ISSN 2319-2720

Volume 6, No.3, July - August 2017

International Journal of Computing, Communications and Networking

Available Online at http://www.warse.org/ijccn/static/pdf/file/ijccn01632017.pdf

# Intrusion Detection for Surveillance Purposes using Wireless Sensor Network

**Khaled Farouk[1], Walid M. Saad[2], Sherif Kishk[3]**

[1]Air defense collage, Egypt, kholoda1111@gmail.com

[2] Egyptian Air Defense Technical R&D Center, Egypt, walid@sce.carleton.ca

[3]Mansura University, Egypt, shkishk@mans.edu.eg

## ABSTRACT

Wireless sensor network (WSN) has numerous applications in our daily life. This paper discusses the usage of wireless sensors in monitoring and surveillance of one or more intruders in a pre-defined area of interest. Detection probability of intruder is analyzed versus different parameters. Results show the intrusion detection probability versus some parameters such as sensor sensing radius, number of nodes, radius of the coverage area, node availability, probability of active nodes and node density. Furthermore, we investigated the performance of the expected time of detecting an intruder by changing the node density and at different scenarios of intruder velocities.

**Keywords**: Wireless sensor network, intrusion detection probability, probability of active nodes, latency.

## 1. INTRODUCTION

WSN is a network consists of multi-sensors that are distributed randomly or organized in a region area to monitor a physical phenomenon. A known (WSN) system is formed by the combination of multi-nodes, which are connected together in a specific way by one or more base station (gateway) ending to a server. Sensor nodes are equipped with a radio transceiver, a small microcontroller and small battery [1]. The size spectrum of nodes varies from very small to large according to the sensor deployment such as using it in battlefield surveillance, healthcare application, traffic control and home automation [2, 3]. The cost of sensors varies from a hundred of dollars to a few cents. The size of sensor nodes is subjected to some constraints as energy and memory. Energy is the main constraint in sensor network design especially in hazardous area and battlefield. In these places, energy is limited in range and bandwidth to extend the lifetime of battery [4]. Sensing coverage is how sensors monitor the target and how target is identified, which are essential parameters in WSN. Sensor may be positioned in ordinary places such as regular pattern, hexagonal, square and triangular. On the other hand, the distribution of nodes in hazard area by throwing it from a plane, then connect it autonomously [5]. Noureddine et al. [6] presents a mathematical mechanism in homogenous WSNs to detect an authorized intrusion in a field of interest and evaluate probability of detection in terms of node density, sensing range and intrusion distance. Ashfaq et al. [7] made a survey about intrusion detection system (IDS) that is more important for securing network. IDS is an additional unit installed in clients, server or both, which works in three sequential steps. These steps are monitoring network behavior, detect intrusion and generates alert in case of abnormal node detection. Hanzhijie et al. [8] propose an efficient traffic prediction algorithm for sensor nodes which exploits the Markov model to detect intruders. Jasvinder et al. [9] designed and implemented a system capable of detecting intruders in homogenous and heterogeneous WSNs and evaluated the energy consumed for detection and routing toward base station. Djallel et al. [10] presented the problem of intrusion detection in a different way that all intrusion detection schemes operated in a single layer of OSI model but in this scheme relied on the attacks are in different layers such as Mac layers and physical layers and used a simulator to proof by detecting different types of attacks in a different layer of OSI mode. Joseph et al. [11] present a new advanced intrusion detection system that improves detection probability rate compared with other systems like, hybrid intrusion detection system (HIDS) and energy prediction based intrusion detection system (EPIDS). In this paper**,** an intrusion detection system analysis using WSN is presented to calculate the probability of intruder detection, which rely on some parameters such as velocity, coverage radius of nodes, node density, and coverage area. This paper is divided as follow**:** section 2 shows a proposed model for intruder detection inside the area of interest and the boundary. In section 3, we analyzed a model for intruder detection latency. Section 4 shows the performance comparison of different scenarios, in terms of system probability of detection. Finally, section 5 is the conclusion.

## 2. INTRUSION SCENARIO

It assumed that there are n sensor nodes that are randomly distributed in a circular area, all nodes are homogenous, which means they have the same coverage radius.

