ISSN 2250-3153

Intrusion Detection: An Energy Efficient Approach in Heterogeneous WSN

Pankaj Kumar Srivastava[*], Priyanka Rai[**], Upama Singh[***]

[*] B.tech Final Year, Student of Computer Science & Engineering, ITM Gida, Gorakhpur
[**] B.tech Final Year, Student of Computer Science & Engineering, ITM Gida, Gorakhpur
[***] B.tech Final Year, Student of Computer Science & Engineering, ITM Gida, Gorakhpur

Abstract- Intrusion detection in Wireless Sensor Network (WSN) is widely used in many applications such as detecting an intruder. The intrusion detection is a mechanism for a Wireless Sensor Network to detect the existence of inappropriate, incorrect or unsuspicious moving attackers. WSN consumes lots of energy to detect an intruder. The main objective of this approach was developed under JFrame Builder tools is to provide simple and secure algorithm for energy efficient approach for external intrusion as well as internal intrusion detection. Wireless sensor networks (WSNs) often consist of tiny devices with limited energy, computational power, transmission range, and memory. WSNs offer a variety of potential means to monitor environments. 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.

Index Terms- Intrusion detection, sensor nodes, Wireless Sensor Network (WSN), Heterogeneous WSN.

I. INTRODUCTION

An Intrusion detection system (IDS) is designed to detect unwanted attempts at accessing, disabling of computer mainly through a network, such as the Internet. Intrusion detection plays an key role in the area of network security, so an attempt to apply the idea in WSNs makes a lot of sense. Intrusion, *i.e.* unauthorized access or login (to the system, or the network or other resources); intrusion is a set of actions from internal or external of the network, which violate security aspects (including integrity, confidentiality, availability and authenticity) of a network's resource. There are two approaches: misuse detection and anomaly detection. Misuse detection identifies an unauthorized use from signatures while anomaly detection identifies from analysis of an event. When both techniques detect violation; they raise an alarm signal to warn the system. Wang divides intrusion detection techniques into single-sensing detection and multi-sensing detection. In single-sensing detection, the intruder can be successfully detected by one sensor. While in multisensing detection, multiple collaborating sensors are used to detect the intrusion.

A wireless sensor network (WSN) is a type of wireless network consist of small nodes with capabilities of sensing physical or environmental conditions, processing related data and send information wirelessly.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 industrial and civilian application areas, including industrial process monitoring and control, machine health monitoring, environment and habitat monitoring, healthcare applications, home automation and traffic control. The sensor nodes are tiny and limited in power. Sensor types vary according to the application of WSN.Whatever be the application, the resources such as power, memory and bandwidth are limited. Moreover, most of the sensors nodes are throw away in nature.

Early study on wireless sensor networks mainly focused on technologies based on the homogeneous wireless sensor network in which all nodes have same system resource. However, heterogeneous wireless sensor network is becoming more and more popular recently. And the results of researches show that heterogeneous nodes can prolong network lifetime and improve network reliability without significantly increasing the cost.A typical heterogeneous wireless sensor networks consists of a large number of normal nodes and a few heterogeneous nodes. The normal node, whose main tasks are to sense and issue data report, is inexpensive and source-constrained.

II. HETEROGENEOUS WSN

A heterogeneous wireless sensor network (WSN) consists of several different types of sensor nodes (SNs). Various applications supporting different tasks, e.g., event detection, localization, and monitoring may run on these specialized sensor nodes. In addition, new applications have to be deployed as well as new configurations and bug fixes have to be applied during the lifetime. In a network with thousands of nodes, this is a very complex task .A heterogeneous node has more complex processor and memory so that they can perform sophisticated tasks compared to a normal node. A heterogeneous node possesses high bandwidth and long distant transceiver than a normal node proving reliable transmission.

2.1. Types of Heterogeneous resources

There are three common types of resource heterogeneity in sensor node:

2.1.1. Computational Heterogeneity:

Computational heterogeneity means that the heterogeneous node has a more powerful microprocessor and more memory than the normal node. With the powerful computational resources, the heterogeneous nodes can provide complex data processing and longer term storage.

2.1.2. Link Heterogeneity:

Link heterogeneity means that the heterogeneous node has high bandwidth and long-distance network transceiver than the normal node. It can provide more reliable data transmission.

2.1.3. Energy Heterogeneity:

Energy heterogeneity means that the heterogeneous node is line powered, or its battery is replaceable.

Among above three types of resource heterogeneity, the most important heterogeneity is the energy heterogeneity because both computational heterogeneity and link heterogeneity will consume more energy resource. If there is no energy heterogeneity, computational heterogeneity and link heterogeneity will bring negative impact to the whole sensor network, i.e., decreasing the network lifetime.

