Deployment and Intrusion Detection Approach in Heterogeneous WSN

Priyanka Rai[1], Pankaj Kumar Srivastava[2], Upama Singh[3]

[1]B.tech Final Year, Student of Computer Science & Engineering, ITM Gida,
Gorakhpur, Uttar Pradesh, India
rai.priyanka80@yahoo.com
[2]B.tech Final Year, Student of Computer Science & Engineering, ITM Gida,
Gorakhpur, Uttar Pradesh, India
sripankaj70@yahoo.com.
[3]B.tech Final Year, Student of Computer Science & Engineering, ITM Gida,
Gorakhpur, Uttar Pradesh, India
singh_upma92@yahoo.com

Abstract - **Intrusion detection is a process of identifying and responding malicious activity. Wireless sensor networks consisting of a large number of sensors are effective for gathering data in variety of environment. The basic sensors are simple and have limited power supplies. Heterogeneous wireless sensor networks are better scalable and lower overall cost than homogeneous sensor networks. In this paper, we are improving the lifetime of wireless network and we present a survey of various energy efficient techniques in a heterogeneous wireless sensor network. It is important to improving wireless network because sensor nodes in wireless networks are constrained by limited energy.**

***Keywords*- energy efficient, heterogeneous wireless sensor network, homogeneous wireless network, Intrusion detection, Wireless sensor network, sensors**

I. INTRODUCTION

Wireless sensor network (WSN) refers to a system that consists of number of low-cost, resource limited sensor nodes to sense important data related to environment and to transmit it to sink node that provides gateway functionality to another network, or an access point for human interface. WSN is a rapidly growing area as new technologies are emerging, new applications are being developed, such as traffic, environment monitoring, healthcare, military applications, home automation. WSN is vulnerable to various attacks such as jamming, battery drainage, routing cycle, cloning. Due to limitation of computation, memory and power resource of sensor nodes, complex security mechanism cannot be implemented in WSN. Therefore energy-efficient security implementation is an important requirement for WSN.

In homogeneous networks all the sensor nodes are identical in terms of battery energy and hardware complexity. With purely static clustering (cluster heads once elected, serve for the entire lifetime of the network) in a homogeneous network, it is evident that the cluster head nodes will be overloaded with the long range transmissions to the remote base station, and the extra processing necessary for data aggregation and protocol co-ordination. As a result the cluster head nodes expire before other nodes. However it is desirable to ensure that all the nodes run out of their battery at about the same time, so that very little residual energy is wasted when the system expires.

On the other hand, in a heterogeneous sensor network, two or more different types of nodes with different battery energy and functionality are used. The motivation being that the more complex hardware and the extra battery energy can be embedded in few cluster head nodes, thereby reducing the hardware cost of the rest of the network.

Thus there are two desirable characteristics of a sensor network, viz. lower hardware cost, and uniform energy drainage. While heterogeneous networks achieve the former, the homogeneous networks achieve the latter. However both features cannot be incorporated in the same network.

An Intrusion Detection System (IDS) detects a security violation on a system by monitoring and analyzing network activity. 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. Intrusion detection is analyzed in two scenarios: single sensing detection and multiple sensing detection .In single sensing detection the intruder is detected by a single sensor. But at least three sensors should detect the intruder in a collaborative manner to find out the exact location of the Intruder. Therefore we have analyzed the multiple sensing detection too. We derive the expected intrusion distance and evaluate the detection probability in different application scenarios. we theoretically capture the impact on the detection probability in terms of different network parameters, including node density, sensing range, and transmission range.

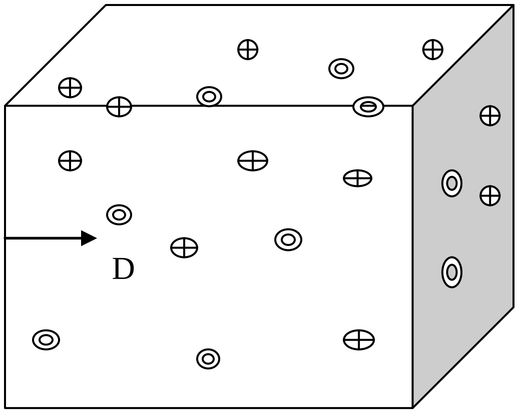

Fig 1. Distance moved by intruder

II. HETROGENEOUS WSN

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. The heterogeneous node, which provides data filtering, fusion and transport, is more expensive and more capable. It may possess one or more type of heterogeneous resource, like for e.g. enhanced energy capacity or communication capability. Their batteries may be replaced easily. Compared with the normal nodes, they may be configured with more powerful microprocessor and more memory. They also may communicate with the sink node via high-bandwidth, long-distance network, such as Ethernet. If heterogeneous node is present in WSN then it can increase network reliability and lifetime.

