JOURNAL OF INFORMATION, KNOWLEDGE AND RESEARCH IN ELECTRONICS AND COMMUNICATION

PROBABILITY OF INTRUSION DETECTION IN WIRELESS SENSOR NETWORKS

[1]NISHA GAHLAWAT, [2] PRADEEP KUMAR

[1]Department of Electronics & Communication, DCRUST Murthal, IGI Jhunndpur Sonipat,
[2]Assistant Professor Department of Electronics & Communication Engineering, IGI Jhundpur,Sonipat

[1]nishu.gahlawat@gmail.com, [2]montu.antil@gmail.com

ABSTRACT: *Intrusion detection in Wireless Sensor Networks have become increasing in many application areas such as military, medical, environment monitoring etc. Intrusion detection system provides a mechanism by which we detect inappropriate and incorrect attackers in WSNs. In this paper we present mathematical relationship between WSN parameters and probability of intrusion detection in WSNs. In this paper we derive detection probability of intrusion for homogeneous and heterogeneous networks. And discuss network connectivity and broadcast reachability which is necessary for communication between nodes. Our simulation results validate the mathematical values.*

KEYWORDS: *Wireless Sensor Networks (WSNs), sensing range, node density, Transmission range, Intrusion Distance (D), Homogeneous WSNs, Heterogeneous WSNs.*

1. INTRODUCTION

A WSN is a network of devices, which consist number of sensor nodes. Each sensor node sense the environment (e.g. humidity, pressure, temperature) and communicate the information gathered from the monitored field (e.g. an area or volume) through wireless link. The communication range of sensor nodes is limited to tens of meters, so data are sent hop-by-hop from one sensor node to another until they reach the base station. WSNs are used in many applications where the sensors have physical interactions with the environment and are accessible by anyone make them more vulnerable to security threats. The limitation of WSNs is memory, energy and other resources make the use of existing security techniques infeasible. So we need another defence mechanism "An Intrusion detection system" that can protect the network from attackers. The intrusion detection concerns how fast the intruder can be detected when it enters the network. There are some probabilities of intrusion detection such as; an intruder can be detected as soon as it enters in the network domain or when it covers some distance in the network domain. One policy is, if all sensors deployed with high density so that sensing range covers the entire area and intruder can be detected immediately when it enter the network or area. But high density deployment policy increases the network investment or may be difficult for large areas. Instead, some applications required that intruder can be detected within a specified intrusion distance after entering the network. Detection probability is defined as the probability that an object is detected in certain observation duration. Probability of intrusion detection heavily depends on the intrusion distance (D) [5]. Intrusion distance can be defined as the distance between the point where the intruder enters the network and the point whereit gets detected by a sensor.

Some parameters that influence the probability of intrusion detection are:-

Node density: - It is defined as the total number of nodes present in the network [2].

Transmission range: - The maximum distance up to which a node can transmit is called transmission range [2].

Sensing range: - The distance up to which a sensor can detect the presence of intruder is called its sensing range [2].

1.1 TYPES OF WSNs

There are two types of Wireless Sensor Networks

1.1.1 Homogeneous WSNs:-

In homogeneous WSNs (Fig.1) all the sensors have same sensing range, transmission range, battery energy [3].

1.1.2 Heterogeneous WSNs:-

A heterogeneous WSNs (Fig. 2) consists different sensor nodes. In this network some sensors have larger sensing range,

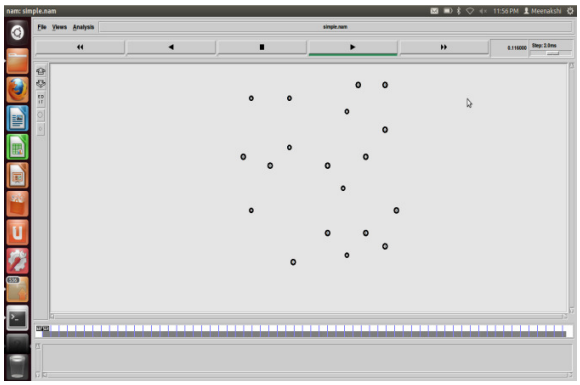

Fig.1:- Homogeneous WSN

transmission range and have more battery energy. Heterogeneous WSNs have comparatively difficult network connectivity because of asymmetrical wireless links. As packets from high capability nodes may reach the low capability nodes but low capability nodes may not be able to transmit information to high capability nodes [3].

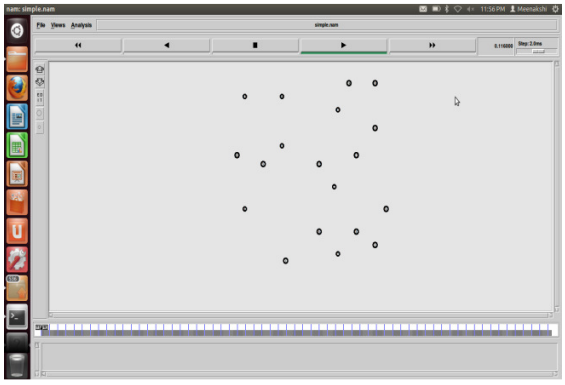

Fig.2:- Heterogeneous WSN

1.2 Types of Sensing Models

We consider two types of sensing models.

