Intrusion Detection in Gaussian Distributed Wireless Sensor Networks

Yun Wang
Department of Computer Science
Southern Illinois University Edwardsville
Edwardsville, USA
Email: yuwang@siue.edu

Weihuang Fu and Dharma P. Agrawal
Department of Computer Science
University of Cincinnati
Cincinnati, USA
{fuwg, dpa}@email.uc.edu

Abstract

Intrusion detection in a Wireless Sensor Network (WSN) is of significant importance in many applications to detect malicious or unexpected intruder(s). The intruder can be an enemy in a battlefield, or a unusual environmental change in a chemical industry etc. With uniform distribution, the detection probability is the same for any point in a WSN. However, some applications may require different degrees of detection probability at different locations in the deployment area. Gaussian distributed WSNs (i.e., normal distribution) can provide differentiated detection capabilities at different locations and are widely deployed in practice. In view of this, this paper analyzes the problem of intrusion detection in a Gaussian distributed WSN, by characterizing intrusion detection probability with respect to intrusion distance and network deployment parameters. Two detection models are considered: single-sensing detection and multiple-sensing detection. Effects of different network parameters on the intrusion detection probability are examined in details. This work allows us to analytically formulate the intrusion detection probability within a certain intrusion distance under various application scenarios, therefore provides insight for directing the application-specific WSN deployment such as intrusion detection.

Keywords: Gaussian distribution, Intrusion detection, Network deployment, Sensing range, Wireless sensor networks

1. Introduction

A large number of wireless sensors can be deployed in an ad hoc fashion to form a Wireless Sensor Network (WSN) for many civil and military applications (e.g., intrusion detection), without relying on any underlying infrastructure support [1], [2], [3]. Intrusion detection (i.e., object tracking) in a WSN can be regarded as a monitoring system for detecting an intruder that is invading the network domain [4], [5], [6], [7]. Fig. 1 gives an example that a number of sensors are deployed in a circular area ($A = \pi R^2$) for protecting the central-located target by sensing and detecting the presence of a moving intruder. The intrusion detection application concerns how fast or how efficient the intruder can be detected by the WSN. Obviously, the sooner the intruder can be detected, the better the intrusion detection capability the WSN offers. In the extreme, the intruder can be detected immediately once it enters a WSN, if the WSN is densely deployed with a large number of sensors, and can almost provide full sensing coverage, and hence immediate detection in which intruder can be detected right away when it enters the WSN. However, full sensing coverage leads to undesirable or unacceptable demand on the network investment, and can hardly be applied or guaranteed in most WSN applications. Therefore, most WSN applications such as intrusion detection usually do not have such a strict requirement of immediate detection. Instead, they specify a maximum allowable intrusion distance and require that the intruder should be detected within the pre-defined distance [4]. As illustrated in Fig. 1, the intrusion distance is referred as D and defined as *the distance between the point the intruder enters the WSN and the point the intruder is first detected by the WSN system* [8]. It is with no doubt that this distance is of central interest to a WSN engaged in intrusion detection.

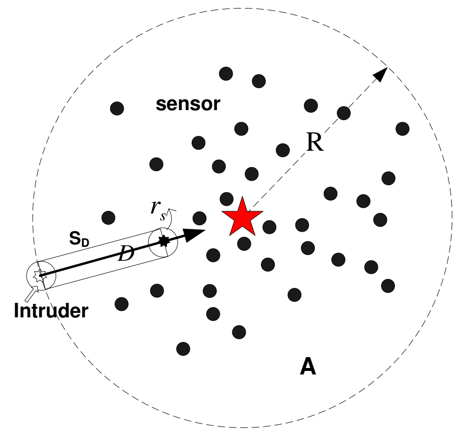

Figure 1. Intrusion strategy model

In [4], the authors analyzed the problem of intrusion detection in uniformly deployed WSNs following Poisson distribution. With uniform sensor distribution, the in-

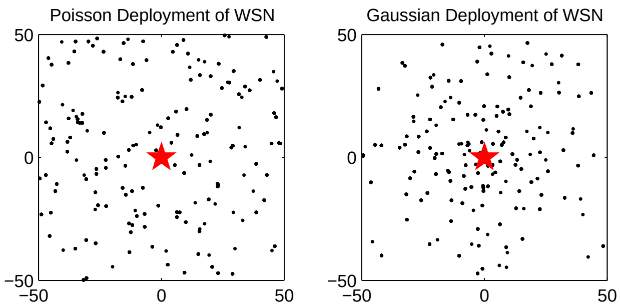

Figure 2. WSN deployments following Poisson and Gaussian Distribution

trusion detection probability is the same for any point in a WSN. The expected intrusion distance is $E(D) = \int_0^{\sqrt{2}L} 2\xi\lambda r_s e^{-\lambda(2\xi r_s + \frac{\pi r_s{}^2}{2})} d(\xi)$, where λ is the uniform node density, r_s is the sensor's sensing range, and L is the side length of the WSN deployment area. This work provides systematical and complete insight for deploying WSNs for intrusion detection, especially when the intruder can only approach the network from the boundary. However, if the intruder can enter the network from an arbitrary point, the uniform WSN deployment can cause an inherent and serious problem. Say, the intruder is dropped from an airplane and arrives at a position $P = (x_p, y_p)$ in the WSN, and the distance between P and the target point $T = (x_t, y_t)$ is less than the expected intrusion distance, i.e., $\sqrt{(x_i - x_t)^2 + (y_i - y_t)^2} \leq E(D)$. In this case, the target can be attacked no matter how large the area of the uniform WSN being deployed. In addition, many intrusion detection applications in WSNs require different degrees of intrusion detection capability at different locations. The system may require extremely high detection capability with densely deployed sensors at certain sensitive areas (e.g., areas close to an important fort in a battlefield). For some not-so-sensitive areas (e.g., the areas comparatively far away from the important fort in a battlefield), relatively low detection capability with sparsely deployed sensors is acceptable. This kind of network configuration is even necessary for reducing the number of deployed sensors in order to decrease the overall WSN deployment cost. Uniform sensor deployment can not fulfill such requirements.

