Hindawi Publishing Corporation
Journal of Computer Networks and Communications
Volume 2015, Article ID 812613, 7 pages
http://dx.doi.org/10.1155/2015/812613

Research Article

Analysis of the Deployment Quality for Intrusion Detection in Wireless Sensor Networks

**Noureddine Assad,[1] Brahim Elbhiri,[2] Moulay Ahmed Faqihi,[3]
Mohamed Ouadou,[1] and Driss Aboutajdine[1]**

[1]LRIT, Research Unit Associated to the CNRST (URAC 29), FSR, Med V University, 10000 Rabat, Morocco
[2]EMSI, 10014 Rabat, Morocco
[3]ENSIAS, Mohammed V University, BP 713, Rabat, Morocco

Correspondence should be addressed to Noureddine Assad; assad.noureddine@gmail.com

Received 10 June 2014; Revised 18 January 2015; Accepted 19 January 2015

Academic Editor: Rui Zhang

The intrusion detection application in a homogeneous wireless sensor network is defined as a mechanism to detect unauthorized intrusions or anomalous moving attackers in a field of interest. The quality of deterministic sensor nodes deployment can be determined sufficiently by a rigorous analysis before the deployment. However, when random deployment is required, determining the deployment quality becomes challenging. An area may require that multiple nodes monitor each point from the sensing area; this constraint is known as k-coverage where k is the number of nodes. The deployment quality of sensor nodes depends directly on node density and sensing range; mainly a random sensor nodes deployment is required. The major question is centred around the problem of network coverage, how can we guarantee that each point of the sensing area is covered by the required number of sensor nodes and what a sufficient condition to guarantee the network coverage? To deal with this, probabilistic intrusion detection models are adopted, called single/multi-sensing detection, and the deployment quality issue is surveyed and analysed in terms of coverage. We evaluate the capability of our probabilistic model in homogeneous wireless sensor network, in terms of sensing range, node density, and intrusion distance.

1. Introduction

Advances in technological developments at the microapplication, the radio communication, and the integration of microprocessors have made it possible to develop a new range of small low-cost electronic devices, called sensor nodes. The latter may be deployed in large numbers to form an intelligent and autonomous wireless sensor network (WSN) which can be used for a wide variety of applications dealing with monitoring, control, and surveillance. Each sensor node senses the environment field of interest, which seems the most time inaccessible and communicates the collected data to the sink, where the end-user can access them [1]. In this paper, we focus on the surveillance wireless sensors network applications, such as detecting an unauthorized or unusual moving intruder in a field of interest. These critical applications require characterizing the WSN parameters that do not exist in traditional ad hoc networks. Intrusion detection model in a homogeneous wireless sensor network introduce parameters, sensing range, and node density, for each point of a field of interest must be within the sensing range of at least one sensor node. In a sensing covered field, the WSN must be able to adapt to changing network topology and environment conditions. An intruder may be detected by single-sensor node or multi sensor nodes that are modeled by single-sensing detection and multi-sensing detection in homogeneous wireless sensor network.

Some works are targeted at particular applications, but the central idea is still centered around a coverage issue. The problem of coverage network is described by several authors in [2, 3], how well an area is monitored or tracked by sensor nodes, and authors in [4, 5] also derived analytical expressions to quantify the coverage enhancing the deployment quality because the network coverage concept is a measure of the quality of service. Efficient distributed algorithms are proposed in [6, 7] to solve the coverage network problem with optimally reduced energy consumption in WSNs.

1.1. Motivations and Problem Statement. These issues are motivated by the following simple reasons including random network topology where all sensor nodes are randomly deployed in a region; this implies the efficient deployment of the required coverage. Specifically, given a monitoring region, how can we guarantee that each point of the region is covered by the required number of sensor nodes? In other words, we need to recognize which areas are covered by enough sensors in order to enhance the probability of intrusion detection and an intruder does not exceed the threshold distance. In addition, the energy conservation is a critical challenge in WSNs due to the limitations of wireless sensors on the energy supply, the available storage space, and the computational capacity. This implies that the network must have self-organizing capabilities. It is important to place or select the effective number of sensor nodes in coverage network; sensor power can be put on/off periodically in order to extend the whole WSN lifetime.

1.2. Contributions and Organization. The major contributions of this paper can be summarized as follows: developing a probabilistic approach by deriving analytical expressions to characterize the topological properties of network coverage, designing and analysing the intrusion detection probability in a homogeneous wireless sensor network, and taking into account the various parameters such as sensing range, node density, node availability, and intrusion distance. This is to enhance the quality of sensor nodes deployment. We investigate our model for intrusion detection in WSNs to single-sensing and multi-sensing detection.

The remainder of the paper is organized as follows. In Section 2, some preliminaries and models are presented and then intrusion detection and network topology are reviewed. Next we analytically evaluate the intrusion detection model in a homogeneous wireless sensor network in Section 3 while, in Section 4, we present the simulation results and their analysis. Finally, conclusions are drawn in Section 5.

