International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/CSEIT2173140

Implementation of Intrusion Detection in Homogeneous and Heterogeneous Wireless Sensor Networks

Manoshri A. Ghawade[1], Dr. Sheetal S. Dhande[2]

[1]PG Scholar, Department of Computer Science & Engineering, Sipna COET Amravti, Maharashtra, India

[2] Professor, Department of Computer Science & Engineering, Sipna COET Amravti, Maharashtra, India

Article Info
Volume 7, Issue 3
Page Number: 664-670

Publication Issue :
May-June-2021

Article History
Accepted : 12 June 2021
Published : 20 June 2021

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. 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.

Keywords : Intrusion detection, Wireless Sensor Network (WSN), Heterogeneous.

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. As shown in Fig. 1, 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.

II. LITERATURE REVIEW

- Intrusion Detection

An Intrusion detection system (IDS) is software and/or hardware designed to detect unwanted attempts at accessing, manipulating, and/or disabling of computer mainly through a network, such as the Internet. These attempts may take the form of attacks, as examples, by crackers,, malware and/or disgruntled employees. IDS cannot directly detect attacks within properly encrypted traffic.

An intrusion detection system is used to detect several types of malicious behaviors that can compromise the security and trust of a computer system. This includes network attacks against vulnerable services, data driven attacks on applications, host based attacks such as privilege escalation, unauthorized logins and access to sensitive files, and viruses

IDS can be composed of several components: Sensors which generate security events, a Console to monitor events and alerts and control the sensors, and a central Engine that a records event logged by the

sensors in a database and uses a system of rules to generate alerts from security events received. There are several ways to categorize an IDS depending on the type and location of the sensors and the methodology used by the engine to generate alerts. In many simple IDS implementations, all three components are combined in a single device or appliance.

- Wireless Sensor Network

A wireless sensor network (WSN) is a wireless network consisting of spatially distributed autonomous devices using sensors to cooperatively monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants, at different locations. The development of wireless sensor networks was originally motivated by military applications such as battlefield surveillance. However, wireless sensor networks are now used in many civilian application areas, including environment and habitat monitoring, health-care applications, home automation, and traffic control.

In addition to one or more sensors, each node in a sensor network is typically equipped with a radio transceiver or other wireless communications device, a small micro-controller, and an energy source, usually a battery. The envisaged size of a single sensor node can vary from shoe box-sized nodes down to devices the size of grain of dust although functioning 'motes' of genuine microscopic dimensions have yet to be created. The cost of sensor nodes is similarly variable, ranging from hundreds of dollars to a few cents, depending on the size of the sensor network and the complexity required of individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and bandwidth.

A sensor network normally constitutes a wireless ad-hoc network, meaning that each sensor supports a multi-hop routing algorithm (several nodes may forward data packets to the base station).

III.SCRUTINY OF ISSUE

Initially, the IDS solutions have been designed for the wired networks. There is a massive difference between these networks in terms of communication protocols, architecture, connections, etc. which needs the new mechanism of IDS that overcomes the limitations of WSN.

The purpose of IDS is to deal with the vulnerability of WSN against multiple attacks; the IDS should support the detection of different types of attacks on different layers of wireless sensor network with high detection accuracy and low false alarm rate. Data mining techniques such as SVM, Random Forest and Neural Networks have also been used as a detection approach in some model which provides high detection accuracy. It is observed that SVM algorithm provided the most accurate results. Since there are multiple proposed IDS frameworks available, each with some strengths and weaknesses, so the selection of the appropriate IDS should be done by considering the requirements of the intended application such as the required accuracy, attacks that need to be detected, acceptable false detection rate, etc.

In WSN, security threats are more different from wired and non-energy constrained wireless networks. These differences are caused from typical properties of WSN. Energy is the most important constraint for WSN and in addition to three components of security (confidentiality, integrity, and availability), there is a new basic aspect that is energy.

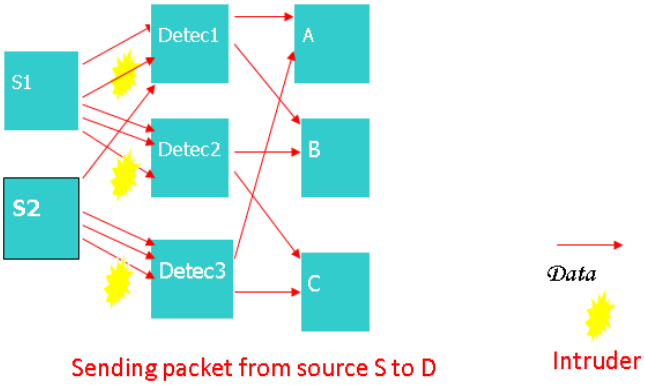
- Confidentiality: Confidentiality means that the information is available or accessible to the authorized users only. It is the most important security goal. To achieve confidentiality Encryption with security key is used.