Fortunately, WSNs with Gaussian distributed sensors can provide differentiated node densities at different locations, and are widely deployed in practice. Fig. 2 illustrates two WSN deployments following Poisson and Gaussian Distribution respectively. In a Gaussian distributed WSN for intrusion detection, the closer the location to the central deployment point of T (the target to be protected), the more the sensors are deployed to provide improved intrusion detection capability. On the other hand, the further the location away from the target T, the less the sensors are deployed to provide relatively low intrusion detection capability to reduce network investment. This motivates us to analyze the intrusion detection problem in Gaussian distributed WSNs. We aim to theoretically and experimentally capture the intrusion detection capability in term of intrusion detection probability by considering different network settings in Gaussian-distributed WSNs. It is to provide guidelines in directing WSN deployments for satisfying different detection requirements at different locations for the sake of intrusion detection.

The rest of this paper is organized as follows: Section 2 describes the system model. Section 3 examines the intrusion detection probability in single-sensing and multiple-sensing detection cases. Section 4 illustrates and explains both the theoretical and simulation results. Section 5 presents some related works. Finally, the paper is concluded in Section 6.

2. System Model and Definitions

The system model includes a network deployment model, a detection model, and the evaluation metrics.

2.1. Network Deployment Model

As illustrated in Fig. 1, we consider a WSN with N randomly deployed sensors. These sensors are deployed around a target point (i.e., the central red star) following a two-dimensional Gaussian distribution. All sensors are assumed to be equipped with the same sensing range r_s, and their sensing coverage is assumed to be circular and symmetrical. To be specific, each sensor is to be deployed in a pre-defined *deployment point* $G_i = (x_i, y_i)$ (i.e., the location of the target or the red star). All sensors finally reside at points around the deployment point according to a two-dimensional Gaussian distribution. The probability density function (PDF) [9] that a sensor resides at point (x, y) with respect to deployment point $G_i = (x_i, y_i)$ can be given by:

$$f(x, y, \sigma_x, \sigma_y | n \in G_i) = \frac{1}{2\pi\sigma_x\sigma_y} e^{-(\frac{(x-x_i)^2}{2\sigma_x^2} + \frac{(y-y_i)^2}{2\sigma_y^2})}. \quad (1)$$

In this model, the center, $G_i = (x_i, y_i)$, is the location of the target to be protected by the WSN, due to the fact that the intruder may enter into the network from any direction and start from any point. σ_x and σ_y are the standard deviations for X and Y dimensions. Without loss of generality, we assume the center-point coordinate of the disk is $G = (0, 0)$. Namely, the mean of the Gaussian distribution is $(0, 0)$, and the PDF for a sensor to be deployed in location (x, y) is the following [10]:

$$f(x, y, \sigma_x, \sigma_y) = \frac{1}{2\pi\sigma_x\sigma_y} e^{-(\frac{x^2}{2\sigma_x^2} + \frac{y^2}{2\sigma_y^2})}. \quad (2)$$

If the sensor deployments in the two dimensions (i.e., X and Y dimensions) are independent and admit the Gaussian

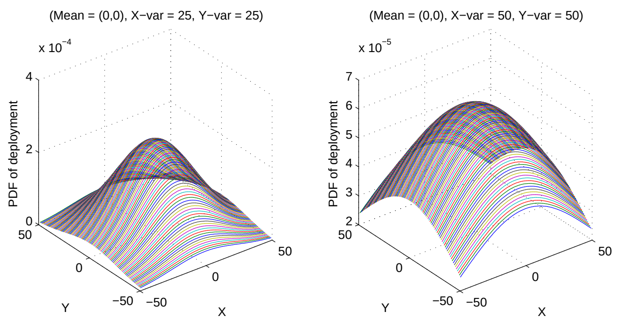

Figure 3. PDF of Gaussian deployment with equal variance in two dimensional case

distribution with the same standard deviation (i.e., $\sigma_x = \sigma_y = \sigma$). The PDF for point (x, y) to be deployed with a sensor is reduced as:

$$f(x, y, \sigma) = \frac{1}{2\pi\sigma^2} e^{-\frac{x^2+y^2}{2\sigma^2}}. \tag{3}$$

In our network model, we assume the same deployment deviation along the two dimensions (i.e., $\sigma_x = \sigma_y = \sigma$), and the case of ($\sigma_x \neq \sigma_y$) will be addressed in our follow-up work. Fig. 3 shows the PDF of sensors deployed in a two dimensional area $A = 100 * 100$ with mean deployment point $G = (0, 0)$ and deployment standard deviation $\sigma_x = \sigma_y = \sigma$. We can see that different deployment deviation leads to different sensor distribution. Furthermore, the closer the location to the center is, the higher is the probability that it can be deployed with a sensor.

Note that for simplicity of notation, $f_{xy}(\sigma)$ is referred to $f(x, y, \sigma)$ in the rest of this paper.

2.2. Detection Model

In a WSN, it has two ways to detect an intruder: *single-sensing detection* and *multiple-sensing detection* [4]. In the single-sensing detection, the intruder can be successfully detected by a single sensor, if the intruder enters the sensing range of the sensor and the sensor is powerful enough to detect such an event. On the other hand, in the multiple-sensing detection model, the intruder should be collaboratively detected by multiple sensors [11]. For example, the location of an intruder should be determined from at least three sensors' sensing information [12], [13], [14], [15].

