IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 1, Ver. IX (Feb. 2014), PP 51-66
www.iosrjournals.org

Probabilistic Model for Single and Multi-Sensing Intrusion Detection in Wireless Sensor Networks

Shaila K[1], Sajitha M[1], Tejaswi V[1], S H Manjula[1], Venugopal K R[1], L M Patnaik[2]
[1]*University Visvesvaraya College of Engineering, Bangalore, India*
[2]*Honorary Professor, Indian Institute of Science, Bangalore, India*

Abstract : *Wireless Sensor Networks consists of tiny devices capable of processing, routing the sensed data and are capable of detecting the intruders. The process of detecting any suspected(anomalous) moving object(attacker) within the reach of a Wireless Sensor Network area is referred to as* intrusion detection*. In this paper, we propose an algorithm to detect the intruder by the cluster heads in a 2D and 3D homogeneous Wireless Sensor Networks. This algorithm overcomes the attacks on implementation and also, reduces the energy consumption. The proposed algorithm considers Single Sensing and Multi-Sensing Intrusion Detection using minimum number of sensor nodes and a probabilistic model has been developed for both 2D and 3D homogeneous networks. Simulation results show that the power analysis attack and energy consumption is minimized by activating only few sensor nodes for detection and using only few sensor nodes for processing of data. The performance of the proposed algorithm is better compared to using all the sensor nodes for detection where the energy consumption is more.*

Keywords: *Cluster head, Intrusion Detection, Multisensing, Power Analysis Attack, Wireless Sensor Networks.*

I. INTRODUCTION

Wireless Sensor Networks(WSNs) consists of a large number of sensor nodes which are deployed in a spatial environment. These nodes are capable of sensing any of the physical or environmental conditions. WSNs are widely used in military applications such as in borders for finding out the infiltrations, industrial process monitoring and control, healthcare applications, environment and habitat monitoring, home automation and traffic control[1]. WSNs finds applications in area monitoring, environmental monitoring, water level monitoring, vehicle detection, agriculture, greenhouse monitoring *etc*.

Sensor nodes perform sensing, data processing and communication with limited resources like power, computational capacities, memory size and low bandwidth. Therefore, utmost care has to be taken while constructing the networks under these constraints. Communication of data in WSNs require large amount of energy. Thus, energy is vital for many applications in WSNs since it is impossible to recharge the deployed nodes. The network lifetime of a sensor node is inturn dependent on the battery lifetime. The energy required can be reduced by using solar cells. But the disadvantage is battery charging using solar power will be less during rainy or winter season. One approach is to make some sensor nodes move to sleep mode and wake them up as and when required to save energy. Considerable efforts have been devoted to minimize the energy consumption and increase the lifetime of the network.

The sensors not only perform computation and communicate data but also sense certain essential parameters in the area of interest and send the information to the base station or sink. So the sensors are deployed throughout the area of interest. Many sensor nodes in WSNs are usually static after deployment and communicate mainly through broadcast rather than point-to-point communication. Sensors are deployed in a variety of domains and many applications should be secure from attacks. The two major parameters, energy and security are interrelated and are difficult to handle. Due to limited power resources, energy issues restricts the implementation of security. Hence, while designing a protocol to incorporate security issues one must ensure to minimize the energy consumption.

The security issues that are to be addressed in a WSNs are data confidentiality, data integrity, service availability and energy consumption. Many security protocols for WSNs have been developed like Sensor Protocol for Information *via* Negotiation (SPINS) that addresses data confidentiality, data authentication and data freshness and provides authenticated broadcast[2]. Localized Encryption and Authentication Protocol(LEAP), supports in-network processing based on different security requirements but restricts the security of node compromise to intermediate network neighborhood[3].

In WSNs many security protocols are based on the nature of attacks like passive, active, internal, external, host and network. These attacks are categorized into layers depending on the type of protocols : physical layer-physical capture, data link layer-energy depletion attacks, network layer-most of the attacks occur in this layer-false message, sinkhole and sybil attack *etc.*, transport layer-run out of memory attack and

Application layer attacks-data gathering, target tracking *etc.*,[4]. The external attack usually comprises of an external intruder entering into the given network. In many sensor networks routing and sensing techniques should have an idea of the location of the intruder with high accuracy or perfection. The internal intrusion may cause jamming, eavesdropping, unauthorized access, spoofing and denial-of-service. The best security solution for any type of network is categorized as: *prevention* and *detection*. Prevention techniques, such as encryption, authentication, secure routing, firewalls *etc.*, are used to prevent attacks from outside. These prevention measures reduce the possibility of intrusion, but cannot eliminate the intrusion completely. Intrusion detection is essential to achieve longer lifetime and defend the network security by the intruders. However, physical links may always be tampered even if any safety precautions are taken in WSNs. Therefore, prevention techniques are becoming obsolete. If any preventive measure protocol fails, then the intruder has to be detected and it has to be tracked by applying intrusion detection techniques.

The intrusion detection techniques are broadly classified into two types[5]. They are *misuse detection* and *anomaly detection*. *(i) Misuse Detection*: The activities of the intruder is expressed interms of a model and check if its main goal is to detect any activities. It detects the known intrusion accurately but is not able to detect the emerging attacks. *(ii) anomaly detection*: It defines a set of parameters for resource utilization like CPU, memory, documents, check sum *etc*. The systems operational values are compared with normal parameters to determine the invasion. The information can be hacked or manipulated in data link layer and network layers in the WSNs security architecture, thus destroying the integrity of the network. So, Intrusion Detection Systems can be used to detect the intruder. Various intrusion detection techniques have been developed which includes statistical, cumulative summation, data clustering, rule and support vector machine, data mining and game theory based techniques[5-6].

***Motivation*:** In WSNs clustering, energy utilization, routing, data aggregation, multimedia, collaborative processing, security *etc*., are related to each other. For any application, if the WSNs formed is not secure from attacks, then the entire effort of data transmission is lost. There are two types of attacks: *external* and *internal*. External attacks may change the nodes to behave maliciously resulting in an abnormal behavior. The internal attack changes the data processed within the nodes. The detection of any change in the data processed is difficult. So, we have to identify the external attacks and detect the internal attacks that occur in WSNs.

***Contribution*:** We have developed an algorithm that handles both external and internal intrusion detection. Internal intrusion detection involves the *Attacks on Implementation*, which includes two types of attacks :*Timing attack* and *Power Analysis Attack* [5]. The power required for processing, detecting and routing is substantial. The internal intrusion detection includes the analysis of data sent by each node. The proposed algorithm detects the intruder externally and its location in the network. The algorithm is also used for internal data analysis, where it selects a node as the cluster head among a set of nodes using the clustering technique and activates its *Intrusion Detection System* (IDS) which transmit the detected data to the sink node. So, the remaining nodes in the cluster are used for processing of data for further routing. Thus, energy consumption is minimized during the intrusion detection process.

***Organization*:** This paper is presented in nine sections. Literature Survey is discussed in Section 2 and Background Work is explained in Section 3. Problem Definition and Intrusion Detection System is given in Section 4. Mathematical model for Intrusion Detection in a 2D-Homogeneous WSNs and 3D-Homogeneous WSNs is derived in Section 5 and Section 6 respectively. Algorithm and Implementation are discussed in Section 7 and 8 respectively. Simulation results and Conclusions are presented in Section 9 and Section 10.

II. LITERATURE SURVEY

Wang *et al.*,[7] have developed an analytical model for both single and multi-sensing homogeneous and heterogeneous WSNs to detect an intruder considering the parameter like node density, sensing range and transmission range. Dousse*et al.*, [8] propose an upper bound to the distance traveled by an object in a straight line. They have considered a giant cluster of sensor nodes and assumed that the intruder moves with a constant speed and hits the giant component. They have developed a probabilistic model based on non-memoryless behavior and Asymptotic behavior. There is a possibility of the intruder misbehaving before hitting the giant cluster.Krontiris*et al*.,[9] propose a light weight scheme in which the nodes monitor their neighbors. They have designed an Intrusion Detection System (IDS) to detect blackhole and selective forwarding attacks and further in [10] discusses about cooperative intrusion detection to reduce the possibility of the nodes being attacked. Since all the nodes are detecting the intruder and the neighboring nodes are exchanging the information to determine if any attack has occurred results in increased time and energy consumption. Ashfaq*et al*., [11] classify and discuss various types of IDS that are capable of detecting malicious behavior of the sensor nodes. Stetsko*et al*., [12] and QiWang*et al.*, [13] present an IDS that employs neighbor-based detection technique. This technique

was applied for the detection of selective forwarding, jamming and hello flood attacks. Here, there is a possibility of a malicious node pretending to be the neighbor node.