- Integrity: Data should not be altered or manipulated by adversary as it travels from sender to the recipient.
- Availability: Data should be available to the authorized user whenever needed despite of any internal or external attacks i.e. DoS attack

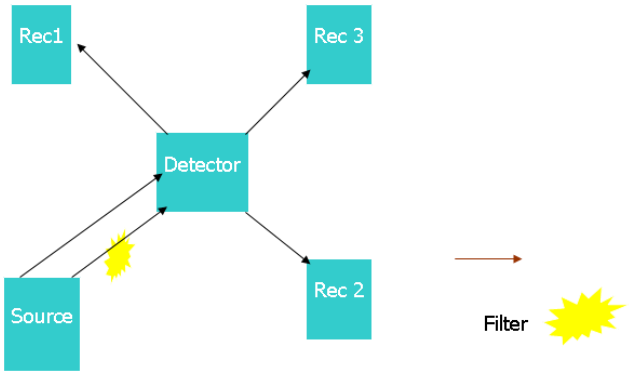
IV. ARCHITECTURE OF IDS

- Constructing Sensor Network - In this module, we are going to connect the network .Each node is connected the neighboring node and it is independently deployed in network area. And also deploy the each port no is authorized in a node.
- Packet Creation - In this module, browse and select the source file. And selected data is converted into fixed size of packets. And the packet is send from source to detector.
- Find authorized and un authorized port - The intrusion detection is defined as a mechanism for a WSN to detect the existence of inappropriate, incorrect, or anomalous moving attackers. In this module check whether the path is authorized or unauthorized. If path is authorized the packet is send to valid destination. Otherwise the packet will be deleted. According port no only we are going to find the path is authorized or Unauthorized.
- Constructing Inter-Domain Packet Filters - If the packet is received from other than the port no it will be filtered and discarded. This filter only removes the unauthorized packets and authorized packets send to destination.
- Receiving the valid packet - In this module, after filtering the invalid packets all the valid Packets will reach the destination.

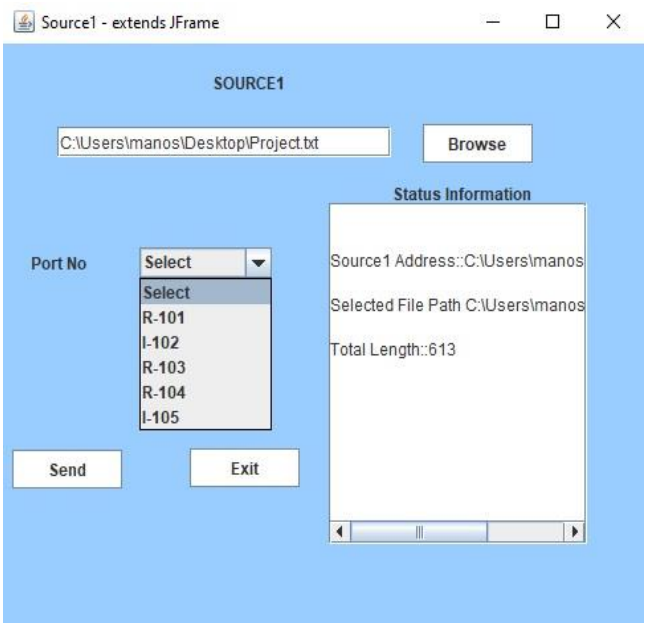
Heterogeneous:

