Intrusion Detection: Energy Efficient Approach in Assorted Wireless Sensor Networks

Parchure Sunil Vinayak
Department of Computer Engineering,
S.B.Patil COE, Indapur, Pune, Maharashtra,India

Yogendra V. Patil
Department Of Computer Engineering,
S.B.Patil COE, Indapur, Pune, Maharashtra, India

Abstract - 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 analyse 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.

Keywords- Intrusion detection, node density, sensing range, Wireless Sensor Network (WSN)

I. INTRODUCTION

WSN is common in different types of application scenarios. It includes a set of sensor nodes deployed over a geographical area to monitor a variety of phenomenons.However, challenges and difficulties still exist. The sensor nodes own limited power, processing and sensing ability. The sensor nodes are prone to failure because of lack of power, physical damage etc. Since the information generated by a single node is usually incomplete or inaccurate, and the applications need collaborative communication and computation among multiple sensors multiple sensing models can be used. 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 e.g. the wireless sensor network is mainly used in military applications such as in borders for finding out the infiltrations. It is also used in industrial process monitoring and control, machine health monitoring, environment and habitat monitoring, healthcare applications, home automation and traffic control [1]. WSN become increasingly useful in variety critical applications, such as environmental monitoring, smart offices, battlefield surveil- lance and transportation traffic monitoring. 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 band width are limited. More over, most of the sensors nodes are throw away in nature. Therefore it is vital to consider energy efficiency so as to maximize the life time of the WSN. Great efforts have been devoted to minimizing the energy consumption and extending the lifetime of the network. One common way is to put some sensor nodes in sleep mode to save energy and wake them up under some strategies. Work towards maximizing the life time of WSN has been studied in many research works. Some of them lead to the need of heterogeneous WSN deployment. Lee et al. [2] analyse heterogeneous deployments both mathematically and through simulations in different deployment environments and network operation models. In [3], Hu et al. investigate some fundamental questions for hybrid deployment of sensor network, and propose a cost model and integer linear programming problem formulation for minimizing energy usage and maximizing lifetime in a hybrid sensor network.Their studies show that network lifetime can be increased Dramatically with the addition of extra micro-servers and the locations of micro-servers can affect the lifetime of network significantly. Intrusion detection 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.Da Silva et al. [4] and Onat and Miri [5] propose similar IDS systems, where certain monitor nodes in the network are responsible for monitoring their neighbours, 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 sensor nodes in WSNs are usually static after deployment, and communicate mainly through broadcast instead of point-to-point communication. Sensors are deployed in a variety of domains and some application should be secure from all types of attacks. A lot of security protocols or mechanisms have been designed for sensor networks. For example, SPINS (Sensor Protocol for Information via Negotiation), a set of protocols, provides secure data confidentiality, two-party data authentication, and data freshness and authenticated broadcast for sensor network [6]. LEAP (Localized Encryption and Authentication Protocol), is designed to support in-network processing bases on the different security requirements for different types of messages exchange [7]. INSENS is an intrusion tolerant routing protocol for wireless sensor networks [8]. In general, security solutions in the network can be divided into two categories: prevention and detection. Prevention techniques, such as encryption, authentication, firewalls, physical isolation, as the first line of defence, are usually to prevent attacks from outside. The goal of intrusion detection is that when preventive measures fail, WSNs can identify and resist the attacks by means of intrusion detection techniques. An intrusion detection system (IDSs) is an important tool for the security of networks. Although, there have existed several intrusion detection techniques in wired networks, they are not suitable for WSNs and cannot transfer directly to WSNs. Therefore, these techniques must be modified or new techniques must be developed to make IDSs work well in WSNs. It is defined as a monitoring system for detecting any malicious intruder that is invading the network domain [9], [10]. 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. The rest of this paper is organized as follows. There are six sections. First section includes the related works. The papers which we referred to start this work are mentioned in this. Following this contribution section is there, which specifies our idea to intrusion detection. Next is problem definition, assumption made for simulation. Intrusion detection in heterogeneous wsn includes the algorithm and probability analysis. The simulation results are specified in simulation and verification section. Finally, the paper is concluded in the last Section.

II. RELATED WORKS

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 [13] are among the first to study the problem of intrusion detection in wireless Adhoc 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. In WSNs, the nodes can not afford the cost. Detecting a moving intruder is a crucial application in wireless sensor networks, thus, attracting considerable research attention in the literature. Intrusion detection is defined as the 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. [14] 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. [15] 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. A straight line or linear motion intrusion path is assumed for an intruder. An intruder can attack the network following a curved path or even a random walk in order to improve its attacking probability. Yun Wang, Yoon Kah Leow, and Jun Yin[16] have provided an approach where the intruder takes a curved path. They propose a novel Sine -curve mobility model to explore the effects of different intrusion paths on the intrusion detection probability using single-sensing and K sensing detections in a given wireless sensor network. Xi Peng et al[17] 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, and can detect most types of attacks in the sensor networks. In this paper, intrusion detection strategy is deployed in the form of layers. Typically a wireless sensor network uses cryptography to secure itself against unauthorized external nodes gaining entry into the network. But cryptography can only protect the network against the external nodes and does little to thwart malicious nodes that already possess one or more keys.Brutch and Ko classify intrusion detection systems (IDS) into two categories: *host-based* and *network-based*. They further classify intrusion detection schemes into those that are signature based, anomaly based, and specification based [18]**.** Byunggil Lee et al., [19] 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 an wsn, its security issues and requirements.Qi wang et al., [20] 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 neighboring nodes to analyses the anomalies if any from the neighbors. The intrusion detection algorithm on detecting anomalies packets received from its neighbors basic alarms to report the anomaly.

III. 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.

3.1. Types of Heterogeneous resources

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

3.1.1. 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.

3.1.2. 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.

3.1.3. 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 = L x L.

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.

7.1Algorithm

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 neighbors' of node a
Repeat
For i=1 to N
Select node a with min N (a) in set Si
If N (a) $\neq$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.

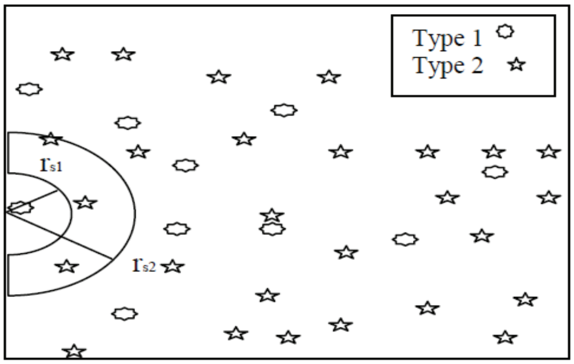

Fig.1 the area covered by sensors at the boundary

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)…..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)=$1-e^{-n1}e^{-n2} \ldots e^{-n N}$.

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

$$P(D<\eta) = 1 - \prod_{i=1}^{N} e^{-n1}$$

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

Proof: This can be proved just like above theorem.

7.2Multi-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.

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

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

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

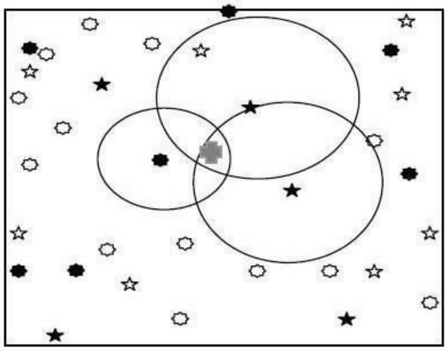

Fig.Multi-Sensing

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.

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

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 algorithms 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.