2.3. Intrusion Strategy Model

Here, we assume that the intruder is aware of its destination (i.e., the target located in the center of the WSN), and follows the shortest path to approach the destination. In this case, the intrusion path is a straight line from the entering point toward the center of the WSN as shown in Fig. 1. Further, we assume that the intruder can enter the WSN from any point, and the starting point of the intruder is at a distance of R, a variable, to its target (i.e., the central star). The corresponding *intrusion detection area* S_D is therefore determined by the sensor's sensing range r_s and intrusion distance D as illustrated in Fig. 1. It is because the intruder can be detected within the intrusion distance D by any sensor(s) situated inside the area of S_D in its invading. Given an intrusion distance $D \geq 0$, the corresponding intrusion detection area S_D is almost an oblong area. This area includes a rectangle area S_r with length D and width $2r_s$, and two half disks S_{c1} and S_{c2} with radius r_s attached to it [4], [16]. It has:

$$S_D = S_{c2} + S_r + S_{c1} = 2 * D * r_s + \pi {r_s}^2. \tag{4}$$

For example, in single-sensing detection, at least one sensor should be located in the area of S_D for detecting the intruder before it moves in the WSN with distance D. While in multiple-sensing detection, at least k sensors should reside in area S_D for recognizing the intruder within intrusion distance D.

2.4. Evaluation metrics

In order to evaluate the quality of intrusion detection in WSNs, we define two metrics as follows [4]:

- **Intrusion Distance**: The intrusion distance, denoted by D, is the distance that the intruder travels before it is detected by a WSN for the first time. Specifically, it is the distance between the point where the intruder enters the WSN and the point where the intruder gets detected by any sensor(s). Following the definition of intrusion distance, the Maximal Intrusion Distance (denoted by ξ, $\xi > 0$) is the maximal distance allowable for the intruder to move before it is detected by the WSN.
- **Intrusion Detection Probability**: The detection probability is defined as the probability that an intruder is detected within a certain intrusion distance (e.g, Maximal Intrusion Distance ξ) specified by a WSN application.

3. Intrusion Detection in a Gaussian distributed WSN

In this section, we analyze intrusion detection in a Gaussian distributed WSN. We derive the detection probability both for single-sensing and k-sensing detection scenarios.

3.1. Single-sensing Detection

In the single-sensing detection model, the intruder can be detected efficiently if it moves into the sensing range of any sensor(s), i.e., one sensor's sensing information is enough to detect the intruder. Of course, the more the merrier.

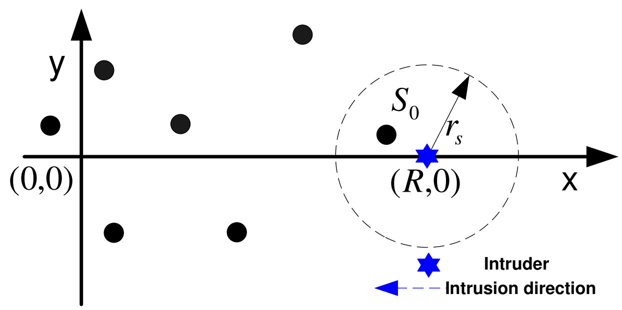

Figure 4. Intrusion detection in a Gaussian distributed WSN with single-sensing detection ($D = 0$)

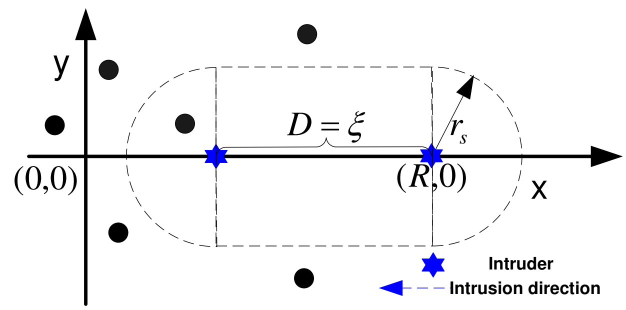

Figure 5. Intrusion detection in a Gaussian distributed WSN with single-sensing detection ($D = \xi$)

Further, based on the intrusion strategy model, the intruder is detected if and only if there exists at least one sensor within the intrusion detection area S_D with respect to the intrusion distance D. Otherwise, the intruder can not be detected by the WSN.

Here, we first examine the detection probability that the intruder can be detected immediately once it enters the network domain at a distance of R from its target. If this is the case, the intruder has intrusion distance $D = 0$. The corresponding intrusion detection area is $S_0 = 2 * D * r_s + \pi {r_s}^2 = \pi {r_s}^2$. This leads to Theorem I as follows:

Theorem I. *Given a Gaussian distributed WSN with N homogeneous deployed sensors of identical sensing range r_s, mean deployment point $(0, 0)$, and standard deployment deviation $\sigma_x = \sigma_y = \sigma$. Let $P_1[D = 0]$ be the probability that, an intruder which enters the network at a distance R to the deployment point $(0, 0)$, can be immediately detected under single-sensing detection model. $P_1[D = 0]$ can be given by:*

$$P_1[D=0] = 1 - \{1 - \int_{R-rs}^{R+r_s} \int_{-\sqrt{r_s^2-(x-R)^2}}^{\sqrt{r_s^2-(x-R)^2}} f_{xy}(\sigma)dydx\}^N. \quad (5)$$

***Proof*:**

In order to analyze the intrusion detection probability in a Gaussian distributed WSN, we build a Cartesian coordinate system as illustrated in Fig. 4 based on the network model. Without loss of generality, $(0, 0)$ is set as the location of the target (i.e., the center of the circular network), and $(R, 0)$ is the starting position of the intruder. The intruder is invading toward the target along the x-axis. Note that the intruder can enter the network from any point in the circle with distance R from its target. Once the starting point is set, the corresponding Cartesian coordinate system can be built accordingly.