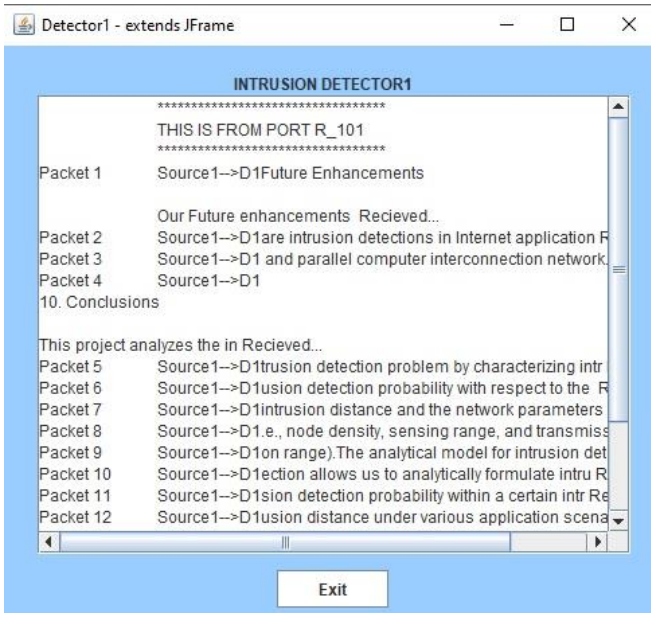


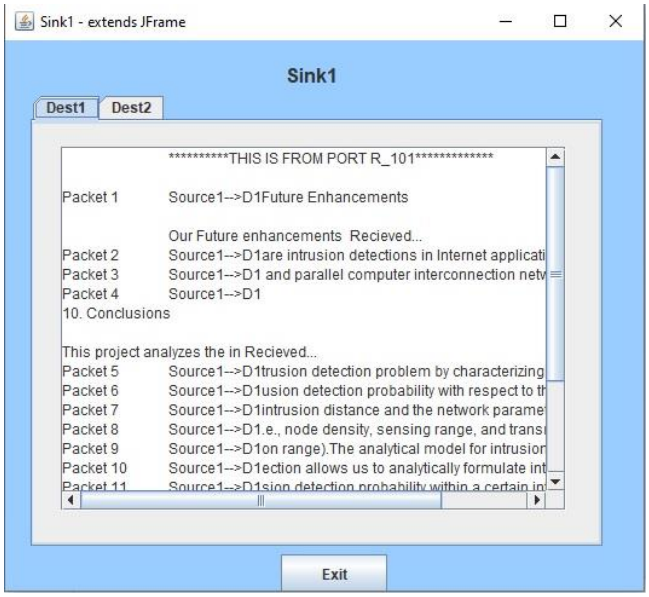
Homogeneous:



V. FINDINGS OF INTRUSION DETECTION SYSTEM







A. Comparative Analysis

3.1 Current Scenario Findings

1. single-sensing detection, the intruder can be successfully detected by a single sensor
2. Previous work was according to homogeneous single sensor in wireless sensor network
3. It is because individual sensors can only sense a portion of the intruder.

3.2 Developed Prototype Findings

1. Intrusion detection in heterogeneous WSNs by characterizing intrusion detection with respect to the network parameters

2. Two detection models are:
   - Single-sensing detection
   - Multiple-sensing detection models

3.3 Pitfalls

3.4

1. The sensed information provided by a single sensor might be inadequate for recognizing the intruder.
2. So that there is no guarantee for our information has been sent securely.

3.5 Supremacy

1. Through sensing the network we able to find possible node in the wireless Sensor network.

By finding the intruders we can send our information in a secured manner.

3.5 COMPARATIVE ANALYSIS OF PROPOSED IDS FRAMEWORKS FOR WSN

References	Detection Technique	Detection Method	Source of Audit Data	Handled Attacks	Energy Efficiency	Strengths	Weakness
Y Maleh et al. [11]	Specifications based on	Hybrid IDS	HyIDS	Selective Forwarding	High	Increased detection	Increased

(2015)	Detection	with Anomaly based SVM Classification and Signature based Detection		, Hello Flood, Black hole.		accuracy and low false positive rate. Increased network lifetime. Reduce energy consumption as IDS is only active when needed.	computation complexity needed for SVM algorithm.
Sushant et al. [12] (2016)	Anomaly Detection	Agent-based Anomaly Detection algorithm	NIDS	Unknown or Novel attacks.	Low	Low False alarm rate. Detect compromised nodes in Homogenous WSN	Communication overhead between the IDS agent and other nodes. Only efficient for small networks.
MM Ozcelik et al. [13] (2017)	Signature based Detection	Hybrid Trust	HyIDS	Malicious Nodes Attack	Moderate	Increased network lifetime Hybrid trust used to increase detection accuracy.	Communication overhead of transmitting CPs.
Park et al. [14] (2018)	Signature based Detection	Random Forest Classification	NIDS	DoS including Black Hole	Moderate	High prediction accuracy.	Increased computation complexity needed for Random Forest algorithm.
Jinhui et al. [15] (2018)	Specification based Detection	Energy Consumption Trust	HyIDS	Hybrid DoS including Sink hole	Moderate	Increased network lifetime. Increased network throughput.	Increased computation overhead. Assumed that CH is not

VI. CONCLUSION AND FUTURE SCOPE

This project 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.

