view of this, we analyze the intrusion detection problem under two application scenarios: single-sensing detection and multiple-sensing detection.

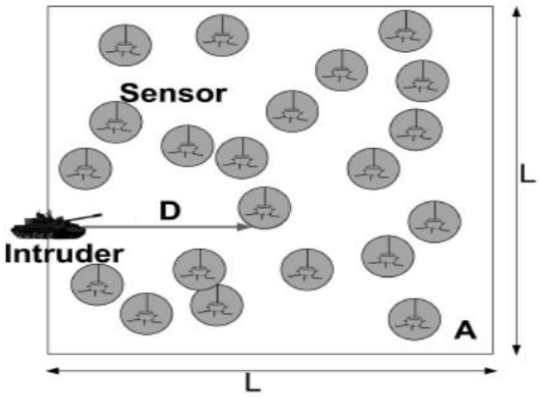

Fig. 1. INTRUSION DETECTION IN A WSN.

According to the capability of sensors, we consider two network types: homogeneous and heterogeneous WSNs [9]. We define the sensor capability in terms of the sensing range and the transmission range. In a heterogeneous WSN[10], [11], [12] 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. On the other hand, a heterogeneous WSN poses the challenge of network connectivity due to asymmetric wireless link. The high-capability sensors have a longer transmission range while low capability sensors have a shorter transmission range. Due to this, the packet sent by a high-capability sensor may reach the low-capability sensor, while the low capability sensor may not be able to send packets to the corresponding high-capability sensor [13].

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 reach ability from high-capability sensors. The network connectivity and broadcast reach ability 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.

II.RELATED WORK

Intrusion detection is one of the critical applications in WSNs, and recently, several approaches for intrusion detection in homogeneous WSNs have been presented [3],[14], [15]. The focus of these approaches aims at effectively detecting the presence of an intruder. First, the problem is investigated from the aspect of the network architecture. Kung and Vlah [14] take advantage of a hierarchical tree structure to effectively track the movement of an intruder. The hierarchical tree consists of connected sensors and is built upon expected properties of intruder mobility patterns such as its movement frequency over a region.

Based on the hierarchical tree, it allows an efficient record of an intruder's moving information and supports fast querying from the base station. Another tree structure for tracking an intruder, called as a logic object-tracking tree, is developed by Lin et al. [15]. The logic object tracking tree reduces the communication cost for data updating and querying by taking into account the physical network topology. In particular, the logic object tracking tree targets to balance the update cost and the query cost so as to minimize the total communication cost.

Second, the intrusion detection problem has been considered from the constraint of saving network resources. For example, Chao et al. have addressed the issue of tracking a moving intruder by power-conserving operations and sensor collaboration. To achieve this, the authors defined a set of novel metrics for detecting a moving intruder and developed two efficient sleep-awake schemes called PECAS and MESH, to minimize the power consumption. Ren et al. [3] further studied the trade-off between the network detection quality (i.e., how fast the intruder can be detected) and the network lifetime. Therefore, the sensor coverage had to be carefully designed according to the detection probability with respect to specific application requirements. The authors then proposed three wave sensing scheduling protocols to achieve the bounded worst case detection probability. Rather than a static WSN architecture as the above approaches,

Liu et al. [17] have modeled the intrusion detection problem in a mobile WSN, where each sensor is capable of moving. The authors have given the optimal strategy for fast detection and shown that mobile WSN improves its detection quality due to the mobility of sensors.

In this paper, we address the intrusion detection problem from the other angle. Most of the above efforts consider intrusion detection and its efficiency in terms of the single-sensing model in a homogeneous WSN. Instead of the network architecture and detecting protocol design, we provide a comprehensive theoretical analysis on the intrusion detection in both homogeneous and heterogeneous WSNs. The detection probability is theoretically captured by using underlying network parameters, and thus, our work is of paramount importance for a network planner to design WSNs for intrusion detection applications.

To the best of our knowledge, this is the first work that considers the intrusion detection problem in a heterogeneous WSN and provides fundamental analytical results on it. The analytical results indicate the improvement on the detection quality in a heterogeneous WSN, as compared to a homogeneous WSN, either for the single sensing detection or the multiple-sensing detection scenarios. Furthermore, we have modeled the network connectivity and broadcast reachability in a heterogeneous WSN, which serve as the necessary conditions for achieving desirable detection probability.

III.INTRUSION DETECTION IN A HOMOGENEOUS WIRELESS SENSOR NETWORK

In this section, we present the analysis of intrusion detection in a homogeneous WSN. We derive the detection probability for single-sensing detection and k-sensing detection.

