IJERMS

International Journal of Engineering Researches and Management Studies

REVIEW OF INTRUSION DETECTION SYSTEM IN A HETEROGENEOUS WIRELESS SENSOR NETWORKS

Dr.M.Jagadeeshwar[*1], Dr.Suman Kumar Shriramoju[2] & Dr. Adloori Ramesh Babu[3]

[*1]Associate Professor, Department of computer science, Chaitanya group of colleges, Warangal
[2]Associate Professor, Department of computer science, Svs group of institutions, Warangal
[3]Associate Professor, Department of computer science, Wolaita Sodo University, Ethiopia

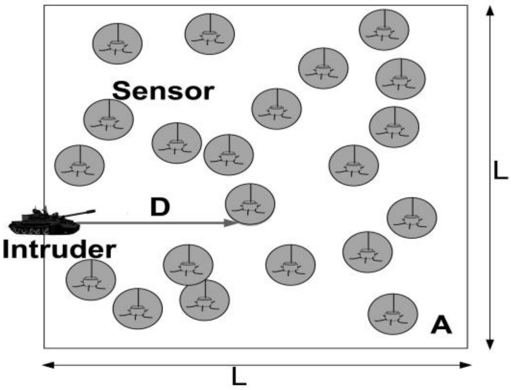
ABSTRACT

IDS in Wireless Sensor Network (WSN) are of useful enthusiasm for some applications, for example, distinguishing an interloper in a war zone. The interruption recognition is characterized as a component for a WSN to distinguish the presence of unseemly, wrong, or irregular moving aggressors. For this reason, it is a basic issue to portray the WSN parameters such as hub thickness and detecting range as far as an alluring recognition likelihood. In this paper, we consider this issue agreeing to WSN model that is heterogeneous WSN. Moreover, we infer the location likelihood by considering two detecting models: single-detecting identification and different detecting discovery. What's more, we talk about the system availability and communicate reach ability, which are essential conditions to guarantee the comparing location likelihood in a WSN. Our reenactment comes about approve the systematic esteems for both homogeneous and heterogeneous WSNs.

KEYWORDS: Intrusion detection system, node density, sensing range, Wireless Sensor Network (WSN).

1. INTRODUCTION

Remote Sensor Network (WSN) is a gathering of spatially sent remote sensors by which to screen different changes of natural conditions (e.g., timberland fire, air contamination fixation, and protest moving) in a collective way without depending on any basic foundation bolster [1]. As of late, a number of research endeavors have been made to create sensor equipment and system models keeping in mind the end goal to successfully convey WSNs for an assortment of utilizations. Due to a wide assorted variety of WSN application prerequisites, be that as it may, a universally useful WSN configuration can't satisfy the necessities of all applications. Many system parameters, for example, detecting run, transmission range, and hub thickness must be precisely considered at the system configuration organize, agreeing to particular applications. To accomplish this, it is basic to catch the effects of system parameters on organizing execution concerning application particulars. Recently, prior research efforts have been made to develop network architectures and sensor hardware in order to effectively deploy WSNs for a variety of applications. However, Due to a wide diversity of WSN application requirements, a general-purpose WSN design cannot fulfill the needs of all applications. Network parameters such as sensing range, node density and transmission range have to be carefully considered according to specific applications, at the network design stage. In order to achieve this, it is essential to capture the impacts of network parameters on network performance.



Intrusion detection in a WSN

2. A HETEROGENEOUS WSN

A Heterogeneous WSN is more complex as compared to homogeneous WSN and which consists of a number of sensor nodes of different types deployed in a particular area and which are collectively working together to achieve a particular aim. The aim may be any of the physical or environmental condition. For this purpose, a number of sensors, N, are deployed in an area of interest, A, to monitor the environmental changes by using optical, mechanical, acoustic, thermal, RF and magnetic sensing modalities . In this way, possible intruder approaching or travelling inside the deployment field can be detected by the WSN if it enters into the sensing range(s) of one or multiple sensor.

Single-sensing detection model

In single-sensing detection model an intruder is successfully detected by single sensor. But in some cases the information provided by singe sensor may not be correct as it can sense only a portion of the network domain. In that case we use multi-sensing detection model.

Multi-sensing detection model

In multi-sensing system an intruder is detected by multiple collaborating sensors. The number of sensors depends upon specific applications. For example at least sensors are required to determine the location of intruder.

3. AN INTRUSION DETECTION SYSTEM (IDS)

An intrusion detection system (IDS) is a type of security software designed to automatically alert administrators when someone or something is trying to compromise information system through malicious activities or through security policy violations. An IDS works by monitoring system activity through examining vulnerabilities in the system, the integrity of files and conducting an analysis of patterns based on already known attacks. It also automatically monitors the Internet to search for any of the latest threats which could result in a future attack. Intrusion detection system plays an important role in the area of computer security, in particular network security, so an attempt to apply the idea in WSNs makes a lot of sense. However, there are currently only a few studies in this area. Where certain monitor nodes in the network are responsible for monitoring their neighbors, looking for intruders. They listen to messages in their radio range and store in a buffer specific message fields that might be useful to an IDS system running within a sensor node.