### 2.1 ASSUMPTION AND NOTATIONS

Assuming we have *n* sensors ($s_1$, $s_2$…..$s_n$), the number of sensors exist in a circular area c is defined as *N(C)*. The number of sensor node per unit area $\delta$=*N/C* is defined as the node density. The number of sensors *N(c)*, placed in area *C*, followed by Poisson distribution with parameter $\delta C$.

$$P\,(N(C)=m) = \frac{e^{-\delta\,C}\,(\delta C)^{m}}{m!} \qquad (1)$$

where, *m* is the minimum number of nodes that detect an intruder, assuming all nodes are stationary and have the same sensing range $r_s$ and the cell is assumed a circular shape.

Intruder will be identified by sensor node if the distance between node and intruder is less than the radius $r_s$. Intruder is identified when it is detected by at least a sensor.

## 2.2 DETECTION OF A TARGET ON THE BOUNDARY OF A detection NETWORK

Let us impose *N* homogenous sensors deployed with node density $\delta$ in a circular region with area *C* as shown in Fig. 1. A random point **X** is detected or discovered by at least one randomly positioned sensor in the desired coverage area with probability of detection given by

$$P(r_s) = \frac{\pi\, r_s^2}{\pi\, R^2} = \left(\frac{r_s}{R}\right)^2 \quad (2)$$

where, *R* is the required coverage and $r_s$ is the radius of sensor node.

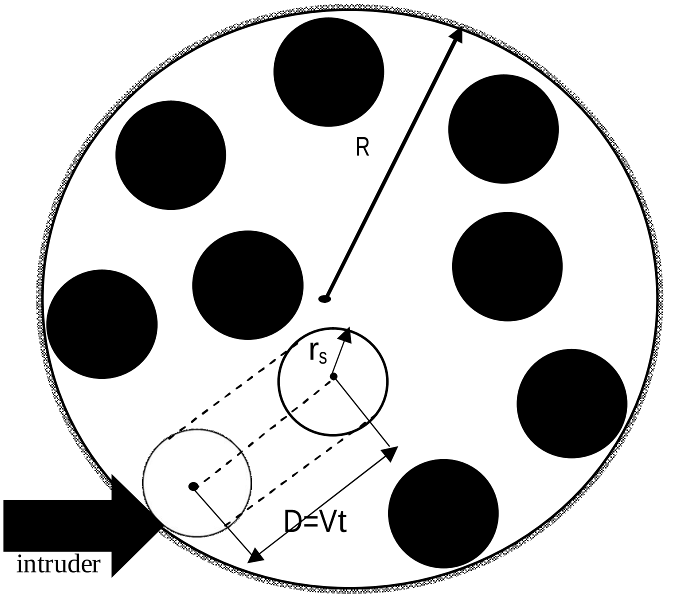

**Figure 1:** Illustration of an intruder disclosed by a WSN.

If point **X** located in the coverage area is not detected or identified by any sensor node then, the detection probability is

$$\overline{P(rs)} = 1 - \left(\frac{r_s}{R}\right)^2 \quad (3)$$

By distributing non-overlapped *N* sensors and for every *n* sensor node in the area of interest, the probability that point **X** is not detected by any of *n* sensors is

$$\overline{PN(rs)} = \left(1 - \left(\frac{r_s}{R}\right)^2\right)^n \quad (4)$$

When $R \to \infty$, the probability that point X is not detected by any of ***n*** sensors is

$$\overline{PN(rs)} = e^{-2n\left(\frac{r_s}{R}\right)} \quad (5)$$

Substitution $\delta = \frac{n}{\pi R^2}$ in equation (5) the probability of non-detection becomes as follow

$$\overline{PN(rs)} = e^{-(2\pi R r_s \delta)} \quad (6)$$

From the previous equation, we can easily calculate the detection probability of an intruder that crossed the area of interest and detected by *n* sensor nodes as follow

$$P_{N(rs)} = 1 - e^{-(2\pi R r_s \delta)} = 1 - e^{-2n\left(\frac{r_s}{R}\right)} \quad (7)$$

We notice that to increase probability of detection we must increase radius of sensor node, increase the number of nodes, increase the node density or decrease the radius of the total coverage area.