2. Intrusion Detection Model and Network Topology

For more comprehensive review on intrusion detection model in WSNs, we describe in this section some key definitions and describe the network topology and degrees and coverage and communication model.

2.1. Preliminaries and Models

Definition 1 (sensing range). The sensing range of a node N_i is a disk of radius R_{SENS}, centred at ξ_i and defined by

$$\text{Disk}_i\left(R_{\text{SENS}}\right) = \left\{\xi_j \in \mathbb{R}^2 : \left|\xi_i - \xi_j\right| \leq R_{\text{SENS}}\right\}, \tag{1}$$

where $|\xi_i - \xi_j|$ stands for the Euclidean distance between ξ_i and ξ_j.

Definition 2 (transmission range). The transmission range of a node N_i is a disk of radius R_{TRANS}, centred at ξ_i and defined by

$$\text{Disk}_i\left(R_{\text{TRANS}}\right) = \left\{\xi_j \in \mathbb{R}^2 : \left|\xi_i - \xi_j\right| \leq R_{\text{TRANS}}\right\}. \tag{2}$$

Definition 3 (collaborating sensors). Consider two nodes N_i and N_j located at ξ_i and ξ_j, respectively. Let us note that d_{ij} is the distance between N_i and N_j. The collaborating set of N_i and N_j is defined as the union between S_{N_i} and S_{N_j}. Besides, N_i and N_j are said to be collaborating if and only if $d_{ij} = |\xi_i - \xi_j| \leq 2R_{\text{SENS}}$, where R_{SENS} is the sensing range. In general, the collaborating sensor set N_i is

$$S_{\text{col}}\left(N_i\right) = \bigcup_{\{N_j : |\xi_i - \xi_j| \leq 2R_{\text{SENS}}\}} S_{N_j}. \tag{3}$$

Definition 4 (overlapped area). The overlapped area S_{ol} of nodes N_i and N_j is defined as the intersection region between S_{N_i} and S_{N_j} areas that is formulated by the following equation:

$$S_{\text{ol}} = S_{N_i} \cap S_{N_j}. \tag{4}$$

We can note that each point located in S_{ol} can be covered by both N_i and N_j nodes.

An example of S_{ol} and S_{col} surface areas and communication between sensor nodes N_i and N_j are represented in Figure 1.

Definition 5 (neighbouring nodes). The neighbouring information of each node N_i from a graph G is defined as

$$\mathcal{N}_i = \left\{N_j \in G : \left|\xi_i - \xi_j\right| \leq R_{\text{TRANS}}\right\}, \tag{5}$$

where $|\xi_i - \xi_j|$ is the Euclidean distance between nodes N_i and N_j. $\mathcal{N}_i$ represents the set of indexes of the nodes which send information to node N_i.

2.2. Network Topology. Throughout this paper, we consider N nodes randomly distributed over a square region A of edge length L in set $\mathbb{R}^2$ following a uniform distribution; we assume that any two nodes (N_i, N_j) are directly connected if the Euclidean distance d_{ij} is smaller than or equal to the transmission range R_{TRANS} (i.e., $d_{ij} = |\xi_i - \xi| \leq R_{\text{TRANS}}$); only bidirectional links are considered. A region R is said to be covered, if every point in R is at distance at most R_{SENS} from at least one sensor node. In homogeneous WSNs, we assume that every node has the same sensing range R_{SENS} and the same transmission R_{TRANS}. The resulting graph is called the covering-reachability graph and is denoted by $G(V, R_{\text{SENS}}, R_{\text{TRANS}})$ where V is a set of nodes indexed with $i = \{1, \ldots, N\}$.

2.3. Degrees and Coverage. The goal of monitoring an area of interest is to have each location in the sensing area within the sensing range of at least one sensor node. Depending on the application scenarios, several coverage models have been proposed in the literature. An area may require that

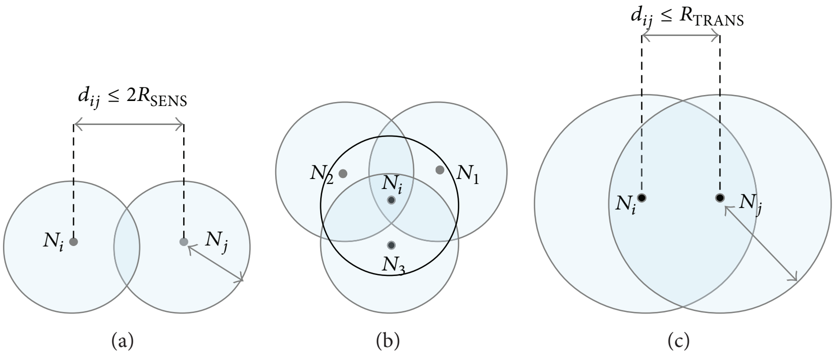

$d_{ij} \leq 2R_{\text{SENS}}$
N_i
N_j
(a)
N_2
N_i
N_1
N_3
(b)
$d_{ij} \leq R_{\text{TRANS}}$
N_i
N_j
(c)

Figure 1: (a) Collaborating sensor nodes N_i and N_j, (b) sensor node N_i totally overlapped by sensor nodes N_1, N_2, and N_3, and (c) communicating sensor nodes N_i and N_j.