Brutch*et al*., [14] classify IDS into two categories: host-based and network-based. Further IDS is classified as signature based, anomaly based and specification based. Liu *et al*., [15] have explored the dynamic aspects of the coverage of a mobile sensor network where, the moving sensors are used for detecting the intruders. They have developed a mathematical model to determine the detection time for stationary and mobile target. The accuracy of detecting a stationary target by the mobile sensor is less and the probability of detection of mobile target by the mobile sensor node is less since, the target has to be within the coverage area of the sensor node.Wang *et al*., [16] propose a novel Sine-curve mobility model to determine the intrusion path using single and *k*-sensing detection in a given WSNs. There is some effect with variation of amplitude and frequency but there is no effect with the phase variation. When a Sine-curve path is used by the intruder, then it has to be approximated to Sine-to-Line factor so that there is a least probability of intrusion detection. Peng*et al*., [17] perform analysis of each layer of networks in security model and describe the security management measures in the data link layer and network layer. They have deployed Intrusion detection strategy in the form of layers. Based on the existing encryption and authentication protocols a structure is built to detect most types of attacks in the WSNs. Zhang *et al*., [18] propose a dynamic key management scheme which uses cryptographic concept.

Misra*et al*., [19] develop a Simple Learning Automata model for the detection of an intruder in WSNs using stochastic learning automata as a self-operating learning model for reducing the energy consumption. The model consists of an automation(self learning system), environment(medium of the machine functions) and reward/penalty structure. The reward function is used to decrease the sampling rate and penalization function is used to increase the sampling rate of the node. Adaptive threshold is used by Techateerawat*et al.*, in [20] to activate the IDS by the process of voting. But, the execution of the protocol is time consuming since, it has to sample every packet. Kung *et al*., [21] describe Scalable Tracking using networked sensors and Drain-and-Balance method to track large number of moving objects and mobility patterns of the objects.Tao *et al*., [22] propose a sensing model which is capable of calculating the sensing signal and integrator model to detect the intruder using uniform and Gaussian distribution. Roman *et al*., [23] and Sun *et al*., [24] present watchdogs to monitor the neighbors and general IDS architecture for a static sensor networks. The energy consumption is taken care by the watchdogs which activate the global agents. Tran *et al*., [25] emphasize that bandwidth and battery power resources are the limited in WSNs. Mostarda*et al*., [26] present a new framework that is capable to output distributed secure protocols in the field of mobile WSNs.

Wang *et al*., [27] develop a probabilistic model using both Poisson and Gaussian distribution for multiple deployment of nodes in the area of interest and detect the intruder efficiently. In our previous work [28] we have developed a probabilistic model and a secure and energy efficient algorithm to detect the intruder in homogeneous WSNs. Here, fewer sensors are activated to detect the intruder, thus reducing the energy consumption based on the sensing range and transmission range of the sensors.Li-Liann*et al*., [29] compare Location based, Neighbor based and Probability based algorithms to minimize energy consumption so as to increase the network lifetime and suggests cluster based algorithm that identifies the redundant nodes. In cluster based algorithm the nodes that are grouped under one cluster head are off-duty nodes, since only the cluster head communicates with other nodes. Yan *et al*., [30] propose an Hybrid Intrusion Detection System within a cluster head. They have used three modules for detection based on the concept of neural networks *i.e*., training and learning: *(i) Anomaly detection model*-Rule based method, *(ii) Misuse detection*-BPN with supervised learning method and *(iii) Decision Making model*-Rule based method. Based on the training samples used for BPN the classification is done and the module is evaluated. Shio*et al*., [31] propose cluster based WSNs to detect the intruder using MAC address and keeps track on the inclusion or omission of the intruder. Ouadoudi*et al*., [32] propose a decentralized clustering algorithm called as Enhanced Low Energy Clustering Protocol for Routing in WSNs (ELECP). The ELECP is applied to areas where sensed data are not perfectly correlated.

III. BACKGROUND

Intrusion detection in Wireless Sensor Networks (WSNs) is of practical interest in many applications such as detecting an intruder in a battlefield. The intrusion detection is defined as a mechanism for a WSNs to detect the existence of inappropriate, incorrect or anomalous moving attackers. It is a fundamental issue to characterize the WSNs parameters such as node density and sensing range in terms of a desirable detection probability. Wang *et al*., [7] discuss two WSNs models: homogeneous and heterogeneous WSNs by considering two sensing models: Single-Sensing Detection and Multiple-Sensing Detection. All the sensor nodes participate in detecting the intruder simultaneously and continuously. This consumes enormous energy and reduces the network life time with any malicious node sending wrong information to the base station. The intruder can move either taking a straight or curved path. In addition, they discuss about the network connectivity and broadcast reachability in WSNs.

Tran *et al*., [25] emphasize on bandwidth and battery power as the limited resources in WSNs. An efficient way of utilizing these resources is essential during the construction of IDSs. Intrusion detection modules on sensor nodes try to detect the malicious action which occurs within its radio range. The monitoring technique like watchdog, local monitoring, *etc*., relies on the broadcast nature of sensor communication and suggests to deploy a large number of sensors in the sensing environment. The intrusion detection module activate only a few sensor nodes called *monitor nodes* and remaining nodes are left in sleep mode. This reduces the power requirement when compared with all the sensor nodes in the network being active. Shio*et al*., [31] propose cluster based WSNs to detect an intruder. The base station holds all the information of each cluster *i.e*., its number and MAC address. It also monitors any inclusion or deletion of nodes within the cluster and tracks the MAC address history and management of database. The cluster head keeps track of each node and sends the information to the base station. The cluster head receives the data, compresses it and sends it to the base station. They mainly discuss about the energy consumption and inclusion of the intruder as a node or as a cluster head within any cluster and is monitored by the base station and sends an alarm signal.

IV. PROBLEM DEFINITION AND INTRUSION DETECTION SYSTEM

(A) Problem Definition

The energy consumption and network lifetime of a WSNs are interdependent on each other. The energy required for internal processing of data is less compared to the transfer of data from one sensor node to the other. When all sensor nodes are in the process of detecting an intruder and communicating this information to the base station a large amount of energy is consumed and the network lifetime is reduced. The main objectives of our work are:

*(i)*to activate only a set of sensor nodes (cluster heads) to participate in detecting an intruder and communicate the information to the sink node.

*(ii)*minimize the attack on implementation attack.

*(iii)*reduce the energy consumption and increase the network lifetime of the WSNs.

Assumptions: *(i)* The WSNs is a static network and intruder is a moving object. *(ii)* Each node consists of omni-directional antenna properties. *(iii)* Sink node knows all the nodes location and their neighbor list. *(iv)* Algorithm is executed at the sink node and it sends a packet to the selected nodes to activate its IDS module.

(B) Intrusion Detection System

Intrusion detection is defined as a mechanism for WSNs to detect the existence of inappropriate, incorrect or anomalous moving attackers. For example, while detecting an intruder in the battle field. Hence, it is necessary to address the fundamental issues like node density and sensing range of WSNs interms of a desired detection probability. The two types of intrusion detection system are *single sensing detection* and *multi-sensing detection*. In single sensing detection, a single sensor is capable of detecting the intruder whereas in multi-sensing detection more than one sensors or multiple sensors are used for detecting the intruder [7]. The intruder may be detected as soon as it enters the vicinity of WSNs or after traveling some distance within the area of interest, since it is mainly depending on the availability of the sensor. If the intruder is aware of the destination then it takes a shortest and straight path, but if it is unaware of the destination then it takes longer path. The intruder can take a straight path or random path or a curved path.

Table I : Notations

Symbols	Definition
A	Area
d	Distance moved by the intruder
r_s	radius of the circle covered by a particular sensor
N	Total number of nodes in the network
m	nodes within a cluster
n_d	probability of sensors detecting the node
t_r	transmission range
s_r	sensing range
pi	diameter of the sensing range
I	set of neighbors whose distance with *i* is less than half sensing range
N(i)	Set of neighboring nodes within the cluster, where, i = selected nodes

V. INTRUSION DETECTION IN A 2D-HOMOGENEOUS WSNS

(A) System Model

A static, homogeneous WSNs model in a two-dimensional 2*D* plane is considered as shown in Figure 1. The notations used are described in Table 1. A set of sensor nodes *N* are deployed in the area of interest $A = L * B$, where, $N = (n_1, n_2, n_3, \ldots, n_n)$ and n_i is the i^{th} sensor, *B* is equal to *L*. The sensors are uniformly and randomly deployed resulting in a 2*D*-network. In a homogeneous WSNs the capacity of all the sensors have to be equal and therefore all the sensors have equal sensing range s_r, transmission range t_r and node density n_d. When an intruder is in the vicinity of the sensor network, a particular sensor node detects the intruder only if it is within its sensing range s_r. So, the sensing range can be assumed to be a circle with diameter $2r_s$ at the sensor node being the center point of the circle as shown in Figure 1. WSNs consists of two regions, the *covered region* and *uncovered region* [7]. The region consists of all sensors capable of detecting within the circle $2r_s$ is referred to as *covered region* within the area of interest and the remaining regions is referred to as uncovered region. When an intruder enters into the area of interest it is unaware of the coverage area by each sensor node in the WSNs. If all the sensors are detecting the intruder simultaneously large amount of power is consumed and there is a possibility that all nodes die together thus reducing the network lifetime. To overcome this problem a set of nodes are formed as a cluster. Each time the IDS activates the nodes in a cluster, the activated nodes elect a node as the cluster head at that point of time. The activated node within the cluster detects the intruder, thus reducing the energy consumption and information is securely routed towards the sink.