### 2.3 Detection of intruder inside the surveillance area

We further explain in this section the detection of a hostile that illegally crosses the area of interest. Let’s assume that the hostile moves with velocity *v* for a time period *t* where, the total traveled distance by the hostile inside the region area is *D= v t*. The area that is covered by the intruder is calculated as shown

$$C(t) = (\pi\, r_s^2/2) + 2 r_s\, v\, t \quad (8)$$

The sensors are randomly distributed over the illuminated area *C* by using Poisson distribution**,** assume that *u* represents the number of nodes n in the region area that snooping the hostile in the time interval *t*

$$P_{C(t)}\ (u=n) = \frac{(\delta\, C(t))^n}{n!}\ e^{-\delta C(t)} \quad (9)$$

In an uninhabited place, we could not easily change the batteries, so efficient energy consumption is mandatory, consequently random independent sleeping scheme is the primary solution to save energy [12]. In this scheme, any sensor stays active with probability $P_{on}$, then $(1 - P_{on})$ is the probability of sleeping mode for that sensor node. In this case, Binomial distribution is suitable to be used to get the probability of selecting *k* active sensor nodes out of *n* sensor nodes as follow

$$P_{C(t)}\ (S=k) = \binom{n}{k} (P_{on})^K (1 - P_{on})^{n-k} \quad (10)$$

we can select k nodes in area *C* at time *t* with probability

$$P_{C(t)}(u=k) = \sum_{n=k}^{\infty} \binom{n}{k} (P_{on})^k (1 - P_{on})^{n-k}\ \frac{(\delta\, C(t))^n}{n!}\ e^{-\delta\, C(t)}$$

$$= \sum_{n=k}^{\infty} \frac{n!}{k!(n-k)!}\ (P_{on})^k (1 - P_{on})^{n-k}\ \frac{(\delta\, C(t))^n}{n!}\ e^{-\delta\, C(t)}$$

$$= \frac{(P_{on})^k}{k!} e^{-\delta C(t)} (\delta C(t))^k \sum_{n=k}^{\infty} \frac{(1-P_{on})^{n-k}}{(n-k)!} (\delta C(t))^{n-k}$$

$$= \frac{(P_{on})^k (\delta C(t))^k}{k!} e^{-\delta C(t)} e^{\delta C(t)(1-P_{on})}$$

$$= \frac{(P_{on})^k (\delta C(t))^k}{k!} e^{-P_{on} \delta C(t)} \quad (11)$$

Substituting equation (8) in (11), we can get

$$P_{C(t)}(u=k) = \frac{(P_{on})^k \left(\delta\left(\frac{\pi r_s^2}{2} + 2r_s vt\right)\right)^k}{k!} e^{-P_{on}\delta\left(\frac{\pi r_s^2}{2} + 2r_s vt\right)} \quad (12)$$

When there is not any active sensor ($k$ = 0) in the snooped area then detection probability calculated as follow

$$P_{C(t)}(u=0) = e^{-P_{on}\delta\left(\frac{\pi r_s^2}{2} + 2r_s vt\right)} \quad (13)$$

When there is at least one active sensor node ($k$ > 0) in the area of interest then, the detection probability is calculated as follow

$$P(u \geq 1) = 1 - e^{-P_{on}\delta\left(\frac{\pi r_s^2}{2} + 2r_s vt\right)} \quad (14)$$

## 3. DETECTION LATENCY IN WSNS

Detection latency is defined as that time delay until the intruder will be detected by at least one sensor node in the monitoring area. The cumulative distribution function (CDF) for the intruder detection is given by

$$P((v.t \leq Z), t) = \int_0^{\infty} 1 - \left(1 - e^{-P_{on}\delta\left(\frac{\pi r_s^2}{2} + 2r_s v t\right)}\right) dt \quad (15)$$

where, $t$ is the run time before the hostile is identified and $E(t)$ is s the expected time for the hostile till identification by sensor nodes and $Z$ is the maximum distance of intruder inside the area of interest

$$E(t) = \int_0^{\infty} 1 - \left(1 - e^{-P_{on}\delta\left(\frac{\pi r_s^2}{2} + 2r_s v t\right)}\right) dt \quad (16)$$

$$= \int_0^{\infty} e^{-P_{on}\delta\left(\frac{\pi r s^2}{2} + 2 r_s v t\right)} dt \quad (17)$$

$$= \frac{e^{\frac{(-P_{on}\delta \pi r_s^2)}{2}}}{2P_{on}\delta r_s v} \quad (18)$$

Equation (18) shows the inverse proportionality between the expected time to detect the intruder and the node density, the intruder velocity and the node sensing range.