Based the Cartesian coordinate system, the probability that a sensor is present in the area $S_0 = \pi r_s^2$ can be represented by the following equation:

$$p_1 = \int_{R-rs}^{R+r_s} \int_{-\sqrt{r_s^2-(x-R)^2}}^{\sqrt{r_s^2-(x-R)^2}} f_{xy}(\sigma)dydx. \quad (6)$$

Under single-sensing detection scenarios, at least one sensor should be located in the area S_0 for immediate detection. The probability that there is no sensor located in the area S_0 is $P(0, S_0) = (1 - p_1)^N$. Then, the complement of $P(0, S_0)$ is the probability that there is at least one sensor located in the area S_0 and can be given as: $1 - (1 - p_1)^N$. In this case, the intruder can be detected once it enters the network with intrusion distance $D = 0$. Thus, the probability that the intruder can be detected immediately by the given Gaussian distributed WSN is $P_1[D = 0] = 1 - (1 - p_1)^N = 1 - \{1 - \int_{R-rs}^{R+r_s} \int_{-\sqrt{r_s^2-(x-R)^2}}^{\sqrt{r_s^2-(x-R)^2}} f_{xy}(\sigma)dydx\}^N$.

$\square$

Based on the above derivation, it is clear that to provide immediate detection of an intruder in a Gaussian-distributed WSN, we need to deploy more sensors N, or enlarge the sensor's sensing range r_s using more expensive and powerful sensors. Either way increases the WSN deployment cost, and it therefore is imperative to explore the intrusion detection problem in a relaxed condition when the intruder is allowed to travel pre-specified distance in the WSN.

Theorem II. *Suppose ξ is the maximal intrusion distance allowable for intrusion detection in a given application, and the intruder starts at a distance of R from its target. Let $P_1[D \leq \xi]$ be the probability that the intruder can be detected within the maximal allowable intrusion distance ξ under single-sensing detection model in a given Gaussian distributed WSN with N homogeneous deployed sensors of identical sensing range r_s, mean deployment point $(0, 0)$, and standard deployment deviation $\sigma_x = \sigma_y = \sigma$. $P_1[D \leq$*

$\xi]$ *can be derived as:*

$$\begin{aligned} P_1[D \leq \xi] &= 1-\{1-\int_{R-\xi}^{R}\int_{-r_s}^{r_s} f_{xy}(\sigma)dydx \\ &- \int_{R-\xi-r_s}^{R-\xi}\int_{-\sqrt{r_s^2-(x-R+\xi)^2}}^{\sqrt{r_s^2-(x-R+\xi)^2}} f_{xy}(\sigma)dydx \\ &- \int_{R}^{R+r_s}\int_{-\sqrt{r_s^2-(x-R)^2}}^{\sqrt{r_s^2-(x-R)^2}} f_{xy}(\sigma)dydx\}^N. \end{aligned} \quad (7)$$

***Proof*:** For simplicity of analysis, we also build a Cartesian coordinate system as illustrated in Fig. 5, the origin $(0,0)$ is the location of the target, and $(R,0)$ is the starting position of the intruder. The intruder is invading toward the target along the x-axis. In order for the intruder to be detected within maximal intrusion distance ξ in single-sensing detection, there should be at least one sensor located in the corresponding intrusion detection area $S_\xi = S_{c1} + S_r + S_{c2} = \frac{\pi r_s^2}{2} + 2\xi r_s + \frac{\pi r_s^2}{2} = 2\xi r_s + \pi r_s^2$.

Let p_r be the probability that a sensor deployed in the rectangle area $S_r = 2\xi r_s$, p_{c1} be the probability that a sensor resides in the left half disk $S_{c1} = \frac{\pi r_s^2}{2}$, and p_{c2} be the probability that a sensor resides in the right half disk $S_{c2} = \frac{\pi r_s^2}{2}$.

Based on the given Gaussian distributed WSN, p_r can be derived as:

$$p_r = \int_{R-\xi}^{R}\int_{-r_s}^{r_s} f_{xy}(\sigma)dydx, \quad (8)$$

where $R-\xi < x \leq R$.

p_{c1} can be calculated as:

$$p_{c1} = \int_{R-\xi-r_s}^{R-\xi}\int_{-\sqrt{r_s^2-(x-R+\xi)^2}}^{\sqrt{r_s^2-(x-R+\xi)^2}} f_{xy}(\sigma)dydx, \quad (9)$$

where $R-\xi-r_s < x < R-\xi$.

p_{c2} can be given by:

$$p_{c2} = \int_{R}^{R+r_s}\int_{-\sqrt{r_s^2-(x-R)^2}}^{\sqrt{r_s^2-(x-R)^2}} f_{xy}(\sigma)dydx, \quad (10)$$

where $R < x < R+\xi$.

Then, the probability p_ξ that a sensor is deployed in the intrusion detection area S_ξ with respect to the maximal intrusion distance ξ, can be computed as:

$$p_\xi = p_{c1} + p_r + p_{c2}. \quad (11)$$

Note that the probability the intruder can be detected within the maximal intrusion distance ξ, is equivalent to the probability that there is at least one sensor located in the corresponding intrusion detection area S_ξ. The probability that there is no sensor located in the area S_ξ is $(1-p_\xi)^N$. Thus, the probability that there is at least one sensor locating in the area S_ξ can be derived as: $P_1[D \leq \xi] = 1-(1-p_\xi)^N = 1-\{1-\int_{R-\xi}^{R}\int_{-r_s}^{r_s} f_{xy}(\sigma)dydx - \int_{R-\xi-r_s}^{R-\xi}\int_{-\sqrt{r_s^2-(x-R+\xi)^2}}^{\sqrt{r_s^2-(x-R+\xi)^2}} f_{xy}(\sigma)dydx - \int_{R}^{R+r_s}\int_{-\sqrt{r_s^2-(x-R)^2}}^{\sqrt{r_s^2-(x-R)^2}} f_{xy}(\sigma)dydx\}^N$. In this case, the intruder can be detected within the maximal intrusion distance ξ with probability $P_1[D \leq \xi]$ in the given Gaussian distributed WSN.

□

3.2. Multiple-sensing Detection

In the k-sensing detection model, an intruder has to be sensed by at least k sensors for intrusion detection in a WSN. The number of required sensors depends on specific applications [4]. For example, at least three sensors' sensing information is required to determine the location of the intruder [15].

