Gaussian versus Uniform Distribution for Intrusion Detection in Wireless Sensor Networks

Yun Wang, Weihuang Fu, and Dharma P. Agrawal, *Life Fellow*, *IEEE*

Abstract—In a Wireless Sensor Network (WSN), intrusion detection is of significant importance in many applications in detecting malicious or unexpected intruder(s). The intruder can be an enemy in a battlefield, or a malicious moving object in the area of interest. With uniform sensor deployment, 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. For example, an intrusion detection application may need improved detection probability around important entities. Gaussian-distributed WSNs can provide differentiated detection capabilities at different locations but related work is limited. This paper analyzes the problem of intrusion detection in a Gaussian-distributed WSN by characterizing the detection probability with respect to the application requirements and the network parameters under both single-sensing detection and multiple-sensing detection scenarios. Effects of different network parameters on the detection probability are examined in detail. Furthermore, performance of Gaussian-distributed WSNs is compared with uniformly distributed WSNs. This work allows us to analytically formulate detection probability in a random WSN and provides guidelines in selecting an appropriate deployment strategy and determining critical network parameters.

Index Terms—Gaussian distribution, intrusion detection, network deployment, uniform distribution, sensing range, wireless sensor network

1 Introduction

Due to recent technological advances in wireless communication, manufacturing of small- and low-cost sensors has become economically feasible [1], [2]. A large number of sensors can be deployed in an ad hoc fashion to form a Wireless Sensor Network (WSN) for many civil and military applications [3], [4]. Intrusion detection has received a great deal of attention since it supports various applications such as environmental monitoring and military surveillance.

Recent studies on the intrusion detection problem fall into two major categories. First, it is considered as a system component for monitoring the security of a WSN and diagnosing compromised/vulnerable sensors to ensure the correct network behavior and avoid false alarm [5], [6], [7]. On the other hand, it is defined as monitoring or surveillance system for detecting a malicious intruder that invades the network domain [8], [9], [10], [11], [12]. This work focuses on the second category. Fig. 1 gives an example in which 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. Intrusion detection implies how effectively an intruder can be detected by the WSN. Obviously, sooner the intruder can be detected, better is the intrusion detection capability of the WSN.

In the extreme, the intruder can be detected immediately after it enters the field of interest *(FoI)*, which is densely deployed with sensors and has full sensing coverage. Full sensing coverage means immediate intrusion detection. However, full sensing coverage demands for a large number of sensors and can be hardly feasible in an actual practice. Therefore, most intrusion detection applications do not have such a strict requirement of immediate detection. Instead, a maximum allowable intrusion distance (ξ) is specified. Suppose the intruder moves a distance of D in the WSN before it is detected. If $D < \xi$, the WSN meets the performance requirements. Otherwise, the WSN needs to be reconfigured. Apparently, intrusion distance is a central issue in an intrusion detection application using a WSN.

A sensor deployment strategy plays a vital role in determining the intrusion detection capability of a WSN. Random sensor deployment is usually adopted due to its fast deployment, easy scalability, fault tolerant, and can be used in a hostile and human-inaccessible region [13], [14]. Depending on specific deployment approach, a randomly deployed WSN can have uniform node density or differentiated node density in the *FoI*. To be specific, if all of the sensors are deployed randomly and uniformly, the resulting network conforms to a uniform distribution. On the other hand, if all sensors are to protect an important entity, the resulting sensor network conforms to a Gaussian distribution. Fig. 2 sketches two example WSNs following a uniform and a Gaussian distribution, respectively.

- *Y. Wang is with the Department of Computer Science and Information Systems, Bradley University, 1501 West Bradley Avenue, Peoria, IL 61625. E-mail: ywang2@fsmail.bradley.edu.*
- *W. Fu and D.P. Agrawal are with the School of Computing Sciences and Informatics, University of Cincinnati, 819D Old Chemistry, Cincinnati, OH 45221-0008. E-mail: {fuwg, agrawadp}@email.uc.edu.*

Manuscript received 9 Aug. 2011; revised 11 Jan. 2012; accepted 28 Feb. 2012; published online 20 Mar. 2012.
Recommended for acceptance by A. Kshemkalyani.
For information on obtaining reprints of this article, please send e-mail to: tpds@computer.org, and reference IEEECS Log Number TPDS-2011-08-0526.
Digital Object Identifier no. 10.1109/TPDS.2012.105.