1.2.1. Single sensing detection model:-

In single-sensing detection model an intruder is detected by a single sensor. But in some cases the information provided by singe sensor may not be correct as it can sense only a portion of the network domain. In that case we use multi-sensing detection model.

1.2.2. Multiple sensing detection models:-

In multi-sensing detection model an intruder is detected by multiple sensors. For example at least three sensors are required to determine the location of intruder.

2. RELATED WORKS

There exist several security techniques in WSNs. Intrusion detection system is one of the most important tool in WSNs.

X. Wang et al., analyses the intrusion detection problem in WSNs by characterizing the relationship between the intrusion distance, the node density and the sensing range. They also extend heterogeneous sensor networks by introducing more powerful sensor nodes that can decreases the possible intrusion distance [2].

PiyaTechateerawat et al., provides a new dynamic adaptive threshold scheme for intrusion detection. They offer linear scalability with cluster size [1].

K Suresh et al., considered this issue according to heterogeneous WSNs models. Furthermore, they considered two sensing detection models: single-sensing detection and multiple-sensing detection. Their simulation results shows the advantage of multiple sensor heterogeneous WSNs [5].

K Shaila et al., have proposed an algorithm Secure and Energy Efficient Approach for Detection of Intruder (SEEDI) in homogeneous Wireless Sensor Networks. Single sensing and Multi-sensing intruder detection are considered in their algorithm. Simulation results showed that the proposed algorithm resulted in better performance [6].

Michael Riecker et al. introduced decentralized algorithms for detecting abnormal data in wireless sensor networks. They tested the algorithms on a real dataset with four kinds of data attacks and compared them to two centralized state-of-the-art classification algorithms. They show that the decentralized

algorithms do not perform as well as the algorithms employing supervised learning, but they are light weight and can be run directly on the nodes [4].

Liu et al. have explored the effects of sensor mobility on sensing coverage and detection capability in mobile WSNs. It is demonstrated that sensor mobility can improve the sensing coverage of the network, and provide fast detection of targeted events [7].

Yun Wang et al analyses the intrusion detection problem in both homogeneous and heterogeneous WSNs by taking intrusion detection probability with respect to the intrusion distance and the network parameters [3].

3. Intrusion Detection Model

In our model we consider a square WSN in two dimensional (2D) planes with area (Lx L) as shown in Fig.3. All the sensors are uniformly distributed in the area. The intrusion distance is denoted by *D*. We find out the detection probability with respect to network parameters: node density, sensing range, and transmission range. We consider two types of WSNs. In homogeneous WSNs, all sensors have same sensing range denoted as r_s and have same transmission range denoted as r_x. The node density is denoted as λ. In heterogeneous WSNs, there are two types of sensors:

Type 1 sensor with larger sensing range r_{s1} and longer transmission range r_{x1} .The node density is denoted as λ_1.

- Type 2 sensors with smaller sensing ranger_{s2}andshorter transmission range r_{x2} .The node density isλ_2.

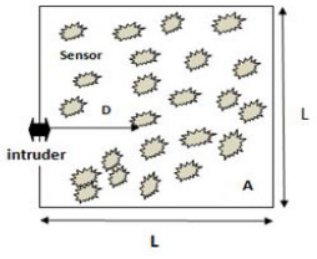

Fig. 3:- Intrusion detection Model

4. Probability of Intrusion Detection in Homogeneous WSEs

In this section, we present the detection probability for homogeneous WSNs. Detection probability is derived for single sensing model and *k*-sensing model.

4.1. Single Sensing Detection Model

In single sensing detection model, the intruder can be detected once when it enters the sensing coverage of a sensor. There are two cases:

1. When intruder enters the network from any point of the network boundary: When intruder enters the network from boundary and the intrusion distance D ≥ 0 as shown in Fig.4. Then corresponding intrusion detection area S_D includes a rectangular area with length *D* and width $2r_s$ and a half disk with radius r_s.

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

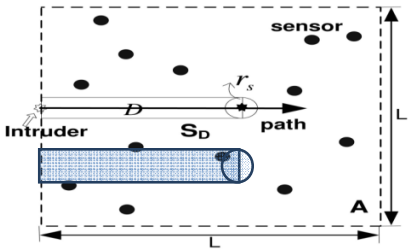

Fig.4:- The intruder starts from the boundary of the WSN

2. When intruder enters the network from a random point: When intruder enters the network from a random point as shown in Fig.5. Then corresponding intrusion detection area is

$$S_D = 2 * D * r_s + \pi * r_s^2 \quad (2)$$

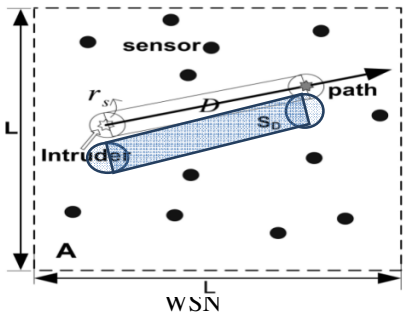

Fig.5:- of the WSN

We first consider the detection probability that the intruder can be immediately detected once it enters the network domain from a random point. In other words, it has an intrusion Distance $D = 0$. The corresponding intrusion detection area $S_D = \pi r_s^2$. We then have Theorem 1 as follows:

Theorem1. The probability p1 [D = 0] that an intruder can be immediately detected once it enters a homogeneous WSN with node density λ and identical sensing range r_S can be given by

$$p1[D = 0] = 1 - e^{-\lambda\pi r_s^2} \quad (3)$$

Proof. In uniformly distributed WSNs with nodedensity λ, the probability of *m* sensors located within the area S follows the Poisson distribution:

$$p(m, S) = \frac{(S\lambda)}{m!} e^{-S\lambda} \quad (4)$$

Therefore, the probability of no sensor in the immediate intrusion detection area $S_0 = \pi r_s^2$is$p(0, \pi r_s^2) = e^{-\lambda\pi r_s^2}$. Then, the complement of $p(0, \pi r_s^2)$is the probability that there is at least one sensor located in$S_0=\pi r_s^2$. In this case, the intruder can be detected once it approaches then et work with intrusion distance D = 0. Thus, the probability that the intruder can be detected immediately by the WSN once it enters the WSN is p_1[D = 0] =1- $p(0, \pi r_s^2) = 1 - e^{-\lambda^{\pi r_s^2}}$.This result shows that the immediate detection probability p_1[D = 0] is determined by the node density and the sensing range. By increasing the node density or enlarging the sensing range, p_1[D=0] can be improved. Immediate detection may need a large sensing range or a high node density, thus increasing the WSN deployment cost. We then consider the detection probability in a relaxed condition when the intruder is allowed to travel some distance in the WSN.

Theorem2. Suppose ξ is the maximal intrusion distance allowable for a given application. The probability p_1[D ≤ ξ]that the intruder can be detected within ξ in the given homogeneous WSN can be derived as

$$p1[D \le \xi] = 1 - e^{-\lambda(2\xi r_s + \pi r_s^2)} \quad (5)$$

Proof. According to the definition of single-sensing detection model, the probability that the intruder can be detected within an intrusion distance of ξ is equivalent to the probability that there is at least one sensor located in the corresponding intrusion detection area$S_\xi=2\xi r_s + \pi r_s^2$ That is, $p1[D \le \xi] = 1 - \mathrm{p}(0, S_\xi)$ while p(0,S_ξ)is obtained from (4). The probability p1[D ≤ ξ] can further be represented as$p1[D \le \xi] = 1 - \mathrm{p}(0, S_\xi) = 1 - e^{-\lambda(2\xi r_s + \pi r_s^2)}$.Then, yields $p1[D \le \xi]$=1 − $e^{-\lambda(2\xi r_s + \pi r_s^2)}$.

4.2 Multiple Sensing Detection Model

In the multiple sensing detection models, an intruder has to be sensed by at least k sensors for intrusion detection in a WSN. The number of required sensors depends on specific applications.

Theorem3. Let p_k [D = 0]be the probability that an intruder is detected immediately once it enters a WSN with node density λ and sensing ranger $_s$in k-sensing detection model. It has

$$p_k[D = 0] = 1 - \sum_{i=0}^{k-1} \frac{(\pi r_s^2 \lambda)^i}{2^i i!} e^{-\pi r_s^2 \lambda} \quad (6)$$

Proof. According to (4), $p(i, \pi r_s^2)$ is the probability thatthere are *i* sensors located in the immediate detection area$S_0 = \pi r_s^2$. $\sum_{i=0}^{k-1} p(i, \pi r_s^2)$is therefore the probability that there are less than *k* sensors in the area S0. Further, 1 - $\sum_{i=0}^{k-1} p(i, \pi r_s^2)$ represents the probability that there are at least *k* sensors located in the area S0. In this case, the intruder can be sensed by at least *k* sensors when it accesses the network boundary. Consequently, it can be said that$p_k[D = 0] = 1 - \sum_{i=0}^{k-1} p(i, \pi r_s^2) = 1 - \sum_{i=0}^{k-1} \frac{(\pi r_s^2 \lambda)^i}{2^i i!} e^{-\pi r_s^2 \lambda}$is the probability of the intruder tobe detected immediately when it enters the WSN domain under k-sensing detection scenarios.

Theorem4. Letp_k[D ≤ ξ] be the probability that the intruder is detected within the maximal intrusion distance ξ in a k-sensing detection model for the given homogeneous WSNs. Then, p_k[D ≤ ξ] can be calculated as

$$p_k[D \le \xi] = 1 - \sum_{i=0}^{k-1} \frac{(S_\xi \lambda)^i}{i!} e^{-\lambda S_\xi} \quad (7)$$

Where $S_\xi = 2\xi r_s + \pi r_s^2$.