Theorem III. *Given a Gaussian distributed WSN with N homogeneous deployed sensors of identical sensing range r_s, mean deployment point $(0,0)$, and standard deployment deviation $\sigma_x = \sigma_y = \sigma$. Let $P_k[D=0]$ be the probability that, an intruder which enters the network at a distance R from the deployment point $(0,0)$, can be immediately detected under k-sensing detection model. $P_k[D=0]$ is given by:*

$$P_k[D=0] = 1-\sum_{i=0}^{k-1}\binom{n}{k}(1-p_1)^{(N-i)} * p_1^i, \quad (12)$$

where $p_1 = \int_{R-rs}^{R+r_s}\int_{-\sqrt{r_s^2-(x-R)^2}}^{\sqrt{r_s^2-(x-R)^2}} f_{xy}(\sigma)dydx$.

Proof: As illustrated in Fig. 4, in order for the intruder to be detected immediately once it enters the WSN under k-sensing detection model, at least k sensors should be located in the immediate detection area of $S_0 = \pi r_s^2$. From Eq. 6, $p_1 = \int_{R-rs}^{R+r_s}\int_{-\sqrt{r_s^2-(x-R)^2}}^{\sqrt{r_s^2-(x-R)^2}} f_{xy}(\sigma)dydx$ is the probability that a sensor is deployed in the area of S_0 according to the given Gaussian distribution. Then, $(1-p_1)^{(N-i)} * p_1^i$ is the probability that there are i sensors deployed in the area S_0. Since these i sensors could be any combination of the N deployed sensors, $\binom{n}{k}(1-p_1)^{(N-i)} * p_1^i$ is the probability that there are exactly i sensors deployed in the immediate intrusion detection area S_0. Therefore, the probability that *less than* k sensors located in the area of S_0 can be computed as $\sum_{i=0}^{k-1}\binom{n}{k}(1-p_1)^{(N-i)} * p_1^i$. Further, the probability that there are *at least* k sensors located in the area of S_0 can be derived as: $P_k[D=0] = 1-\sum_{i=0}^{k-1}\binom{n}{k}(1-p_1)^{(N-i)} * p_1^i$ in the given Gaussian distributed WSN.

Based on the above derivation and the requirement of having at least k sensors to sense the intruder for successful detection in k-sensing detection case, we can obtain the probability that an intruder is detected immediately once it enters the given Gaussian distributed WSN, i.e., $P_k[D = 0] = 1 - \sum_{i=0}^{k-1} \binom{n}{k}(1 - p_1)^{(N-i)} * p_1^i$, where $p_1 = \int_{R-rs}^{R+r_s} \int_{-\sqrt{r_s^2-(x-R)^2}}^{\sqrt{r_s^2-(x-R)^2}} f_{xy}(\sigma)dydx$. In other word, the intruder can be detected by k sensors once it enters the WSN with probability $P_k[D = 0]$.

□

Theorem IV. *Suppose ξ is the maximal intrusion distance allowable for a given application for intrusion detection, and the intruder starts at a distance of R from its destination, in a given Gaussian distributed WSN with N homogeneous deployed sensors of identical sensing range r_s, mean deployment point $(0, 0)$, and standard deployment deviation $\sigma_x = \sigma_y = \sigma$. Let $P_k[D \leq \xi]$ be the probability that the intruder can be detected within the maximal allowable intrusion distance ξ under k-sensing detection model. $P_k[D \leq \xi]$ can be calculated as:*

$$P_k[D \leq \xi] = 1 - \sum_{i=0}^{k-1} \binom{n}{k}(1 - p_\xi)^{(N-i)} * p_\xi^i, \tag{13}$$

where $p_\xi = \int_{R-\xi}^{R} \int_{-r_s}^{r_s} f_{xy}(\sigma)dydx + \int_{R-\xi-r_s}^{R-\xi} \int_{-\sqrt{r_s^2-(x-R+\xi)^2}}^{\sqrt{r_s^2-(x-R+\xi)^2}} f_{xy}(\sigma)dydx + \int_{R}^{R+r_s} \int_{-\sqrt{r_s^2-(x-R)^2}}^{\sqrt{r_s^2-(x-R)^2}} f_{xy}(\sigma)dydx.$

Proof: As illustrated in Fig. 5, $S_\xi = S_{c1} + S_r + S_{c2} = 2\xi r_s + \pi {r_s}^2$ 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 that need to collaborate with each other to recognize the intruder before it travels a distance of ξ in the WSN. From Eq. 8 $\sim$ 11, we know that the probability that a sensor deployed in the area of S_ξ is: $p_\xi = p_{c1} + p_r + p_{c2} = \int_{R-\xi}^{R} \int_{-r_s}^{r_s} f_{xy}(\sigma)dydx + \int_{R-\xi-r_s}^{R-\xi} \int_{-\sqrt{r_s^2-(x-R+\xi)^2}}^{\sqrt{r_s^2-(x-R+\xi)^2}} f_{xy}(\sigma)dydx + \int_{R}^{R+r_s} \int_{-\sqrt{r_s^2-(x-R)^2}}^{\sqrt{r_s^2-(x-R)^2}} f_{xy}(\sigma)dydx$. Then, $(1-p_\xi)^{(N-i)} * p_\xi^i$ is the probability that i sensors are deployed in the area of S_ξ. Again, these i sensors could be any combination of the deployed N sensors, $\binom{n}{k}(1 - p_\xi)^{(N-i)} * p_\xi^i$ is therefore the probability that there are exactly i sensors located in the area of S_ξ. Furthermore, $\sum_{i=0}^{k-1} \binom{n}{k}(1-p_\xi)^{(N-i)} * p_\xi^i$ is the probability that there are *less than* k sensors located in the intrusion detection area S_ξ with respect to ξ.