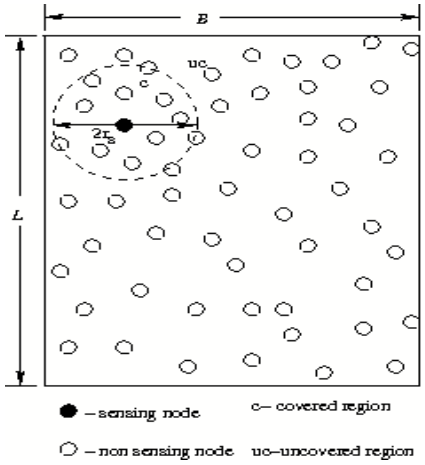

Fig. 1 System Model for a 2D-Homogeneous WSNs.

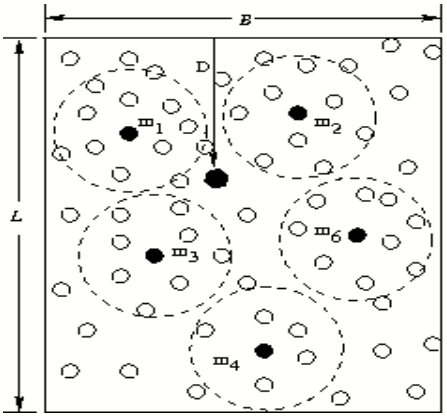

Fig. 2 Intrusion Detection in a 2D-Homogeneous WSNs.

(B) Mathematical Model

We derive the probability for single-sensing detection and multi-sensing detection for a 2*D* WSN model.

***Single Sensing Detection Model*:** Consider an intruder moving from the boundary as shown in Figure 2. The intruder moves a distance *D* from the boundary without being detected by the sensor m_1 or m_2, because the intruder is not within their sensing range. When it reaches a distance *D*, node m_1 (say) detects the intruder, the intruder position is now near to the activated node m_1 intruder is detected only when there is a sensor in the area moved by the intruder. The intruder can take a straight path or random path or a curved path. In this paper, for the purpose of analysis we have considered a straight path. The area moved by the intruder is,

$$A_{IS} = 2 * D * r_s + \pi \frac{r_s^2}{2} \quad \textbf{(1)}$$

which includes the distance traversed *D* and radius of the sensing range of the circle r_s.

***Definition*:** Single Sensing Detection states that, the intruder is detected if and only if there existsatleast one sensor within the coverage area *A*.

***Corollary*:** The intruder is detected if it comes in the sensing range of any of the sensors, otherwise it is not detected if it is in the uncovered area.

Let us now consider that, the intruder is dropped from the aircraft at a random point as shown in Figure 3, then the area moved by the intruder is given by,

$$A_{IR} = 2 * D * r_s + \pi r_s \quad \textbf{(2)}$$

In this case, the sensing area consists of two half circles and the distance traversed is *D*. The intruder is detected if it is within the sensing range s_r of the circle(cluster) around the sensing node as shown in Figure 3. The theorems are stated considering that the intruder is moving from the boundary of the network.

Theorem 1: An intruder is detected immediately by a single cluster head when it enters the boundary of a 2*D*-homogeneous WSNs.

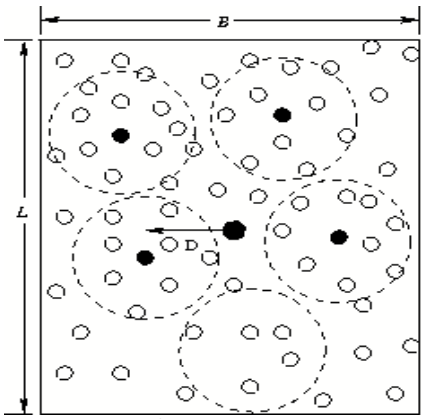

Fig. 3 Detection of Intruder by the sensor when dropped from air for a 2D-Homogeneous WSNs.

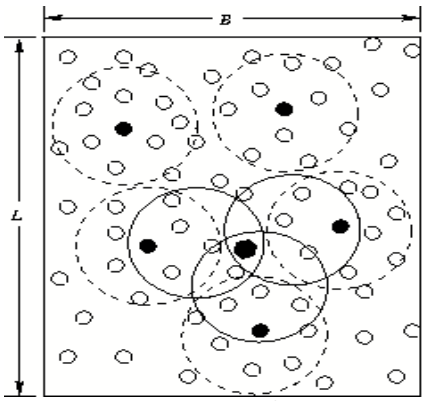

Fig. 4 Multisensing detection model for a 2D-Homogeneous WSNs.

Proof: Let us consider only one sensor node is activated by the Intrusion Detection System to detect an intruder, then *P(D)* be the probability that an intruder is detected immediately by the cluster head as it enters a 2*D*-homogeneous WSNs with node density n_d and identical sensing range of radius r_s and is given by,

$$P(D = 0) = 1 - e^{-n} \quad \textbf{(3)}$$

where, $n = n_d r_s^2/2$.Since the nodes are uniformly distributed in a particular area *A*, it follows Poisson distribution. According to Poisson distribution,

$$P(m, A) = \frac{(An_d)^m e^{-An_d}}{m!} \quad \textbf{(4)}$$

where, *m* = number of sensor nodes in the cluster, *A* = area of interest, n_d = probability of the sensor node responsible for intrusion detection.In this paper, only *i* sensor nodes perform the intrusion detection at any instant. Therefore,$n_d = (i/A)$.

Consider the case when no sensors are available for detection in the area *A*, then, probability is equal to

$$P(0, A) = e^{-An_d} \quad \textbf{(5)}$$

Take the complement of probability to determine the probability that there is atleast one sensor node in a cluster in area *A* and the intruder being detected by this sensor is,

$$1 - P(0, A) = 1 - e^{-i} \quad \textbf{(6)}$$

This shows that even if one sensor within a cluster is active then it can detect the intruder effectively, reducing the energy consumption, thus increasing the lifetime of the nodes to detect the intruder further. The remaining nodes can pass information to the sink by performing encryption on the data. Hence the theorem is proved.

Theorem 2: No intruder can travel a maximum distance of D_M from the boundary before being detected in a 2*D*-homogeneous WSNs.

Proof: If D_M is the maximum distance an intruder can travel before detection, then the probability of the intruder being detected is *P(D)* and is given by,

$$P(D \leq D_M) = 1 - e^{-i_n} \quad \textbf{(7)}$$

where, i_n is the number of sensor nodes(cluster head) activated to participate in the intrusion detection.. The area moved by the intruder is,

$$A = 2 * D_M * r_s + \frac{1}{2}\pi r_s^2 \quad \textbf{(8)}$$

If sensor nodes are not activated in that area, then the probability of detection is P(0, A).

$$P(0, A) = e^{-An_d} \quad \textbf{(9)}$$

Substituting Equation 5 for *P(n, A)*. When, $n_d = i_n/A$.Then,

$$P(0, A) = e^{-Ai_n/A} = e^{-i_n} \quad \textbf{(10)}$$

The sensors are activated in the area to detect the intruder, then, probability is complement of the above equation,

$$1 - P(0, A) = 1 - e^{-i_n} \quad \textbf{(11)}$$

that give the probability of detecting an intruder by the activated node in any cluster within the coverage area.

Theorem 3: When an intruder enters the 2*D*-homogeneous WSNs then an event occurs.

Proof: The probability of activating a single node in a cluster depends on the occurrence of an event i_A in a 2*D*-homogeneous network and is given by,

$$i_A = \frac{\sum p(i_n)}{\sum i_n} = \frac{p(i_1) + p(i_2) + \cdots + p(i_n)}{m} \quad \textbf{(12)}$$

where, *m* = Total number of nodes in the cluster.

If the total number of nodes in the cluster is i_n then, probability of any node being activated is like performing a random experiment on *n* trials. Then,

$$i_A = \frac{p(i_1) + p(i_2) + \cdots + p(i_n)}{n} \quad \textbf{(13)}$$

$$i_A = \frac{\sum p(i_n)}{\sum i_n} \quad \textbf{(14)}$$

where, *n* = number of trials that can be less than or equal to the number of nodes in the cluster *m* and $p(i_1)$, $p(i_2)$, . . . , $p(i_n)$ = probability of the node being activated in the cluster.

Multi-Sensing Detection Model: Some applications require more than one sensor information about the intruder like finding the position of the intruder. In such cases, the intruder is said to be detected only when it is within a sensing range of *y* sensors as shown in Figure 4.

Theorem 4: An intruder will be detected immediately by multiple sensors when it enters the boundary of 2*D*-homogeneous WSNs.