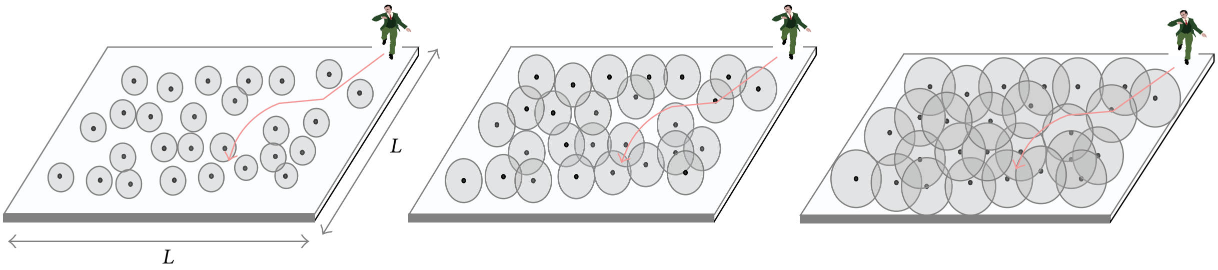


Figure 2: A typical network generated via uniform distribution of the x, y coordinates of the sensor nodes. The sensing ranges of the node are increased gradually (from left to right).

multiple sensor nodes monitor each point in the sensing area [8]. The constraint is known as k-coverage where k represents the number of nodes. We can define any convex region A of $\mathbb{R}^2$ with a coverage degree k, where every point of the considered region is covered by at least k nodes [9]. Given the surface area S and specified by the application (either before or after deployment) as illustrated in Figure 2, what would be the required value of the sensing range R_{SENS} to achieve a specified coverage degree k, $k > 0$? In practice, a network with a higher degree of coverage can achieve higher sensing accuracy and be more robust against sensing failure. An example of k-coverage is illustrated in Figure 1: the middle picture (b) shows an example of redundant node, where the monitored area by the node N_i is totally overlapped by nodes N_1, N_2, and N_3. Therefore, it is important to place or select the effective number of sensor nodes to cover the same monitored area as much as possible without diminishing the overall field coverage and specified coverage degree k, $k > 0$. The authors in [10] extend the problem to connected k-coverage which they define as the minimum number of sensors that must stay active, so that each point in the field is k-covered and every one of these sensors must be connected to each other.

Data accuracy depends on the size of the connected component that contains the sink. It reaches the highest value when the sink belongs to the largest connected component of the network. Thus, high-quality coverage requires that all source sensors be connected to the sink. One of the most interesting questions regarding the connectivity of random WSNs concerns finding limiting regimes for which the connectivity becomes almost sure to occur. Typically these regimes involve the number of nodes and transmitting range becoming large [8, 11]. In other words, connectivity of WSNs should be so defined as to take into consideration the inherent structure of this type of network.

In this paper, we assume that any two nodes N_i and N_j can directly communicate with each other if their Euclidean distance is less than the transmitting range R_{TRANS} (i.e., $|\xi_i - \xi_j| \leq R_{\text{TRANS}}$) as shown in the last picture (c) from Figure 1. A point P is covered by a node N_i if the Euclidean distance between the point p and the node N_i is less than the sensing range R_{SENS} of the node N_i.

Given a coverage region A and a nodes coverage degree k, the goal of an integrated coverage and connectivity configuration is maximizing the number of nodes that are scheduled to sleep under the constraint that the remaining nodes must guarantee: A is at least k-covered and all active nodes are connected.

3. Intrusion Detection Model in a Homogeneous Wireless Sensor Network

Intrusion detection in wireless sensor networks is defined as a mechanism to detect unauthorized intrusions or anomalous moving attackers. The quality of deterministic nodes deployment can be determined sufficiently by analysis before the deployment. However, when random deployment is required, determining the deployment quality becomes challenging [10]. To assess the deployment quality of sensor nodes, appropriate measures can be employed that reveal the weaknesses in the coverage of WSNs, with respect to the success ratio and intrusion detection probability. For this purpose, it is a fundamental issue to characterize WSN parameters such as node density and sensing range in terms of high detection probability. In this section, several probabilistic intrusion detection models are adopted and deployment quality issue is surveyed and analysed in terms of coverage.

