International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org, editorijettcs@gmail.com
Volume 2, Issue 3, May – June 2013 ISSN 2278-6856

Intrusion Detection in Homogeneous and Heterogeneous Wireless Sensor Networks

Sandhya Kaushik[1] , Dr. Suresh Kumar[2]

[1]M. Tech. – Student-U.I.E.T., M.D.U. Rohtak,
[2]Assistant Professor, U.I.E.T., M.D.U. Rohtak

ABSTRACT: ***WSNs have become increasing one of the most promising and interesting area over the past few years. The various potential applications in WSNs dictate that they should be secure. Intrusion detection is a mechanism to detect inappropriate and incorrect attackers in WSNs. In this paper we present a mathematical analytical model to find the probability of intrusion detection in homogeneous as well as heterogeneous WSNs. In this paper we have considered two sensing model: single- sensing detection model and multi-sensing detection model. Finally the simulation results verify the mathematical analysis.***

KEYWORDS: Wireless sensor networks (WSNs), Homogeneous WSNs, Heterogeneous WSNs, node density, Intrusion distance (ID).

1 INTRODUCTION

A WSN is a highly distributed network of wireless devices known as sensor nodes. Each sensor node monitors some physical phenomenon's (e.g., humidity, temperature, pressure, light) inside the area of deployment [1]. The monitored information is sent to base station through wireless links. 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 limitations of WSNs in 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 [2]. There are some probabilities of intrusion detection 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. 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 [5]. Intrusion distance denoted as D can be defined as the distance between the point where the intruder enters the network and

the point where it 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.

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

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

We consider these three parameters in our model.

Depending on sensors capability there are two types of WSNs:-

1.1 Homogeneous WSNs

In homogeneous WSNs (Fig.1) all the sensors have same capabilities. They all have same battery energy, hardware complexity sensing range, and transmission range [3]. Homogeneous WSNs have simple network connectivity because of symmetrical wireless link.

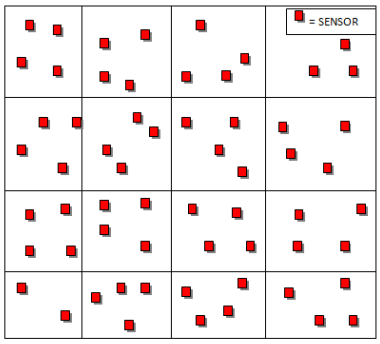

Fig 1 Homogeneous WSN

1.1 Heterogeneous WSNs

A heterogeneous WSNs (Fig. 2) consists different sensor nodes. In heterogeneous WSNs some sensors have larger capabilities than other sensors. In this network some sensors have larger sensing range, transmission range and have more battery power. Heterogeneous WSNs are most suitable for real life applications as compared to homogeneous. In heterogeneous WSNs a large no. of inexpensive nodes perform sensing, while a few nodes having comparatively more energy perform other tasks as data filtering, transport. 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. In real world the assumption of homogeneous sensors may not be practical because sensing application may require heterogeneous nodes in terms of sensing and communication capabilities in order to enhance network [4].

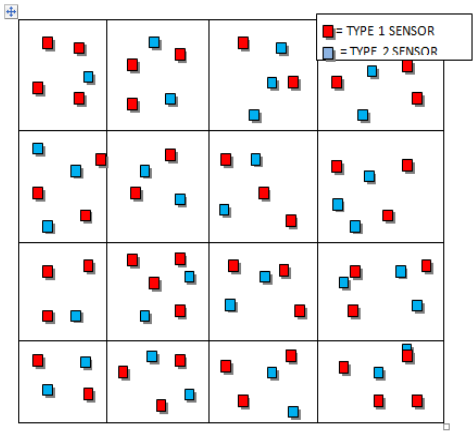

Fig 2 Heterogeneous WSN

We consider two sensing models:-

1.2 Single-sensing detection model

In single-sensing detection model an intruder is successfully detected by 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.

1.3 Multi-sensing detection model

In multi-sensing system an intruder is detected by multiple collaborating sensors. The no. of sensors depends upon specific applications. For example at least sensors are required to determine the location of intruder.

