Effective Intrusion Detection System for Wireless Sensor Networks Using Node Localization Mechanism

Mr. S.V.N. Vamsidhar[1], G. Nanditha[2], G. Krishna Pujitha[3], A. Mastanamma[4], D. Jayasurya[5]
[1]Asst. Prof, Dept of CSE, Tirumala Engineering College, Narasaraopet, Guntur, A.P., India
[2,3,4,5]B. Tech Students, Dept of CSE, Tirumala Engineering College, Narasaraopet, Guntur, A.P., India

ABSTRACT - In the recent development of wireless sensor networks, diverse functional areas are dealt with, to carry out various functionalities such as disaster revitalization, deep scan, intrusion detection, and a host of other functionalities in a tidy digital environment. The feature of the wireless sensor network, node localization, is primarily used for calculating the network's liveliness proficient. Localization of nodes necessitates advising root incidents, assisting community requests, and routing a solution to the deployed network framework. This proposed study focuses on these issues in heterogeneous Wireless Sensor Networks (WSN) models, as well as estimating various methods for node position discovery. The detection of intrusion in WSN will concentrate on realistic implementations. Many of these tools are used for detecting interference in smart offices and recent network infrastructure. This paper presents the Liveliness Proficient Node Localization (LPNL) algorithm for network connectivity and broadcast reachability, both of which are needed for some corresponding detection possibilities in WSN. The simulation results validate and confirm the empirical values for heterogeneous WSN.

Keywords: Intrusion Detection, Node Localization, Wireless Sensor Networks (WSN)

I. INTRODUCTION

Wireless Sensor Network (WSN) is a network of spatially distributed wireless sensors that track different changes in environmental conditions in a mutual manner without relying on any underlying infrastructure support [1]. Several network parameters, such as sensing range, propagation range, and node density range, are carefully considered during the network design process, depending on the application. To do so, it is important to capture the effects of network parameters on network output in relation to device requirements. Given that most technologies depend on effective localization, i.e., estimating their locations in various predetermined coordinate structures, designing efficient localization algorithms is a consideration.

The sensor nodes are small and have limited resources. Sensor styles vary depending on the implementation of WSNs. Regardless of the application, resources such as power, memory, and band width are reduced. Furthermore, since the majority of sensor nodes are discarded in the real world, it is critical to understand energy quality in order to increase the life cycle of the WSN. Significant attempts have been made to reduce electricity demand and increase the network's lifespan. One popular strategy is to put several sensor nodes to sleep in order to save energy and then wake them up using different techniques. Working to optimise the life of WSNs is a current field of study.

In recent years, there has been a need for heterogeneous WSN implementation. Sensor nodes in WSNs are typically static once deployed and communicate primarily through broadcast rather than point-to-point communication. Sensor nodes are deployed in a variety of scenarios, and systems must be protected from all kinds of intruders. For sensor networks, a set of safety protocols or mechanisms has been created. SPINS (Sensor Protocol for Information through Negotiation), for example, is a system of protocols that provides protected information protection, two-way information authentication and invention, and legal broadcast for sensor networks [6].

LEAP (Localized Encryption and Authentication Protocol) is intended to enable in-network processing based on the various security specifications for various forms of message sharing [7]. In general, network protection solutions are classified into two types: avoidance solutions and detection solutions. As the first line of defence, prevention methods such as encryption, authentication, firewalls, and physical isolation are typically used to deter external threats. In a WSN, intrusion detection (i.e., target tracking) may be viewed as a control device for identifying the attacker entering the network domain.

II. RELATED WORK

[2] describes the implementation of a vast number of inexpensive homogeneous and heterogeneous sensor systems of varying capabilities. One of the important applications of WSNs is intrusion detection, and many methods for intrusion detection in homogeneous WSNs have recently been proposed [3], [4]. A detection-based protection scheme with limited computing and communication capability for sensor nodes. They have precise properties, such as stable neighbourhood knowledge, which allows for the identification of anomalies in networking and transceiver activities of neighbouring nodes [5].

As sensor networks approach sensor node implementation, security concerns have emerged as a critical problem for making sensor networks viable and usable [6]. LEAP (Localized Encryption and Authentication Protocols), a key management protocol for sensor networks intended to facilitate network device processing while breaching the security effect of a node breach to the compromised node's immediate network neighbourhood, has been proposed [7].