3.1. Sensing Model Probability. We consider a random network topology as discussed in Section 2.2 where all nodes are randomly deployed in field of interest. The deployment quality increases with the increase in the detection probability. The sensing model probability is generally closely coupled with the specific sensor application and the type of sensor device used [12, 13]. We adopt a sensing model probability where a sensor node can detect any events located in the sensing area. All sensor nodes are assumed to be homogeneous, and they have the same sensing range.

For a uniformly distributed sensor network of node density λ, we denote the number of sensor node, which deployed in the surface area S_{area}, by N. For each sensor node, the probability of each sensor node, within the sensing range R_{SENS} distance of a point, is a Bernoulli trial, where the probability of success is

$$p = \frac{\pi R_{\text{SENS}}^2}{S_{\text{area}}}. \tag{6}$$

Hence, the number of sensor nodes, within distance R_{SENS} of a point, forms a Binomial distribution. Moreover, for large N and small p, this Binomial distribution can be represented by a Poisson process. Then, the mean value of the equivalent Poisson process is

$$Np = \frac{N\pi R_{\text{SENS}}^2}{S_{\text{area}}}. \tag{7}$$

The sensing model probability that an intruder is detected by k sensor nodes follows the Poisson distribution; it is given by the following formula:

$$P(n = k) = \frac{(S\lambda)^k}{k!} e^{(-S\lambda)}, \tag{8}$$

where S is the area swept by intruder following a trajectory l. We assume that the intruder starts from a random point in the sensing area and moves in a random fashion as illustrated in Figure 3:

$$S = 2R_{\text{SENS}} l + \pi R_{\text{SENS}}^2. \tag{9}$$

Hence, the previous probability can further be represented by

$$P(n = k) = \frac{\left(\left(2R_{\text{SENS}} l + \pi R_{\text{SENS}}^2\right)\lambda\right)^k}{k!} e^{-(2R_{\text{SENS}} l + \pi R_{\text{SENS}}^2)\lambda}. \tag{10}$$

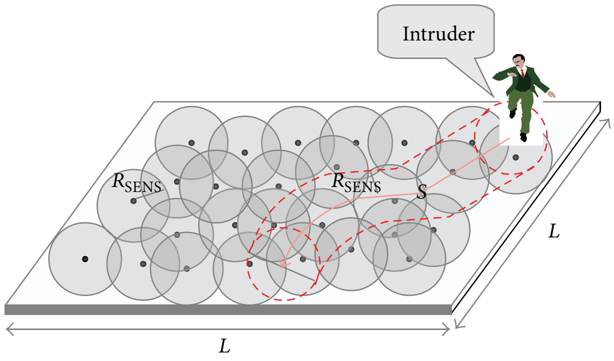


FIGURE 3: A simple intrusion scenario: an intruder starts from a random point in the WSN and moves in a random fashion and sweeps the surface area S following a trajectory l.

Intrusion Distance l. As a result of random movement of the intruder, the intrusion distance l can be derived as an arc length of a parametric curve that is formulated by the following equation:

$$l = \int_a^b \sqrt{(f'(x))^2 + (g'(x))^2}\, dx. \tag{11}$$

Proof. A parametric curve l can be thought of as trajectory of a point that moves through the plane with coordinates $(x, y) = (f(t), g(t))$, where f and g belong to C^1 class functions of the parameter t. For each value of t from the interval $[a, b]$, we get a point $P = (f(t), g(t))$ of the curve and we divide the curve denoted l into m points:

$$l = \{P_0, P_1, P_2, P_3, \ldots, P_m\}. \tag{12}$$

The corresponding points in the arc have the coordinates $(f(t_i), g(t_i))$ where $a \le t_i \le b$, so two consecutive points are separated by a distance equal to

$$\Delta P_i = |P_i - P_{i-1}| \quad i \in \{1, 2, \ldots, m\}. \tag{13}$$

More generally, we approximate the length of the arc l by inscribing a polygonal arc (i.e., made up of straight line segments) and adding up the lengths of the segments. Therefore, this limit $\lim_{|\Delta P| \to 0} \sum_{i=1}^{m} |P_i - P_{i-1}|$ exists because the two functions f and g are of class C^1. Consider

$$l = \lim_{|\Delta t| \to 0} \sum_{i=1}^{m} \sqrt{(f(t_i) - f(t_{i-1}))^2 + (g(t_i) - g(t_{i-1})^2)}. \tag{14}$$

As both functions f and g are of Class C^1, $e \in [t_{i-1} t_i]$ there as $f(t_i) - f(t_{i-1}) = f^{'}(e)(t_i - t_{i-1})$ and $g(t_i) - g(t_{i-1}) = g'(e)(t_i - t_{i-1})$, the arc length formula then becomes

$$l = \lim_{|\Delta t| \to 0} \sum_{i=1}^{m} \sqrt{g'(e)^2 + f'(e)^2}\, \Delta t_i, \tag{15}$$

where l is the Riemann sum of the function $\sqrt{g'(x)^2 + f'(x)^2}$ from the point $(a, f(a))$ to a point $(b, f(b))$. This formula can also be expressed in the following way:

$$l = \int_a^b \sqrt{\left(f'(x)\right)^2 + \left(g'(x)\right)^2} dx. \quad (16)$$