The rest of the paper is organised as follows: in section 2 we describe the related work in this field. In section 3 we present our intrusion detection model. In section 4 we present analytical model for homogeneous WSNs. In section 5 the same is done for heterogeneous WSNs. In section 6 the simulation results verify the mathematical analysis. And finally we conclude our paper in section 7.

2 RELATED WORK

There exist several security techniques in WSNs. Intrusion detection system is one of the most important tool in WSNs. Many solutions have been proposed in traditional networks but they cannot be applied directly to WSNs because of restricted resources.

Zhang et al., studied the problem of intrusion detection in Wireless Ad-hoc Networks. They have proposed architecture for distributed and cooperative intrusion detection system for Ad-hoc Networks, which was based on statistical anomaly detection techniques which requires much time to detect intrusion in data and during traffic [6].

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

Wang et al. have provided a unifying approach in relating the intrusion detection probability with respect to the intrusion distance and the network parameters (i.e., node density, sensing range and transmission range), under single-sensing detection and multiple-sensing detection models, in both homogeneous and heterogeneous WSNs [8].

Xi Peng et al proposed a security management model for self organizing wireless sensor networks based on intrusion detection. It can prevent most of attacks. Then an analysis of each layer of networks in security model is discussed and the security management measures in the data link layer and network layer are described in detail especially. Such a structure is built based on the existing encryption and authentication protocols [9].

Byunggil Lee et al., have developed management platform and security framework for WSNs. The proposed framework has advantages as regard secure association and intrusion detection. This also provides the background a wsn, its security issues and requirements [10].

Qi Wang et al., have developed a intruder detection algorithm of low complexity for static wireless sensor network. The intrusion detection model includes characteristics that determine the average frequency of execution of order. A distributed algorithm in which the sensor collects the information from the neighbouring nodes to analyses the anomalies if any from the neighbours. The intrusion detection algorithm on detecting anomalies packets received from its neighbours basic alarms to report the anomaly [11].

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 [12].

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 [6].

3 OUR INTRUSION DETECTION MODEL

In our intrusion detection model we consider a square WSN in two dimensional (2D) plane with area ($L \times L$). The intrusion distance is denoted as D (Fig. 3). All the sensors are uniformly distributed in the deployment area. We find out the detection probability by considering three network parameters: node density, sensing range, and transmission range. We consider two types of WSNs. In homogeneous WSNs all the sensors have same sensing range denoted as r_s , and have same transmission range denoted as r_t. The node density is denoted as λ. In heterogeneous WSNs we have two types of sensors:

- Type 1 sensors with larger sensing range r_{s1} and longer transmission range r_{t1}.The node density is denoted as λ_1.

• Type 2 sensors with smaller sensing range $r_{s2}$and shorter transmission range r_{t2}.The node density is denoted as λ_2.

We consider two sensing models: in single-sensing model the intruder can be detected by single sensor and in multi-sensor model we consider at least *k* sensors to detect the intruder.

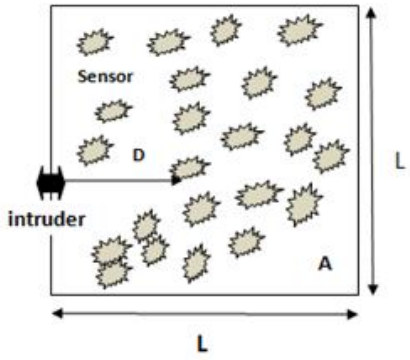

Fig. 3 Intrusion detection model

4 DETECTION PROBABILITY IN HOMOGENEOUS WSNs

In this section we derive the intrusion detection probability for homogeneous WSNs. we present the analysis in single sensing and multi sensing detection model.

4.1 SINGLE- SENSING DETECTION MODEL

In the single-sensing detection model, the intruder can be recognized once it moves into the sensing coverage disk of any sensor. We consider two cases:-

CASE I

Intruder may access the network domain from any point in the network boundary:-

When the intruder starts from a point of the network boundary (Figure 7) given an intrusion distance D ≥ 0, the corresponding intrusion detection area S_D is almost an oblong area. This area includes a rectangular area with length D and width 2rs and a half disk with radius r_s attached to it. It has