Proof. $S_\xi = 2\xi r_s + \pi r_s^2$ is the intrusion detection area with respect to the maximal intrusion distance ξ. If there are at least *k* sensors in the area S_ξ, the intruder can be sensed by the *k* sensors, and the *k* sensors could collaborate with each other to recognize the intruder. From (4), $p(i, S_\xi) = \frac{(S_\xi \lambda)^i}{i!} e^{-\lambda S_\xi}$ denotes the probability that *i* sensors are located in the area of S_ξ. Then, $\sum_{i=0}^{k-1} p(i, S_\xi) = \sum_{i=0}^{k-1} \frac{(S_\xi \lambda)^i}{i!} e^{-\lambda S_\xi}$ is the probability that less than *k* sensors are located in the area S_ξ. Thus, the complement of $\sum_{i=0}^{k-1} p(i, S_\xi)$, $1 - \sum_{i=0}^{k-1} \frac{(S_\xi \lambda)^i}{i!} e^{-\lambda S_\xi}$ is the probability that there are at least *k* sensors located in the area S_ξ. If this is the case, the intruder can be sensed by at least k sensors from the WSN with probability $1 - \sum_{i=0}^{k-1} \frac{(S_\xi \lambda)^i}{i!} e^{-\lambda S_\xi}$ before it travels a distance of ξ. Finally, the probability $p_k[D \le \xi]$ that the intruder is detected within the maximal intrusion distance ξ in *k* sensing detection model can be derived as $p_k[D \le \xi] = 1 - \sum_{i=0}^{k-1} \frac{(S_\xi \lambda)^i}{i!} e^{-\lambda S_\xi}$.

5. Probability of Intrusion Detection in Heterogeneous WSNs

In this section, we present the detection probability for heterogeneous WSNs. Detection probability is derived for single sensing model and *k*-sensing model. We consider two types of sensors: Type 1 and Type 2 with the node density of λ_1 and λ_2 respectively. Type 1 sensor has the sensing range r_{s1}, and the sensing range is a disk of area $S_1 = \pi r_{s1}^2$ as shown in Fig. 6. Type 2 sensor has the sensing coverage of $S_2 = \pi r_{s2}^2$ with the sensing range r_{s2}.

5.1 Single Sensing Detection Model

We denote the intrusion distance by D_h in the given heterogeneous WSN. Again, an intruder may be detected by the WSN once it approaches the network and the corresponding intrusion distance is $D_h = 0$. This leads to the following theorem.

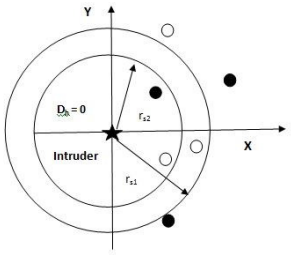

Fig.6:- Sensing range in heterogeneous WSN

Theorem5. The probability p_1 [D_h= 0]that an intruder can be immediately detected once it enters the given heterogeneous WSN in a single-sensing detection model can be represented by

$$p_1[D_h = 0] = 1 - e^{-\lambda_1 \pi r_{s1}^2} e^{-\lambda_2 \pi r_{s2}^2} \quad . \quad (8)$$

Proof. According to the single-sensing detection model, the intruder is detected if and only if one of the following conditions is satisfied:

- The intruder enters into the sensing coverage area of any Type 1 sensor(s).
- The intruder enters into the sensing coverage area of any Type 2 sensor(s).

If a Type 1 sensor is located inside the disk $S_1 = \pi r_{s1}^2$ which is cantered at the point (0, 0) with radius r_{s1}, the first condition holds. Similarly, the second condition holds if there is a Type 2 sensor inside the disk $S_2 = \pi r_{s2}^2$ which is cantered at the point (0, 0) with radius r_{s2}. Then from (4), the probability that no Type 1 sensor lies inside S_1 is $p_1(0, S_1) = e^{-\lambda_1 S_1} = e^{-\lambda_1 \pi r_{s1}^2}$, and the probability of no Type 2 sensor inside S_2 is $p_2(0, S_2) = e^{-\lambda_2 S_2} = e^{-\pi r_{s2}^2 \lambda_2}$. Considering Type 1 and Type 2, sensors are independently deployed according to our heterogeneous WSNs model, the probability of neither Type 1 sensor nor Type 2 sensor that senses the intruder is $p_1(0, S_1) p_2(0, S_2) = e^{-\pi r_{s1}^2 \lambda_1} e^{-\pi r_{s2}^2 \lambda_2}$. Thus, the probability of at least one sensor (either Type1 or Type 2) around the boundary that can sense the intruder is $1 - p_1(0, S_1) p_2(0, S_2) = 1 - e^{-\pi r_{s1}^2 \lambda_1} e^{-\pi r_{s2}^2 \lambda_2}$. Therefore, the probability that the intruder is detected immediately once it enters the

network domain can be represented as p_1 [D_h= 0] $=1-e^{-\pi r_{s1}^2\lambda_1}e^{-\pi r_{s2}^2\lambda_2}$

Theorem6. Suppose ξ is the maximal intrusion distance allowable for the intruder to travel within the given heterogeneous WSNs in single-sensing detection. The probability $p_1[D_h \le \xi]$that the intrusion distance $D_h$isless than ξ can be calculated as

$$p_1[D_h \le \xi] = 1 - e^{-\lambda_1 S_1'}e^{-\lambda_2 S_2'} \quad (9)$$

Where $S_i' = 2\xi r_{si} + \pi r_{si}^2$, (i =1, 2).