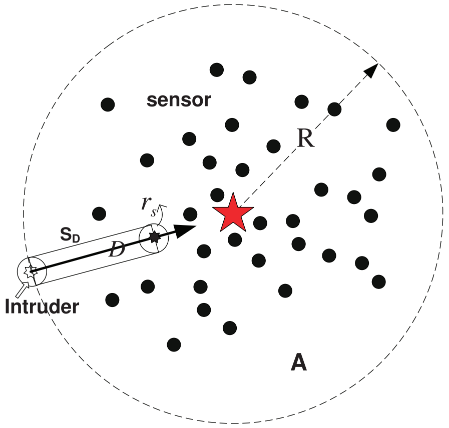

Fig. 1. Intrusion detection in a wireless sensor network.

To date, most of the related work assumes a WSN following uniform distribution for intrusion detection analysis [9], [10], [15], [11], [12], [16]. In [9], the problem of intrusion detection is analyzed in a randomly deployed WSN following a uniform distribution. The intrusion detection probability is the same for any point in the *FoI* and the expected intrusion distance is derived as: $E(D) = \int_0^{\sqrt{2}L} 2\xi\lambda r_s e^{-\lambda(2\xi r_s + \frac{\pi r_s^2}{2})} d(\xi)$, where λ is the node density, r_s is the sensor's sensing range, and L is the side length of the *FoI*. This work provides a systematic and complete insight for intrusion detection in uniformly deployed WSNs, when the intruder approaches the network from the boundary. However, if an intruder enters the network at an arbitrary point inside the *FoI*, the uniform WSN deployment can have an inherent serious problem. Suppose the intruder is dropped from an airplane at an arbitrary 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.,

$$\sqrt{(x_i - x_t)^2 + (y_i - y_t)^2} \le E(D).$$

In this case, the target can be attacked no matter how large the area of the uniform WSN is 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 hot spots (e.g., areas close to an important entity in a battlefield). For some not-so-sensitive areas, relatively sparsely deployed sensors could be acceptable. Uniform sensor deployment cannot fulfill such requirements either.

Fortunately, WSNs with Gaussian distributed sensors can provide differentiated node densities at different locations as illustrated in Fig. 2b. Different from uniformly distributed WSNs as illustrated in Fig. 2a, in a Gaussian-distributed WSN, the closer the area is to the central deployment point T (i.e., the important entity), more sensors are deployed to provide enhanced detection capability. On the other hand, fewer sensors are deployed in areas that are far away from the hot spot T, which decreases the network deployment cost as well. This makes it important to address the intrusion detection problem in a Gaussian-distributed WSN and we will establish the results from modeling, analysis, and simulation perspectives. Moreover, we extend our discussion to the truncated Gaussian WSNs. It is due to the fact that Gaussian distribution allows the placement of sensors in an *unbounded* area while most real-life WSN applications take place in a *bounded* field of interest. Truncated Gaussian distribution allows the placement of sensors in a *bounded* field and our results based on truncated Gaussian distributed sensor networks thus have significant importance in directing real-life WSN design for intrusion detection, especially for small-scale WSNs. To sum up, the main contributions of this work include

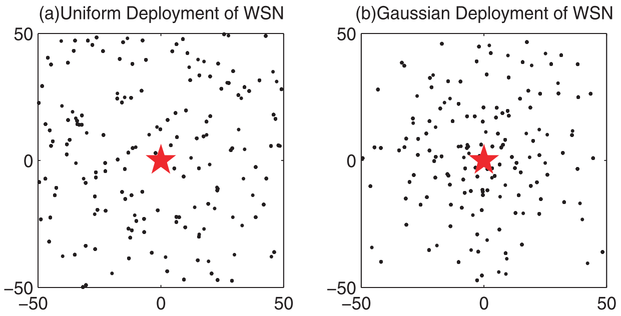

Fig. 2. WSN deployments following uniform and Gaussian distribution.

- Develop an analytical model for intrusion detection in a (truncated) Gaussian-distributed WSN, and mathematically derive detection probability with respect to various network parameters, employing both single-sensing detection and multiple-sensing detection models.
- Investigate the interplays between the network parameters and the detection capability of the (truncated) Gaussian-distributed WSN, and validate theoretical derivations and results by Monte-Carlo simulations.
- Compare the performance of intrusion detection in a WSN following uniform distribution with that of (truncated) Gaussian distribution and provide guidelines in choosing a random sensor deployment strategy and parameters.

The rest of this paper is organized as follows. Section 2 introduces the system model and definitions. Section 3 examines the intrusion detection probability in a Gaussian-distributed WSN for single-sensing and multiple-sensing detection. Section 4 illustrates and explains both the theoretical and simulation results. Section 5 compares the intrusion detection probability of a Gaussian-distributed WSN with that following a uniform distribution. Section 6 presents the related works. Finally, the paper is concluded in Section 7.