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

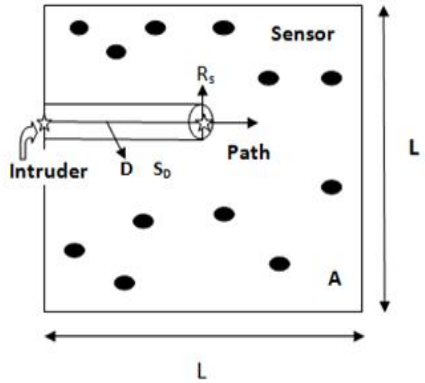

Fig. 4 Intruder enters from boundary

CASE II

Intruder may access the network from a random point in the network domain (Fig. 5) for example, the intruder can be dropped from the air and starts from any point in the network domain:-

When the intruder starts from a random point in the network domain, corresponding intrusion detection area is

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

In the following analysis we focus on when the intruder starts from random point in the network domain.

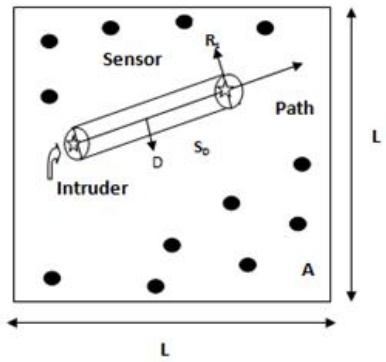

Fig. 5 Intruder enters from random point

We first consider the detection probability that the intruder can be immediately detected once it enters the network domain. In other words, it has an intrusion Distance D = 0. The corresponding intrusion detection area $S_0 = \pi r_s^2$. We then have Theorem 1 as follows:

Theorem1. The probability $p_1[D=0]$ 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

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

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

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

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 the network with intrusion distance D = 0. Thus, the probability that the intruder can be detected immediately by the WSNs once it enters the WSN is given by $p_1[D = 0] = 1 - P(0,\pi r_s^2) = 1 - e^{\lambda \pi r_s^2}$,

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 WSNs 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 $p_1[D \le \xi]$ that the intruder can be detected within ξ in the given homogeneous WSN can be derived as

$$p_1[D \le \xi] = 1 - e^{-\lambda(2\xi r_s + \pi r_s^2)} \quad (5)$$

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,$p_1[D \le \xi] = 1 - P(0, S_\xi)$ while $P(0, S_\xi)$ is obtained from(4) . The probability,$p_1[D \le \xi]$ can further be represented as,
$p_1[D \le \xi] = 1 - P(0, S_\xi) = 1 - e^{-\lambda(2\xi r_s + \pi r_s^2)}$.
Then it yields, $p_1[D \le \xi] = 1 - e^{-\lambda(2\xi r_s + \pi r_s^2)}$.

Theorem3. Let $p_1[D = \zeta]$ be the probability that the intruder is detected at an intrusion distance ζ, ζ > 0 and $E_1(D)$ be the average intrusion distance. Then,

$$p_1[D = \zeta] = 2\lambda r_s e^{-\lambda(2\zeta r_s + \pi r_s^2)} \text{ and}$$

$$E_1(D) = \int_0^{\sqrt{2L}} 2\zeta\lambda r_s e^{-\lambda(2\zeta r_s + \pi r_s^2)} d(\zeta). \quad (6)$$

Proof. In Theorem 2 gives the cumulative density function (CDF) of intrusion distance such as$p_1[D \le \zeta]$. Therefore, $p_1[D = \zeta]$ can be obtained from the differential of, $p_1[D \le \zeta]$ and it can be calculated as
$p_1[D = \zeta] = \frac{d(p_1[D \le \zeta])}{d(\zeta)} = 2\lambda r_s e^{-\lambda(2\zeta r_s + \pi r_s^2)}$.
The average intrusion distance $E_1(D)$ can be easily derived from the PDF of the intrusion distance (i.e. $p_1[D = \zeta]$). Since the intruder is assumed to
move in the network along a straight path, and the network domain is a square area with size A = L * L, the maximum distance the intruder may travel is$\sqrt{2L}$.
Then, the average intrusion distance is given as
$E_1(D) = \int_0^{\sqrt{2L}} p_1[D = \zeta] d(\zeta)$
$= \int_0^{\sqrt{2L}} 2\zeta\lambda r_s e^{-\lambda(2\zeta r_s + \pi r_s^2)} d(\zeta)$.
Theorems 1-3 indicate that the quality of intrusion detection in single-sensing detection scenario for a given WSN improves as the sensing range or the node density increases.