Proof: In a multi-sensing detection model if an intruder enters the region with n_d number of nodes with s_r as the sensing range, then probability that an intruder is detected immediately by more than one activated sensor node can be proved using Poisson distribution and is given by,

$$P_m\,(D = 0)1 - \sum_{i=0}^{N-1} e^{-i_n} \quad \textbf{(15)}$$

where, i_n = number of activated sensors within the area $A = \pi\, r_s^2/2$

The area is only one half circle with radius r_s. The probability of detection of an intruder by more than one cluster head is given by $P(i_n, A) \sum_{i=0}^{N-1} P(i_n,\ A)$ gives the sum of probabilities of detecting the intruder with less than i_n sensor. So, the complement will be the multi-sensing probability.

Theorem 5: The intruder travels a maximum distance D_{MK} from the boundary before being detected by multiple sensors in a 2D-homogeneous WSNs.

Proof: Let D_{MK} be the maximum distance an intruder traverses before detection, then the probability *P(D)* that the intruder can be detected by more than one cluster head in a given 2*D*-homogeneous WSN is given by,

$$P(D > D_{MK}) = 1 - \sum_{i=0}^{3} e^{-i_n} \quad \textbf{(16)}$$

If the sensor node are not activated in that area, then the probability of detection is *P(0,A)*.

$$P(0, A) = e^{An_d} \quad \textbf{(17)}$$

$$P(0, A) = e^{\frac{-Ai_n}{A}} = e^{-i_n} \quad \textbf{(18)}$$

If three sensors are detecting at the same time to determine various parameters of an intruder then,

$$P(0, A) = e^{-i_1} + e^{-i_2} + e^{-i_3} = \sum_{i=1}^{3} e^{-i_n} \quad \textbf{(19)}$$

Taking the complement, then, the probability is,

$$1 - P(0, A) = 1 - \sum_{i=1}^{3} e^{-i_n} \quad \textbf{(20)}$$

VI. INTRUSION DETECTION IN A 3D-HOMOGENEOUS WSNS

(A) System Model

A static, homogeneous WSNs model in a three-dimensional 3*D*-plane is considered as shown in Figure 5. A set of sensor nodes *N* are deployed in the area of interest $A = L * B * H$, where, $N=(n_1, n_2, n_3, \ldots, n_n)$ and n_i is the i^{th} sensor, where, $B=H=L$. The sensors are uniformly and randomly deployed resulting in 3*D*-network. In a homogeneous WSNs the capacity of all the sensors have to be equal, therefore all the sensors have equal sensing range s_r, transmission range t_r and node density n_d. If the intruder entering the network is aware of the

destination and the network model, then it takes the shortest path to reach the destination. Suppose, the intruder follows a straight path and moves a distance *D* to reach the destination, then there is a possibility of the activated sensor nodes detecting the intruder as shown in Figure 6. Now, if the intruder is unaware of its destination, it follows a random path or a curved path as shown in Figure 7. For our analysis, we consider a straight path. The intruder can move either from the boundary or from any random point, *i.e.*, intruder being dropped from air within the network.

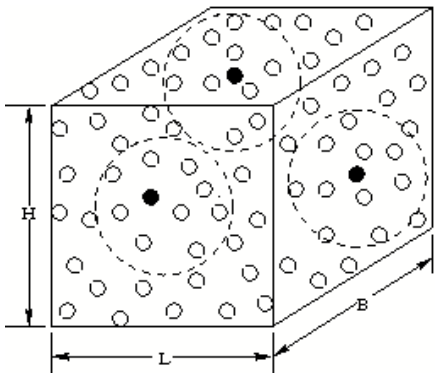

Fig. 5 Multi-sensing detection model for a 3D-Homogeneous WSNs.

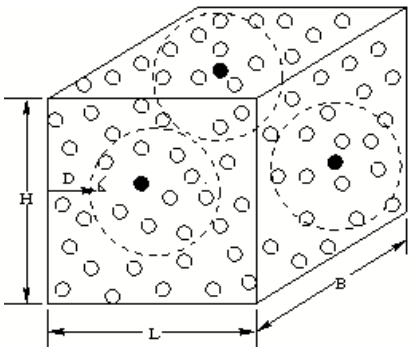

Fig. 6 Intruder moving in Straight Path for a 3D-Homogeneous WSNs.

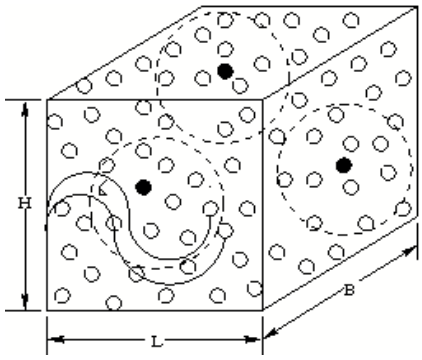

Fig. 7 Intruder moving in Curved Path for a 3D-Homogeneous WSNs.

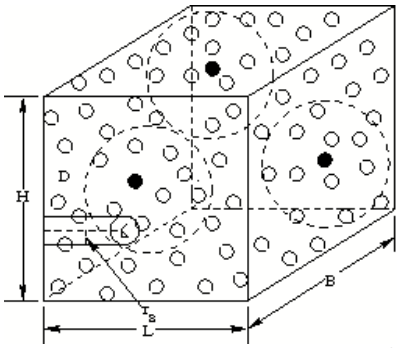

Fig. 8 Area moved by the Intruder Entering from Boundary for a 3D-Homogeneous WSNs.

(B) Mathematical Model

We derive the detection probability for single-sensing detection and multi-sensing detection for a 3*D* Wireless Sensor Network model.

Single Sensing Detection Model: When an intruder enters the sensing range then, it is detected by the sensors. When the intruder enters the boundary of WSNs and if nodes near the boundary are activated by the IDS then the intruder is immediately detected by those sensors. The information is later passed on to the base station by the cluster head. Suppose, the intruder is not detected, it moves a distance *D* from any of the boundary as shown in Figure 8. The intrusion distance $D>0$ and activated nodes in the cluster is within the area A_v. The area includes a cylindrical volume, length *D* and diameter $2r_s$ and is given by,

$$A_{vb} = \pi r_s^2 * D + (2/3)\pi r_s^3 \quad \textbf{(21)}$$

As defined in Section IV, the intruder is detected only if it is within the sensing range of the sensors.

Next, consider that the intruder is dropped from the aircraft and its movement starts from a random point as shown in Figure 9, then the area moved by the intruder is given by,

$$A_{vr} = \pi r_s^2 * D + (4/3)\pi r_s^3 \quad \textbf{(22)}$$

where, the area of intrusion detection consists of sensing range as a sphere, with radius of a sphere r_s and length *D*.In this case, the sensing area consists of two half circles and the distance traversed is *D*. The intruder is detected if it is within the sensing range s_r of the circle(cluster) around the sensing node as shown in Figure 8. The theorems are stated considering that the intruder is moving from the boundary of a given network.

Theorem 6: An intruder is detected immediately by a single cluster head when it enters the boundary of a 3*D*-homogeneous WSNs.

Proof: When only one sensor node is activated by the Intrusion Detection System to detect an intruder, then the probability *P(D)* indicates that an intruder is detected immediately by the cluster head as it enters a 3*D*-homogeneous WSNs with node density n_d and identical sensing range of radius r_s is given by,

$$P(D = 0) = 1 - e^{-n} \quad \textbf{(23)}$$

where, $n=n_d*(2/3)\pi r_s^3$. Since the nodes are uniformly distributed in a particular area of interest A_v, it follows Poisson distribution. According to Poisson distribution,

$$P(m, A_v) = \frac{(A_v n_d)^m . e^{-A_v n_d}}{m!} \quad \textbf{(24)}$$

where, m=number of sensor nodes in the cluster, A_v = area of interest in terms of volume, n_d=probability of the sensor node responsible for intrusion detection.

When no sensors are available for detection in area A_v, then, the probability is,

$$P(0, A_v) = e^{-A_v n_d} \quad \textbf{(25)}$$

To determine the probability of atleast one sensor node available in a cluster in area A_v and the intruder being detected is,

$$1 - P(0, A_v) = 1 - e^{-A_v (2/3)\pi r_s^2 D_M} \quad \textbf{(26)}$$

Hence the theorem is proved.

Theorem 7: No intruder can travel a maximum distance of D_M from the boundary before being detected in a 3*D*-homogeneous WSNs.

Proof: If D_M is the maximum distance an intruder traverses before detection, then the probability *P(D)* that the intruder can be detected within D_M in the given 3*D*-homogeneous WSN is given by,

$$P(D \leq D_M) = 1 - e^{-A_v \pi r_s^2 D_M} \quad \textbf{(27)}$$

The area moved by the intruder in a 3*D*-homogeneous network is,

$$A_v = \pi * r_s^2 * D_M \quad \textbf{(28)}$$

If the sensor nodes are not activated in area A_v, then the probability of detection *P(0, A)* is,

$$P(0, A) = e^{-An_d} \quad \textbf{(29)}$$

The probability of detecting the intruder *D* is obtained by taking the complement of *P(0, A_v)*.

$$1 - P(0, A) = 1 - e^{-An_d} \quad \textbf{(30)}$$

From equation 10,

$$1 - P(0, A) = 1 - e^{-A_v i_{n/A}} = 1 - e^{-i_n} \quad \textbf{(31)}$$

Theorem 8: An intruder travels a maximum distance greater than zero before being detected in a 3*D*-homogeneous WSNs.