2 System Model and Definitions

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

2.1 Network Deployment Model

As illustrated in Fig. 1, we consider a WSN with randomly deployed N sensors around a target point (i.e., the central

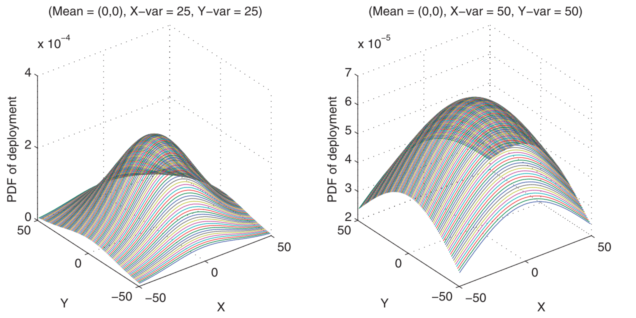

Fig. 3. PDF of Gaussian deployment with equal variance in 2D case.

red star) following a 2D Gaussian distribution. The *FoI* A is assumed to be a square area with side length L. Without loss of generality, we assume the coordinate of the target point as $G = (0, 0)$ and the same standard deviation (i.e., $\sigma_x = \sigma_y = \sigma$) along X and Y dimensions in the deployment field $(-\frac{L}{2} \leq X \leq \frac{L}{2}, -\frac{L}{2} \leq Y \leq \frac{L}{2})$. The PDF for point (x, y) to be deployed with a sensor is therefore given by [17]

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

Fig. 3 shows the PDF of sensors deployed in a 2D area $A = 100 \times 100$ with mean deployment point $G = (0, 0)$ and deployment standard deviation $\sigma = 25$ and $\sigma = 50$, respectively. We can see that different deviation leads to different sensor distribution. Furthermore, the closer the location is to the center, the higher is the probability of deploying sensors there. Note that when the standard deviation σ is increased to some extent, some sensors may be deployed outside the *FoI* A. If all sensors ought to be deployed inside A, a truncated Gaussian distribution can be used and the corresponding PDF is

$$f'(x, y, \sigma) = \frac{f(x, y, \sigma)}{\int_{-\frac{L}{2}}^{\frac{L}{2}} \int_{-\frac{L}{2}}^{\frac{L}{2}} f(x, y, \sigma) dy dx}. \tag{2}$$

Fig. 4 compares a Gaussian-distributed WSN with the corresponding truncated Gaussian-distributed WSN with $\sigma = 15$ and $\sigma = 50$, respectively. Note that when σ increases toward infinity, the truncated Gaussian distribution tends toward a uniform distribution. The methodology we develop in the following analysis can be applied to both Gaussian and truncated Gaussian-distributed WSNs by replacing $f'_{xy}(\sigma)$ with $f(x, y, \sigma)$ or $f'(x, y, \sigma)$, respectively.

2.2 Sensing and Detection Model

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 following a Boolean sensing model [18]. In a WSN, there are two ways to detect an intruder: *single-sensing detection* and *multiple-sensing detection* [9]. In single-sensing detection, the intruder can be successfully detected by a single sensor when entering its sensing range. On the other hand, in the m-sensing detection model, an intruder has to be sensed by at least m sensors and m depends on a specific application [9], [19]. Note that these m sensors need *not* sense the intruder simultaneously in the considered model.

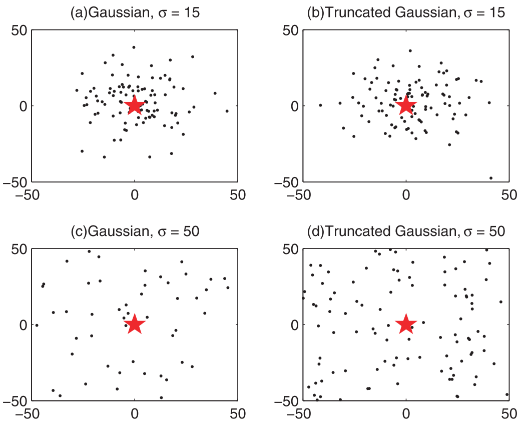

Fig. 4. Gaussian versus truncated Gaussian-distributed WSN.

2.3 Intrusion Strategy Model

The intruder is assumed to be aware of its target (i.e., the hot spot), and follows the shortest intrusion path D toward the target as shown in Fig. 1. The straight-line intrusion path model was adopted in [10], [9], [20], [21], etc. It is due to the fact that abstractions and assumptions are inevitable to conduct theoretical analysis [22] and make influencing factors tractable.