4.2 MULTI-SENSING DETECTION MODEL

In the multi - sensing detection model, an intruder has to be sensed
by at least *k* sensors for intrusion detection in a WSNs. The number of required sensors depends on specific applications.

Theorem4. 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 range r_s in k-sensing detection model. It has

$$p_k[D=0] = 1 - \sum_{i=0}^{k-1} \frac{(\pi r_s^2\lambda)^i}{i!} e^{-\pi r_s^2\lambda} \quad (7)$$

Proof. According to (3),$P(i, \pi r_s^2)$ is the probability that there 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 S_0. 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 S_0. 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 $p_k[D=0] = 1 - \sum_{i=0}^{k-1} P(i, \pi r_s^2) = 1 - \sum_{i=0}^{k-1} \frac{(\pi r_s^2\lambda)^i}{i!} e^{-\pi r_s^2\lambda}$ is the probability of the intruder to be detected immediately when it enters the WSN domain under *k*-sensing detection scenarios.

Theorem5. Let $p_k[D \le \xi]$ 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, $p_k[D \le \xi]$ can be calculated as

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

$$S_\xi = 2\xi r_s + \pi r_s^2 \quad (8)$$

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), $P(i, S_\xi) = \frac{(S_\xi\lambda)^i}{i!} e^{-S_\xi\lambda}$ denotes the probability that *i* sensors are located in the area of S_ξ. Then,$\sum_{i=0}^{k-1} P(i, S_\xi) = \sum_{i=0}^{k-1} \frac{(S_\xi\lambda)^i}{i!} e^{-S_\xi\lambda}$ is the probability that less than *k* sensors are located in the area S_ξ . Thus, the complement of $\sum_{i=0}^{k-1} P(i, S_\xi) = 1 - \sum_{i=0}^{k-1} \frac{(S_\xi\lambda)^i}{i!} e^{-S_\xi\lambda}$ 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 $1-\sum_{i=0}^{k-1}\frac{(S_\xi\lambda)^i}{i!}e^{-S_\xi\lambda}$ 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 $p_k[D \le \xi] = 1-\sum_{i=0}^{k-1}\frac{(S_\xi\lambda)^i}{i!}e^{-S_\xi\lambda}$.

Theorem 6. Let $E_k(D)$ be the average intrusion distance in the *k*-sensing detection model for the given WSN with node density λ and sensing range r_s, it has

$$E_k(D) = \frac{k\sum_{i=0}^{k-1}(\pi r_s^2\lambda)^i e^{-\pi r_s^2\lambda}}{2r_s\lambda i!} \qquad (9)$$

Proof. $E_k(D)$ is the average intrusion distance. Then, $\overline{S_k} = E_k(D) * 2r_s$ is the average intrusion detection area, and $\lambda * E_k(D) * 2r_s$ is the average number of sensors located in the area of $\overline{S_k}$. Based on the definition of *k*-sensing detection model, *k* sensors are required to identify the intruder. Thus, the average number of sensors located in the average intrusion detection area should be equal to *k*, that is, $\lambda * E_k(D) * 2r_s = k$. Considering the case when the intruder is detected immediately once it enters the WSN domain, the average intrusion distance is $E_k(D) = 0$, while $\lambda * E_k(D) * 2r_s = 0$. In this case, $\lambda * E_k(D) * 2r_s = k$ does not hold. Thus, it is necessary to eliminate this boundary effect, and we get $\lambda * E_k(D) * 2r_s = k(1 - p_k[D=0])$. By replacing $p_k[D=0]$ by (7) following Theorem 4, we further obtain

$\lambda * E_k(D) * 2r_s =$
$k\sum_{i=0}^{k-1}P(i,\pi r_s^2) = k\sum_{i=0}^{k-1}(\pi r_s^2,\lambda)^i e^{-\pi r_s^2\lambda}$
.

Finally, the average intrusion distance in the *k*-sensing detection model for
the given WSN can be calculated as

$$E_k(D) = \frac{k\sum_{i=0}^{k-1}(\pi r_s^2\lambda)^i e^{-\pi r_s^2\lambda}}{2r_s\lambda i!}$$

Theorems 4-6 show that the quality of intrusion detection in the *k*-sensing detection scenario for a given WSNs improves as the sensing range and node density increase and decreases as *k* grows.

