INTRUSION DETECTION MECHANISM WITH INCREASING AND MAINTAINING THE ENERGY EFFICIENCY OF A WIRELESS SENSOR IN WIRELESS NETWORKS

[1]Ramkumar Ramaswamy, [2]Anandaraj Shunmugam
Lecturer II,
Department of Computer Science and Information Technology, DMI- St. John the Baptist University,
Mangochi, The Republic of Malawi

ABSTRACT- Intrusion detection in Wireless Sensor Network (WSN) is a type of security management system for computers and networks. An intrusion detection system gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organization) and misuse (attacks from within the organization). The system uses vulnerability assessment (sometimes referred to as scanning), which is a technology developed to assess the security of a computer system or network. 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.

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.

II. PROBLEM DEFINITION

The life span of wireless sensor network directly depends on the power. The power required to transfer a data from sensor is more compared to its internal processing. All sensors are performing the intrusion detection and passing this information to base station may cause unnecessary usage of power. It is better to activate only few sensors within a region of WSN at a time for intrusion detection. So in the case of intrusion detection, if we are able to save battery power of each sensor, then it is very easy to increase the WSN life span. This paper is proposing a new technique of energy efficient Intrusion detection, which will maximize the network life time, and its probability analysis.

III. INTRUSION DETECTION

ID system gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organization) and misuse (attacks from within the organization). ID uses vulnerability assessment (sometimes referred to as scanning), which is a technology developed to assess the security of a computer system or network.

IV. INTRUSION DETECTION IN WIRELESS SENSOR NETWORK (WSN) FUNCTIONS INCLUDE

- Monitoring and analyzing both user and system activities
- Analyzing system configurations and vulnerabilities
- Assessing system and file integrity
- Ability to recognize patterns typical of attacks
- Analysis of abnormal activity patterns
- Tracking user policy violations

ID systems are being developed in response to the increasing number of attacks on major sites and networks, including those of the Pentagon, the White House, NATO, and the U.S. Defense Department. The safeguarding of security is becoming increasingly difficult, because the possible technologies of attack are becoming ever more sophisticated; at the same time, less t1echnical ability is required for the novice attacker, because proven past methods are easily accessed through the Web.

V.PROCESS IN INTRUSION DETECTION

1. Constructing Sensor Network
2. Packet Creation
3. Find authorized and unauthorized port
4. Constructing inter-domain packet filtering
5. Receiving the valid packet

VI. SPECIFIC OBJECTIVE

Intrusion detection in heterogeneous WSNs by characterizing intrusion detection with respect to the network parameters detection models:

1. Single-sensing detection
2. Multiple-sensing detection models

These are the two detection models we are using for detecting the intruder in both single sensor and multiple sensor heterogeneous wireless sensor networks.

The objective 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. 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.

VII. SCOPE OF THE RESEARCH

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. Moreover, 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. An analysis states heterogeneous deploys both mathematically and through simulations in different deployment environments and network operation models. In certain investigation 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 proposes similar IDS systems, 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.

VIII. SAMPLE LITRETURE REVIEW - AN INTRUSION DETECTION SYSTEM

Onat and A. Miri, IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, vol. 3, Montreal, Canada, August 2005, pp.

In many sensor applications, intrusion detection systems included, the sensors gather a vast amount of data. Most cyber security sensor systems assume that all the data gathered by the sensors can be sent to the fusion engine, and furthermore that the fusion engine is capable of processing all of the data acquired in a timely manner. The ability to send all data to the fusion engine is not a valid assumption because there are many constraints in the network (Wang, 2004), likewise the ability of the fusion engine to process all sensor data may be invalid because of constraints in the processing power of the fusion engine. Due to network bandwidth constraints and fusion engine processing constraints, only a subset of data generated by all the sensors can be sent to the fusion engine. Which sensors to pull data from, at what time, and what data to pull from the chosen sensors become important questions to ask in a resource constrained network.

Bandwidth constraints exist in computer networks. Even though standard computer networks often have high bandwidth, sending too many sensor messages has the potential to slow down the communication for daily network activities and cause slow network performance. While there may not be a tight constraint, minimizing bandwidth use by network sensors is important in order to not interfere with required network performance. There has been a significant amount of research recently in the field of sensor management and sensor scheduling. Much of the research is applied to distributed sensor networks with tight bandwidth and energy constraints. While cyber networks do not have the same tight bandwidth constraints, much can still be learned from the research. Research is focused mainly on using algorithms to schedule sensors, using weights for information quality, 21 and applying novel concepts such as network calculus or market based management to schedule sensors.