Proof: Let *P(D=D_M)* be the probability that the intruder is detected at a distance D_M>0 when it is traversing within the given 3*D*-homogeneous WSN as shown in Figure 9 and is given by,

$$P(D = D_M) = \pi n_d r^2 * e^{-n_d \pi r^2 D_M} \quad \textbf{(32)}$$

Differentiating,

$$P(D \leq D_M) = 1 - e^{-A_v \pi r_s^2 D_M} \quad \textbf{(33)}$$

$$P(D = D_M) = \pi n_d r^2 * e^{-n_d \pi r^2 D_M} \quad \textbf{(34)}$$

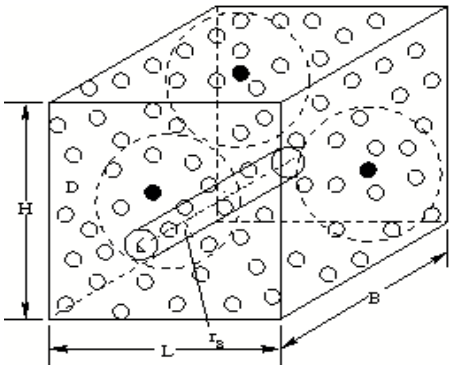

Fig. 9 Area moved by the Intruder thrown from Air for a 3D-Homogeneous WSNs.

Multi-Sensing Detection Model: In multisensing, more than one node has to be activated to detect the intruder in a 3D-homogeneous WSN.

Theorem 9: An intruder will be detected immediately by multiple sensors when it enters the boundary of a 2*D*-homogeneous WSNs.

Proof: In a multi-sensing detection model if an intruder enters the 3*D*-homogeneous WSN with the number of nodes n_d and sensing range s_r, then the probability that an intruder is detected immediately by more than one activated sensor node is given by,

$$P(D = 0) = 1 - \sum_{i=0}^{N-1} e^{-i_n(2/3)\pi r^3} \quad \textbf{(35)}$$

where, i_n = number of activated sensors within the area A_v.

Theorem 10: The intruder travels a maximum distance D_{MK} from the boundary before being detected by multiple sensors in a 2*D*-homogeneous WSNs.

Proof: Let D_{MK} be the maximum distance an intruder traverses before detection, then the probability *P(D)* that the intruder can be detected by more than one cluster head in a given 3*D*-homogeneous WSNs is given by,

$$P(D > D_{MK}) = 1 - \sum_{i=0}^{3} e^{-i_n(2/3)\pi r^3} \quad \textbf{(36)}$$

VII. ALGORITHM

The data transmission in any type of network has to be routed securely and energy consumed for data processing has to be minimized. In order to achieve this one has to take care if any intruder is entering into the network to jeopardize the effects of data communication. The Node Selection for Intrusion Detection (NSID) algorithm is shown in Table II. The algorithm developed to detect the intruder and attacks on implementation are carried out in four phases: *Phase 1*: Node Deployment; *Phase 2*: Cluster Formation, *Phase 3*: Node selection for coverage, *Phase 4*: Determining the location of the intruder and Passing the information to base station.

Phase 1: Node Deployment : A set of nodes is generated such that they have the same properties like sensing range, transmission range *etc*. Deploy minimum number of sensors n to cover the network area uniformly and randomly. Before deployment, generate a global pool of keys using random function on a particular value. Eliminate if any values are repeated in the global pool. The local pools of keys are generated randomly from the global pool of keys. The global pool of keys generated must be greater than local keys. The global keys are then randomly selected from the pool of keys and are stored in the corresponding nodes. The local pools of keys generated are stored in the nodes that are deployed randomly. Suitable encryption and decryption algorithms can be adopted to ensure that global key pool is resilient to any types of attacks.

Phase 2: Cluster Formation: After the nodes are deployed randomly in the area of interest, a network topology is formed. Every node in the network sends a *Hello* packet to all its neighboring nodes. The neighboring nodes respond by sending an acknowledgment consisting of node IDs and its position in the network. This information along with various routing information like key-matches, next hop *etc*., are updated in every node in the neighbor table. When the keymatches between any two cluster heads, a secure path is established between the nodes. The sensor nodes in the network topology are divided into clusters of equal size. One node is elected as the cluster head in each cluster which senses the intruder and acts like a gateway to communicate with other cluster heads and sink node.

Phase 3: Selection of nodes for coverage: This phase is responsible to select minimum number of sensors required to cover the area depending on both the sensing range and transmission range. A group of nodes are selected from each region with the nodes having minimum number of neighbors within the cluster, thus consisting of *m* nodes. The *minnode* function selects the number of nodes *k* to cover the total area. The value of *k* is calculated considering the total area and area covered by a single sensor node and number of sensor nodes participating in intrusion detection. While selecting nodes for the coverage, care has to be taken that it must be greater or equal to atleast the number of sensor nodes required for detecting the intruder.

Phase 4: Determining the location of the intruder and transmit information to base station: The selected nodes along with its neighbors having a distance less than half the transmission range is removed from the cluster. This establishes good network connectivity and effective broadcasting. Instead, if all the neighbors are removed then there is a chance of loosing the network connectivity. So, selected nodes are intimated to activate its IDS module within the clusters. When an intruder either enters from the boundary of the network or is dropped in-between the network, the activated sensor node within the coverage area detects the intruder and determines its location and transmits information to the base station. This process is done by the activated node in the cluster and the information is passed on to the cluster head elected by the activated nodes. The cluster head then transmits the encrypted information to the base station communicating either directly or *via* other

cluster heads in the network. Hence, the energy consumption is reduced when compared to all the nodes sensing the intruder and collecting information of its location and sending data to the base station. Hence, the lifetime of the cluster head is also increased. This phase is repeated until the intruder is located.

Table II. Algorithm: Node Selection for Intrusion Detection (NSID)

***First Phase** : Node Deployment*
begin
input: transmission range
Set k=1, r_i=0, r_j=0, n=50, p=40, *max(i=j*=1000);
for $i = n$, $i<n - r_i$, i++;
for $j = p$, $j<p - r_j$, j++;
Generate all the nodes using *rnd* function;
increment k;
if ($k>N$) exit
else repeat
endif
end
	***Second Phase** : Cluster Formation*
	begin
	Find Neighboring nodes;
	if(distance between nodes <t_r
	Find Neighbor function;
	Set sensing range(s_r), node density(n_d) and counter = 0;
	Perform the clustering considering all the sensors;
	for(k = 1 to N)
	group a set of nodes into clusters;
	cluster of size = m nodes;
	Broadcast *Hello* Message;
	Set all the nodes with the neighbor table and next hop;
	endif
	end

***Third Phase** : Selection of nodes for coverage*
begin
input : Sensing range, area covered by one sensor
Determine number of sensors required to cover the area minimum node function(t_r, s_r)
m < (Total area L*L/area covered by one sensor)*n;
Generates k< area covered by one sensor node;
Check if the selected number of nodes(m <= n);
for(i = 1 to m)
find the location x_1 and y_1 of the nodes;
for(j = 1 to m)
find the location x_2 and y_2 of the nodes.
calculate the distance between the nodes d using d=sqrt(x_2 - x_1)^2 + (y_2 - y_1)^2
if(d< transmission range(t_r) and t_r>= s_r) then
m \pi s_r^2 = k mod L^2; where, 0 <= k \pi s_r^2 -1;
elseift_r<s_r;
m \pi t_r^2 = k mod L^2, where, 0 <k \pi t_r^2 -1;
increment count;
include this node with corresponding cluster.
else
remove selected nodes(s, n) and repeat;
output : minimum nodes selected to cover the area.
end
	***Fourth Phase**: Determining location of the intruder and Communicating to base station*
	begin
	input: cluster of size m, transmission range t_r.
	intruder: Generate an intruder.
	move the intruder using y = (m*x) +c;
	Generate the Schedule Table;
	output: selection of nodes in the cluster.
	N_c< set of nodes in the cluster;
	$N(i)$ = set of neighboring nodes within the cluster;
	for cluster size m do
	for i = 0 to N-1 do
	if $N(i)$ \neq NULL;
	determine i with $N(i)_{min}$;
	stack <= i;
	if(a/D_{ai}<t_r/2);
	Selected node is$I$<a/D_{ai};
	if $N(i)$> 1
	Remove selected nodes and the neighbors when neighbor is > 1;
	$N_c = N_c$ - [i \cup I];
	else
	Remove only the selected nodes;
	$N_c = N_c - I$;N_c= NULL;
	Determine the initial position of the intruder;
	distIni= (p2-p1^2) + (q2-q1^2);
	Determine the position of the intruder moved;
	distOut = distOut + round($sqrt$(distIni));
	Encrypt the information and send to sink via cluster heads;
	end

VIII. IMPLEMENTATION

An intruder is defined as any moving object that enters into the WSNs area. When all nodes are detecting the intruder, the time required for the nodes to process data is more or they may not process the data resulting in the implementation attack. This results in the node failure of the network at the earliest and the node dies fast. There is a possibility that all nodes die simultaneously and also resulting in increase in consumption of energy. We have selected only few nodes for sensing and found that the above problem can be minimized. So the nodes are grouped into clusters and in each cluster one node is activated randomly to detect the intruder.