5 DETECTION PROBABILITY IN HETEROGENEOUS WSNs

In this section, we present the analysis of intrusion detection probability of a heterogeneous WSNs in single sensing detection and multiple-sensing detection models. We consider two types of sensors: Type 1 and Type 2 with the node density of λ_1 and λ_2, respectively. A Type 1 sensor has the sensing range r_{s1}, and the sensing coverage is a disk of area $S_1 = \pi r_{s1}^2$.(Fig. 6) A Type 2 sensor has the sensing coverage of $S_2 = \pi r_{s2}^2$ with the sensing range r_{s2}. Without loss of generality, we can assume that $r_{s1} > r_{s2}$ in our network model. In a heterogeneous WSN, any point in the network domain is said to be covered if the point is under the sensing range of any sensor (Type 1, Type 2 , or both).

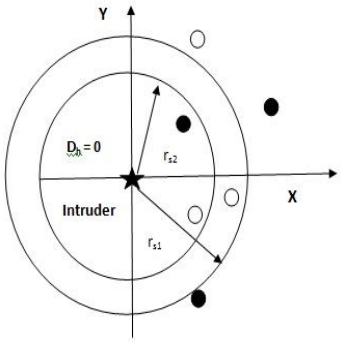

Fig. 6 Node range in heterogeneous WSN

5.1 SINGLE-SENSING DETECTION MODEL

We denote the intrusion distance by D_h in the given heterogeneous WSNs. 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.

Theorem7. 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

$$p_1[D_h = 0] = 1 - e^{-\lambda_1\pi r_{s1}^2}e^{-\lambda_2\pi r_{s2}^2} \qquad (10)$$

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 centered 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 centered at the point (0, 0) with radius r_{s2}. Then from (4), the probability that no Type 1 sensor lies inside S_1 is $P_1(0,S_1) = e^{-\lambda_1\pi r_{s1}^2}$, and the probability of no Type 2 sensor inside S_2 is $P_2(0,S_2) = e^{-\lambda_2\pi r_{s2}^2}$. 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 $P_1(0,S_1)P_2(0,S_2) = 1 - e^{-\lambda_1\pi r_{s1}^2}e^{-\lambda_2\pi r_{s2}^2}$. Thus, the probability of at least one sensor (either Type I or Type II) around the boundary that can sense the intruder is

$1 - P_1(0, S_1)P_2(0, S_2) = 1 - e^{-\lambda_1 \pi r_{s1}^2} e^{-\lambda_2 \pi r_{s2}^2}$. Therefore, the probability that the intruder is detected immediately once it enters the network domain can be represented as

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

Theorem8. 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 is less than ξ can be calculated as

$p_1[D_h \le \xi] = 1 - e^{-\lambda_1 s_1'} e^{-\lambda_2 s_2'}$

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

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 area S_ξ' . For Type 1 sensors, the intrusion detection area S_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 of S_1'.
- If condition 1 does not hold, at least one Type 2 sensor is located in the area of S_2'.

Note that is the probability $P_1(0, S_1') = e^{-\lambda_1 s_1'}$ of no Type 1 sensor in the area of S_1' , and $P_2(0, S_2') = e^{-\lambda_2 s_2'}$ is the probability of no Type 2 sensor in the area of S_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 $P_1(0, S_1')(1 - P_2(0, S_2'))$. Thus, $1 - P_1(0, S_1') + P_1(0, S_1')(1 - P_2(0, S_2')) = 1 - P_1(0, S_1')P_2(0, S_2')$ represents the probability of at least one sensor (either Type 1 or Type 2) that can detect the intruder within the maximal intrusion detection area S_ξ' . Finally, the probability that the intrusion distance D_h is less than ξ can be derived as $p_1[D_h \le \xi] = 1 - e^{-\lambda_1 s_1'} e^{-\lambda_2 s_2'}$.