A. Deployment

In heterogeneous sensor networks, the basic sensors can be deployed randomly as in homogeneous sensor networks. The cluster heads, on the other hand, should be more carefully deployed to make sure all basic sensors are covered, that is, each sensor can hear from at least one cluster head. However, since the number of cluster heads is small, their best locations can be found within a reasonable amount of time and they can even increase their transmission power to cover remote sensors. The problem of sending packets from sensors to a single sink node with energy constraints has been studied. However, the difference between our work and those is profound. First, assume that data should be gathered by a data-forwarding tree, that a tree is not the best structure for data gathering applications. The best structure can be found by running a network flow algorithm, which is what we will adopt in our work. Second, in essence, focus on traffic routing, whereas we consider both traffic routing and media access control.

In this paper, an Intruder is defined as any moving object that enters into the WSN area .It may enter from a random point, or through boundary of the deployment area. If dropped from the air then the entry point can be considered as a random point. We present the analysis of intrusion detection in a heterogeneous WSN.

B. Types of resource heterogeneity

1) Computational heterogeneity- A heterogeneous node has more complex processor and memory so that they can perform sophisticated tasks compared to a normal node.

2) Link heterogeneity- A heterogeneous node possesses high bandwidth and long distant transceiver than a normal node proving reliable transmission.

*3) Energy heterogeneity***-** A heterogeneous node is line powered (its battery is replaceable).Out of the above the energy heterogeneity is the most important, since computation and link heterogeneity consumes more energy.

C. Impact of heterogeneity on WSN

Placing heterogeneous nodes in the sensor network, decreases response time and improve battery life time. As discussed above, Computation and link heterogeneity decreases the waiting time thereby, decreasing the response time. The average energy consumption will be less in heterogeneous sensor networks for forwarding a packet from the normal nodes to sink, hence life time is increased.

III. INTRUSION DETECTION SYSTEM

Event Data is the network activities (for example number of success and failure of authentication). This set of data is prepared for further analysis.

Misuse Detection analyses event data from signature record. In case of event data is matched with any rules, alert signal will be raised. Otherwise, event data is forwarded to anomaly detection for further analysis.

Anomaly Detection compares event data with signature record to find harmful attacks from intruder. If probability reaches the risk threshold, alert signal will be raised.

Signature Record is a database which contains signature of unauthorized and high risk activities. In addition, each record contains level of harm for misuse detection and probability chance for anomaly detection.

Alert is an interface between operating system and IDS. Duties of alert are broadcasting alarm and alert information.

IV. RELATED WORK

The research of heterogeneous wireless sensor network is not new. In an application for habitat monitoring, Estrin et al. [1] proposed a system architecture in which data filtered by local processing on way through larger, more capable and more expensive nodes.

References [2] [3] provide other two examples of real sensor networks with heterogeneous nodes for processing and transport tasks. In above works, the necessity of heterogeneity and the mechanisms of packet forwarding and processing are demonstrated and described.

Sensing models are of two types. They are single sensing model and multi sensing model. Intrusion detection process in these two models is explored by Wang et al. [4]. In his work, the combination of detection probability and network parameters such as transmission range, sensing range, and node density are considered for experiments under single sensing models**.**

Lee et al. [5] analyzed WSN in heterogeneous network environment under various kinds of deployments for maximizing lifetime of network. Their studies revealed that life time of WSN can be maximized by using certain mechanisms and especially by adding micro servers that affect life time of network positively.

Xi Peng et al [6] 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., [7] 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.

Zhang and Lee [8] 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. [9] 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. [10] 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.

Qi Wang et al., [11] 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. PURPOSED MODEL

Our objective is to detect all intrusions in heterogeneous WSN.In this section, we purposed single sensing model and multiple sensing detection model in heterogeneous WSN to detect intruder .The purposed system aims to manage available energy in efficient manner to enhance the network scalability, flexibility and lifetime. We divide sensor network into clusters which are again partitioned into sectors. It will minimize the energy consumption by avoiding all the nodes needing to send data to a distant sink node. It uses anomaly detection technique in such a way so that phantom intrusion detection can be avoided logically.