□

Node Density λ. Density of nodes is a crucial parameter sensor nodes deployment to require the intrusion detection quality of WSN applications. The deployment quality depends directly on node density; mainly a random nodes deployment is required [14, 15]. The network connectivity probability becomes higher as the density of nodes increases, even though the degree of coverage also increases. To improve the accuracy of node density, we take into account the partial density as shown in the following formula:

$$\lambda = \sum_{i=1}^{m} \lambda_i = \sum_{i=1}^{m} \frac{n_i}{S_i}, \quad (17)$$

where λ is the sum of the partial densities. The number of active nodes remains steady with respect to node density for the same requested coverage degree.

3.2. Single-Sensing Detection. The probability that no sensor in a sensing area can detect an event is $\overline{P} = e^{-\lambda S}$. The complement of $\overline{P}$ is the probability that there is at least one sensor node which detects an event. This sensing model probability can be represented as

$$P(n \geq 1) = 1 - \overline{P} = 1 - e^{-\lambda S}. \quad (18)$$

According to the intrusion scenario, the intruder starts from a random point in the sensing area and moves in a random fashion as illustrated in Figure 3. The probability that an intruder does not exceed the threshold distance l_{THR} is

$$P(n \geq 1, 0 \leq l < l_{\mathrm{THR}}) = 1 - e^{-(2R_{\mathrm{SENS}} l_{\mathrm{THR}} + \pi R_{\mathrm{SENS}}^2)\lambda}. \quad (19)$$

An Intrusion Detection Probability with Distance Threshold $l_{\mathrm{THR}} = 0$ in a Homogeneous WSN. We consider N nodes randomly distributed over a square region A of edge length L in the set $\mathbb{R}^2$ following a uniform distribution. We consider also that all sensors are static once the homogeneous WSN has been deployed. If we want to be sure that any intruder can be immediately detected, we use the following formula:

$$P_{\mathrm{sensing}}(\mathrm{nbrs} \geq 1, l_{\mathrm{THR}} = 0) \geq P_{\mathrm{threshold\_sensing}}, \quad (20)$$

where $P_{\mathrm{threshold\_sensing}}$ is a threshold probability. We must set the sensing range of all sensor nodes as follows:

$$R_{\mathrm{SENS}} \geq \sqrt{\frac{-\ln\left(1 - P_{\mathrm{threshold}_{\mathrm{sensing}}}\right)}{\lambda\pi}}. \quad (21)$$

3.3. Multi-Sensing Detection. In the WSN applications, the number of required sensors depends on the coverage quality; it can be determined sufficiently in advance by analysis of nodes deployment. To achieve a specified coverage degree k ($k > 0$), we derive the probability P that an intruder can be detected within the threshold intrusion distance l_{THR}, by the multi-sensing detection model in the following formula:

$$P(n \geq k, 0 \leq l < l_{\mathrm{THR}}) = 1 - \sum_{i=0}^{k-1} \frac{(S\lambda)^i}{i!} e^{-S\lambda}. \quad (22)$$

S is the surface swept by intruder following a trajectory l:

$$\begin{aligned} S &= 2R_{\mathrm{SENS}} l_{\mathrm{THR}} + \pi R_{\mathrm{SENS}}^2 \\ &= 2R_{\mathrm{SENS}} \int_a^b \sqrt{\left(f'(x)\right)^2 + \left(g'(x)\right)^2} dx + \pi R_{\mathrm{SENS}}^2. \end{aligned} \quad (23)$$

λ is the sum of the partial densities:

$$\lambda = \sum_{i=1}^{m} \lambda_i = \sum_{i=1}^{m} \frac{n_i}{S_i}. \quad (24)$$

While increasing the sensing range and the number of nodes per unit, the intrusion detection probability in single-sensing and multi-sensing increases. All events that happen in the network will be covered. According to the formulas discussed above, the optimal values of sensing range and node density can be determined in advance to totally cover a sensing area.