Theorem9. The probability $p_1[D_h = \zeta]$ that the intruder is detected at an intrusion distance ζ (ζ>0) when it travels within the given heterogeneous WSN in single-sensing detection can be derived as

$p_1[D_h = \zeta] = 2(\lambda_1 r_{s1} + \lambda_2 r_{s2}) e^{-(\lambda_1 s_1' + \lambda_2 s_2')}$

$S_i' = 2\zeta r_{si} + \pi r_{si}^2$ (i=1,2) (12)

Proof. Equation (11) gives the CDF of intrusion distance in a single-sensing detection scheme. Therefore, the probability $p_1[D_h = \zeta]$ that the intruder is detected at an intrusion distance ζ can be derived by the differential of $p_1[D_h \le \zeta]$. It has $p_1[D_h = \zeta] = \frac{d(p_1[D_h \le \zeta])}{d(\zeta)} = 2(\lambda_1 r_{s1} + \lambda_2 r_{s2}) e^{-(\lambda_1 s_1' + \lambda_2 s_2')}$ .Then, based on the PDF of an intrusion detection distance such as $p_1[D_h = \zeta]$, it is easy to obtain the expected intrusion distance as

$$E_1(D_h) = \int_0^{\sqrt{2}L} 2(\lambda_1 r_{s1} + \lambda_2 r_{s2}) e^{-(\lambda_1 s_1' + \lambda_2 s_2')} d(\zeta)$$

: This is because the maximum intrusion distance that the intruder could travel in the square network domain is $\sqrt{2}L$ by following a straight path.

Theorems 7-9 indicate that the quality of intrusion detection in single-sensing detection scenario for a given heterogeneous WSN increases with the increasing of sensing range and node density. In addition, the existence of high-capability sensors improves the network detection probability further due to a larger sensing range.

5.2 MULTI- SENSING DETECTION MODEL

In the multi-sensing detection model of a 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 sensors,
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.

Theorem 10. 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

$p_k[D_h = 0] = 1 - \sum_{m=0}^{k-1}[\sum_{j=0}^{m} P_1(j, \pi r_{s1}^2) P_2(m - j, \pi r_{s2}^2)]$ (13)

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), $P_1(j, S_1) = \frac{(S_1\lambda_1)^j}{j!} e^{-S_1\lambda}$ is the probability of *j* Type I sensors that can sense the intruder within the corresponding intrusion detection area $S_1 = \pi r_{s1}^2$ and $P_1(m - j, S_2) = \frac{(S_2\lambda)^{m-j}}{(m-j)!} e^{-S_2\lambda}$ probability of *m-j* Type II sensors that can sense the intruder within the area of $S_2 = \pi r_{s2}^2$. Consequently, $P_1(j, S_1)P_1(m - j, S_2)$ represents the probability of *m* sensors (*j* Type I sensors plus *m-j* Type II sensors) that can sense the intruder at the start point. Since these *m* sensors can be any combination of sensor types $\sum_{j=0}^{m} P_1(j, S_1)P_1(m - j, S_2)$ 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, $\sum_{m=0}^{k-1}[\sum_{j=0}^{m} P_1(j, \pi r_{s1}^2) P_2(m - j, \pi r_{s2}^2)]$ 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 $\sum_{m=0}^{k-1}[\sum_{j=0}^{m} P_1(j,\pi r_{s1}^2)P_2(m-j,\pi r_{s2}^2)]$, yielding

$p_k[D_h = 0] = 1 - \sum_{m=0}^{k-1}[\sum_{j=0}^{m} P_1(j,\pi r_{s1}^2)P_2(m-j,\pi r_{s2}^2)]$

.

Theorem 11. Let $p_k[D_h \le \xi]$ be the probability that the intrusion distance is less than $\xi(\xi > 0)$ in the *k*-sensing detection model, ξ is the maximal intrusion distance allowable for an intruder to move in the given heterogeneous WSN. It has

$$p_k[D_h \le \xi] = 1 - \sum_{m=0}^{k-1}[\sum_{j=0}^{m} P_1(j,S_1')P_2(m-j,S_2')$$

$S_i' = 2\xi r_{si} + \pi r_{si}^2$ (i=1,2) (14)

Proof. From (4), $P_1(j,S_1')$ is the probability that *j* Type I 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 II sensors located in the corresponding intrusion detection area $S_2' = 2\xi r_{s2} + \pi r_{s2}^2$. Then, $P_1(j,S_1')P_2(m-j,S_2')$ represents the probability of *m* sensors, consisting of *j* Type I sensors and *m-j* Type II sensors 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 . Since these *m* sensors can be any combination of sensor types, $\sum_{j=0}^{m} P_1(j,S_1')P_1(m-j,S_2')$ is the probability that there are totally *m* sensors can sense the intruder. The $\sum_{m=0}^{k-1}[\sum_{j=0}^{m} P_1(j,S_1')P_2(m-j,S_2')$ is the probability that there are at most *k-1* (i.e., less than *k*) sensors that can sense the intruder within the intrusion detection area $S_i' \cup S_j'$.