Protection in sensor networks is critical in smart world surveillance and home security applications because it prevents intruders from eavesdropping, interfering with sensor data, and launching denial-of-service (DOS) attacks against the whole network [8]. The tracking of the movement of an intruder detection issue has been considered for resource restrictions [9]. Theoretical work on intrusion detection in both homogeneous and heterogeneous WSNs has been introduced and compared with either single sensing detection or multiple-sensing detection scenarios [10].

Scalable Monitoring Using Networked Sensors (STUN), a tracking system that scales well to large numbers of sensors and moving objects by using hierarchy, has been studied [11] [12].

III. PROPOSED ARCHITECTURE

The overall device design of intrusion detection in heterogeneous wireless sensor networks is described in this section. The user or applications, network setup, network execution, and liveliness estimation are all part of the System Architecture model. The System architecture is depicted in Figure 1.

The main task for configuring the network in a defined manner is by the user, which involves user tasks such as setting network size, node size, sensor radius, transmission time, transmission radius, transmission cost, and receiver cost, among others. The network implementation can mostly handle node deployment depending on user configuration or automatic programmes.

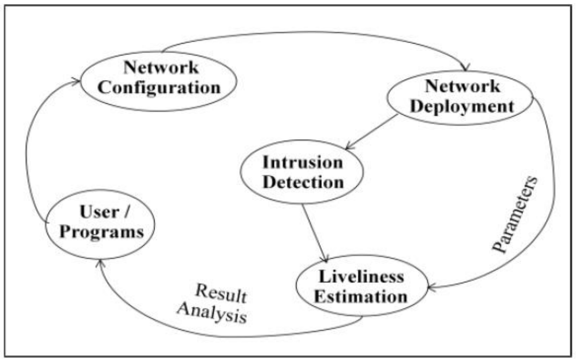

Figure 1. Proposed Architecture

Intrusion Detection can identify intruders in deployed wireless sensor networks and dynamically notify sink or intelligent sensor nodes as soon as they are identified. The power efficiency will be estimated by Liveliness Estimation based on network implementation parameters and detection accuracy. Finally, the consumer can track the predicted effects and take appropriate measures.

In terms of how many sensors are needed to identify an intruder, there are two detection models: single sensing detection model and multiple-sensing detection model. The attacker can be detected using only one sensor and their intelligent actions in the single-sensing detection model.

The intruder can only be detected using mutual information from at least m sensors (m is specified by particular application requirements) in the multiple-sensing detection model. Multiple sensing and m-sensing will be addressed interchangeably in this paper for ease of speech.

IV. RESULTS AND OBSERVATION

This section outlines the simulation and the interpretation of the results. To begin, the user should set the necessary parameters for network deployment as shown. The consumer must configure the network size, sensor radius, transmission radius, transmitter period, transmission cost, and receiver cost for this configuration environment.

Second, the consumer must configure power, with initial power set to 1000 units and residual power set to 1000 units. Often displays sensor behaviour for real intrusion detection sensing in WSN. As seen in Figure, the grid depicts the deployment of sinks in a WSN. The simulation control will display the network deployment, start simulation, replay simulation, and simulation status will display output metrics, as shown in Figure. The simulation control's first button is the deployment network, which is used to deploy the sensors in the 2D plane. The second button is used to launch the simulation; if pressed, it will show the simulation of the analytical model. The next button is replay simulation, which is used to react to the previous simulation once more. The next button is the exit button, which when pressed would exit the analytical model. The performance metrics, or status, test all of the performance measures that were used to analyse the results.