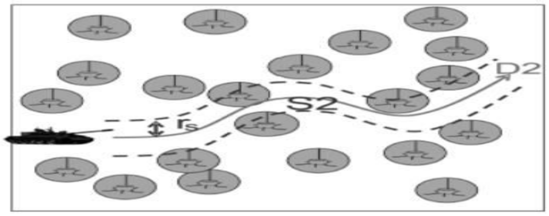

Fig. 2. INTRUSION STRATEGY 2.

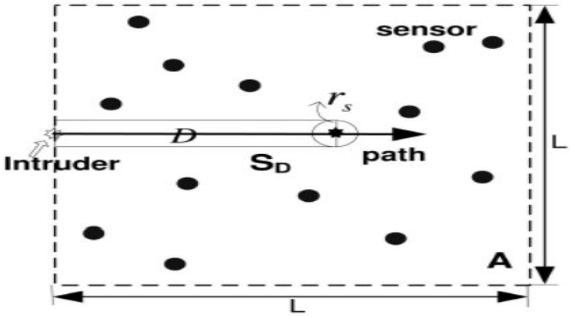

FIG. 3: THE INTRUDER STARTS FROM THE BOUNDARY OF THE WSN.

In a heterogeneous WSN, consider two types of sensors: Type I and Type II with the node density, respectively. A Type I sensor has the sensing range rs1, and the sensing coverage is a disk of area S1.

1. A Type II sensor has the sensing coverage of S2 ¼ _r2s

2. with the sensing range rs2. Without loss of generality, we can assume that rs1 > rs2 in our network model.

In a heterogeneous WSN, any point in the network domain is said to be covered if the point is under the sensing range of any sensor (Type I, Type II, or both). In this section, we present the analysis of intrusion detection probability of a heterogeneous WSN in single sensing detection and multiple-sensing detection models. We denote the intrusion distance by Dh in the given heterogeneous WSN. Again, an in>truder may be detected by the WSN once it approaches the network boundary, and the corresponding intrusion distance is Dh ¼ 0. This leads to the following theorem. Theorem 7. The probability p1½Dh ¼ 0_ that an intruder can be immediately detected once it enters the given heterogeneous WSN in a single-sensing detection model can be represented by Proof.

According to the single-sensing detection model, the intruder is detected if and only if one of the following conditions is satisfied:

. The intruder enters into the sensing coverage area of any Type I sensor(s).

. The intruder enters into the sensing coverage area of any Type II sensor(s).

Based on our network model, Theorems statistically characterize the intrusion detection probability in terms of the intrusion distance, the node density, the sensing range, and the node heterogeneity. Given a maximal allowable intrusion distance, a predefined detection probability, and the sensor capability (i.e., sensing range), the network planner can calculate the required node density by using Theorems. Hereafter, the network planner knows the number and type of sensors that have to be deployed in the WSN.

However, detecting the intruder is the first step in intrusion detection. To operate successfully, a WSN must provide satisfactory connectivity so that sensors can communicate for data collaboration and reporting to the administrative center (i.e., base station). The sensing data may have to be reported to the base station, which may be in any location of the network. If the network connectivity is not assured, it is meaningless even the sensor(s) detect the presence of the intruder. Zhang and Hou have proven that in a homogeneous WSN, if the transmission range is equal to or higher than twice of the sensing range, a given coverage probability guarantees a connectivity probability. In this manner, when the coverage is satisfied in the homogeneous WSN, the network connectivity is also statistically guaranteed so that it allows two sensors to communicate with each other. However, in a heterogeneous WSN, the deployment of sensors with different capability complicates the network operation with the asymmetric links. Specifically, a sensor with longer transmission range (i.e., Type I sensor) might reach some sensors with shorter transmission range (i.e., Type II sensors), while the Type II sensors may not be able to reach the Type I sensor.

The network connectivity has to be reconsidered. In a heterogeneous WSN, sensors mainly use a broadcast paradigm for communication [12] and high-capacity sensors usually undertake more important tasks (i.e., for broadcasting power management information or synchronization information to all the sensors). This motivates us to examine two fundamental characteristics of a heterogeneous WSN. The definitions are listed below: .Network connectivity. The probability that a packet broadcasted from any sensor (either Type I or Type II sensor) can reach all the other sensors in the network.. Broadcast reach ability. The probability that a packet broadcasted from any Type I sensor can reach all the other sensors in the network.

