Multisensor Based Intrusion Detection in Heterogeneous Wireless Sensor Networks

Shiva Krishna[#1], K. Srimathi[*2]

[#]*M.Tech CSE Department, JNTU University*
Sree Chaitanya College Of Engineering,Karimnagar-505527,AP
[1]shiva.duppalli@gmail.com

[*]*Associate Professor*
Sree Chaitanya College Of Engineering,Karimnagar-505527,AP
[2]sri.shetti1@gmail.com

***Abstract*-Due to the innovations in sensor technologies, Heterogeneous Wireless Sensor Networks (WSNs) are playing key role in many applications with monitoring phenomena. With increasing popularity of the WSNs, the security risks are also growing and that is evident in the incidents of intrusions in terms of various kinds of attacks recorded in this domain. Therefore it is essential to have intrusion detection systems built into the framework of the WSN. Research in this area has revealed that intrusion detection demands more energy. As wireless sensors have restrictions with respect to energy and memory resources, paramount importance has to be given to energy efficient intrusion detection mechanisms in WSN. This paper presents mechanisms that help in detecting intrusions with less energy consumption and also estimates the data loss occur in transmission. The empirical results revealed that the energy efficiency of our approach for intrusion detection in WSN is competitive and that can be used in real time sensing.**

*Key Words:-***WSN, energy efficiency, intrusion detection, Data loss, Energy consumption, Heterogeneous**

I. INTRUSION DETECTION SYSTEM

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.

Intrusion is any set of actions that attempt to compromise the integrity, confidentiality, or availability of a resource and an intrusion detection system (IDS) is a system for the detection of such intrusions. There are three main components of IDS: data collection, detection, and response.

The ***data collection component*** is responsible for collection and pre-processing data tasks: transferring data to a common format, data storage and sending data to the detection module . IDS can use different data sources as inputs to the sys-tem: system logs, network packets, etc. In the ***detection component*** data is analyzed to detect intrusion attempts and indications of detected intrusions are sent to the ***response component***.

II. WIRELESS SENSOR NETWORKS

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.

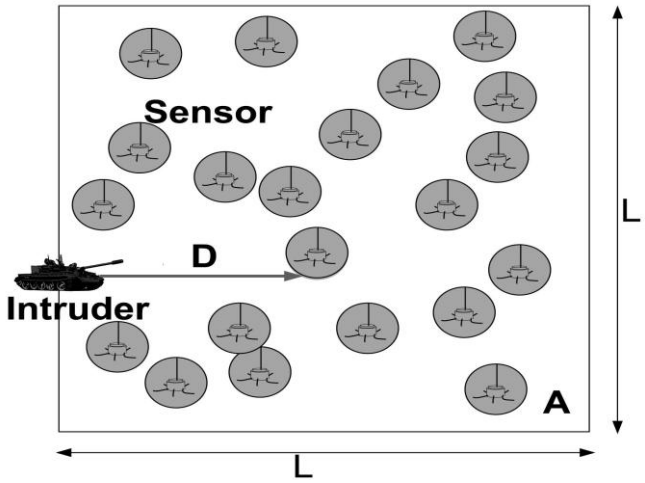

Fig. 1 Intrusion detection in a WSN.

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.

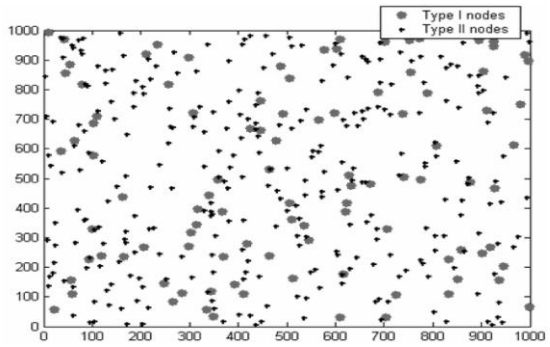

Fig. 2 Heterogeneous wireless Sensor Networks

A. Types of Heterogeneous resources

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

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) 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) *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.

B. Intrusion Detection Models

Our intrusion detection model includes a network model, a detection model, and an intrusion strategy model. The

network model specifies the WSN environment. The detection model defines how the intruder can be detected and the intrusion strategy illustrates the moving policy of the intruder.