A heterogeneous node is line powered (its battery is replaceable).The heterogeneous WSN consists of different types of sensors with different sensing and transmission range. So while selecting the sensor nodes for intrusion detection, we need to consider these inequality of sensing and transmission range. For example, if two nodes have different transmission range it is better to select the one whose transmission range is higher. In this paper, we are considering N types of sensors. Here the sensing range and transmission range is high for Type 1 compared to Type2 and so on. The sensors are uniformly and independently deployed in a area A = LxL.

III. COMPARATIVE STUDY OF HETROGENEOUS WSN AND HOMOGENEOUS WSN

In homogeneous networks, all the sensor nodes are identical in terms of battery energy and hardware complexity. heterogeneous networks achieve the former and the homogeneous networks achieve the latter. In homogeneous network, single (uniform) platform is used for per research group and all nodes in the network share the same functionality where as in heterogeneous network all the nodes treated differently. In the real world, the assumption of homogeneous sensors may not be practical because sensing applications may require heterogeneous sensors in terms of their sensing and communication capabilities in order to enhance network reliability and extend network lifetime. Also, even if the sensors are equipped with identical hardware, they may not always have the same communication and sensing models. In fact, at the manufacturing stage, there is no guarantee that two sensors using the same platform have exactly the same physical properties. This taxonomy focuses on heterogeneity at the designing stage, when sensors are designed to have non identical capabilities to meet the specific needs of sensing applications.

In the heterogeneous wireless sensor network, the average energy consumption for forwarding a packet from the normal nodes to the sink in heterogeneous sensor networks will be much less than the energy consumed in homogeneous sensor network.

IV. LITERATURE SURVEY

There exist several tools for security in networks and IDSs are important tools. Many solutions have been proposed in traditional networks but it cannot be applied directly to WSN because the resources of sensor nodes are restricted. Ad-hoc and WSNs security has been studied in a number of proposals.

Zhang and Lee [5] are among the first to study the problem of intrusion detection in wireless Ad-hoc networks. They proposed architecture for a distributed and cooperative intrusion detection system for Ad-hoc networks; their scheme was based on statistical anomaly detection techniques. But the scheme need much time, data and traffic to detect intrusion.

Detecting a moving intruder is a crucial application in wireless sensor networks, thus, first contact time when the intruder hits the sensing range of a sensor belonging to the large sensor cluster. To date, most of the existing work focus on the problem of network configuration for efficiently detecting the intruder within a pre-specified time threshold, under the constraints of tight power saving and/or cost efficiency.

Liu et al. [6] have explored the effects of sensor mobility on sensing coverage and detection capability in a mobile WSN. It is demonstrated that sensor mobility can improve the sensing coverage of the network, and provide fast detection of targeted events.

Wang et al. [7] have provided a unifying approach in relating the intrusion detection probability with respect to the intrusion distance and the network parameters (i.e., node density, sensing range and transmission range), under single-sensing detection and multiple-sensing detection models, in both homogeneous and heterogeneous WSNs.

Xi Peng et al[3] proposed a security management model for self organizing wireless sensor networks based on intrusion detection. It can prevent most of attacks. Then an analysis of each layer of networks in security model is discussed and the security management measures in the data link layer and network layer are described in detail especially. Such a structure is built based on the existing encryption and authentication protocols.

Byunggil Lee et al., [4] have developed management platform and security framework for wsn. The proposed framework has advantages as regard secure association and intrusion detection. This also provides the background a wsn, its security issues and requirements.

Qi Wang et al., [8] have developed a intruder detection algorithm of low complexity for static wireless sensor network. The intrusion detection model includes characteristics that determine the average frequency of execution of order. A distributed algorithm in which the sensor collects the information from the neighbouring nodes to analyses the anomalies if any from the neighbours. The intrusion detection algorithm on detecting anomalies packets received from its neighbours basic alarms to report the anomaly.

V. OUTCOME

In our survey we have studied about the intrusion detection, wireless sensor network and about the heterogeneous wireless sensor network and about the homogeneous wireless sensor network. In this approach we see that ID becomes very

fast and effective. Its detection rate and accuracy are high for using hybrid approach. Also we have studied about the WSN, Wireless sensor networks (WSN) consist of tiny devices. These tiny devices have limited energy, computational power, transmission range and memory. However, wireless sensor networks are deployed mostly in open and unguarded environment. There are two types of WSN first, homogeneous WSN and second, heterogeneous WSN. We have chosen heterogeneous WSN for our servay because there are following advantages of heterogeneous WSN:

1. Prolonging network lifetime
2. Improving reliability of data transmission.
3. Decreasing latency of data transportation.

These qualities are not present in homogeneous WSN.