The remaining nodes are used for processing the data or any other applications. The detected information of the intruder is passed to the sink node. Using any cryptographic technique encrypts the information about the intruder and their location before transmitting to the sink node. This avoids any passive or active attacks that may be caused due to node compromise by the malicious nodes. The location of the intruder also can be determined by using more than one sensor. Simulation results proves that three sensor nodes (cluster heads) are sufficient to detect the intruder and its location. If more than three nodes are used for detection then the performance remains the same.

IX. SIMULATION AND EVALUATION

(A) Simulation setup: The simulation is performed in MATLAB. The topological area set up is for 500 sensors placed in a space of 1000*1000 meters. The node density is set as 0.0005 per square meter. The sensing range is

varied from 0 to 50 meters and maximal allowable intrusion distance is 50 meters. The deployment of sensors is randomly and uniformly distributed.

(B) Simulation: Sensors are deployed in accordance with a uniform distribution in a square network domain. We are assuming that each sensor knows its neighbors and sink has the knowledge of each sensor and its neighbors. First, the sink executes the algorithm and selects a set of sensors which can cover the entire area. The intruder is allowed to move through the WSNs area starting from any point. These sensors activates its Intrusion Detection Module(IDM) and if it detects an intruder the information is passed to the base station. In multi-sensing we are considering whether the intruder is within the visibility of multiple sensors *i.e.,* the sensors that is selected. So, the intruder has to be within the sensing range of atleast three sensors during multi-sensing of an intruder. Monte-Carlo simulation is performed and each data point shown in the graphs is average of 500 simulation results. The sensors are uniformly redistributed in the network domain for successive simulation runs. The analytical results are verified through simulation in MATLAB for single-sensing and multi-sensing detection models in WSNs by changing node parameters such as density, transmission range and sensing range.

(C) Performance Evaluation: The energy consumption and probability of detection are shown in the graphs. The results obtained from simulation are compared with the analytical model. Figure 10 indicates the number of nodes selected for Intrusion detection from the total number of sensors used for detection for a 2*D*-homogeneous WSNs. It is observed that the number of selected nodes is less than the total number of nodes. The selection of number of nodes decreases with increase in node density from 500 nodes. Figure 11 shows that the number of selected nodes is less than the total number of nodes in a 3*D*-homogeneous WSNs. But the number of selected nodes is greater compared to 2*D*-homogeneous network. The selection of the nodes decreases with the increase in node density from 550 nodes.

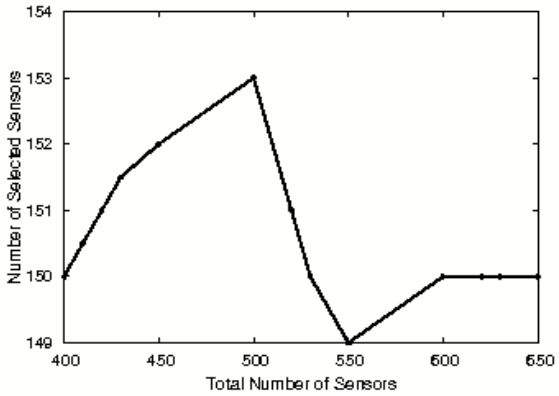

Fig. 10 Number of Nodes Selected for Intrusion Detection for 2D WSNs.

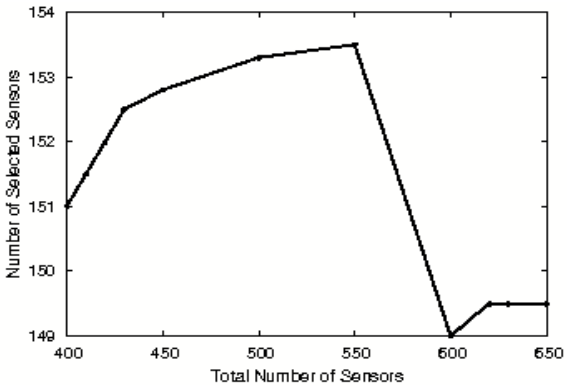

Fig. 11 Number of Nodes Selected for Intrusion Detection for 3D WSNs.

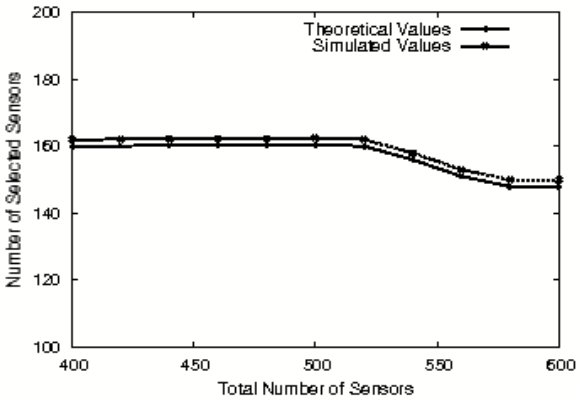

Fig. 12 Number of Sensors activated by the IDS Module for 2D WSNs.

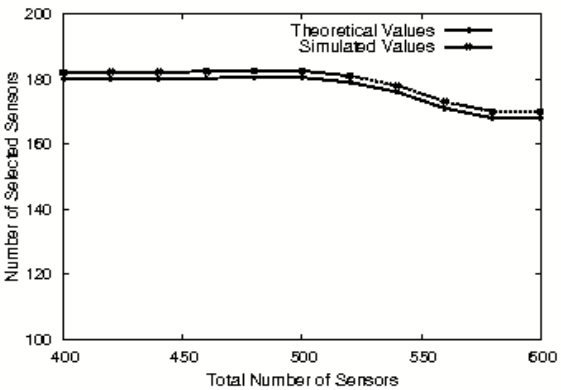

Fig. 13 Number of Sensors activated by the IDS Module for 3D WSNs.

Figure 12 demonstrates the number of nodes selected by the IDS module considering the Sensing Range and Transmission Range to be fixed at 45 and the density of the nodes is varied for a 2*D*-homogeneous WSNs. The number of nodes activated by its IDS module is determined by varying density of nodes in the given

network. The results show that even if density of nodes in the area increases, the number of nodes selected for intrusion detection remains within a small range. The average number of nodes selected by IDS module considering Sensing Range and Transmission Range is 45 and the density of nodes is varied. Figure 13 shows that initially out of 400 sensors around 180 sensors were selected by the IDS module. Then, gradually there is decrease in number of nodes selected and then remains constant within a small range.

In Figure 14, it is observed that, with increase in Sensing Range the probability of the intruder being detected by a Single Sensor increases and remains constant when the sensing range is around 40meters for a 2*D*-homogeneous WSNs. The simulated values are almost same as the theoretical values. For a 3*D*-homogeneous WSNs, the probability of detecting the intruder is around 0.6 which is more compared to 2*D*-homogeneous WSNs and the probability of detection is one when the sensing range is around 30meters as shown in Figure 15.

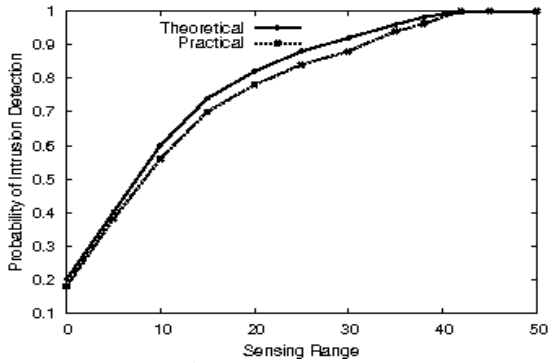

Fig. 14 Probability of Intrusion Detection with increase in Sensing Range for Single Sensor for 2D WSNs.

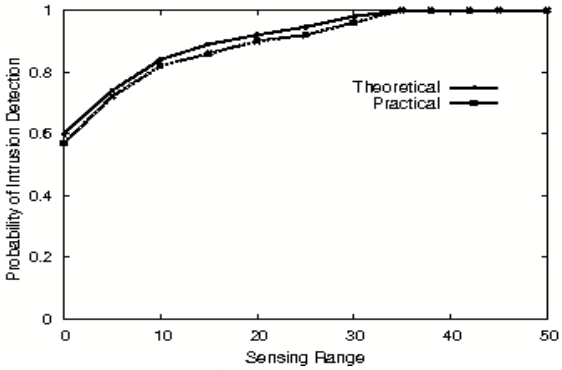

Fig. 15 Probability of Intrusion Detection with increase in Sensing Range for Single Sensor for 3D WSNs.