Proof. The probability of an intruder to be detected within the maximal intrusion distance ξ is equivalent to the probability of at least one sensor (either Type 1 or Type 2) inside the corresponding intrusion detection areaS_ξ' . For Type 1 sensors, the intrusion detection areaS_1' is the region that includes a rectangular area with length ξ and width $2r_{s1}$. It gives$S_1' = 2\xi r_{s1} + \pi r_{s1}^2$. Similarly, the intrusion detection area for Type 2 sensors is $S_2' = 2\xi r_{s2} + \pi r_{s2}^2$. Then, we obtain the maximal intrusion detection area with respect to ξ as$S_\xi' = S_1' \cup S_2'$.The intruder can be detected within the intrusion distance ξ if one of the following conditions is satisfied:

- At least one Type 1 sensor is located in the area ofS_1'.
- If condition 1 does not hold, at least one Type 2 sensors located in the area of S_2'.

Note that $p_1(0, S_1') = e^{-\lambda_1 S_1'}$is the probability of no Type 1 sensor in the area ofS_1', and$p_2(0, S_2') = e^{-\lambda_2 S_2'}$ is the probability of no Type 2 sensor in the area ofS_2'. The first condition can be satisfied with the probability of$1 - p_1(0, S_1')$, and the second condition holds with the probability of$p_1(0, S_1')\big(1 - p_2(0, S_2')\big)$. . Thus, $1 - p_1(0, S_1') + p_1(0, S_1')\big(1 - p_2(0, S_2')\big) = 1 - p_1(0, S_1')p_2(0, S_2')$represents the probability of at least one sensor (either Type 1 or Type 2) that can detect the intruder within the maximal intrusion detection areaS_ξ'. Finally, the probability that the intrusion distance$D_h$is less than ξ can be derived as$p_1[D_h \le \xi] = 1 - p_1(0, S_1')p_2(0, S_2') = 1 - e^{-\lambda_1 S_1'}e^{-\lambda_2 S_2'}$.

5.2 Multiple Sensing Detection Model

In the multi-sensing detection model of heterogeneous WSNs with two types of sensors, at least *k* sensors are required to detect an intruder. These *k* sensors can be any combination of Type 1 and Type 2 sensors. For instance, if three sensors are required to detect an intruder for a specific application, the intruder can be detected by any of the following sensor combinations:

1. Three Type 1 sensor,
2. Three Type 2 sensors,
3. One Type 1 sensor and two Type 2 sensors, and
4. Two Type 1 sensors and one Type 2 sensor.

Theorem7. Let p_k [D_h= 0] be the probability that an intruder can be immediately detected once it enters the given heterogeneous WSNs in the k-sensing detection model. It has

$$p_k[D_h = 0] = 1 - \sum_{m=0}^{k-1}[\sum_{j=0}^{m} p_1(j, \pi r_{s1}^2)p_2(m - j, \pi) \quad (10)$$

Proof. According to *k*-sensing detection model, an intruder is detected immediately once it enters the network if and only if at least *k* sensors are located within their sensing disk centred at the intrusion stating point. Based on (4), $p_1(j, S_1) = \frac{(S_1\lambda)^j}{j!}e^{-\lambda S_1}$is the probability of*j* Type1 sensors that can sense the intruder within the corresponding intrusion detection area $S_1 = \pi r_{s1}^2$,and$p_2(m - j, S_2) = \frac{(S_2\lambda)^{m-j}}{(m-j)!}e^{-\lambda S_2}$is probability of (*m-j*)Type 2 sensors that can sense the intruder within the area of$S_2 = r_{s2}^2$ .Consequently,$p_1(j, S_1)p_2(m - j, S_2)$represents the probability of *m* sensors (*j* Type 1 sensors plus *m-j* Type 2 sensors) that can sense the intruder at the start point. Since these *m* sensors can be any combination of sensor types,$\sum_{j=0}^{m} p_1\ (j, S_1)p_2(m - j, S_2)$ is the probability that there are totally *m* sensors that can sense the intruder in the intrusion detection area of $S_1 \cup S_2$.Therefore,$\sum_{m=0}^{k-1}[\sum_{j=0}^{m} p_1(j, S_1)p_2(m - j, S_2)]$ is the probability of at most *k-1* (less than k) sensors that can sense the intruder when it approaches the WSNs. Finally, the probability that the intruder can be immediately detected once it enters the heterogeneous WSN in the *k* sensing detection model

is equivalent to the complement of $\sum_{m=0}^{k-1}[\sum_{j=0}^{m} p_1(j,S_1)p_2(m-j,S_2)]$, yielding

$$p_k[D_h = 0] = 1 - \sum_{m=0}^{k-1}[\sum_{j=0}^{m} p_1(j,S_1)p_2(m-j,S_2)].$$

$1 - \sum_{m=0}^{k-1}[\sum_{j=0}^{m} p_1(j,\frac{\pi r_{s1}^2}{2})p_2(m-j,\frac{\pi r_{s2}^2}{2})]$.