The energy consumption and network lifetime of a WSNs are interdependent on each other. The energy required for internal processing of data is less compared to the transfer of data from one sensor node to the other. When all sensor nodes are in the process of detecting an intruder and communicating this information to the base station a large amount of energy is consumed and the network lifetime is reduced. The main objectives of our work are:

a. to activate only a set of sensor nodes (cluster heads) to participate in detecting an intruder and communicate the information to the sink node.
b. Minimize the attack on implementation attack.
c. Reduce the energy consumption and increase the network lifetime of the WSNs.

***Assumptions*:**

(i) The WSNs is a static network and intruder is a moving object.
(ii) Each node consists of Omni-directional antenna properties.
(iii) Sink node knows all the nodes location and their neighbor list.
(iv) Algorithm is executed at the sink node and it sends a packet to the selected nodes to activate its IDS module.

4. METHODOLOGY

Intrusion detection plays an important role in the area of security in WSN. Detection of any type of intruder is essential in case of WSN. WSN consumes a lot of energy to detect an intruder. Therefore we derive an algorithm for energy efficient external and internal intrusion detection. We also analyze the probability of detecting the intruder for heterogeneous WSN. This paper considers single sensing and multi sensing intruder detection models. It is found that our experimental results validate the theoretical results.

5. INTRUSION DETECTION IN HETEROGENEOUS WSN

In this paper, an Intruder is defined as any moving object that enters into the WSN area. We have derived the detection probability for single-sensing and multi-sensing detection.

Implementation and Algorithm

Let *n* be the minimum number of sensors required to cover the network area. The minimum number of sensors participating in intrusion detection is equal to the minimum number of sensors required to cover the WSN area. Intrusion detection module performs two functions:

(i) Finding the intruder,
(ii) Passing the information to the base station.

The MEID in Phase I determine the minimum number of sensors required to cover the area depending on both sensing range and transmission range as shown in algorithm. The MEID algorithm in Phase II determines the number of nodes required to perform intrusion detection is at least *n* as shown in Phase II.
algorithm

Phase I

```
MinNode(tr,rs)
{
if tr >= rs then
n Π r2
s ≡ kmodL2
where k = {0 to Π r2
s-1}
if tr < rs
≡ kmodL2
nΠtr2
where k = {0 to Π tr2-1}
}
```

Phase II

```
At sink node
{
Assign U = {R} the set of nodes in the WSN area.
Let N(i) is the set of neighbors of node i. repeat
If N(i) ≠ Ø
Find min N(i)
Put i in Stack;
I={a / the distance between i and N(i) < (rs/2)}
if N(i) > 1;
U = U - [i U I];
else
U = U - I;
Until U is Null
}
```

Algorithm:-Minimization of External Intrusion Detection Algorithm

6. CONCLUSION

This paper examines the IDS issue in heterogeneous WSNs by describing ID discovery likelihood regarding the interruption separate and the system Two discovery models are viewed as: single-detecting discovery and multiple detecting identification models. The explanatory model for interruption location enables us to scientifically plan interruption discovery likelihood inside a specific interruption separate under different application situations. In addition, we think about the system availability what's more, the communicate reach ability in a heterogeneous WSN. Our reenactment comes about confirm the rightness of the proposed logical model. This work gives experiences in outlining heterogeneous WSNs and helps in choosing basic system parameters in order to meet the application prerequisites

7. ACKNOWLEDGMENT

The authors are deemed to express their gratitude to UGC-SERO-HYD (ROMRP-SERO-COMP 2015-16-10946) for the financial assistance and we are grateful to the chairman Dr.Ch.V.Purushotham Reddy garu and principal Dr.K.Veera Venkataiah for providing research facilities.

REFERENCES

1. S Zhu, S Setia and S Jajodia, LEAP: Efficient Security Mechanisms for Large-scale Distributed Sensor Networks, in Proceedings of the 10th ACM Conference on Computer and Communications Security (CCS '03), October 2003, 62-72.
2. Yang Xia Luo and Ye Guo, A Survey on Intrusion Detection of Wireless Sensor Network, in Proceedings of the Second International Conference on Information Science and Engineering(ICISE), 2010, 1798-1802.
3. William Stallings, Cryptography and Network Security, in 3rd Edition, (Singapore: Prentice Hall, Pearson Education, 2004).
4. SutharshanRajasegarar, Christopher Leckie and MarimuthuPalaniswami, Anomaly Detection in Wireless Sensor Networks, in IEEE Wireless Communications, 2008, 34-40.
5. Yun Wang, Xiaodong Wang, Bin Xie, Demin Wang and Dharma P Agrawal, Intrusion Detection in Homogeneous and Heterogeneous Wireless Sensor Networks, in IEEE Transactions on Mobile Computing, 7(6), 2008, 698-711.
6. I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, “ASurvey on Sensor Networks”, IEEE Communication Magazine, vol. 40, no.8, pp. 102-14, Aug. 2011.
7. Y.Wang, Y. K. Leow, and J. Yin, “Is straight-line path always the best for intrusion detection in wireless sensor networks,” in Proceedings of Fifteenth International Conference on Parallel and Distributed Systems, 2009, pp. 564-571.