3.4. Node Availability. In a dense network, sensing areas of different nodes may be similar to their neighbor nodes, so they will transmit redundant information and the WSN total energy consumption will increase. Therefore, it is important to place or select the effective number of sensor nodes, to cover the same monitored area as much as possible without diminishing the overall field coverage. Thus, we must identify the redundant nodes in a dense network and change their operating mode between sleep and active modes. We can express the efficient number of nodes which can be deployed to cover the sensing area by node availability rate p as a variable in event detection probability P. We can efficiently reduce the energy consumption in most of the WSN applications and extend the whole network lifetime, when sensor power can be put on/off periodically. Thus, it is appropriate to take into account the node availability rate p in our analysis. Each sensor node can decide whether to become active with probability p or to move to the sleep mode with probability $1 - p$ which means to be off in every sensing period. Thus, the sensing model probability that exactly k sensor nodes detect an intruder is given by the formula

$$P(n = k) = \frac{(Sp\lambda)^k}{k!} e^{(-Sp\lambda)}, \quad (25)$$

where S is the surface swept by intruder following a trajectory l and $\lambda = \sum_{i=1}^{m}(n_i/S_i)$ is the sum of the partial densities. Consider

$$S = 2R_{\text{SENS}}l + \pi R_{\text{SENS}}^2. \quad (26)$$

The intrusion distance l can be derived as an arc length of a parametric curve:

$$l = \int_a^b \sqrt{(f'(x))^2 + (g'(x))^2}dx. \quad (27)$$

In the single-sensing, the probability that an intruder can be detected without exceeding the threshold distance l_{THR} in homogeneous WSNs of node density λ, sensing range R_{SENS}, and node availability p is determined by

$$P(n \geq 1, 0 \leq l < l_{\text{THR}}) = 1 - e^{-(2R_{\text{SENS}}l_{\text{THR}} + \pi R_{\text{SENS}}^2)p\lambda}. \quad (28)$$

In the multi-sensing, the probability P that an intruder can be detected within threshold intrusion distance l_{THR} in k-sensing in homogeneous WSNs of node density λ, sensing range R_{SENS}, and node availability p is determined by

$$P(n \geq k, 0 \leq l < l_{\text{THR}}) = 1 - \sum_{i=0}^{k-1}\frac{(Sp\lambda)^i}{i!}e^{-Sp\lambda},$$
$$S = 2R_{\text{SENS}}l_{\text{THR}} + \pi R_{\text{SENS}}^2. \quad (29)$$

4. Discussions Results

In this section, we evaluate our intrusion detection model probability in a homogeneous wireless sensor network by using MATLAB software. According to the intrusion scenario as described in Section 2, we evaluate our model probability in single-sensing and multi-sensing intrusion detection in terms of sensing range, node density, and intrusion distance. We consider a random wireless sensor network composed of N static sensor nodes, which are independent and distributed uniformly in a square field.

The results illustrated in Figure 4 show the intrusion detection probability P and that there is at least one sensor node, which detects an intruder in surface area A: $A = 100 \times 100\,\text{m}^2$ versus $A = 200 \times 200\,\text{m}^2$; it is determined by the node number N and the sensing range R_{SENS}. Intrusion detection may need a large sensing range or a high node number, thus increasing the WSN deployment cost. We can note that if we increase the node number N or the sensing range R_{SENS}, the probability to cover an intrusion which happens in the network increases too. This is because the increase of sensing range or node number significantly enhances the network coverage. However, increasing more N or R_{SENS} the probability attend 1 and remains constant, will not affect the robustness of detection. Consequently, for a given value of sensing range R_{SENS}, we can find the optimal node number which can be deployed to cover efficiently the controlled region. This node number and sensing range will be the optimal values, which must be used to totally cover an area of interest.

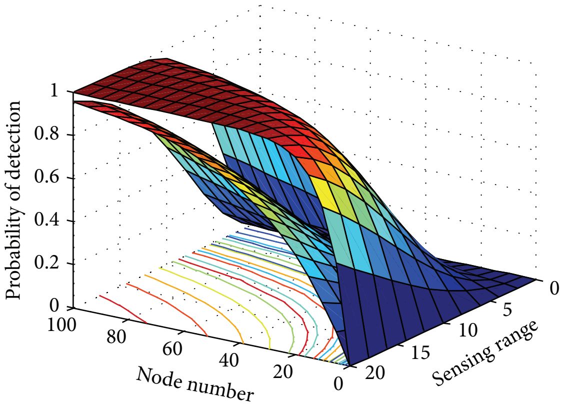


FIGURE 4: Intrusion detection probability that there is at least one node which detects an intruder, as a function of node number N and sensing range R_{SENS} in surface area A: $A = 100 \times 100\,\text{m}^2$ versus $A = 200 \times 200\,\text{m}^2$.

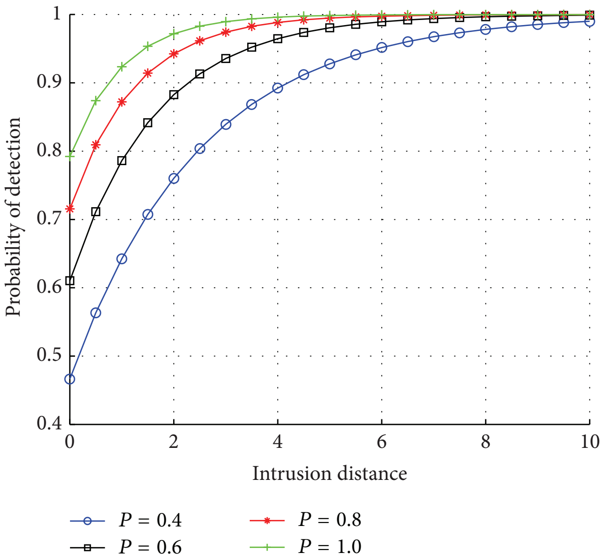


FIGURE 5: Intrusion detection probability as a function of the intrusion distance for different values of node availability.