Theorem8. Let $p_k[D_h \le \xi]$be the probability that the intrusion distance is less than ξ ($\xi > 0$)in the k-sensing detection model, ξ is the maximal intrusion distanceallowable for an intruder to move in the given heterogeneous WSN. It has

$p_k[D_h \le \xi] = 1 - \sum_{m=0}^{k-1}[\sum_{j=0}^{m} p_1(j,S_1')p_2(m-j,S_2')]$.

Where $S_i' = 2\xi r_{si} + \pi r_{si}^2$, (i =1, 2). (11)

Proof. From (4), $p_1(j,S_1')$is the probability that *j* Type 1 sensors are located in the intrusion detection area$S_1' = 2\xi r_{s1} + \pi r_{s1}^2$.$p_2(m-j,S_2')$is the probability of that (*m-j*)Type 2 sensors located in the corresponding intrusion detection area $S_2'$and $S_2' = 2\xi r_{s2} + \pi r_{s1}^2$. Then,$p_1(j,S_1')p_2(m-j,S_2')$represents the probability of *m* sensors, consisting of *j* Type 1 sensors and (*m-j*)Type 2sensors can sense the intruder within the intrusion detection area$S_1' \cup S_2'$ with respect to ξ. If *m=k*,$p_1(j,S_1')p_2(m-j,S_2')$stands for the probability that the intruder can be detected by the WSN within intrusion distance ξ. Since these *m* sensors can be any combination of sensor types,$[p_1(j,S_1')p_2(m-j,S_2')]$ is the probability that there are totally *m* sensors can sense the intruder. The $[p_1(j,S_1')p_2(m-j,S_2')]$ is the probability that there are at most *k-1* (i.e., less than *k*) sensors that can sense the intrusion detection area $S_1' \cup S_2'$.

6. Network Connectivity and Broadcast Reachability

After sensing or detecting the intrusion, it is necessary to provide communication between nodes and reporting to the base station. If there is no connectivity between nodes, it is meaningless either the sensor detect the intruder or not. There are two types of communication possible.

6.1. Network Connectivity

In network connectivity a packet transmitted from any sensor can reach all the other sensors in the network.

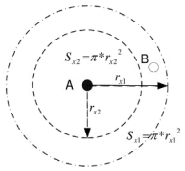

Fig.7:- Transmission range in heterogeneous WSN

Theorem9. Consider a heterogeneous WSN consisting of independently deployed Type I and Type II sensors with node densities λ_1 and λ_2 and transmission range r_{x1} and r_{x2} ($r_{x1} > r_{x2}$), respectively. The upper bound of the network connectivity is

$$P_{con}^{N} = [1 - e^{-(\lambda_1+\lambda_2)\pi r_x^2}]^N \quad (12)$$

Proof. As illustrated in Fig. 9. If there is one Type 1 sensor (e.g., B) located in the area of $S_{x1} = \pi r_{x1}^2$while outside of the area$S_{x2} = \pi r_{x2}^2$, a packet generated from sensor A may not be able to reach sensor B. This is because sensor B may be out of sensor A's transmission range if sensor A is a Type2 sensor with transmission range r_{x2}, and $r_{x2} < r_{x1}$. In view of this, for a packet generated from sensor A to be received by all the other sensors in WSN, at least one sensorshould lie in the area of the smaller transmission range S_{x2}. Further, if all thesensors have at least one neighbour in the relatively smaller transmission rangeS_{x2}, the network is connected.
Assuming all the other N-1 sensors except A are connected, with probability $1 - p(0,S_{x2}) = 1 - e^{-(\lambda_1+\lambda_2)\pi r_x^2}]$, there is at least one sensor located in thesmaller transmission range S_{x2}. Then, sensor A can broadcast itspacket to at least one of the other N-1 sensors, and the packet can further be broadcasted to all the sensors in the network. Thus, we obtain the conditional probability$P_{con}^{A} = 1 - e^{-(\lambda_1+\lambda_2)\pi r_x^2}$. Due to the fact that sensor A is chosen arbitrarily and the statistical independence for all the sensors, the probability that the other N-1 sensors are connected can be calculated as$P_{con}^{N-1} = [1 - e^{-(\lambda_1+\lambda_2)\pi r_x^2}]^{N-1}$. Finally, the upper bound of the network connectivity

can be derived as $P_{con}^{N} = P_{con}^{A} * P_{con}^{N-1} = [1 - e^{-(\lambda_1+\lambda_2)\pi r_x^2}]^N$

6.2 Broadcast Reachability

In broadcast reach ability a packet transmitted from any Type1 sensor can reach all the other sensors.