## 4. PERFORMANCE COMPARISON

Matlab is used to analyze the intruder detection probability against sensing range, node density, velocity of the intruder and availability of sensor node. In our simulation, we assumed circular monitoring area with radius $R$, the number of nodes is assumed to be 100 which are distributed randomly in this area. We will illustrate the relation between the intrusion detection probability and the sensor range at different values of $R$. Fig. 2 shows the relation between the detection probability of intruder versus sensing radius up to 15 when the radius of the coverage area $R$ varies from 0:100 m.

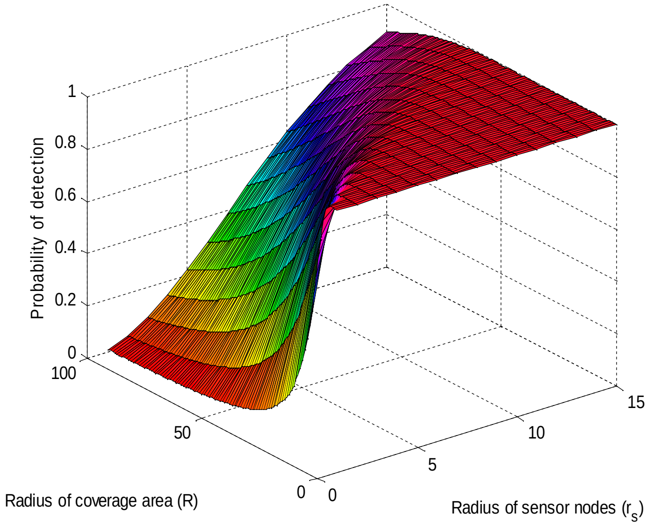

**Figure 2:** Detection probability versus different sensing for different values of $R$.

As shown in Fig. 2, when $r_s$ increases the probability of intruder detection increases at the same value of $R$. However, when $R$ increases the probability of intruder detection decreases at the same value of $r_s$. Fig. 2 illustrates the exact values of $r_s$ and $R$ for the required probability of intruder detection.

Fig.3 illustrates how the probability of intrusion detection varies by changing the number of nodes $N$ and the node density $\delta$ for a given sensing range $r_s$. From Fig.3 we can determine the number of required nodes and the required sensing range for a specific detection probability in a predetermined monitoring area. It is very clear that by increasing $N$ and /or $r_s$ the probability of detection is increased.

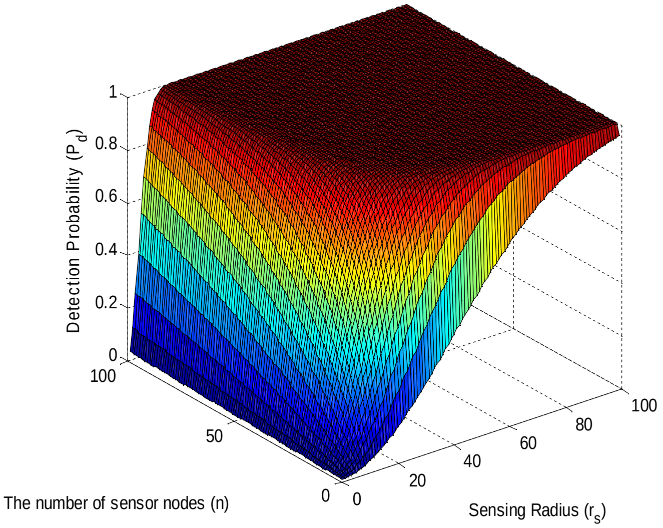

**Figure 3:** Detection probability of an intruder that can be detected by at least a sensor node for different values of n and $r_{s.}$

Fig. 4 shows the detection probability for different node availability $k$ and $r_s$. Assuming 100 nodes are deployed randomly in the area of interest with radius $R$=50 m. The intruder is assumed to enter the area of interest with velocity 2 m/s and the time required $t$ until the intruder is identified by any of sensor node is 1 sec and the node density $N/A$ = 0.0127. We note that when $r_s$ = 10 m and the availability of sensor node $k$ =1, the detection probability is 0.81. As $k$ increases to 3 and 5 at the same $r_s$, then, the detection probability becomes 0.24 and 0.028 respectively. Then we can deduce from this analysis that by increasing the node availability in area of interest it causes better fault tolerance in the network which decreases the detection probability of intruder therefore, the single sensing system has better probability of detection than multi- sensing system but the fault tolerance gets worst.