1) Network Model

We consider a WSN in a two-dimensional (2D) plane with sensors, denoted by a set N ¼ ðn1; n2; . . . ; nNÞ, where Ni is the ith sensor. These sensors are uniformly and independently deployed in a square area A ¼ L _ L. Such a random deployment results in a 2D Poisson point distribution of sensors. All sensors are static once the WSN has been deployed. In particular, we consider two WSN types: homogeneous and heterogeneous WSNs. In a homogeneous WSN, each sensor has the same sensing radius of r_s, and the transmission range of r_x. A sensor can only sense the intruder within its sensing coverage area that is a disk with radius r_s centered at the sensor. Denote the node density of the homogeneous WSN as _. We then focus on a heterogeneous WSN with two types of sensors, as shown in Fig. 2: Type I sensor that has a larger sensing range r_{s1},as well as a longer transmission range r_{x1}, and Type II sensor that has a smaller sensing range r_{s2},as well as a shorter transmission range r_{x2}.The densities of Type I and Type II sensors are represented as $\__1$ and $\__2$, respectively. Fig. 2 shows a heterogeneous WSN, where both Type I and Type II sensors follow the2D Poisson point distribution. In a homogeneous or heterogeneous WSN, a point is said to be covered by a sensor if it is located in the sensing range of any sensor(s).The WSN is thus divided into two regions, the covered region, which is the union of all sensor coverage disks, and the uncovered region, which is the complement of the covered region within the area of interest A. In our network model, the intruder does not know the sensing coverage map of the WSN.

2) Detection Model

There are two detection models in terms of how many sensors are required to recognize an intruder: single sensing detection model and multiple-sensing detection model. It is said that the intruder is detected under the single-sensing detection model if the intruder can be identified by using the sensing knowledge from one single sensor. On the contrary, in the multiple-sensing detection model, the intruder can only be identified by using cooperative knowledge from at least k sensors (k is defined by specific application requirements). For simplicity of expression, multiple sensing and k-sensing are interchangeable in the following discussion:

In order to evaluate the quality of intrusion detection in WSNs, we define three metrics as follows:

Intrusion distance The intrusion distance, denoted by D, is the distance that the intruder travels before it is detected by a WSN for the first time. Specifically, it is the distance between the point where the intruder enters the WSN and the point where the intruder gets detected by any sensor(s).Following the definition of intrusion distance, the Maximal Intrusion Distance (denoted by _, _ > 0)is the maximal distance allowable for the intruder to move before it is detected by the WSN.

Detection probability The detection probability is defined as the probability that an intruder is detected within a certain intrusion distance (e.g. Maximal Intrusion Distance _).

Average intrusion distance The average intrusion distance is defined as the expected distance that the intruder travels before it is detected by the WSN for the first time.

Intrusion Strategy Model we consider two intrusion strategies for the movement of the intruder in a WSN. If the intruder (say, a panzer) already knows its destination before entering the network domain, it follows the shortest path to approach the destination. In this case, the intrusion path is a straight line ðD1Þ from the entering point to the destination, as illustrated in Fig. 3. The main idea behind this strategy is that the straight movement causes the least risk for the intruder due to the least area that it has to explore by following a straight line toward the destination. The corresponding intrusion detection area S_1 is determined by the sensor's sensing range r_s and intrusion distance D_1, as shown in Fig. 3. It is because the intruder can be detected within the intrusion distance D_1 by any sensor(s) situated within the area of S_1.

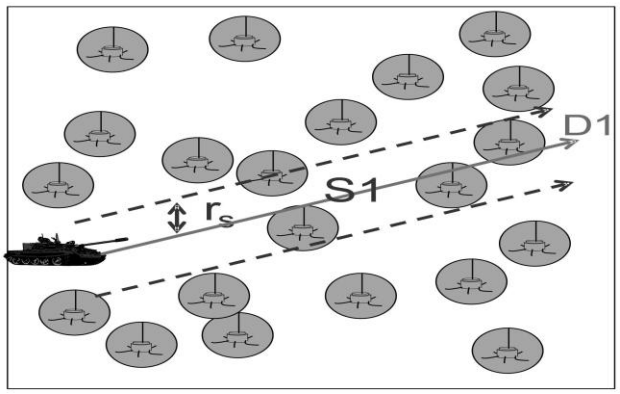

Fig. 3 Intrusion Strategy

On the contrary, if the intruder does not know its destination, it moves in the network domain in a random fashion. We consider that the intruder tends to minimize the overlapping on its path. Thus, the intrusion path of the intruder can be regarded as a non overlapping curved line ðD2Þ, and the intrusion area accordingly is a curved band S_2, as illustrated in Fig. 4.In the above two strategies, if the intruder travels the same distance, i.e., D_1 ¼ D_2, the corresponding intrusion detection areas approximately satisfy S_1 ¼ S_2. Therefore, we adopt a straight path in the following discussion, and the analytical results can be directly applied to the case of the curved path. Furthermore, the intruder can start its intrusion from the network boundary or a random point inside the network domain. For example, the intruder can be dropped from the air and starts from any point in the network domain.