Theorem10. Consider a heterogeneous WSN consisting of independently deployed Type1 and Type2 sensors, with node densities λ_1 and λ_2 and transmission range $r_{x1}$and r_{x2}(r_{x1}>r_{x2}), respectively. The upper bound of the network broadcast reachability is

$$P_{br}^{N} = [1 - e^{-\lambda_1\pi r_{x1}^2} e^{-\lambda_2\pi r_{x2}^2}]^N \quad (13)$$

Proof. As illustrated in Fig. 9, $A \in N$ is anarbitrary sensor in the WSN. It has the responsibility to receive the packet broadcasting from any Type 1sensor(s). In order for A to receive the packet, it has to be in the transmission range of at least one of the other N-1 sensors. In other words, sensor A should not be isolated from the rest of the network, and at least one sensor can reach A in its transmission range. The probability of no Type1 sensor in its transmission range from A is $P_1(0, \pi r_{x1}^2) = e^{-\lambda_1\pi r_{x1}^2}$. The probability that notype 2 sensor lies in its transmission range from A is $P_2(0, \pi r_{x2}^2) = e^{-\lambda_1\pi r_{x2}^2}$. Then,$P_1(0, \pi r_{x1}^2)P_2(0, \pi r_{x2}^2) = e^{-\lambda_1\pi r_{x1}^2} e^{-\lambda_1\pi r_{x2}^2}$ is the probability that neither Type 1sensors nor Type 2 sensors can reach sensor A. Therefore, the probability that at least one sensor can reach A is $1 - e^{-\lambda_1\pi r_{x1}^2} e^{-\lambda_1\pi r_{x2}^2}$. Due to statistical independence among all sensors, the probability that the other N-1sensors are reachable from the broadcast can be calculated as $P_{br}^{N-1} = [1 - e^{-\lambda_1\pi r_{x1}^2} e^{-\lambda_2\pi r_{x2}^2}]^{N-1}$.consequently, we obtain the upper bound of broadcast reachability as $P_{br}^{N} = [1 - e^{-\lambda_1\pi r_{x1}^2} e^{-\lambda_2\pi r_{x2}^2}]^N$.

6. Simulation and Results

In this section, analytical results are verified by the network simulation tool.

Figure.8 shows the graph between detection probability and number of nodes for both homo and hetero network. In this graph the red line shows the

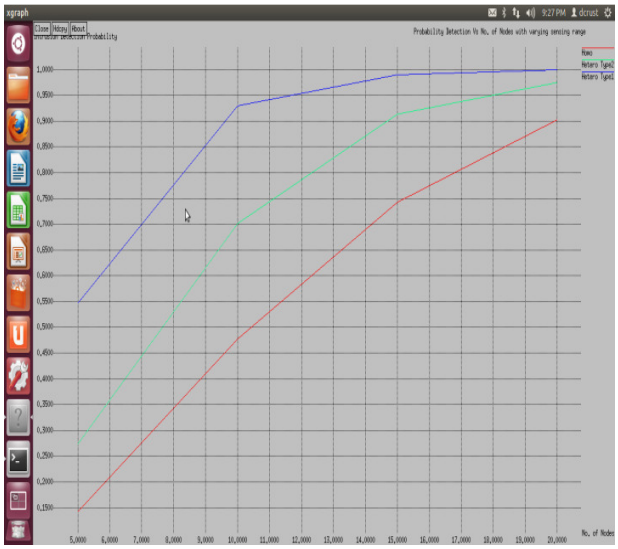

Fig.8 Graph between detection probability and number of nodes with varying sensing range.

detection probability for homogeneous WSN and green line is for type2 heterogeneous nodes with sensing range 10 m and blue line is for type1 heterogeneous nodes with sensing range 15 m. As shown in figure as the no. of nodes is increasing from 5 to 20 detection probability is also increasing.

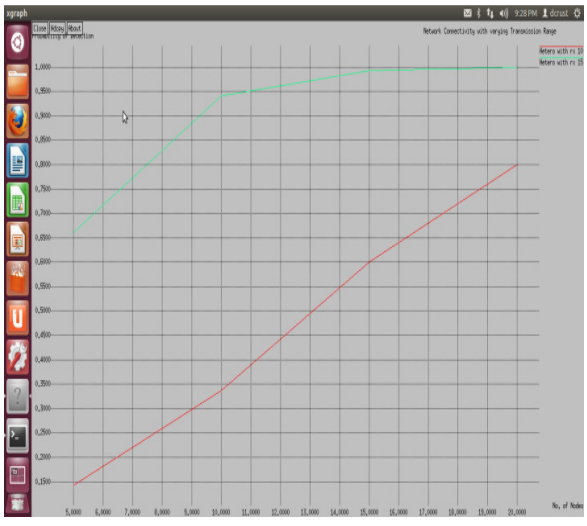

Fig.9 Graph of Network connectivity with varying transmission range.