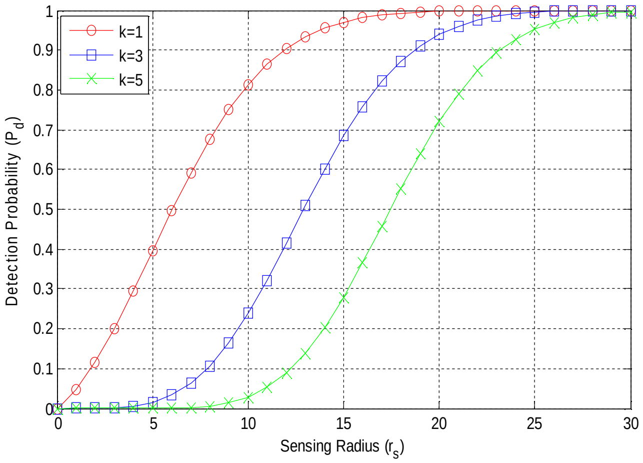

**Figure 4:** Probability of detection versus sensing range for different values of k at $R$= 50 m.

We monitored the probability of intruder detection after changing the radius of the coverage area to 60 and 70 m. By observing $P_d$ when $k$ = 1, 3 and 5 then we notice that the probability of intruder detection is dramatically decreased as shown in Figs 5 and 6.

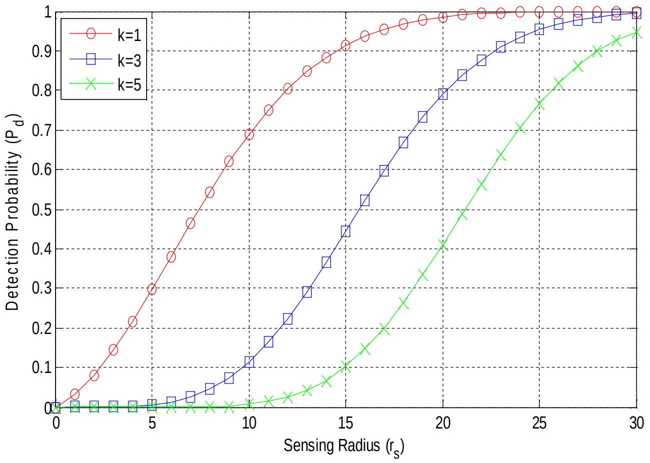

**Figure 5:** Probability of detection versus sensing range at different values of k when $R$= 60 m.

It is clear that $P_d$ increases by increasing the sensing range and decreases the node availability. We deduce that the detection probability relies on sensing range and number of active nodes so we can easily improve the detection probability by knowing the parameters of the network and the properties of the sensor.

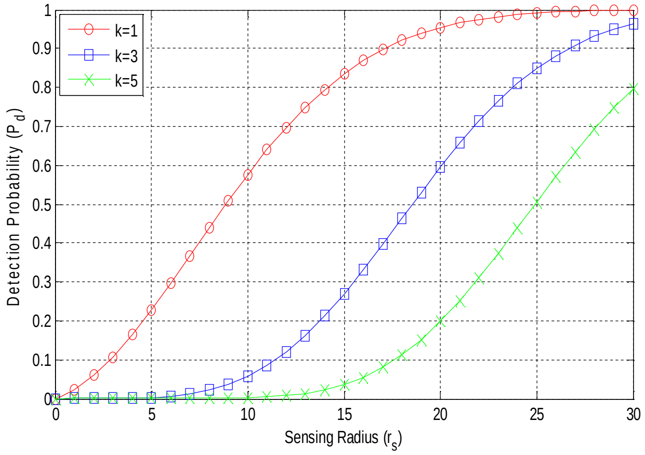

**Figure 6:** Probability of detection versus sensing range at different values of k when $R$= 70 m.

For further illustration, we analyzed $P_d$ at different values of active nodes k ranging from 0 to 10 and different values of $r_s$ varies from 0:30 m when $R$ = 60 m as shown in Fig. 7. As we increase the sensing range and decrease the node availability, the intrusion detection probability approaches to one. Fig. 7 illustrates the required $r_s$ at certain $R$ that can achieve the desired $P_d$ for specific $k$ active nodes.