Therefore, the probability that there are *at least* k sensors located in the area S_ξ can be derived as the complement of $\sum_{i=0}^{k-1} \binom{n}{k}(1 - p_\xi)^{(N-i)} * p_\xi^i$, i.e., $1 - \sum_{i=0}^{k-1} \binom{n}{k}(1 - p_\xi)^{(N-k+i)} * p_\xi^i$. If this is the case, the intruder can be sensed by at least k sensors from the WSN with probability $1 - \sum_{i=0}^{k-1} \binom{n}{k}(1 - p_\xi)^{(N-i)} * p_\xi^i$ before it travels a distance of ξ. Finally, the probability $P_k[D \leq \xi]$, that the intruder is detected with the maximal intrusion distance ξ in k-sensing detection model, can be derived as: $P_k[D \leq \xi] = 1 - \sum_{i=0}^{k-1} \binom{n}{k}(1 - p_\xi)^{(N-i)} * p_\xi^i$, where $p_\xi = \int_{R-\xi}^{R} \int_{-r_s}^{r_s} f_{xy}(\sigma)dydx + \int_{R-\xi-r_s}^{R-\xi} \int_{-\sqrt{r_s^2-(x-R+\xi)^2}}^{\sqrt{r_s^2-(x-R+\xi)^2}} f_{xy}(\sigma)dydx + \int_{R}^{R+r_s} \int_{-\sqrt{r_s^2-(x-R)^2}}^{\sqrt{r_s^2-(x-R)^2}} f_{xy}(\sigma)dydx.$

□

The results in single-sensing and multiple-sensing detection cases indicate that intrusion detection probability in a given Gaussian distributed WSN is determined by the network deployment parameters including number of deployed sensors N, sensing range r_s, intruder's starting point R, deployment deviation σ, and maximal allowable intrusion distance ξ. Intuitively, enlarging the sensing range or the number of deployed sensors, the intrusion detection probability can be improved. Further, the deployment deviation affects the intrusion detection probability. We will analyze them in details in the following discussion.

4. Theoritcal Analysis and Simulation Verification

In this section, we examine the effect of various network deployment parameters on the intrusion detection probability under both single-sensing detection and multiple-sensing detection cases in a Gaussian distributed WSN in MATLAB $R2007a$. Then we validate the correctness of our proposed model and analysis by extensive simulations, based on a WSN simulator developed in C++. The simulation results match very well with the analytical results.

4.1. Effect of Number of Deployed Sensors N

In order to analyze the effect of number of deployed sensors on the intrusion detection probability in a Gaussian distributed WSN, we set deployment point, intruder's starting point, the deployment standard deviation, the sensing range, and the maximal intrusion distance as $G = (0, 0)$, $R = 80$, $\sigma = 25$, and $D_{max} = \xi = 30$ respectively. Unless otherwise specified, the deployment point is set as $G = (0, 0)$.

Fig. 6 shows the detection probability in both single-sensing (marked as '1-sensing') and multiple-sensing (marked as '3-sensing') detection model, with varying number of deployed sensors. From the figure, the detection probabilities in all the cases are improving with the increasing of number of deployed sensors. This is because, given intrusion distance (e.g., $D_{max} = 30$), more sensors could be deployed

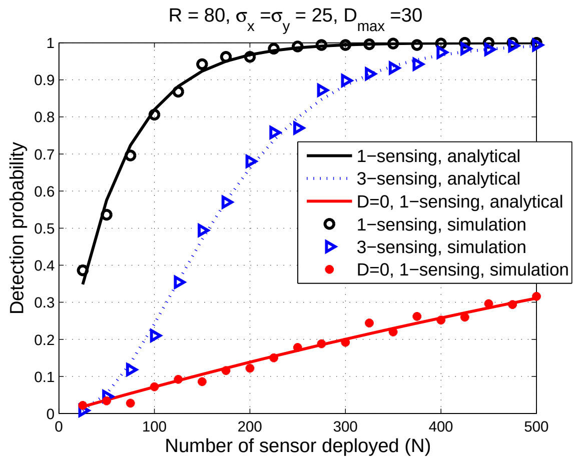

Figure 6. Effect of number of deployed sensors N on the detection probability in a Gaussian distributed WSN

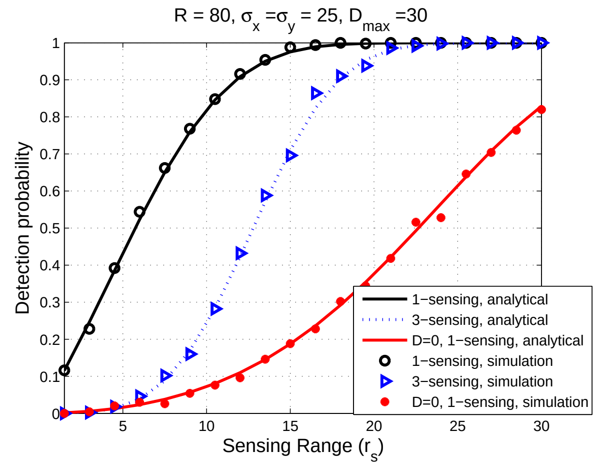

Figure 7. Effect of sensing range r_s on the detection probability in a Gaussian distributed WSN

in the corresponding intrusion detection area for detecting the intruder.

It can also be seen from Fig. 6 that the 1-sensing detection probability is much higher than that of 3-sensing detection. This is due to the fact that multiple-sensing detection imposes a more strict requirement on detecting the intruder, e.g., at least 3 sensors are required.

Note that fig. 6 also plots the immediate detection probability (i.e., $D_{max} = 0$, marked as '$D = 0$'), in contrast to the detection probability with maximal intrusion distance $D_{max} = 30$ in single-sensing detection. The results point out that the immediate detection probability is much lower than the detection probability with certain allowable intrusion distance, implying that more sensors should be deployed for immediate detection under specified detection probability. This substantiates our intuition that allowing intruder to travel some distance in the WSN can save the network deployment cost.