Figure.9 shows the graph of network connectivity between no. of nodes and probability of connection with varying transmission range. Red line shows the

probability of connection with transmission range 10m. And Green line shows the probability of connection with transmission range 15m. Figure.10 shows the graph of broadcast reachability

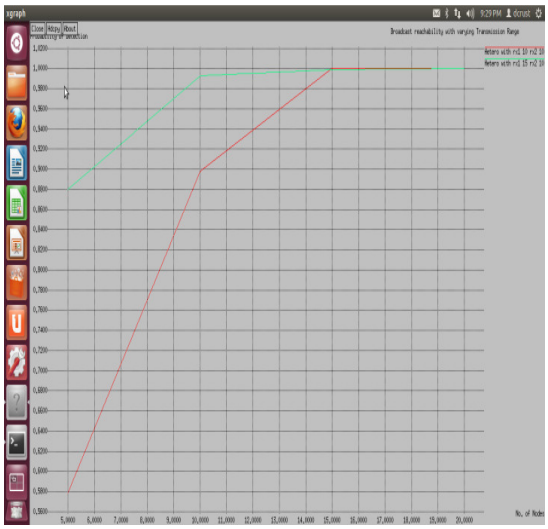

Fig.10 Graph of Broadcast Reachability with varying transmission range.

between no. of nodes and probability of broadcast with varying transmission range. Red line shows the probability of broadcast with transmission range 10m. Green line shows the probability of broadcast with transmission range 15m.

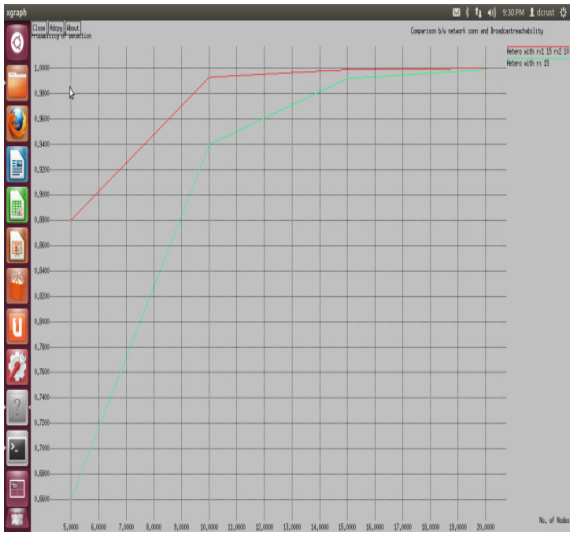

Fig.11 Comparison between Network Connectivity and Broadcast Reachability.

7. Conclusion

The result shows that detection probability increases with increasing networks parameters such as node density, sensing range. And heterogeneous network gives better detection probability as compare to homogeneous network. Network connectivity and Broadcast reachability increases with increasing transmission range and with node density. Broadcast reachability gives better probability than network connectivity. This result helps in selecting networks parameters to meet desired application requirement.

REFERENCES

[1] PiyaTechateerawat, Andrew Jennings, Adaptive Intrusion Detection in Wireless Sensor Networks.Proc. IEEE Conf. on Intelligent Pervasive Computing,0-7695-3006-0/07, DOI 10.1109/IPC.2007.34

[2] Xiaodong Wang, YounghwanYoo, Yun Wang and Dharma P. Agrawal, Impact of Node Density and Sensing Range on Intrusion Detection in Wireless Sensor Networks. 1-4244-0572-6/06, 2006 IEEE.

[3] Yun Wang, Xiaodong Wang, Bin Xie, Demin Wang and Dharma P. Agrawal, Intrusion Detection in Homogeneous and Heterogeneous Wireless Sensor Networks. IEEE Transactions on Mobile Computing, VOL. 7, NO. 6, June 2008, 1536-1233/08.

[4] Michael Riecker, Ana Barroso, Matthias Hollick, On Data-centric Intrusion Detection in Wireless Sensor Networks. IEEE Conf. on Green Computing and Communications, Conf. on Internet of Things, Conf. on Cyber, Physical and Social Computing, 978-0-7695-4865-4/12.GreenCom.2012.

[5] K.Suresh, A.Sarala Devi, Jammi Ashok,A NovelApproach Based Wireless Intrusion Detection System.Proc. of the International Journal of Computer Science and Information Technologies, Vol. 3 (4), 2012,4666 – 4669.

[6] K. Shaila, M. Sajitha, V. Tejaswi, S. H. Manjula, K.R. Venugopal, and L. M. Patnaik, Secure andEnergy Efficient Approach for Detection of anIntruder in Homogeneous Wireless Sensor Networks, International Journal of Computer Theory and Engineering,Vol. 4, No. 6, December 2012.

[7] B. Liu, P. Brass, O. Dousse, P. Nain, and D. Towsley,Mobility improves coverage of sensor networks. Proc. of The Sixth ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc), 2005.

[8] Y. Zhang and W. Lee,Intrusion detection in wireless ad-hoc networks.Proc. of ACM MobiCom, 2000, pp. 275-283.

[9] 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.