Intrusion Detection in Heterogeneous Wireless Sensor Networks

In a heterogeneous WSN, as defined in Section 3.1, we consider two types of sensors: Type I and Type II with the node density of _1 and _2, respectively.

- A Type I sensor has the sensing range r_{s1}, and the sensing coverage is a disk of area $S_1 ¼ \_r_{2s}$
- A Type II sensor has the sensing coverage of $S_2 ¼ \_r_{2s2}$ with the sensing range r_{s2}.

Without loss of generality, we can assume that $r_{s1} > r_{s2}$ in our network model. In a heterogeneous WSN, any point in the network domain is said to be covered if the point is under the sensing range of any sensor (Type I, Type II, or both).
In this section, we present the analysis of intrusion detection probability of a heterogeneous WSN in single sensing detection and multiple-sensing detection models.

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.

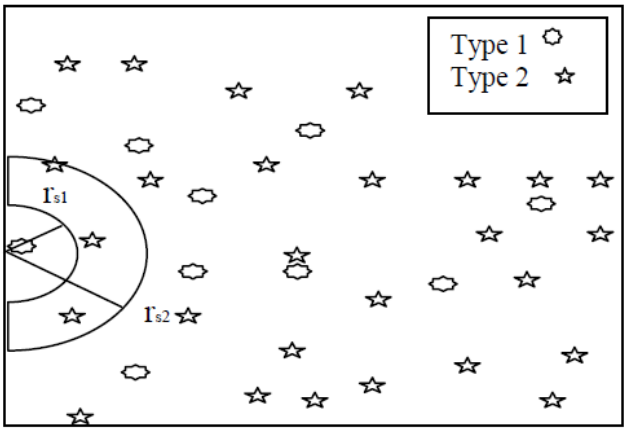

Fig. 4 Area Covered by the Sensors at the boundary

Multiple 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.

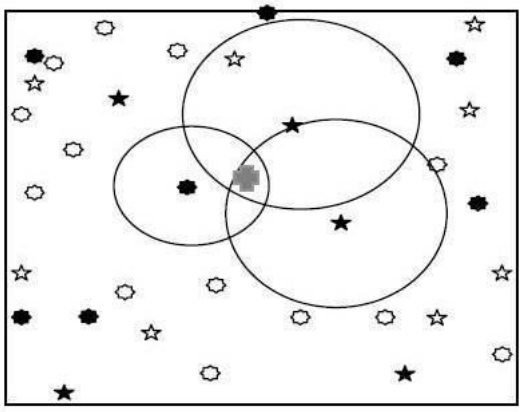

Fig. 5 Multisensing Detection

IV. EXISTED WORK

The Existed Work is related to identifying the Intruders in homogenous single sensor environment. The Intrusion System used was the monitoring based intrusion detection. Which lead to several Disadvantages

1. Using one sensor can only sense a portion of the Intruder.

2. Monitoring Based Intrusion Detection produced high false positives and it may effect the performance of the network.

V. PROPOSED WORK

Here the contribution towards intrusion detection in WSN is an algorithm which detects intrusions with energy efficient way. The following things are considered in this work

- The consumption of energy for the purpose of intrusion detection.
- Exploring the mechanism for internal and external detection.

The proposed algorithms keeps these two in mind as they are essential in WSN because the intrusions might be from within the network or from outside of it.

Advantages of our proposed system

The Intrusion Detection using Multiple Sensor Provides the Following Advantages

1. Even if the Primary Detector Fails the Secondary Detector Senses the Intruder.

2. Intruder can be easily detected both in homogenous and heterogeneous Environments.

Algorithm for selecting the Node

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.

VI. 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. On the Effectiveness of Monitoring for Intrusion Detection in Mobile Ad Hoc Networks (IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 10, NO. 8, AUGUST 2011)
2. Guide to Intrusion Detection and Intrusion Prevention Systems
3. Intrusion Detection System by J Bretano
4. Wireless Sensor Networks at the University of Texas.
5. Wireless Sensor Networks Technology, Protocols and Applications
6. Sensor Networks by Bharthidasan
7. Mohamed Mubarak T, Syed Abdul Sattar, G.Appa Rao, Sajitha M" Intrusion detection: An Energy efficient approach in Heterogeneous WSN".
8. [2] Mohamed Mubarak. T, Syed Abdul Sattar, Appa Rao, Sajitha M"Intrusion Detection: A Probability Model for 3D Heterogeneous WSN"
9. [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.
10. [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.
11. [5] Y. Zhang and W. Lee. Intrusion Detection in Wireless Ad-Hoc Networks. In Proc. ACM MobiCom, pages 275-283, 2000.
12. [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.