IV. RESULTS

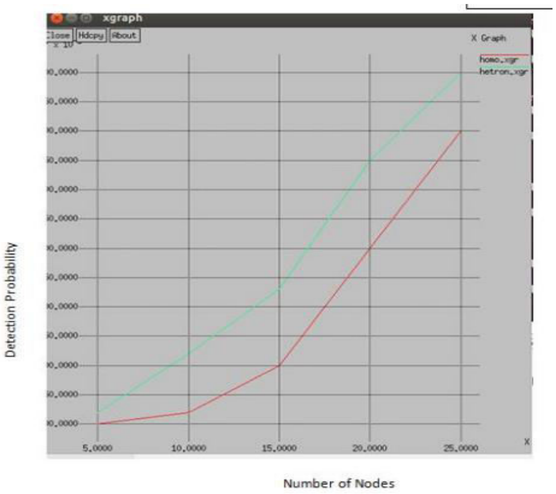

Fig. 4: GRAPH BETWEEN DETECTION PROBABILITY AND NO. OF NODES

V. CONCLUSION

This paper analyzes the intrusion detection problem in both homogeneous and heterogeneous WSNs by characterizing intrusion detection probability with respect to the intrusion distance and the network parameters (i.e., node density, sensing range, and transmission range). Two detection models are considered: single-sensing detection and multiple-sensing detection models. The analytical model for intrusion detection allows us to analytically formulate intrusion detection probability within a certain intrusion distance under various application scenarios. Moreover, we consider the network connectivity and the broadcast reachability in a heterogeneous WSN. Our simulation results verify the correctness of the proposed analytical model. This work provides insights in designing homogeneous and heterogeneous WSNs and helps in selecting critical network parameters so as to meet the application requirements.

VI. REFERENCES

[1] D.P. Agrawal and Q.-A. Zeng, Introduction to Wireless and Mobile Systems. Brooks/Cole Publishing, Aug. 2003.

[2] B. Liu and D. Towsley, “Coverage of Sensor Networks: Fundamental Limits,” Proc. Third IEEE Int’l Conf. Mobile Ad Hoc and Sensor Systems (MASS), Oct. 2004.

[3] S. Ren, Q. Li, H. Wang, X. Chen, and X. Zhang, “Design and Analysis of Sensing Scheduling Algorithms under Partial Coverage for Object Detection in Sensor Networks,” IEEE Trans. Parallel and Distributed Systems, vol. 18, no. 3, pp. 334-350, Mar. 2007.

[4] S. Banerjee, C. Grosan, A. Abraham, and P. Mahanti, Intrusion Detection on Sensor Networks Using Emotional Ants,” Int’l J. Applied Science and Computations, vol. 12, no. 3, pp. 152-173, 2005.

[5] S. Capkun, M. Hamdi, and J. Hubaux, “GPS-Free Positioning in Mobile Ad-Hoc Networks,” Proc. 34th Ann. Hawaii Int’l Conf. System Sciences, Jan. 2001.

[6] N. Bulusu, J. Heidemann, and D. Estrin, “Gps-Less Low Cost Outdoor Localization for Very Small Devices,” IEEE Personal Comm. Magazine, special issue on smart spaces and environments, 2000.

[7] D. Niculescu, “Positioning in Ad Hoc Sensor Networks,” IEEE Network, vol. 18, no. 4, pp. 24-29, July-Aug. 2004.

[8] Y. Wang, X. Wang, D. Wang, and D.P. Agrawal, “Localization Algorithm Using Expected Hop Progress in Wireless Sensor Networks,” Proc. Third IEEE Int’l Conf. Mobile Ad hoc and Sensor Systems (MASS ’06), Oct. 2006.

[9] P. Traynor, R. Kumar, H. Choi, G. Cao, S. Zhu, and T.L. Porta, “Efficient Hybrid Security Mechanisms for Heterogeneous Sensor Networks,” IEEE Trans. Mobile Computing, vol. 6, no. 6, June 2007.

[10] J.-J. Lee, B. Krishnamachari, and C.J. Kuo, “Impact of Heterogeneous Deployment on Lifetime Sensing Coverage in Sensor Networks,” Proc. First Ann. IEEE Comm. Soc. Conf. Sensor and Ad Hoc Comm. and Networks, pp. 367-376, Oct. 2004.

[11] V.P. Mhatre, C. Rosenberg, D. Kofman, R. Mazumdar, and N. Shroff, "A Minimum Cost Heterogeneous Sensor Network with a Lifetime Constraint," IEEE Trans. Mobile Computing, vol. 4, no. 1, pp. 4-15, 2005.

[12] M. Yarvis, N. Kushalnagar, H. Singh, A. Rangarajan, Y. Liu, and S. Singh, "Exploiting Heterogeneity in Sensor Networks," Proc. IEEE INFOCOM, 2005.

[13] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A Survey on Sensor Networks," IEEE Comm. Magazine, vol. 40, no. 8, pp. 102-114, Aug. 2002.

[14] H. Kung and D. Vlah, "Efficient Location Tracking Using Sensor Networks," Proc. IEEE Wireless Comm. and Networking Conf., vol. 3, pp. 1954-1961, Mar. 2003.

[15] C.-Y. Lin, W.-C. Peng, and Y.-C. Tseng, "Efficient in-Network Moving Object Tracking in Wireless Sensor Networks," IEEE Trans. Mobile Computing, vol. 5, no. 8, pp. 1044-1056, 2006.