Further, we assume that the intruder can enter the WSN from an arbitrary point with distance R to the target (R is a random variable). The corresponding *intrusion detection region* S_D is indirectly determined by the sensor's sensing range r_s and intrusion distance D as in Fig. 1, and the area of S_D is given by

$$|S_D| = |S_{c1}| + |S_r| + |S_{c2}| = 2 * D * r_s + \pi {r_s}^2. \tag{3}$$

It is important to observe that in a single-sensing detection, at least one sensor should be located in the region S_D for detecting the intruder. Similarly, in multiple-sensing detection, at least m sensors should reside in the region S_D for recognizing the intruder.

2.4 Evaluation Metrics

In order to evaluate the performance of intrusion detection in a Gaussian-distributed WSN, we use the following two metrics [9], [23]:

- **Intrusion distance** D. It 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).
- **Detection probability** $P[D \leq \xi]$. It is defined as the probability that an intruder is detected within the maximal allowable intrusion distance ξ, specified by a WSN application.

To be specific, if the intruder moves less than or equal to ξ, i.e., $D \leq \xi$ before it is detected, the intrusion detection of the WSN is regarded as a successful case. Otherwise, the intrusion detection is considered as a failed one when $D > \xi$.

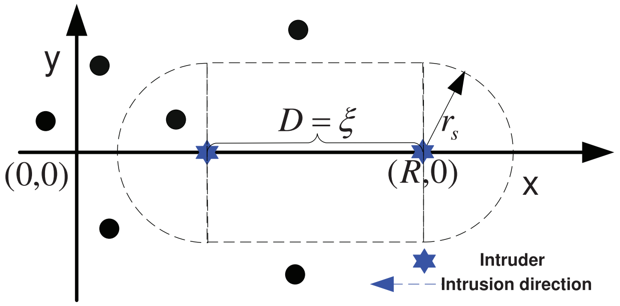

Fig. 5. Intrusion detection area in a Gaussian-distributed WSN for relaxed detection ($D = \xi$).

3 Intrusion Detection in a Gaussian-Distributed WSN

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

3.1 Single-Sensing Detection

In the single-sensing detection model, the intruder can be detected if it moves into the sensing range of any sensor, i.e., one sensor's sensing information is enough to detect the intruder if it resides in the intrusion detection region S_ξ. In the case of $\xi > 0$, the intruder is allowed to travel some distance within the WSN. It is so called *relaxed* intrusion detection. On the other hand, if $\xi = 0$, the intruder has to be detected before it can make any movement inside the WSN and is therefore referred to as *immediate* intrusion detection.

In the following theorem, we show that the intrusion detection probability under single-sensing detection model is determined by the network settings and the application requirements:

Theorem 1. *Suppose ξ ($\xi > 0$) is the maximal allowable intrusion distance for intrusion detection in a given application, and the intruder starts at a distance R to its target $(0, 0)$. Let $P_1[D \le \xi]$ be the probability that the intruder can be detected within ξ under single-sensing detection in the considered network model. $P_1[D \le \xi]$ can be derived as*

$$P_1[D \le \xi] = 1 - \Bigg\{1 - \int_{R-\xi}^{R}\int_{-r_s}^{r_s} f'_{xy}(\sigma)dydx - \int_{R-\xi-r_s}^{R-\xi}\int_{-\sqrt{r_s^2-(x-R+\xi)^2}}^{\sqrt{r_s^2-(x-R+\xi)^2}} f'_{xy}(\sigma)dydx - \int_{R}^{R+r_s}\int_{-\sqrt{r_s^2-(x-R)^2}}^{\sqrt{r_s^2-(x-R)^2}} f'_{xy}(\sigma)dydx\Bigg\}^N.$$

Proof. In order to analyze the intrusion detection probability in a (truncated) Gaussian-distributed WSN, we build a Cartesian coordinate system as illustrated in Fig. 5. Without loss of generality, $(0, 0)$ is set as the location of the target (i.e., the important entity), and $(R, 0)$ is the starting position of the intruder. The intruder is moving toward the target along the x-axis. Note that the intruder can enter the network from any point in the circle with radius R to its target $(0, 0)$. Once the starting point is set, the corresponding Cartesian coordinate system can be built accordingly.

For the intruder to be detected within distance ξ in single-sensing detection, there should be at least one sensor located in the corresponding intrusion detection region S_ξ. The area of S_ξ is given by $|S_\xi| = 2\xi r_s + \pi r_s^2$, as illustrated in Fig. 5.