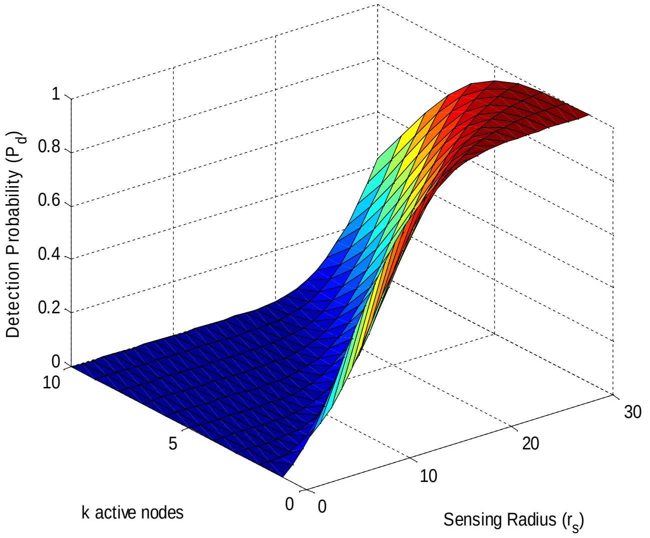

**Figure 7:** Probability of detection of an intruder versus sensing range and node availability.

The probability of active nodes affects the probability of intruder detection as given in Equation (12). For that reason, we illustrated the probability of intruder detection versus different sensing range for different active node probability $P_{on}$ in Fig. 8. It is assumed that 100 nodes are spatially distributed in random manner in the monitoring area where $R$ = 50 m, the intruder moves in this area with velocity 5 m/s and the time required $t$ until the intruder be detected is 2 sec. It is noted that when $r_s$ = 5 m and probability of active nodes $P_{on}$= 0.1, the detection probability of intruder is nearly 0.16. When we increase $P_{on}$ to 0.5 at the same sensing radius, the probability of intruder detection will increase to nearly 0.59. By increasing $P_{on}$ to 1, the detection probability will increase to almost 0.83. Then we conclude that by either increasing the sensing range or the probability of active nodes, the probability of intruder detection is increased.

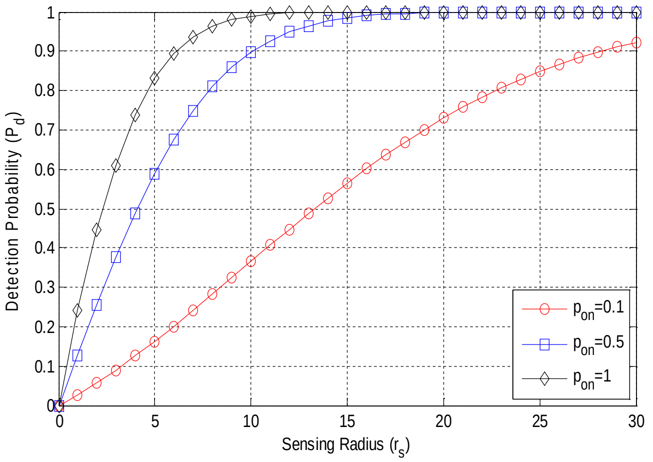

**Figure 8:** Probability of detection versus sensing range for different probability of active nodes when *R*= 50 m.

More study has been done to monitor the effect of increasing the radius of the coverage area $R$ on the probability of intruder detection at a certain probability of active nodes. Figs. 9 and 10 show the probability of intrusion detection at different $p_{on}$ when $R$ = 70 and 90 m respectively. We notice that when $R$ is increased at the same $p_{on}$ and $r_s$, the probability of intruder detection is decreased.

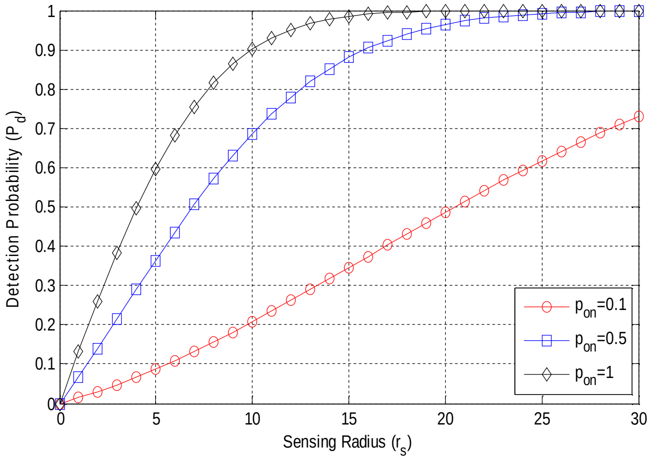

**Figure 9:** Probability of detection versus sensing range for different probability of active nodes when *R*= 70 m.

Fig. 11 shows the relationship between the sensing radius and the expected time to detect the intruder by any of the sensor nodes at different values of the node density $\delta$. As illustrated, the expected time to detect the intruder *E(t)* is getting shorter as $r_s$ is increased. *E(t)* is also decreased dramatically when the node density $\delta$ is increased.