4.2. Effect of Sensing Range r_s

We analyze the effect of sensing range on the detection probability in a Gaussian distributed WSN, where the intruder's starting point, standard deviation, and number of deployed sensors is set as $R = 80$, $\sigma = 25$, and $N = 100$ respectively, with the maximal intrusion distance $D_{max} = \xi = 30$.

Fig. 7 depicts the intrusion detection probability in 1-sensing detection and 3-sensing detection with varying sensing range. From the figure, the intrusion detection probability increases with the increasing of the sensing range. This is because larger sensing range improves the network coverage, and higher network coverage leads to a quicker detection of the intruder in a WSN. Furthermore, under the given network parameters, the detection probability approaches 1 while the sensing range increases to a certain threshold. For example, in 1-sensing detection, the intruder can be detected with probability 1 if the sensing range exceeds 20. While in 3-sensing detection, the intruder can be detected with probability 1 if the sensing range exceeds 25. This results can be used to direct the design of network deployment and power saving schemes. For example, the sensor's sensing range can be tuned to the threshold to save sensing energy while satisfying the required QoS for intrusion detection in a WSN. We also plot the analytical and simulation results for immediate intrusion detection under single-sensing detection, given different sensing ranges, as a contrast. It is observed from the figure that under the same network deployment scenario, the detection probability for immediate detection is much lower than the case that the intruder should be detected within a pre-defined maximum allowable intrusion distance, which further validates our intuition.

4.3. Effect of Deployment Deviation σ

In a Gaussian distributed WSN with fixed deployment point (i.e., $G = (0, 0)$) and unvarying number of deployed sensors, the deployment deviation determines the node distribution and affects the performance of intrusion detection in the WSN. For the purpose of exploring the effect of the deployment deviation σ on the detection probability in a Gaussian distributed WSN, we set the intruder's starting point, number of deployed sensors, sensing range, and maximal allowable intrusion distance as $R = 80$, $N = 100$, $r_s = 20$, and $D_{max} = \xi = 30$ respectively.

Fig. 8 presents the intrusion detection probability with varying deployment deviations σ, under different network scenarios under both singe-sensing detection and multiple-sensing detection. From the figure, the detection probability improves when the deployment deviation increase from 0 to

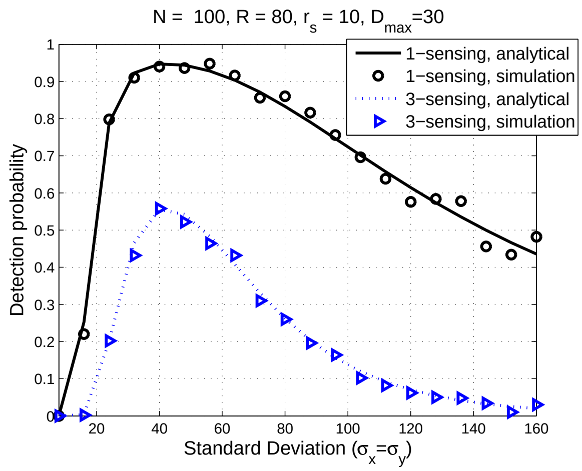

Figure 8. Effect of deployment deviation σ on the detection probability in a Gaussian distributed WSN $(D_{max} = 30)$

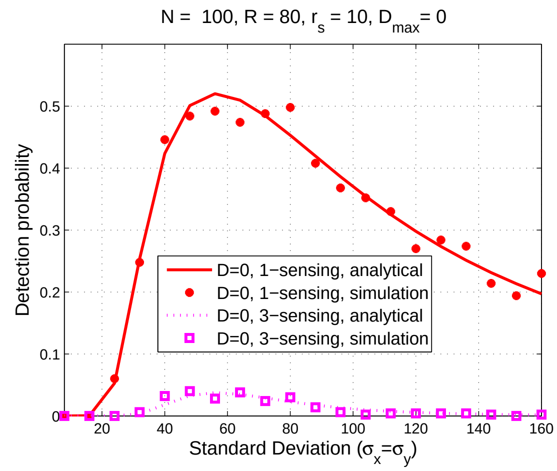

Figure 9. Effect of deployment deviation σ on the immediate detection probability in a Gaussian distributed WSN $(D_{max} = 0)$

a certain threshold, then the detection probability decreases while the deployment deviation keeps increasing. For example, in single-sensing detection, the detection probability archives its peak when the deployment deviation is set as 40. This is due to the fact that when the deployment deviation grows from 0 to the threshold, more sensors can be deployed around the starting point of the intruder to detect it sooner. However, when the deployment deviation keeps increasing from the threshold, the number of sensors deployed in the intrusion detection area around the intruder's start point is decreasing, thus reduces the detection probability.

Fig. 9 illustrates the immediate intrusion detection probability under the same network scenarios depicted in Fig. 8. Obviously, the same trend is found in Fig. 9. Specifically, the detection probability improves when the deployment deviation increase from 0 to a certain threshold, then the detection probability decreases while the deployment deviation keeps increasing. However, the threshold deviation leading to optimum immediate detection probability is different from the case that intruder can travel some distance in the network before being detected. For example, in both single-sensing and three-sensing detection, the detection probability archives its peak when the deployment deviation is equal to 55 for immediate detection, different from 40 where intruder is allowed to travel some distance shown in Fig. 8.

In a word, optimal deployment deviation can be chosen to maximize the network QoS in terms of intrusion detection in a Gaussian distributed WSN.