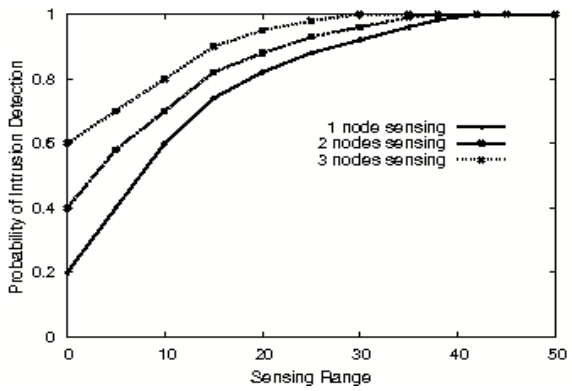

Fig. 16 Probability of Intrusion Detection with increase in Sensing Range for Multiple Sensors for 2D WSNs.

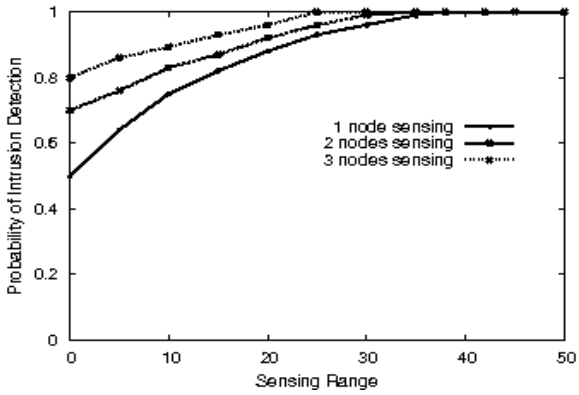

Fig. 17 Probability of Intrusion Detection with increase in Sensing Range for Multiple Sensors for 3D WSNs.

Figure 16 illustrates the effect of the increase in number of sensors to detect the intruder for a 2*D*-homogeneous WSNs. As the number of sensors is increased, the probability of detecting the intruder also increases. At zero, it is 0.2 when one node is sensing and 0.6 for three nodes sensing. The simulation was performed for 100 simulation runs and the numbers of nodes used for detecting the intruder were increased. It showed that a minimum of atleast three sensors is required for better detection and to determine the location of the intruder. Figure 17 indicates that for a 3*D*-homogeneous WSNs, the probability of detection increases with increase in the number of cluster heads sensing the intruder, *i.e.*, for a sensing range of zero the probability of detection is 0.5 for single node sensing, 0.7 for two nodes sensing and 0.8 for three nodes sensing.

Figure 18 and Figure 19 shows that the probability of detection using single-sensor is higher than multi-sensing-detection probability. This is because multi-sensing detection imposes a stricter requirement on detecting the intruder (*e.g.*, atleast three sensors are required). The results illustrate the variation in the sensing range from 0 to 40 by performing 100 simulation runs for a 2*D*-and 3*D*-homogeneous WSNs. It is observed that single sensing is possible even at lower ranges, but sensing range is higher for multi-sensing or it takes some time to get the results. The results prove that atleast three sensors are required to detect the intruder. The values of probability detection are higher for 3D-homogeneous WSNs. The probability of single sensing is around 0.2 and for multi-sensing, it is 0.4, since atleast three nodes will be detecting simultaneously.

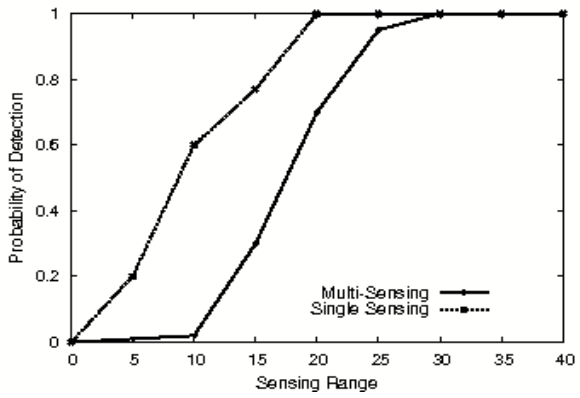

Fig. 18 Sensing Range Vs Probability of Detection for 2D WSNs.

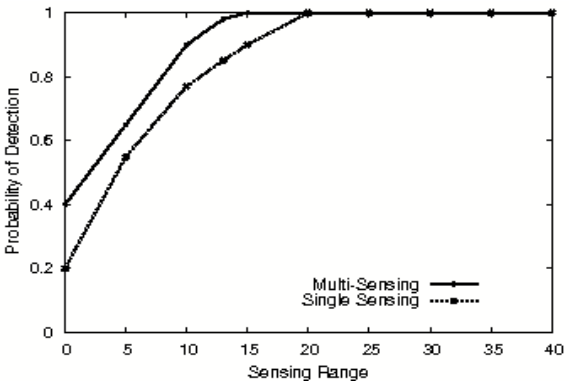

Fig. 19 Sensing Range Vs Probability of Detection for 3D WSNs.

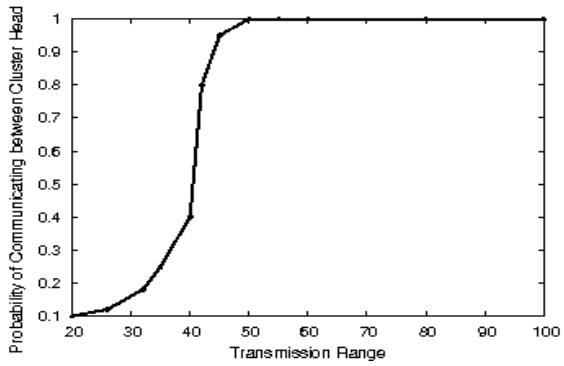

Fig. 20 Communication between Cluster head with respect to Transmission Distance for 2D WSNs.

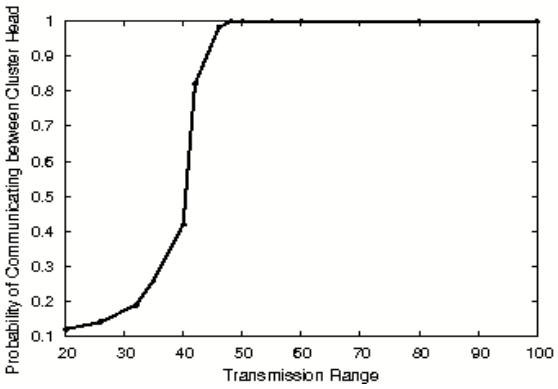

Fig. 21 Communication between Cluster head with respect to Transmission Distance for 3D WSNs.

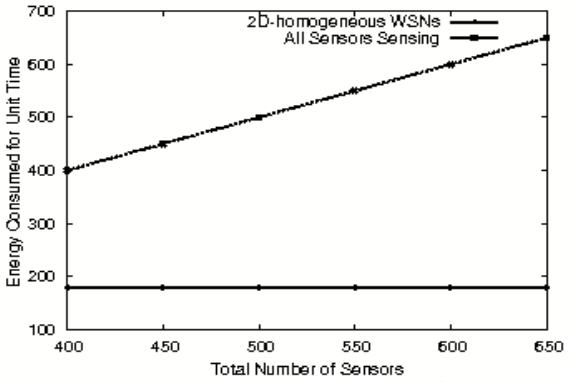

Fig. 22 Energy Consumption Vs. Total Number of Sensors Sensing for 2D WSNs.

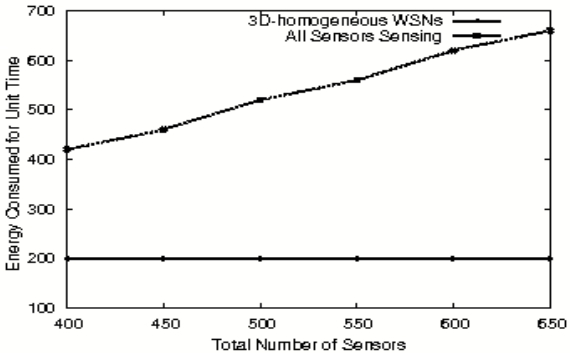

Fig. 23 Energy Consumption Vs. Total Number of Sensors Sensing for 3D WSNs.

The information collected by sensor nodes has to be transmitted to the sink node. Therefore, communication has to be established between cluster heads. To achieve this, there should be sufficient transmission range values. Figure 20 shows that as the transmission range values increases, probability of communication between cluster heads also increases for a 2*D*- homogeneous WSNs. Once it reaches a particular value, say 50meters probability of transmission is same. Even if transmission range is increased it makes no difference in transmission of the information. The communication between cluster heads in a 3*D*-homogeneous WSNs is almost same as 2*D*-homogeneous WSNs as shown in Figure 21. From the results we can observe that the communication between the cluster heads is higher since the number of clusters in a 3*D*-homogeneous WSNs is more. Hence, boundaries of transmission range of the clusters are closer. Figure 22 and Figure 23 analyzes energy consumption for 2*D* and 3*D*-homogeneous WSNs. Energy used by one node for a unit time is assumed as one unit. It is observed that minimum amount of energy is consumed, since all the nodes are not

involved in detecting the intruder. The amount of energy consumed increases slightly for 3*D* homogeneous WSNs than 2*D*-homogeneous WSNs since more nodes are activated for detection. But it is still lower compared to the case when all sensors are sensing the intruder.