VI. PROPOSED SYSTEM

1. Intrusion detection in heterogeneous WSNs by characterizing, intrusion detection with respect to the network parameters.
2. Detectors filter the packets and deliver only authorized packet to sink node.
3. Awake and sleep mechanism for the detector to save power.
4. In Heterogeneous wireless sensor, Intruder detected anywhere in the network. We are detecting the intruder in multiple sensor heterogeneous wireless sensor networks.
5. Two detection models are: Single-sensing detection model & Multiple-sensing detection model

VII. PROBLEM FORMULATION AND METHODOLOGY

1. Improving response scheduling, priority responses and having more control on response production mechanism;
2. Providing higher level of security, fault tolerant and robustness for suggested architecture;
3. Centralizing more detailed information about system activities for forensic analysis.
4. Efficient data management.
5. Developing user friendly interfaces which allow dynamic reconfiguration of systems and representing the activities of these systems in graphical.
6. Approaches for data aggregation in WSNs different protocols.
7. Techniques for using of mobile nodes in WSNs.

7.1. Algorithm

The algorithm for node selection trying to select the high capacity nodes compared to other one. High capacity means large sensing range and transmission range.

Si- set of type i sensors in the WSN area.
S- set of all sensors
N (a) - set of neighbours of node a

Repeat
For i=1 to N
Select node a with min N (a) in set Si
If N (a) ≠Ø
Select a
SN= {j/the distance between a and
N (a) < (r_{si}/2)}
If *SN* > 1
S=S-(SN U a)
Else
S= S-a
Until S is null set.

The algorithm select a certain set of nodes that cover the entire area based on type of node, its transmission range and sensing range.

7.2. Single-Sensing Detection

An intruder is detected when it enters the sensing range of a sensor. When the intruder enters the area through the boundary and the boundary is covered by the sensors, then the intruder will be detected as soon as it enters the WSN area. Otherwise it has to move a certain distance D before detected by any of the sensors. When the intruder starts from a point of the network boundary, given an intrusion distance D > 0, the corresponding intrusion detection volume V is almost an oblong volume.

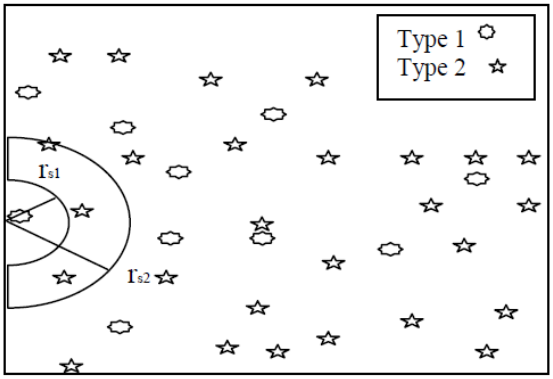

fig 1: The area covered by sensors at the boundary

Theorem 1

The probability *P(D)* that an intruder can be immediately detected once it enters a heterogeneous WSN can be given by,

$$p(D=0) = 1 - \prod_{i=1}^{N} e^{-n1}$$

Where ni is the number of type i nodes activated in the area $\pi r Si^2/2$.

Proof:

Here the area we need to consider when the intruder enters from the boundary is $A1=(\pi rS1^2)/2, A2=(\pi rS2^2)/2, \ldots AN=\pi rSN^{2/}2$ as shown in figure 1.So P(0, A1),(0,A2)….P(0,AN) gives the probability that there is no Type 1, Type 2…Type N sensors in that area. the probability that neither type 1 nor type 2….nor type N are given $P(0,A1)P(0, A2)\ldots..P(0.AN)=1-e^{-n1}e^{-n2}\ldots e^{-nN}$ where

n1,n2,…nN are the number of selected nodes from each type. So the probability of detecting the intruder when it enters the boundary is given by complement $P(0,A1)P(0,A2)….P(0,AN)=1-e^{-n1}e^{-n2}$ ….e^{-nN}.

Theorem 2

Suppose η is the maximal intrusion distance allowable for a given application, the probability P *(*D) that the intruder can be detected within η in the given heterogeneous WSN can be derived as

$$p(D < \eta) = 1 - \prod_{i=1}^{N} e^{-ni}$$

Where ni is the number of sensors participating in intrusion detection area $\mathbf{Ai= 2\eta r_{Si}+(1/2)\ r_{Si}^2}$

Proof: This can be proved just like above theorem.

7.3. Multi-Sensing Detection

In the multi-sensing detection model, an intruder has to be sensed by at least m sensors for intrusion detection in a WSN. The number of required sensors depends on specific applications. For example, at least three sensors' sensing information is required to determine the location of the intruder. Multi sensing in a heterogeneous WSN is explained in fig 2. Here multiple sensors have to detect a intruder at the same time.