Theorem 12. Let $E_K(D_h)$ be the average intrusion distance under the *k*-sensing detection model in the given heterogeneous WSNs. Then

$$E_K(D_h) = \frac{k\sum_{m=0}^{k-1}[\sum_{j=0}^{m} P_1(j,\pi r_{s1}^2)P_2(m-j,\pi r_{s2}^2)]}{2r_{s1}\lambda_1 + 2r_{s2}\lambda_2} \quad (15)$$

Proof. $E_K(D_h)$ is the average intrusion distance in the heterogeneous WSNs. Then, the corresponding average intrusion detection areas for Type 1 and Type 2 sensors are, $\bar{S_1} = 2r_{s1}E_K(D_h)$ and $\bar{S_2} = 2r_{s2}E_K(D_h)$, respectively. While the node densities of Type 1 and Type 2 sensors are λ_1 and λ_2. The average number of Type 1 sensors that with the intruder during its invasion is $N_1 = \lambda_1\bar{S_1}$. At the same time, the average number of Type 2 sensors that hit the intruder in its intrusion is $N_2 = \lambda_2\bar{S_2}$. In the *k*-sensing detection model, *k* sensors are required to detect the intruder, it has $N_1 + N_2 = \lambda_1\bar{S_1} + \lambda_2\bar{S_2} = 2r_{s1}E_K(D_h)\lambda_1 + 2r_{s2}E_K(D_h)\lambda_2$. The only exception is $2r_{s1}E_K(D_h)\lambda_1 + 2r_{s2}E_K(D_h)\lambda_2 = 0$ while $E_K(D_h) = 0$ in the case of immediate intrusion detection. In view of this, we eliminate this boundary effect (i.e., $E_K(D_h) = 0$) and obtain $k(1 - p_k[D_h = 0]) = 2r_{s1}E_K(D_h)\lambda_1 + 2r_{s2}E_K(D_h)\lambda_2$. Substituting $p_k[D_h = 0]$ with (12), we further obtain $\sum_{m=0}^{k-1}[\sum_{j=0}^{m} P_1(j,\pi r_{s1}^2)P_2(m-j,\pi r_{s2}^2)]$.

Theorems 10-12 indicates that the quality of intrusion detection in the *k*-sensing detection scenario for a given heterogeneous WSN improves with the increase in the sensing range and the node density and decreases as *k* grows. In addition, the existence of high-capability sensors further improves the network detection quality due to the enlarged sensing coverage.

6 SIMULATION AND RESULTS

In this section theoretical results are verified by using simulation tool. In this work ns2 is used for simulation and verification. The work is done on both homogeneous as well as heterogeneous WSNs.

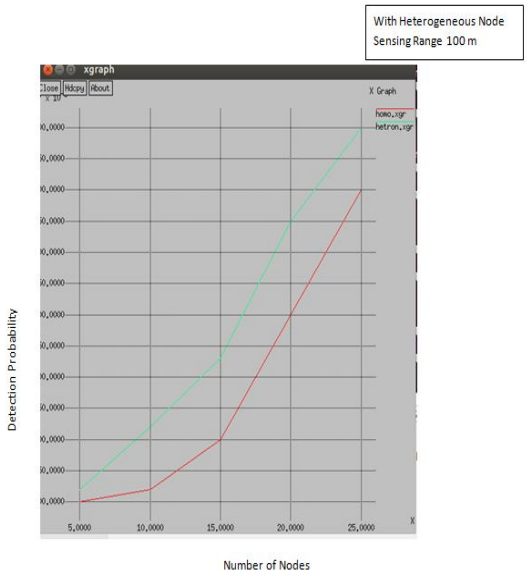

Fig 7 Graph between detection probability and no. of nodes with sensing range 100 m.