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

Following the Gaussian distributed network model, p_r can be derived as

$$p_r = \int_{R-\xi}^{R}\int_{-r_s}^{r_s} f'_{xy}(\sigma)dydx, \tag{4}$$

p_{c1} can be calculated as

$$p_{c1} = \int_{R-\xi-r_s}^{R-\xi}\int_{-\sqrt{r_s^2-(x-R+\xi)^2}}^{\sqrt{r_s^2-(x-R+\xi)^2}} f'_{xy}(\sigma)dydx, \tag{5}$$

and p_{c2} can be calculated as

$$p_{c2} = \int_{R}^{R+r_s}\int_{-\sqrt{r_s^2-(x-R)^2}}^{\sqrt{r_s^2-(x-R)^2}} f'_{xy}(\sigma)dydx. \tag{6}$$

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

$$p_\xi = p_{c1} + p_r + p_{c2}. \tag{7}$$

Replacing $f'_{xy}(\sigma)$ with $f'_{xy}(x, y, \sigma)$ in p_r, p_{c1}, p_{c2} and p_ξ, we can obtain the corresponding probability that a sensor is deployed in S_r, S_{c1}, S_{c1}, and S_ξ in a truncated Gaussian-distributed WSN, respectively.

In the given network model, a number of N sensors are deployed. Then, the probability that there is no sensor located in the intrusion detection region S_ξ is calculated as $(1 - p_\xi)^N$. Hence, the probability that there is at least one sensor located in the region S_ξ can be derived as $1 - (1 - p_\xi)^N$.

The probability that the intruder can be detected within ξ is equivalent to the probability that there is at least one sensor located in the corresponding intrusion detection region S_ξ, and is derived as

$$P_1[D \le \xi] = 1 - (1 - p_\xi)^N. \tag{8}$$

Combing (4) to (8), it yields:

$$P_1[D \le \xi] = 1 - \Bigg\{1 - \int_{R-\xi}^{R}\int_{-r_s}^{r_s} f'_{xy}(\sigma)dydx - \int_{R-\xi-r_s}^{R-\xi}\int_{-\sqrt{r_s^2-(x-R+\xi)^2}}^{\sqrt{r_s^2-(x-R+\xi)^2}} f'_{xy}(\sigma)dydx - \int_{R}^{R+r_s}\int_{-\sqrt{r_s^2-(x-R)^2}}^{\sqrt{r_s^2-(x-R)^2}} f'_{xy}(\sigma)dydx\Bigg\}^N.$$

□

Next, we can evaluate the detection probability that the intruder is detected *immediately* after it enters the network domain according to Theorem 1. In this case, $\xi = 0$, and the corresponding intrusion detection region is reduced to a circular region S_0 with area of πr_s^2. The probability that a sensor is present in the area S_0 can be represented by the following double integral:

$$p_0 = \int_{R-rs}^{R+r_s} \int_{-\sqrt{r_s^2-(x-R)^2}}^{\sqrt{r_s^2-(x-R)^2}} f'_{xy}(\sigma) dydx. \tag{9}$$

Replacing p_ξ with p_0 in (8), we obtain

$$\begin{aligned} P_1[D=0] &= 1-(1-p_0)^N \\ &= 1-\left\{1-\int_{R-rs}^{R+r_s} \int_{-\sqrt{r_s^2-(x-R)^2}}^{\sqrt{r_s^2-(x-R)^2}} f'_{xy}(\sigma) dxdy\right\}^N. \end{aligned} \tag{10}$$

Based on Theorem 1, it is clear that the intruder's starting distance R, the sensor's sensing range r_s, the number of deployed sensors N, and the sensor distribution play an important role in determining the intrusion detection probability of a Gaussian-distributed WSN for both relaxed and immediate intrusion detection. Detailed numerical and simulation-based discussions are presented in Section 4.

3.2 Multiple-Sensing Detection

In this section, we explore the intrusion detection problem under the $m(m>1)$-sensing detection model.

Theorem 2. *Suppose $\xi(\xi>0)$ is the maximal allowable intrusion distance specified by a given application for intrusion detection, and the intruder starts at a distance of R to its target $(0,0)$. Let $P_m[D \le \xi]$ be the probability that the intruder is detected within ξ under the m-sensing detection. $P_m[D \le \xi]$ can be calculated as*

$$P_m[D \le \xi] = 1-\sum_{i=0}^{m-1} \binom{N}{i} (1-p_\xi)^{(N-i)} * p_\xi^i, \tag{11}$$

where

$$\begin{aligned} p_\xi = &\int_{R-\xi}^{R} \int_{-r_s}^{r_s} f'_{xy}(\sigma) dydx \\ &+ \int_{R-\xi-r_s}^{R-\xi} \int_{-\sqrt{r_s^2-(x-R+\xi)^2}}^{\sqrt{r_s^2-(x-R+\xi)^2}} f'_{xy}(\sigma) dydx \\ &+ \int_{R}^{R+r_s} \int_{-\sqrt{r_s^2-(x-R)^2}}^{\sqrt{r_s^2-(x-R)^2}} f'_{xy}(\sigma) dydx. \end{aligned}$$