X. CONCLUSIONS

In this paper, the internal and external intrusion detection is minimized in an energy efficient way and probability of intrusion detection in a two dimensional and three dimensional spaces. We have developed a probabilistic model for intrusion detection and applied the same into single-sensing detection and multiple-sensing detection scenarios for a 2*D* and 3*D* homogeneous WSNs. This model gives an insight to the required number of sensors in a given deployment area, their sensing and transmission range to securely detect an intruder in WSNs. The correctness of the analytical model is proved by simulation.

Here, only few nodes are activated for intrusion detection at any instant and only the cluster head is used for communication. The remaining nodes are used for other applications or processing. The details of the intruder and its location is encrypted and then transmitted to the sink. Internal IDS detects the selected nodes which transfers data between the nodes. Since the selected nodes activate the IDS for a long time, its energy will be lost resulting in early death of node. So, we randomly redistribute the nodes after certain period of time. The same concept can be extended for Heterogeneous Wireless Sensor Networks.

REFERENCES

[1] Ian F Akyildiz, Weilian Su, YogeshSankarasubramaniam and ErdalCayirci, A Survey on Sensor Networks, *in IEEE Communications Magazine, 40(8),* August 2002, 102-114.

[2] Perrig A, Robert S, J D Tygar, Victor W and David C, SPINS: Security Protocols for Sensor Networks, in Journal on Wireless Networks, *8(5),* September 2002, 521-534.

[3] S Zhu, S Setia and S Jajodia, LEAP: Efficient Security Mechanisms for Large-scale Distributed Sensor Networks, *in Proceedings of the 10th ACM Conference on Computer and Communications Security (CCS '03)*, October 2003, 62-72.

[4] Yang Xia Luo and Ye Guo, A Survey on Intrusion Detection of Wireless Sensor Network, *in Proceedings of the Second International Conference on Information Science and Engineering(ICISE),* 2010, 1798-1802.

[5] William Stallings, Cryptography and Network Security, *in 3rd Edition,* (Singapore: Prentice Hall, Pearson Education, 2004).

[6] SutharshanRajasegarar, Christopher Leckie and MarimuthuPalaniswami, Anomaly Detection in Wireless Sensor Networks, *in IEEE Wireless Communications*, 2008, 34-40.

[7] Yun Wang, Xiaodong Wang, Bin Xie, Demin Wang and Dharma P Agrawal, Intrusion Detection in Homogeneous and Heterogeneous Wireless Sensor Networks, *in IEEE Transactions on Mobile Computing*, 7(6), 2008, 698-711.

[8] Olivier Dousse, Christina Tavoularis and Patrick Thiran, Delay of Intrusion Detection in Wireless Sensor Networks, *in Proceedings of the Seventh ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)*, 2006, 155-165.

[9] KrontirisIoannis and TassosDimitriou, Towards Intrusion Detection in Wireless Sensor Networks, in Proceedings of The 13th European *Wireless Conference*, 2007.

[10] IoannisKrontiris, ZinaidaBenenson and ThanassisGiannetsos, Cooperative Intrusion Detection in Wireless Sensor Networks, *in Proceedings of The Sixth European Conference on Wireless Sensor Networks(EWSN'09), LNCS*, 2009, pp. 263-278.

[11] AshfaqHussainFarooqi and FarrukhAslam Khan, A Survey of Intrusion Detection Systems for Wireless Sensor Networks, *in International Journal of Ad Hoc and Ubiquitous Computing, 9(2),*2012 , 69-83.

[12] AndriyStetsko, Lukas Folkman and VashekMatyas, Neighbor-based Intrusion Detection for Wireless Sensor Networks, *in Proceedings of Sixth International Conference on Wireless and Mobile Communications,* 420-425, 2010.

[13] Qi Wang, Shu Wang and ZhonglouMeng, Applying an Intrusion Detection Algorithm to Wireless Sensor Networks, *in Proceedings of Second International Workshop on Knowledge Discovery and Data Mining,* 284-287, 2009.

[14] P Brutch and C Ko, Challenges in Intrusion Detection for Wireless Ad-hoc Networks, *in Proceedings of 2003 Symposium on Applications and the Internet Workshops (SAINT'03 Workshops),* 2003, 368-373.

[15] Benyuan Liu, Peter Brass, Olivier Dousse, Philippe Nain and Don Towsley, Mobility Improves Coverage of Sensor Networks, *in Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc),* 2005, 300-308.

[16] Yun Wang, Yoon KahLeow and Jun Yin, Is Straight-line Path Always the Best for Intrusion Detection in Wireless Sensor Networks, *in Proceedings of The 15th International Conference on Parallel and Distributed Systems,* 2009, 564-571.

[17] Xi Peng, Zheng Wu, Debao Xiao and Yang Yu, Study on Security Management Architecture for Sensor Network based on Intrusion Detection, *in Proceedings of 2009 International Conference on Networks Security, Wireless Communications and Trusted Computing, 2009, 503-507.*

[18] Xing Zhang, Jingsha He and Qian Wei, Key Management Integrated with Intrusion Detection in Wireless Sensor Networks, *in Proceedings of The IEEE International Conference on fjfjd, 2009,* 1-1.

[19] SudipMisra, P Venkata Krishna and Kiran Isaac Abraham, Energy Efficient Learning Solution for Intrusion Detection in Wireless Sensor Networks, *in Proceedings of The International Conference on Communication Systems and Networks(COMSNETS),* 2010, 1-6.

[20] PiyaTechateerawat and Andrew Jennings, Adaptive Intrusion Detection in Wireless Sensor Networks, *in Proceedings of the International Conference on Intelligent Pervasive Computing*, 2007, 23-28.

[21] H T Kung and D Vlah, Efficient Location Tracking Using Sensor Networks, *in Proceedings of the IEEE Conference on Wireless Communication and Networking(WCNC'03),* 2003, 1954-1961.

[22] Tao Liu, Zhishu Li, Feng Yin and Jun Yang, Applying General Sensing Mode to Intrusion Detection in Wireless Sensor Networks, *in Proceedings of Fifth International Conference on Wireless Communications, Networking and Mobile Computing*, 2009, 3314-3317.

[23] Rodrigo Roman, Jianying Zhou and Javier Lopez, Applying Intrusion Detection Systems to Wireless Sensor Networks, *in Proceedings of IEEE Conference on Consumer Communication and Networking(CCNC 2006),* 2006, 640-644.

[24] Bo Sun, Lawrence Osborne, Yang Xiao and SghaierGuizani, Intrusion Detection Techniques in Mobile Ad Hoc and Wireless Sensor Networks, *in IEEE Wireless Communications,* October 2007, 56-63.

[25] Tran Hoang Hai and Eui-Nam Huh, Optimal Selection and Activation of Intrusion Detection Agents for Wireless Sensor Networks, *in Future Generation Communication and Networking(FGCN 2007), 1(2),* 200, 350-355.

[26] Leonardo Mostarda and Alfredo Navarra, Distributed Intrusion Detection Systems for Enhancing Security in Mobile Wireless Sensor Networks, *in International Journal of Distributed Sensor Networks, vol. 4*, 2008, pp. 83-109.
[27] Yun Wang and ZhendongLun, Impact of Deployment Point Arrangement on Intrusion Detection in Wireless Sensor Networks, *in Proceedings of the 18th Annual IEEE/ACM International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems*, 2010, 421-423.
[28] Shaila K, Sajitha M, Tejaswi V, S H Manjula, Venugopal K R and L M Patnaik, SEEDI: Secure and Energy Efficient Approach for Detection of an Intruder in Homogeneous Wireless Sensor Networks, *in Proceedings of the International Conference on Intelligent Network and Computing (ICINC-2010)*, 2010, 279-283.
[29] Li-Liann Lu, Jean-Lien C Wu and San-Hao Chen, A Cluster based Algorithm for Redundant Nodes Discovery in Dense Sensor Networks, *in International Journal on Sensor Network, Inderscience Publication, 10(1/2)*, 2011, 59-72.
[30] K Q Yan, S C Wang, S S Wang and C W Liu, Hybrid Intrusion Detection System for Enhancing the Security of a Cluster-based Wireless Sensor Network, *in Proceedings of The Third IEEE International Conference on Computer Science and Information Technology(ICCSIT)*, 2010, 114-118.
[31] Shio Kumar Singh, M P Singh and D K Singh, Intrusion Detection Based Security Solution for Cluster-Based Wireless Sensor Networks, *in International Journal of Advanced Science and Technology, vol. 30*, 2011, 83-95.
[32] OuadoudiZytoune, Mohamed El Aroussi and DrissAboutajdine, An Energy Efficient Clustering Protocol for Routing in Wireless Sensor Networks, *in International Journal on Ad Hoc and Ubiquitous Computing, Inderscience Publications, 7(1)*, 2011, pp. 54-59.