Figure 5 shows the curves of intrusion detection probability model as a function of the intrusion distance for different values of node availability rate p. It is obvious that if the intrusion distance l increases, the detection probability P increases too. In the normal cycle, the node availability p is usually less than 1.0; it is considered to be satisfied to monitor an area as much as possible without diminishing the overall field coverage. If an intruder is detected by a node, an alarming message is broadcasting over the entire network, to improve the detection efficiency by assuring the network connectivity; it is illustrated by node availability rate $p = 1.0$.

We plot in Figure 6 the detection probability in multi-sensing detection as a function of intrusion distance. The detection probability increases with the increase of the intrusion distance. At the same time, the single-sensing detection probability ($k = 1$) is higher than that of multi-sensing

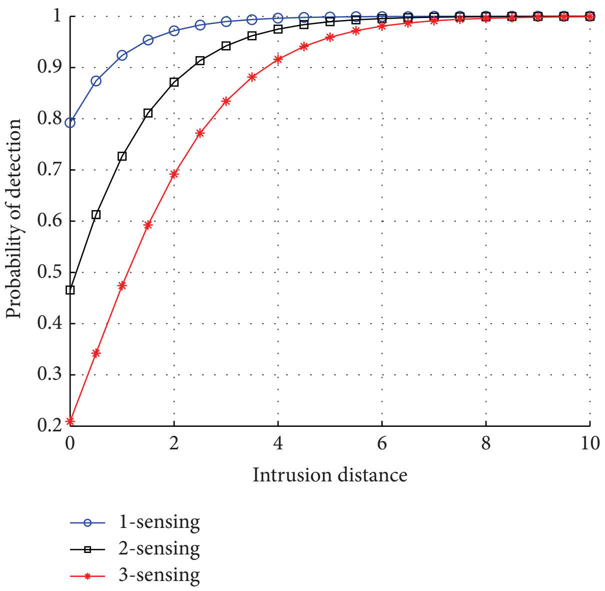


FIGURE 6: Single-sensing detection probability versus multi-sensing detection probability.

detection ($k = 2$ and $k = 3$). This is because the multi-sensing detection imposes a more strict requirement on detecting an intruder in the network; at least $k = 2$ ($k = 3$) sensors are required.

5. Conclusion

In this paper, we have investigated the fundamental characteristics for a random deployment of sensor nodes on the surveillance WSN applications, such as detecting an unauthorized intruder in a field of interest. Intrusion detection model is proposed to address the problem of network coverage and enhance the deployment quality. Therefore, each point of the sensor network is within the sensing range of at least one sensor node. We developed a probabilistic model, by deriving analytical expressions to characterize the topological properties of network coverage, designing and analysing the intrusion detection probability in a homogeneous wireless sensor network, and taking into account the various parameters such as sensing range, node density, node availability, and intrusion distance. We investigate our model for intrusion detection in WSNs to single/multi-sensing detection. Our results enable us to design and analyse the homogeneous WSNs and help us to select the critical parameters of network in order to meet the WSN application requirements.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

References

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “Wireless sensor networks: a survey,” *Computer Networks*, vol. 38, no. 4, pp. 393–422, 2002.

[2] R. Mulligan and H. M. Ammari, “Coverage in wireless sensor networks: a survey,” *Network Protocols and Algorithms*, vol. 2, no. 2, pp. 27–53, 2010.

[3] V. Ravelomanana, “Extremal properties of three-dimensional sensor networks with applications,” *IEEE Transactions on Mobile Computing*, vol. 3, no. 3, pp. 246–257, 2004.

[4] E. Onur, C. Ersoy, and H. Deliç, “How many sensors for an acceptable breach detection probability?” *Computer Communications*, vol. 29, no. 2, pp. 173–182, 2006.

[5] C. Gui and P. Mohapatra, “Power conservation and quality of surveillance in target tracking sensor networks,” in *Proceedings of the 10th Annual International Conference on Mobile Computing and Networking (MobiCom ’04)*, pp. 129–143, ACM, October 2004.

[6] H. Gupta, Z. Zhou, S. R. Das, and Q. Gu, “Connected sensor cover: self-organization of sensor networks for efficient query execution,” *IEEE/ACM Transactions on Networking*, vol. 14, no. 1, pp. 55–67, 2006.