(Figure 7) shows the graph between detection probability and number of nodes for both homo and hetero network. In this graph the red line shows the detection probability for homogeneous WSN and green line is for heterogeneous WSNs. In this type1 heterogeneous nodes are considered with sensing range 100 m. As shown in figure as the no. of nodes are increasing from 5 to 25 detection probability is also increasing.

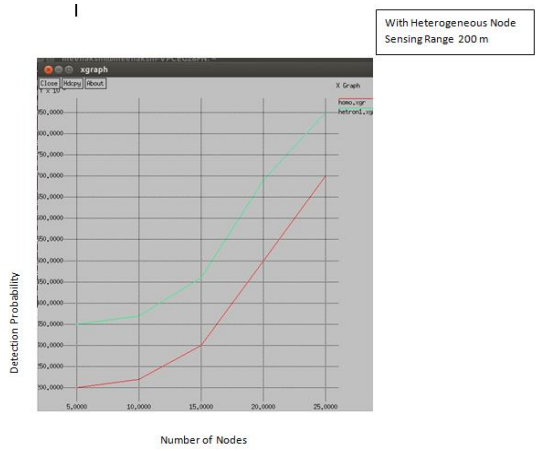

Fig 8 Graph between detection probability and no. of nodes with sensing range 200 m.

(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 detection probability for homogeneous WSN and green line is for heterogeneous WSNs. In this type2 heterogeneous nodes are considered with sensing range 200 m. As shown in figure as the no. of nodes are increasing from 5 to 25 detection probability is also increasing.

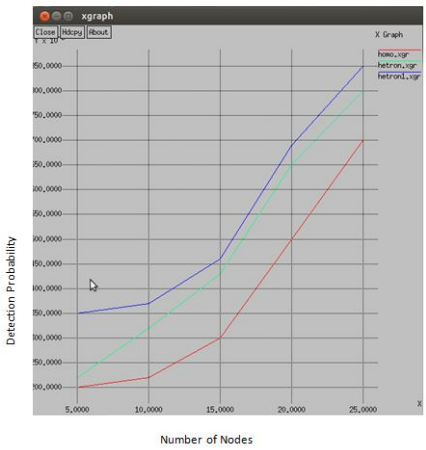

Fig. 9 Combined graph

7 CONCLUSION

The final result shows that the detection probability is better in heterogeneous WSN as compared to homogeneous WSN (Fig 9). It shows that the detection probability increases with node density. This Graph also shows that the detection probability also increases with increasing sensing range as detection probability for nodes having sensing range 200 m is more than the nodes having sensing range 100 m. This work can be enhanced in future by taking transmission range in consideration along with sensing range and node density.

REFERENCES

[1] Stetsko, A., L. Folkman and V. Matyáš, 2010. "Neighbour-based intrusion detection for wireless sensor networks". Proceedings of the 6th International Conference on Wireless and Mobile Communications (ICWMC), Sept. 20-25, IEEE Xplore Press, Valencia, pp: 420-425. DOI: 10.1109/ICWMC.2010.61.

[2] Krontiris, I., T. Dimitriou and F.C. Freiling, 2007. "Towards intrusion detection in wireless sensor networks". Proceeding of the 13th European Wireless Conference, (EW' 07), CiteSeer.

[3] Jasvinder Singh, Er. Vivek Thapar, Er.Amit Kamra"Deployment Strategy of Homogeneous and Heterogeneous Wireless Sensor Network"Proceeding of International Journal of Computer Science and Communication Engineering Volume 1 Issue 2 (December 2012 Issue).

[4] Tapalina Bhattasali,Rituparna Chaki,2011. "Lightweight Hierarchical Model for HWSNET" Proceeding of the International Journal Of Advanced Smart Sensor Network Systems (Ijassn), Vol 1, No.2, October 2011.

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

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

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

[8] Y. Wang, X. Wang, B. Xie, D. Wang, and D. P. Agrawal, "Intrusion detection in homogeneous and heterogeneous wireless sensor networks," in Proceedings of IEEE Transactions on Mobile Computing, vol. 7, no. 6, pp. 698-711, 2008.

[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.

[10] Byunggil Lee, Seungjo Bae and Dong Won Han, "Design of network management platform and security frame work for WSN", IEEE International conference on signal image technology and internet based system, 2008.

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

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