There are many examples of research that use algorithms and integer and linear programming to schedule sensors. Algorithms offer a promising solution to sensor management because when executed these algorithms can provide an optimal sensor schedule. Algorithms have been developed to schedule the polling of data from sensors in order to maximize information value of data gathered while not exceeding bandwidth and energy constraints of the network. Unfortunately, often when using algorithm scheduling techniques, the algorithms developed are too difficult to solve in a timely manner. Heuristics, such as a one step ahead method or other techniques, are used to provide sub-optimal solutions to scheduling algorithms in real time (Sciacca, 2002 and Krishnamurthy, 2002).

Another drawback of much of the algorithm based research is that the focus is only on polling one sensor at a time due to the assumption of a heavily bandwidth constrained network. In the case of network intrusion detection sensors, bandwidth is not as severe a constraint. More than one sensor can be polled at a time in a computer network, and in the cyber realm the focus is more on minimizing bandwidth use rather than meeting an extreme bandwidth constraint. These algorithms also assume that sensors are controlled by a central sensor polling agent, and do not allow sensors to decide for themselves whether they should send data or not. An interesting approach in use to enhance the ability of algorithms to properly schedule data collection is to split up a single sensor into multiple “virtual sensors”. Each virtual sensor holds a different type of information or a different quality level of information. For example, for a temperature sensor, one virtual sensor may hold temperature measured to the nearest degree, while another virtual sensor may hold the temperature to the nearest hundredth degree, while yet 22 another virtual sensor may only hold the binary information of whether the temperature is above freezing or not. By using virtual sensors, data can be polled that fits best with the current bandwidth constraints (Sciacca, 2002).

The flexibility of an algorithm approach allows a variety of considerations to be incorporated into the models. One algorithm includes the recognition that some sensor measurements may take more time and contribute more value to the overall observation than other sensors, so that sensors should not all be treated equally. The use of Hidden Markov models can make the past observations and past sensor choices influence the sensor that is chosen next (Krishnamurthy, 2002).

Some algorithm based research is focused heavily on giving weights to sensors based on data quality (Zhang, 2002 and Nicholson, 2004). Weights are been used to assign values for data quality, data timeliness, and data importance related to the overall sensor network objective. The weights are used to effectively choose the data that would best serve the network objective (Zhang, 2002). Weighted values are also used to differentiate between the quality of the information and the information value. Information value is defined as a measure of relevance related to "how much does the information cost to acquire and what is the expected pay-off as a consequence of action upon it" (Nicholson, 2004, p.129).

Assigning weighted values to sensor data addresses the problem of a sensor that produces so much information that only a subset can be sent to the fusion engine. The results of the scheduling system, which use a one step ahead scheduling algorithm, are compared to a sensor scheduler that went in cyclical order giving each sensor a chance to send data. The scheduler that took information value and quality into account naturally performs better (Nicholson, 2004). 23 Other approaches to sensor management include a network calculus approach that uses network calculus to mathematically find resource allocation so as not to exceed bandwidth (Zhang, 2002). The network calculus approach focuses on a dynamic environment where one might want to look at different sensors depending on the current picture of the environment. The research focuses on a hierarchal distributed sensor network that was not very similar to the cyber intrusion detection sensor network.

Another novel approach to sensor management uses a market based approach to effectively sell sensor resources to various buyers (Mullen, 2006 and Viswanath, 2005). The approach uses combinatorial auctions so that buyers can bid on the services of several sensor combined. The market based sensor management approach seems more aimed at a sensor network that is providing information to several fusion engines that are competing for the same sensor resources, but the market based approach is interesting and unique.

Research is done in the area of using sensor networks to track mobile targets, such as airplanes, traveling over a set of distributed sensors. In such studies mobile targets are assumed to originate beyond the borders of the sensor network. The sensors' job is then to track the mobile target as the target passes through the space monitored by the sensors. One approach taken to schedule such a sensor network is to keep all sensors on the perimeter of the sensor network on and sensing at all times. Keeping the perimeter sensors on, allows the network to consistently observe new targets entering the sensor area.

IX. IMPLEMENTATION METHODOLOGY

Intrusion detection in heterogeneous WSNs by characterizing intrusion detection with respect to the network parameters detection models:

1. Single-sensing detection
2. Multiple-sensing detection models

These are the two detection models we are using for detecting the intruder in both single sensor and multiple sensor heterogeneous wireless sensor networks.

The objective 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. 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.

A WSN consists of different types of sensors with different sensing and transmission range. So while selecting the sensor nodes for intrusion detection, 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, consider 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. Such a random deployment results in a 2D Poisson point distribution of sensors. A sensor can only sense the intruder within its sensing coverage area that is a disk with radius rs centered at the sensor.