[7] G. Xing, X. Wang, Y. Zhang, C. Lu, R. Pless, and C. Gill, “Integrated coverage and connectivity configuration for energy conservation in sensor networks,” *ACM Transactions on Sensor Networks*, vol. 1, no. 1, pp. 36–72, 2005.

[8] J. Li, L. L. H. Andrew, C. H. Foh, M. Zukerman, and H.-H. Chen, “Connectivity, coverage and placement in wireless sensor networks,” *Sensors*, vol. 9, no. 10, pp. 7664–7693, 2009.

[9] S. Kumar, T. H. Lai, and J. Balogh, “On k-coverage in a mostly sleeping sensor network,” in *Proceedings of the 10th Annual International Conference on Mobile Computing and Networking (MobiCom ’04)*, pp. 144–158, ACM, October 2004.

[10] C.-F. Huang and Y.-C. Tseng, “The coverage problem in a wireless sensor network,” *Mobile Networks and Applications*, vol. 10, no. 4, pp. 519–528, 2005.

[11] Y. Wang, “Topology control for wireless sensor networks,” in *Wireless Sensor Networks and Applications*, pp. 113–147, Springer, Berlin, Germany, 2008.

[12] C.-Y. Chong and S. P. Kumar, “Sensor networks: evolution, opportunities, and challenges,” *Proceedings of the IEEE*, vol. 91, no. 8, pp. 1247–1256, 2003.

[13] J. Jia, X. Wu, J. Chen, and X. Wang, “Exploiting sensor redistribution for eliminating the energy hole problem in mobile sensor networks,” *EURASIP Journal on Wireless Communications and Networking*, vol. 2012, article 68, 2012.

[14] H. Zhang and J. C. Hou, “Maintaining sensing coverage and connectivity in large sensor networks,” *Ad Hoc & Sensor Wireless Networks*, vol. 1, no. 1-2, pp. 89–124, 2005.

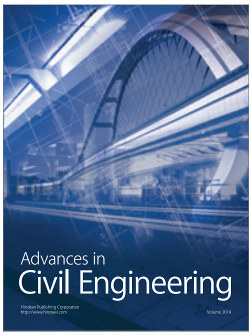
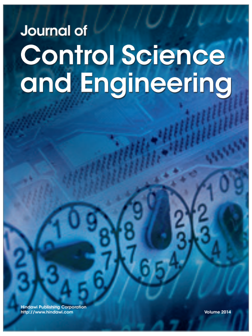
[15] B. Liu and D. Towsley, “A study of the coverage of large-scale sensor networks,” in *Proceedings of the IEEE International Conference on Mobile Ad-Hoc and Sensor Systems*, pp. 475–483, IEEE, October 2004.

Journal of
Engineering

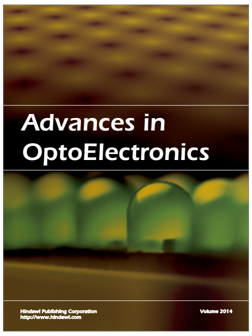
The Scientific World Journal

International Journal of
Rotating Machinery

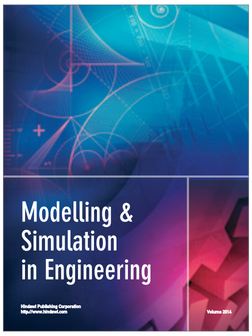
Journal of
Sensors

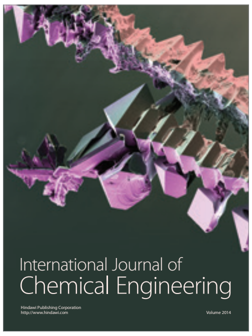
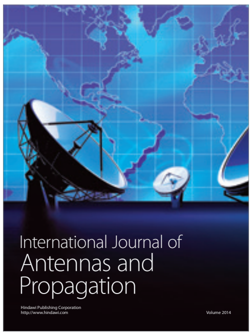
International Journal of
Distributed Sensor Networks

Advances in
Civil Engineering

Journal of
Control Science and Engineering

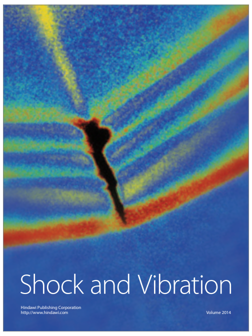
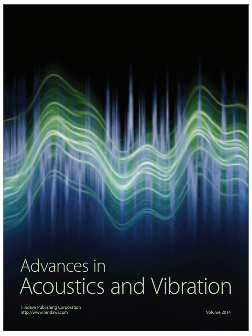
Journal of
Robotics

Journal of
Electrical and Computer Engineering

Advances in
OptoElectronics

VLSI Design

International Journal of
Navigation and Observation

Modelling &
Simulation
in Engineering

International Journal of
Aerospace Engineering

International Journal of
Chemical Engineering

International Journal of
Antennas and Propagation

Active and Passive
Electronic Components

Shock and Vibration

Advances in
Acoustics and Vibration