5. Related Works

Intrusion detection is one of the critical applications in WSNs, and has thus received considerable attention in the literature. Most of the existing work is so far devoted to the problem of intrusion detection analysis from the perspectives of network deployment and tracking protocol design [5], [16], [6], [7], [17]. The purpose of these approaches aims at effectively detecting the presence of an intruder and compressing the detection delay under the constraints of power saving and network lifetime enhancement. Dousse et al. [5] have characterized the time traveled by an intruder before the detection alarm reaches the base station. It provides the distribution of the distance traveled by a moving intruder until it comes within the sensing range of a node in a uniformly distributed sensor network according to Poisson distribution. Ren et al. [16] have examined the tradeoff between the network detection quality (i.e., how fast the intruder can be detected) and the network lifetime, and have proposed three wave sensing scheduling protocols to achieve the bounded worst-case detection probability. Liu et al. [17] have taken the node mobility into consideration and present the optimal strategy for fast detection by illustrating that a mobile WSN improves its detection quality due to mobility of sensors. However, most of the existing work on intrusion detection are based on the assumption that the sensors are uniformly deployed according to Poisson distribution. For example, Wang et al.[4] have explored the intrusion detection problem in both homogenous and heterogeneous wireless sensor networks following Poisson distribution. On the contrary, WSN deployments conforming to Gaussian distribution, i.e., Normal distribution are widely used in reality, and the corresponding analysis of intrusion detection problem has been neglected. In this paper, we address the intrusion detection problem in a Gaussian distributed WSN by providing a comprehensive theoretical and experimental analysis on intrusion detection probability, employing both single-sensing detection and multiple-sensing detection models. The detection probability is theoretically captured by using underlying network parameters, and validated by extensive simulation results. This work is paramount for network planner to design Gaussian distributed WSNs in terms of efficient intrusion detection, and provide differentiated detection probability in the deployed field.

6. Conclusion

This paper examines the intrusion detection problem in a homogenous Gaussian distributed WSNs by characterizing intrusion detection probability with respect to intrusion distance and network parameters (i.e., intruder's starting point, deployment point, deployment deviation, number of deployed sensor, and sensing range), under two detection model, i.e., single-sensing detection and multiple-sensing detection. Extensive simulations have been performed to validate the correctness of the proposed model and analysis. The proposed model for intrusion detection allows us to analytically formulate the intrusion detection probability within a certain intrusion distance under various network settings. Effects of different network parameters on the intrusion detection probability are also explored in details, to provide insights in designing Gaussian distributed WSNs and help in selecting critical network parameters, so as to meet the differentiated detection capability requirements with respect to different locations/area in WSN applications for intrusion detection.

References

[1] D. P. Agrawal and Q-A Zeng, *Introduction to Wireless and Mobile Systems*. Brooks/Cole Publishing, August 2003.

[2] J. N. Al-Karaki and A. E. Kamal, "Routing techniques in wireless sensor networks: a survey," *IEEE Wireless Communications*, vol. 11, no. 6, pp. 6–28, December 2004.

[3] S. Tilak, N. B. Abu-Ghazaleh, and W. Heinzelman, "A taxonomy of wireless micro-sensor network models," *ACM Mobile Computing and Communication Review*, vol. 6, no. 2, April 2002.

[4] Y. Wang, X. Wang, B. Xie, D. Wang, and D. P. Agrawal, "Intrusion detection in homogenous and heterogeneous wireless sensor networks," *IEEE Transactions on Mobile Computing*, vol. 7, no. 6, 2008.

[5] O. Dousse, C. Tavoularis, and P. Thiran, "Delay of intrusion detection in wireless sensor networks," in *Proceedings of the Seventh ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)*, 2006.

[6] H. Kung and D. Vlah, "Efficient location tracking using sensor networks," in *IEEE Wireless Communications and Networking Conference*, ser. 3, vol. 3, March 2003, pp. 1954–1961.

[7] C.-Y. Lin, W.-C. Peng, and Y.-C. Tseng, "Efficient in-network moving object tracking in wireless sensor networks," *IEEE Transactions on Mobile Computing*, vol. 5, no. 8, pp. 1044–1056, 2006.

[8] X. Wang, Y. Yoo, Y. Wang, and D. P. Agrawal, "Impact of node density and sensing range on intrusion detection in wireless sensor networks," in *the Fifteenth International Conference on Computer Communications and Networks (Icccn)*, October 2006.

[9] A. Leon-Garcia, *Probability and Random Processes for Electrical Engineering, 2nd Edition*. Addison-Wesley, July 1993.

[10] D. Wang, B. Xie, and D. P. Agrawal, "Coverage and lifetime optimization of wireless sensor networks with gaussian distribution," *IEEE Transactions on Mobile Computing*, 2008.

[11] S. Banerjee, C. Grosan, A. Abraham, and P. Mahanti, "Intrusion detection on sensor networks using emotional ants," *International Journal of Applied Science and Computations*, vol. 12, no. 3, pp. 152–173, 2005.

[12] S. Capkun, M. Hamdi, and J. Hubaux, "Gps-free positioning in mobile ad-hoc networks," in *Hawaii International Conference on System Sciences, HICSS-34*, 2001.

[13] N. Bulusu, J. Heidemann, and D. Estrin, "Gps-less low cost outdoor localization for very small devices," in *IEEE Personal Communications Magazine, Special Issue on Smart Spaces and Environments*, 2000.

[14] Dragos, Niculescu, and Rutgers, "positioning in ad hoc sensor networks," in *University IEEE Network*, July August 2004.

[15] Y. Wang, X. Wang, D. Wang, and D. P. Agrawal, "Localization algorithm using expected hop progress in wireless sensor networks," in *the Third IEEE International Conference on Mobile Ad hoc and Sensor Systems (Mass)*, October 2006.

[16] S. Ren, Q. Li, H. Wang, X. Chen, and X. Zhang, "Design and analysis of sensing scheduling algorithms under partial coverage for object detection in sensor networks," *IEEE Transaction on Parallel and Distributed Systems*, vol. 18, no. 3, pp. 334–350, March 2007.

[17] B. Liu, P. Brass, O. Dousse, P. Nain, and D. Towsley, "Mobility improves coverage of sensor networks," in *Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)*, 2005.