A. Assumptions

- A sensor can be in any one of the following states:

NEW→ MEMBER→SUSPECTED→ MALICIOUS
GENUINE → DEAD ISOLATED

- Each sensor node has a unique id in the network.
- Each member node has authentic wake-up token.
- A protocol is used to assign a secure wakeup and sleep schedule for the sensor nodes.
- Sink node is honest gateway to another network.
- Sensor nodes excluding leaf nodes and forwarding sector heads in the system participate in intrusion detection process.
- Generally, sector coordinator is responsible for anomaly detection and sector monitor is responsible for detection of intrusion.
- Anomaly can be detected on the basis of energy consumption rate, allotted wakeup schedule, authentic wakeup token, number of packets received within a time interval. Reputation of sensor node needs to be considered during intrusion detection.

VI. 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.

A. 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.

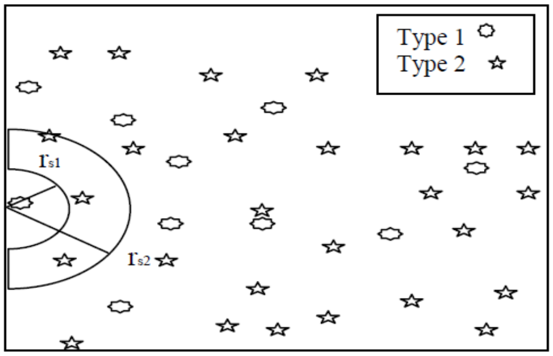

Fig 2: The area covered by sensors at the boundary

Theorem 1

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

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

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

Proof:

Here the area we need to consider when the intruder enters from the boundary is $A1=(\pi rS1^2)/2$, $A2=(\pi rS2^2)/2$,..$AN =\pi rSN^{2/}2$ 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-$e^{-n1}e^{-n2}…e^{-nN}$ 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

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

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

Proof: This can be proved just like above theorem.

B. Multisensing

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

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

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.

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

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

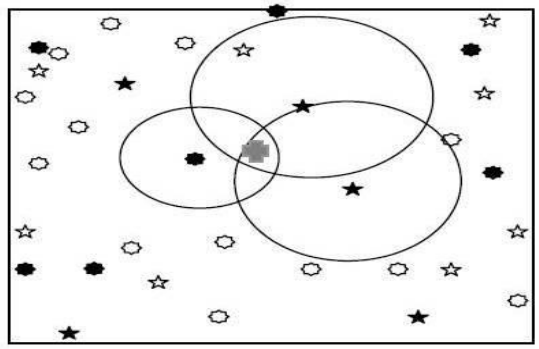

Fig 3- Multi-Sensing

VII. CONCLUSION

In this paper, we propose a novel solution to decide how many and where the heterogeneous nodes should be deployed in the randomly deployed sensor network. The simulation results show that our solution is practicable and useful to increase the network lifetime and reliability. It has been observed that these intrusion detection systems are not adequate for protecting WSN from intruders efficiently. The need of the day is an IDS for detecting intrusions accurately in an energy-efficient manner. Simulation proves the effectiveness of proposed model.

REFERENCES

[1] A. Cerpa, J. Elson, D. Estrin, L. Girod, M. Hamilton, and J. Zhao,"Habitat monitoring: application driver for wireless communications technology," in Proc. ACM SIGCOMM Workshop on Data Communications in Latin America and the Caribbean, Costa Rica, April 2001

[2] A. Mainwaring, J. Polastre, R. Szewczyk, D. Culler, and J. Anderson, "Wireless Sensor Networks for Habitat Monitoring," Intl. Workshop on Wireless Sensor Networks and Applications (WSNA '02), Atlanta, GA, Sept. 2002.

[3] H. Wang, D. Estrin, and L. Girod, "Preprocessing in a Tiered Sensor network for Habitat Monitoring," in Proc. of the IEEE Conf. on Acoustics, Speech, and Signal Processing, Hong Kong, China, April 2003 .

[4] 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..

[5] Lee, J.J., Krishnamachari, B., Kuo, C.C.J.: Impact of Heterogeneous Deployment on Lifetime Sensing Coverage in Sensor Networks (IEEE SECON). (2004).

[6] 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.

[7] 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.

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

[9] 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.

[10] 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.

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

AUTHORS

First Author – Priyanka Rai, B.tech Final Year, Student of Computer Science & Engineering, ITM Gida, Gorakhpur
Second Author – Pankaj Kumar Srivastava, B.tech Final Year, Student of Computer Science & Engineering, ITM Gida, Gorakhpur
Third Author – Upama Singh, B.tech Final Year, Student of Computer Science & Engineering, ITM Gida, Gorakhpur