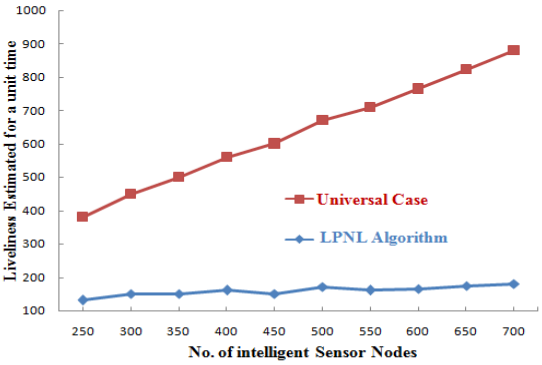

Figure 1. Results Observed

V. CONCLUSION

This paper investigates intrusion detection in heterogeneous wireless sensor networks by characterising the likelihood of intrusion detection based on network parameters such as sensing range, propagation size, node density range, and node distance. The key trade-offs found in WSN are the deployment of high-cost sensors or intelligent sensor nodes while keeping overall cost constraints in mind. The intelligent sensor devices will act as a cluster-head or sink to capture and process data from low-cost sensors, extending the network sensing operation's length. Under overall cost constraints, the LPNL algorithm minimises the implementation of intelligent sensor nodes in an optimal manner. Furthermore, improve intruder detection in a liveliness proficient manner. The findings of the established analytical model validate the correctness of the proposed analytical model, which is demonstrated by simulation. The analysis can be expanded to investigate a variety of topics, such as architecture problems, the anomaly detection paradigm, and the multilayer integration solution. The architecture research is updating its concept and planning to incorporate it, as well as studying the efficiency consequences.

VI. REFERENCES

[1] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam , E. Cayirci, “A Survey on Sensor Networks”, IEEE Communication Magazine, vol.40, no. 8, pp. 102-14, Aug. 2011.

[2] Lee, J.J., Krishnamachari, B., Kuo, C.C.J.: Impact of Heterogeneous Deployment on Lifetime Sensing Coverage in Sensor Networks (IEEE SECON). (2010).

[3] Hu, W., Chou, C.T., Jha, S., and Bulusu, N.: Deploying Long-Lived and Cost-effective Hybrid Sensor Networks. Elsevier Ad-Hoc Networks, Vol. 4, Issue 6. (2010) 749-767.

[4] A. P. da Silva, M. Martins, B. Rocha, A. Loureiro, L. Ruiz, and H. C. Wong, “Decentralized intrusion detection in wireless sensor networks,” in Proceedings of the 1st ACM international workshop on Quality of service & security in wireless and mobile networks.

[5] I. Onat and A. Miri, “An intrusion detection system for wireless sensor networks,” in Proceeding of the IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, vol. 3, Montreal, Canada, August 2009, pp. 253– 259.

[6] A. Perrig, et al., “SPINS: Security Protocols for Sensor Networks”, Wireless Networks, 8(5):521- 534, Sep. 2008.

[7] S. Zhu, S. Setia, and S. Jajodia, “LEAP: Efficient Security Mechanisms for Large-scale Distributed Sensor Networks”, Proc. Of the 10th ACM Conference on Computer and Communications Security (CCS '03), Oct. 2004.

[8] J. Deng, R. Han, and S. Mishra, “A Performance Evaluation of Intrusion-tolerant Routing in Wireless Sensor Networks”, Proc. Of the 2nd Int. IEEE Workshop on Information Processing in Sensor Networks (IPSN’03), Apr. 2003.

[9] Y. Wang, X. Wang, B. Xie, D. Wang, and D. P. Agrawal, “Intrusion detection in homogeneous and heterogeneous wireless sensor networks,” IEEE Transactions on Mobile Computing, vol. 7, no. 6, pp. 698–711, 2008.

[10] O. Dousse, C. Tavoularis, and P. Thiran, “Delay of intrusion detection in wireless sensor networks,” in Proceedings of theSeventh ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc), 2006.

[11] H. Kung and D. Vlah, “Efficient location tracking using sensor networks,” in IEEE Wireless Communications and Networking Conference, ser. 3, vol. 3, March 2005, pp. 1954–1961.

[12] C.-Y. Lin, W.-C. Peng, and Y.-C. Tseng, “Efficient in-network moving object tracking in wireless sensor networks,” IEEE Transactions on Mobile Computing, vol. 5, no. 8, pp. 1044– 1056, 2005.

[13] L. Doherty, K. S. Pister, and L. E. Ghaoui., Convex optimization methods for sensor node position estimation. In Proceedings of IEEE INFOCOM ’01, 2001.

[14] A. Savvides, C. Han, and M. Srivastava. Dynamic fine-grained localization in ad-hoc networks of sensors. In Proceedings of ACM MobiCom ’01, pages 166-179, 2001.