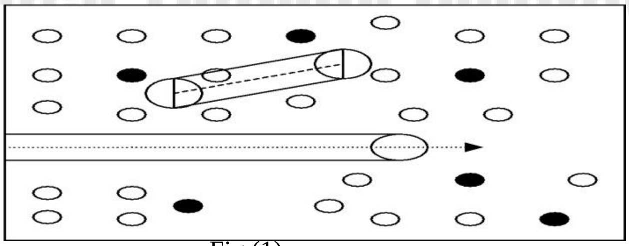


Fig (1)

Consider figure 1, here the intruder is coming from the boundary and the distance moved by the intruder is D, the intruder is detected only when there is any sensor in the area moved by the intruder.In this project, consider only straight path.

Figure 1 shows the case when the intruder enters from the boundary. Here the area moved by the intruder

$$S=2*D*rs+ \Pi rs2/2 \qquad (1)$$

If the intruder is entering the WSN area from a random point,i.e , the intruder is dropped from the air, then the area movedby the intruder is also shown in figure 1.This area is given by

$$S=2*D*rs+ \Pi rs2 \qquad (2)$$

2. 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)<(rsi/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.

B. Single sensing detection model

The intruder is detected only when it enters the sensing range of any one sensor nodes. 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.

Theorem 1

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

$$P(D=O)= 1-\prod_{i=1}^{N} e^{-ni}$$

where ni is the number of type i nodes activated in the area πrsi2/2.

Proof:

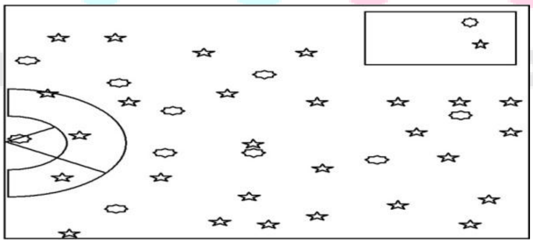
Here the area we need to consider when the intruder enters from the boundary is A1=(π rs12)/2, A2=(πrs22)/2 ,…AN=πrsN2/2 as shown in figure 2. So P (0, A1) , P (0, A2)….P(0,AN)gives the probability that there is no Type 1,Type 2…type N sensors in that area. the probability that neither type 1 nor type 2….nor type N are given P(0,A1) P (0, A2)…..P(0.AN)= 1-e-n1e-n2…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 of P (0, A1) P (0, A2)….P(0,AN) =1-e-n1e-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

$$P(D<=n)= 1-\prod_{I=0}^{N} e^{-ni}$$

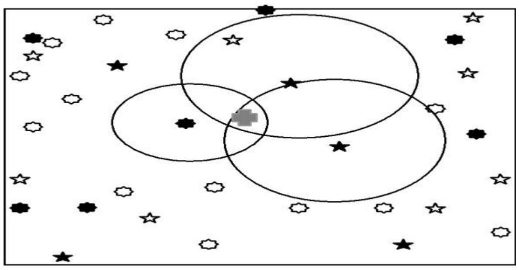
where **ni** is the number of sensors participating in intrusion detection area Ai= 22η*rsi* + (1 /2)π*rsi*



Proof: This can be proved just like above theorem.

C. Multi sensing detection model

Multi sensing in a heterogeneous WSN is explained in figure 3. Here multiple sensors have to detect a intruder at the same time. Three sensors are considered. The intruder is within the sensing range of three sensors. In the k-sensing detection model of a heterogeneous WSN with two types of sensors, at least k sensors are required to detect an intruder. These k sensors can be any combination of any type of sensors.



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

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

whereAj is the area covered by type j sensor and assume 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.

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

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

CONCLUSION:

A WSN consists of different types of sensors with different sensing and transmission range. The sensors are uniformly and independently deployed in an area, In ***Single sensing***the intruder is detected only when it enters the sensing range of any one sensor nodes. 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 before detected by any of the sensors.

Multiple sensors have to detect an intruder at the same time. Three sensors are considered. The intruder is within the sensing range of three sensors. In the k-sensing detection model of a heterogeneous WSN with two types of sensors, at least k sensors are required to detect an intruder. These k sensors can be any combination of any type of sensors.

REFERENCES:

[1] 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. (2006) 749-767.

[2] I. Onat and A. Miri, “An intrusion detection system for wireless sensor networks,” in Proceeding of the IEEE InternationalConference on Wireless and Mobile Computing, Networking andCommunications, vol. 3, Montreal, Canada, August 2005, pp.253–259.

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

[4] 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

[5] 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 inSensor Networks (IPSN’03), Apr. 2003.

[6] 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 CommunicationsSecurity (CCS '03), Oct. 2003.