Proof. As illustrated in Fig. 5, S_ξ is the intrusion detection region with respect to ξ and its area is given by $|S_\xi| = 2\xi r_s + \pi {r_s}^2$. If there are at least m sensors located in the region S_ξ, the intruder can be detected by the m sensors before it travels the distance of ξ in the WSN domain. From (7), we know that the probability of a sensor deployed in the region of S_ξ is p_ξ. Then, $(1-p_\xi)^{(N-i)} * p_\xi^i$ is the probability that i sensors are deployed in the region S_ξ. These i sensors could be any combination of the N deployed sensors as $\binom{N}{i}(1-p_\xi)^{(N-i)} * p_\xi^i$, which is the probability that there are exactly i sensors located in the region of S_ξ. Furthermore, the probability that there are *less than* m sensors located in the intrusion detection region S_ξ is $\sum_{i=0}^{m-1}\binom{N}{i}(1-p_\xi)^{(N-i)} * p_\xi^i$. The probability for *at least* m sensors located in the region S_ξ can be derived as the complement of

$$\sum_{i=0}^{m-1} \binom{N}{i} (1-p_\xi)^{(N-i)} * p_\xi^i,$$

that is, $1-\sum_{i=0}^{m-1}\binom{N}{i}(1-p_\xi)^{(N-i)} * p_\xi^i$.

In other words, the intruder can be sensed by at least m sensors from the WSN with probability $1-\sum_{i=0}^{m-1}\binom{N}{i}$ $(1-p_\xi)^{(N-i)} * p_\xi^i$ before it travels a distance of ξ. Finally, the probability $P_m[D \le \xi]$, that the intruder is detected with the maximal allowable intrusion distance ξ in m-sensing detection model, can be derived as $P_m[D \le \xi] = 1-\sum_{i=0}^{m-1}\binom{N}{i}(1-p_\xi)^{(N-i)} * p_\xi^i$, where

$$\begin{aligned} p_\xi = &\int_{R-\xi}^{R} \int_{-r_s}^{r_s} f'_{xy}(\sigma) dydx \\ &+ \int_{R-\xi-r_s}^{R-\xi} \int_{-\sqrt{r_s^2-(x-R+\xi)^2}}^{\sqrt{r_s^2-(x-R+\xi)^2}} f'_{xy}(\sigma) dydx \\ &+ \int_{R}^{R+r_s} \int_{-\sqrt{r_s^2-(x-R)^2}}^{\sqrt{r_s^2-(x-R)^2}} f'_{xy}(\sigma) dydx. \end{aligned}$$

□

Following the same methodology we exploited in Section 3.1, we can obtain the probability of an intruder being detected immediately once it enters the given Gaussian-distributed WSN under the m-sensing detection model as

$$P_m[D=0] = 1-\sum_{i=0}^{m-1} \binom{N}{i} (1-p_0)^{(N-i)} * p_0^i,$$

where

$$p_0 = \int_{R-rs}^{R+r_s} \int_{-\sqrt{r_s^2-(x-R)^2}}^{\sqrt{r_s^2-(x-R)^2}} f'_{xy}(\sigma) dydx.$$

Note that Theorem 1 can seen as a special case of Theorem 2 by setting $m=1$. It is because single-sensing detection can be regarded as a special case of multiple-sensing detection.

3.3 Remarks on the Modeling and Derivation

In this work, even though we adopt a simplified binary sensing model and a hot spot, our results are applicable in several practical scenarios with some modifications.

First, our results based on the binary sensing model can be extended to provide the upper and lower bounds of intrusion detection in a real-life WSN. For example, based on a more realistic exponential sensing model as described in [24], [25], the sensor can sense an intruder with probability 1 if $d \le r_{min}$ and with probability $e^{f(d)}$ if $r_{min} < d \le r_{max}$, where d is the distance between a sensor and the intruder in the exponential sensing model, and $f(d)$ denotes a function of d

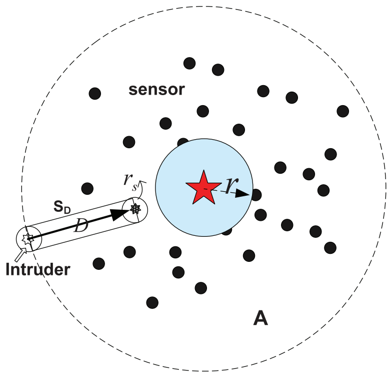

Fig. 6. Extension to a Hot Region.

and simulates the decay of sensing probability. Replacing r_s with r_{min} and r_{max} in our analysis can be used to compute the lower and upper bounds of intrusion detection probability, respectively, in a practical WSN. The lower bound leads to a conservative bound on the number of sensors needed to provide desirable detection probability.