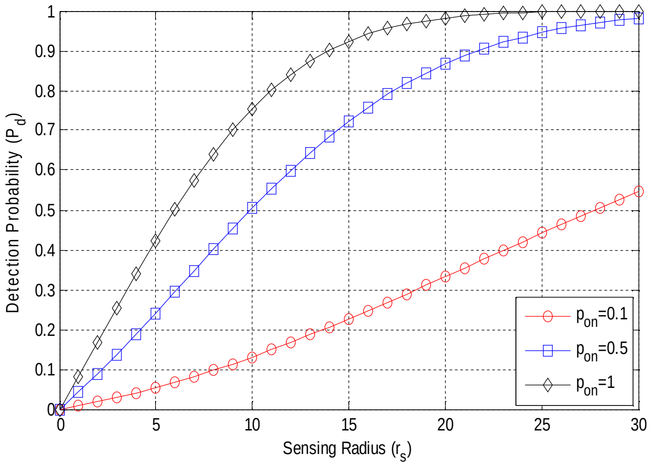

**Figure 10:** Probability of detection versus sensing range for different probability of active nodes when *R*= 90 m.

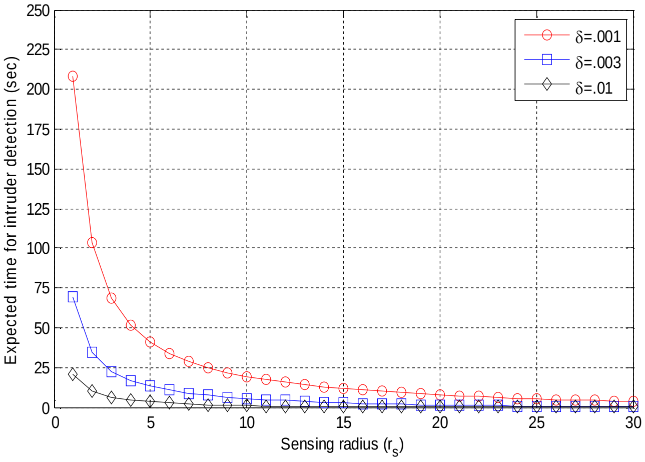

**Figure 11:** Illustration of the expected time to detect the intruder versus the sensing radius at different values of $\delta$.

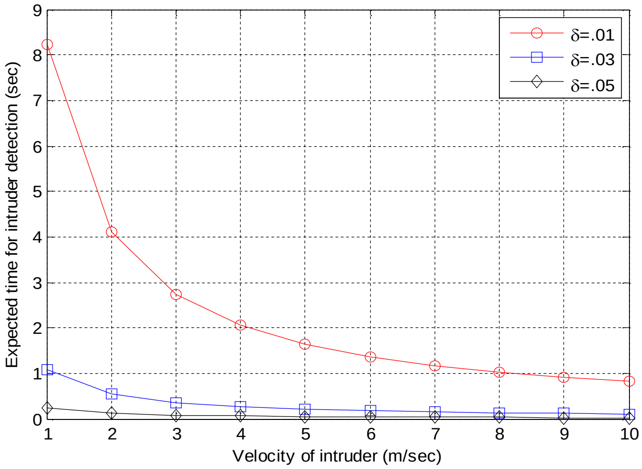

**Figure 12:** Illustration of the expected time to detect the intruder versus the intruder velocity at different values of $\delta$.

Fig. 12 shows how the velocity of the intruder influence the expected time to detect it at different values of node density. It is obvious that by increasing the velocity of the intruder and/or the node density the expected time of intruder will be reduced. When the velocity = 2 m/sec and $\delta$ = 0.01 node/m$^2$ then the intruder is detected after 4.12 sec. By increasing δ to 0.03 and 0.05 node/m$^2$ at the same velocity then, the intruder will be detected after 0.0.54 and 0.13 sec respectively. We can deduce that as the speed of the intruder getting higher and/or the node density getting larger, the time required for the detection and the identification of the intruder by the sensor nodes is getting shorter.