Our Future enhancements are intrusion detections in Internet application and parallel computer interconnection network.

VII. REFERENCES

[1]. R. Hemenway, R. Grzybowski, C. Minkenberg, and R. Luijten, "Optical-packet-switched interconnect for supercomputer applications,"OSA J. Opt. Netw., vol. 3, no. 12, pp. 900–913, Dec. 2004.

[2]. Minkenberg, F. Abel, P. Müller, R. Krishnamurthy, M. Gusat, P.Dill, I. Iliadis, R. Luijten, B. R. Hemenway, R. Grzybowski, and E.Schiattarella, "Designing a crossbar scheduler for HPC applications,"IEEE Micro, vol. 26, no. 3, pp. 58–71, May/Jun. 2006.

[3]. E. Oki, R. Rojas-Cessa, and H. Chao, "A pipeline-based approach formaximal-sized matching scheduling in input-buffered switches," IEEE Commun. Lett., vol. 5, no. 6, pp. 263–265, Jun. 2001.

[4]. Minkenberg, I. Iliadis, and F. Abel, "Low-latency pipelined crossbar arbitration," in Proc. IEEE GLOBECOM 2004, Dallas, TX, Dec. 2004, vol. 2, pp. 1174–1179.

[5]. Minkenberg, R. Luijten, F. Abel, W. Denzel, and M. Gusat, "Current issues in packet switch design," ACM Comput. Commun. Rev., vol. 33, no. 1, pp. 119–124, Jan. 2003.

[6]. C. Minkenberg, F. Abel, P. Müller, R. Krishnamurthy, and M. Gusat,"Control path implementation of a low-latency optical HPC switch," inProc. Hot Interconnects 13, Stanford, CA, Aug. 2005, pp. 29–35.

[7]. C.-S. Chang, D.-S. Lee, and Y.-S. Jou, "Load-balanced Birkhoff-von Neumann switches, part I: One-stage buffering," Elsevier Comput.Commun., vol. 25, pp. 611–622, 2002.

[8]. Tanenbaum, Computer Networks, 3rd ed. Englewood Cliffs, NJ: Prentice Hall.

[9]. R. Krishnamurthy and P. Müller, "An input queuing implementation for low-latency speculative optical switches," in Proc. 2007 Int. Conf.Parallel Processing Techniques and Applications (PDPTA'07), Las Vegas, NV, Jun. 2007, vol. 1, pp. 161–167.

[10]. H. Takagi, Queueing Analysis, Volume 3: Discrete-Time Systems. Amsterdam: North-Holland.

[11]. Maleh, Yassine, Abdellah Ezzati, Youssef Qasmaoui, and Mohamed Mbida. "A global hybrid intrusion detection system for wireless sensor networks." Procedia Computer Science 52 (2015): 1047-1052.

[12]. Pandey, Sushant Kumar, Prabhat Kumar, Jyoti Prakash Singh, and M.P. Singh. "Intrusion detection system using anomaly technique in wireless sensor network." In 2016 International Conference on Computing, Communication and Automation (ICCCA), pp. 611-615. IEEE, 2016.

[13]. Ozcelik, Mert Melih, Erdal Irmak, and Suat Ozdemir. "A hybrid trust based intrusion detection system for wireless sensor networks." In 2017 International Symposium on Networks, Computers and Communications (ISNCC), pp. 1-6. IEEE, 2017.

[14]. Park, Taehwan, Dongkeun Cho, and Howon Kim. "An Effective Classification for DoS Attacks in Wireless Sensor Networks." In 2018 Tenth International Conference on Ubiquitous and Future Networks (ICUFN), pp. 689-692. IEEE, 2018.

[15]. Jinhui, Xie, Tao Yang, Yang Feiyue, Pan Leina, Xu Juan, and Hou Yao. "Intrusion Detection System for Hybrid DoS Attacks using Energy Trust in Wireless Sensor Networks." Procedia computer science 131 (2018): 1188-1195.

Cite this article as :

Manoshri A. Ghawade, Dr. Sheetal S. Dhande, "Implementation of Intrusion Detection in Homogeneous and Heterogeneous Wireless Sensor Networks", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 7, Issue 3, pp.664-670, May-June-2021. Available at

doi : https://doi.org/10.32628/CSEIT2173140

Journal URL : https://ijsrcseit.com/CSEIT2173140