Second, our analysis is based on the assumption that the hot spot is an important entity located at the center of the network. In reality, however, the important/sensitive entity is usually a region instead of a point. Fortunately, the proposed analytical model and the results can be applied to the situation where the hot spot is a region by regulating the maximum allowable intrusion distance ξ. Suppose the hot region is a circular area centered at the hot spot $(0,0)$ with radius r. In this case, the maximum allowable intrusion distance ξ should be reduced by the hot region's radius r such as $\xi' = \xi - r$. This is because the shortest distance between the starting point of the intruder and the hot region is reduced by the hot region radius r as illustrated in Fig. 6. The corresponding results can be derived from the above analysis by revising p_ξ as

$$\begin{aligned} p_\xi^r = & \int_{R-\xi+r}^{R} \int_{-r_s}^{r_s} f'_{xy}(\sigma)dydx \\ & + \int_{R-\xi+r-r_s}^{R-\xi+r} \int_{-\sqrt{r_s^2-(x-R+\xi-r)^2}}^{\sqrt{r_s^2-(x-R+\xi-r)^2}} f'_{xy}(\sigma)dydx \\ & + \int_{R}^{R+r_s} \int_{-\sqrt{r_s^2-(x-R)^2}}^{\sqrt{r_s^2-(x-R)^2}} f'_{xy}(\sigma)dydx. \end{aligned}$$

The results in single-sensing and multiple-sensing detection cases indicate that the intrusion detection probability in a given (truncated) Gaussian-distributed WSN is determined from three sets of parameters: the network parameters (represented by N, r_s, and σ), the application requirements (represented by m and ξ), and the intruder's approaching strategy (represented by R). We investigate their interdependence using analytical and simulation approaches in the following section.

4 Theoretical Analysis and Simulation Verifications

Based on the derivations in Section 3, we theoretically examine the effect of network parameters on the intrusion detection probability under both single-sensing detection and multiple-sensing detection cases in a Gaussian-distributed WSN using MATLAB. Then, we validate the correctness of our proposed model and analysis by Monte-Carlo simulations, based on a WSN simulator developed in C++. Unless otherwise specified, 10^4 runs are performed for generating the simulation results plotted in each figure of this section. Simulation outcomes are shown to match well with the analytical results.

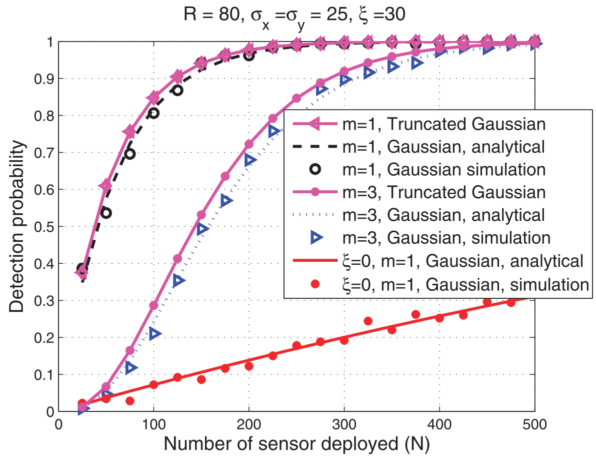

Fig. 7. Effect of number of deployed sensors N on the detection probability in a Gaussian-distributed WSN.

4.1 Effect of the Number of Deployed Sensors N

In order to observe the effect of the number of deployed sensors on the intrusion detection probability in a Gaussian and a truncated Gaussian-distributed WSN, we set the deployment point, the intruder's starting distance, the deployment standard deviation, the sensing range, and the maximal allowable intrusion distance as $G = (0,0)$, $R = 80$, $\sigma = 25$, and $\xi = 30$, respectively.

Fig. 7 shows the detection probability in the single-sensing (marked as "$m = 1$") and the multiple-sensing (marked as "$m = 3$") detection scenarios, with a varying number of deployed sensors. From the figure, the detection probabilities in all of the cases improve as the number of deployed sensors is increased. This is because, with increased number of deployed sensors, there is a higher probability that enough sensors are deployed in the intrusion detection region, given the maximal allowable intrusion distance. Further, Fig. 7 shows that one-sensing detection probability is much higher than that of three-sensing, due to the fact that multiple-sensing detection imposes a more strict requirement, i.e., at least three sensors are required for detecting the intruder. In addition, the truncated Gaussian-distributed WSNs perform a little better than its Gaussian counterpart in the studied cases. It is because in truncated Gaussian all sensors are deployed inside the area of interest, while some sensors may be deployed outside the area of interest in its Gaussian counterpart.