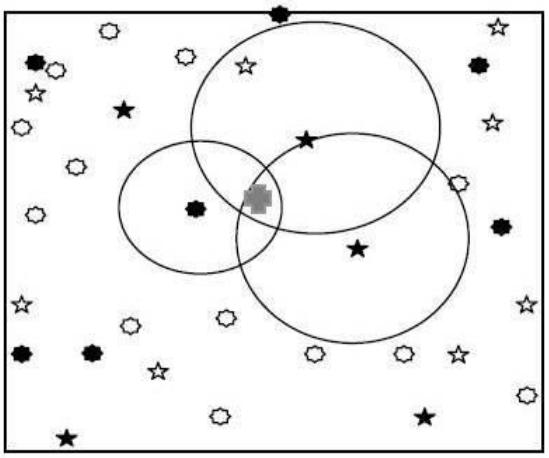

fig 2. Multi-Sensing

Theorem 3

Let Pm (D= 0) be the probability that an intruder is detected immediately once it enters a WSN in multi sensing detection model. It has

$$\mathbf{Pm(D=0) = 1\prod_{j=1}^{N}\sum_{i=0}^{m-1} P(i,Aj)}$$

Where Aj is the area covered by type j sensor and we are assuming that nj of type j sensors are activated in the area Aj.

Proof: This theorem can be proved just like above theorems. Here the area is only one half circles with radius rs.. P (i, A) gives the probability of detecting the intruder with i sensors.

$$\sum_{i=0}^{m-1} \mathbf{P(i,Aj)}$$

gives the sum of the probabilities of detecting the intruder with less than m sensors. So the complement will give the multi sensing probability.

VIII. RESULT AND SIMULATIONS

In the results, it shows a number of alarm messages and active nodes. This also represents the energy consumption. IDS mechanism detects unusual behavior from incorrect format. In case an incorrect packet is not related to transmission error (for example an incorrect node id), it raises an alarm signal to prepare for intruders. Then a group of activated nodes will be surrounded the intruders to protect from breaking into network. We have performed a simulation-based verification of our analytical results in both homogeneous and heterogeneous WSNs. The simulation is carried out for single-sensing. The analytical results are calculated by using Theorems 1-3.For successive simulation runs, the sensors are uniformly redistributed in the network domain.

IX. CONCLUSION

This paper presents an energy efficient intrusion detection mechanism that improves life of WSN. Wireless sensor networks are vulnerable to several attacks because of their deployment in an open and unprotected environment. This paper describes the major security threats in heterogeneous WSN and also describes different intrusion detection techniques by using various algorithm Moreover, the paper also describes several existing approaches to find out how they have implemented their intrusion detection system.

REFERENCES

[1] Mohamed Mubarak T, Syed Abdul Sattar, G.Appa Rao, Sajitha M" Intrusion detection: An Energy efficient approach in Heterogeneous WSN".

[2] Mohamed Mubarak.T, Syed Abdul Sattar, Appa Rao, Sajitha M"Intrusion Detection: A Probability Model for 3D Heterogeneous WSN"

[3] Xi Peng, Wuhan Zheng Wu, Debao Xiao, Yang Yu," Study on Security Management Architecture for Sensor Network Based on Intrusion Detection '" IEEE, Volume: 2,25-26 April 2009.

[4] Byunggil Lee, Seungjo Bae and Dong Won Han, "Design of network management platform and security frame work for WSN", IEEE International conference on signal image technology and internet based system, 2008.

[5] Y. Zhang and W. Lee. Intrusion Detection in Wireless Ad-Hoc Networks. In Proc. ACM MobiCom, pages 275-283, 2000.

[6] B. Liu, P. Brass, O. Dousse, P. Nain, and D. Towsley, "Mobility improves coverage of sensor networks," in Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc), 2005.

[7] 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.

[8] Qi Wang, Shu Wang, "Applying an Intrusion detection algorithm to wireless sensor networks", Second international workshop on Knowledge Discovery and Data Mining, 2009.

[9] Yun Wang, Yoon Kah Leow, and Jun Yin," Is Straight-line Path Always the Best for Intrusion Detection in Wireless Sensor Networks," in 15th International Conference on Parallel and Distributed Systems, 2009.

[10] P. Brutch and C. Ko. Challenges in intrusion detection for wireless ad-hoc networks. In 2003 Symposium on Applications and the Internet Workshops (SAINT'03 Workshops), 2003.

AUTHORS

First Author – Pankaj Kumar Srivastava, B.tech Final Year, Student of Computer Science & Engineering, ITM Gida, Gorakhpur, Email: sripankaj70@yahoo.com.
Second Author – Priyanka Rai, B.tech Final Year, Student of Computer Science & Engineering, ITM Gida, Gorakhpur, Email: rai.priyanka80@yahoo.com
Third Author – Upama Singh, B.tech Final Year, Student of Computer Science & Engineering, ITM Gida, Gorakhpur, Email: singh_upma92@yahoo.com