## 5. CONCLUSIONS

In this paper, we studied some parameters that influence the probability of intruder detection such as sensor range $r_s$, the node density $\delta$, the number of active nodes $k$, the radius of the coverage area $R$ and the probability of active nodes $p_{on}$. The time delay until the intruder is detected inside the desired surveillance area and the various parameters that influence it are also studied. We assumed a homogenous network using Poisson distribution to randomly distribute the sensor nodes in a circular coverage area with radius $R$. Binomial distribution is used to select the active node from all available sensor nodes in the surveillance coverage area. Mathematical analysis for the probability of intruder detection and the expected time to detect intruders are studied and illustrated against node density, sensing range, number of active nodes and the radius of the coverage area.

As illustrated in this paper, the probability of intruder detection is sensitive to many different parameters. To enhance its performance, we need to increase the sensor radius, the number of sensor nodes, the node density or the probability of active nodes. On the other hand, the probability of intruder detection performance could be enhanced by decreasing the node availability and/or the radius of the coverage area. The expected time to detect the intruder is also investigated. It is noted that as the sensing radius and/or the node density increased, the delay time until detect the intruder becomes shorter.

## REFERENCES

1. H. Karl, and A Willing. ***Protocols and Architectures for Wireless Sensor Network,*** Chichester, UK: Wiley 2005, ch.2, pp. 17-31.
2. S. R. Prabhu, S. Sophia, S. Maheswaran and M. Navaneethakrishnan. **Real-World Applications of Distributed Clustering Mechanism in Dense Wireless Sensor Networks**, *International Journal of Computing, Communications and Networking (IJCCN)*, vol.2, PP. 99-105, 2013.
3. M. F. Othman, and K. Shazali. **Wireless Sensor Network Applications: A Study in Environment Monitoring System**, *International symposium on Robotics and Intelligent Sensors*, vol.14, PP.1204-1210, 2012.
4. I. Yoon, D. K. Noh, and H. Shin. **Energy-Aware Hierarchical Topology Control for Wireless Sensor Networks with Energy-Harvesting Nodes,** *International Journal of Distributed Sensor Networks*, vol. 2015, pp.12, March 2015.
5. A. K. Sagar, D. K. Lobiyal. **Probabilistic Intrusion Detection in Randomly Deployed Wireless Sensor Networks;** New York: Springer, vol.84, Issue 2, September 2015, pp. 1017-1037.
6. N. Assad, B. Elbhiri, M. A. Faqihi, M. Ouadou, and D. Aboutajdine. **Analysis of the Deployment Quality for Intrusion Detection in Wireless Sensor Networks,** *Journal of Computer Networks and Communications*, July 2014, vol. 2015, pp. 1-7.
7. A. H. Farooqi, and F. A. Khan. **Intrusion Detection Systems for Wireless Sensor Networks: A Survey,** *Springer J. Communication and networking*, 2009, vol.56, pp. 234-241.
8. H. Zhijie, and W. Ruchuang. **Intrusion Detection for Wireless Sensor Network Based on Traffic Prediction Model,** *International Conference on Solid State Devices and Materials Science*, 2012, vol.25 pp. 2072 – 2080.

**9.** J. Singh, and E. V. Thapar. **Intrusion Detection System in Wireless Sensor Network,** *International Journal of Computer Science and Communication Engineering*, December 2012, vol.1, Issue 2, pp. 76-80.

**10.** D. E. Boubiche, and A. Bilami. **Cross layer Intrusion Detection System for Wireless Sensor Network,** *International Journal of Network Security & Its Applications,* March 2012, vol.4, No. 2.

**11.** J. R. S. CEng, AMIE and K. Vijayan. **Advanced Intrusion Detection System for Wireless Sensor Networks,** *International Conference on Signal Processing, Embedded System and Communication Technologies and their applications for Sustainable and Renewable Energy (ICSECSRE '14)*, April 2014, vol.3, pp. 167-172.

**12.** Z. Rezaei, and S. Mobininejad. **Energy Saving in Wireless Sensor Networks,** *International Journal of Computer Science & Engineering Survey*, February 2012, vol.3, No.1.