Note that Fig. 7 also plots the immediate detection probability (marked as "$\xi = 0$"), in contrast to the relaxed detection probability with $\xi = 30$ in single-sensing detection. The results demonstrate that the immediate detection probability is much lower than the relaxed detection probability under the same network settings. It implies that

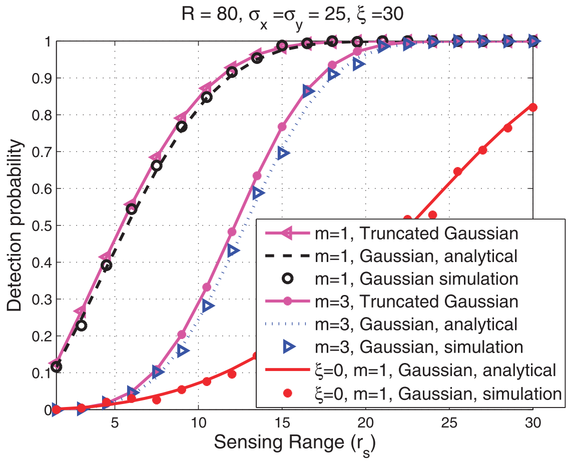

Fig. 8. Effect of sensing range r_s on the detection probability in a Gaussian-distributed WSN.

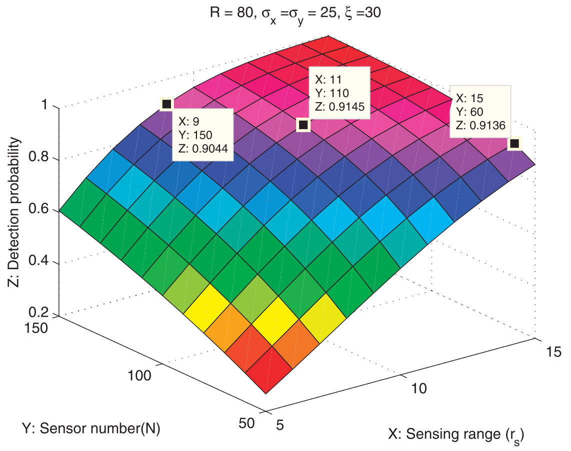

Fig. 9. Three-sensing detection probability of a WSN following a truncated Gaussian distribution under varying sensing range r_s and sensor number N.

more sensors should be deployed for immediate detection to provide the same level intrusion detection probability, as compared to the relaxed detection in which the intruder is allowed to travel some distance.

4.2 Effect of the Sensing Range r_s

We analyze the effect of the sensing range and set the intruder's starting distance, the standard deviation, the number of deployed sensors, and the maximal allowable intrusion distance as $R = 80$, $\sigma = 25$, $N = 100$, and $\xi = 30$, respectively.

Fig. 8 depicts the impact of sensing range on the intrusion detection probability in one-sensing and three-sensing detections in both Gaussian and truncated Gaussian WSNs. The detection probability is observed to improve as the sensing range increases, as a larger sensing range improves the network coverage, and higher network coverage leads to a quicker detection of the intruder. Furthermore, under the given network parameters, the detection probability approaches 1 while the sensing range is increased to a certain threshold. For example, the sensing range threshold is 20 for one-sensing detection and is 25 for three-sensing detection, as three-sensing is more demanding. Furthermore, the truncated Gaussian WSNs are shown to outperform their Gaussian counterparts in both one-sensing and three-sensing detections to some extent for studied cases. It is because the standard deviation is relatively small and the corresponding truncated Gaussian distribution does not differ from its counterpart Gaussian distribution to a significant extent. Moreover, analytical results and simulation outcomes for immediate intrusion detection are plotted as well and the immediate detection probability is much lower than if the intruder is allowed to travel some distance like 30 meters. Interestingly, different from a gradual increase on the immediate detection probability when N increases as in Fig. 7, the immediate detection improves dramatically when r_s is increased. It is because increasing N does not enlarge the intrusion detection region as $S_\xi = 2\xi r_s + \pi r_s^2$ but increasing r_s does improve the intrusion detection region to a significant extent and the size of the intrusion detection region plays a crucial part in determining the intrusion detection probability of a WSN as derived in Theorems 1 and 2 in Section 3.

Fig. 9 illustrates three-sensing detection probability of a WSN following a truncated Gaussian distribution when the number of deployed sensors is changed from 50 to 150 and the sensing range is varied from 5 to 15. Here, we fix $R = 80$, $\sigma_x = \sigma_y = 25$, $\xi = 30$, and $m = 3$. The results further confirm the importance of sensing range and the number of sensors on the intrusion detection probability of a Gaussian-distributed WSN and help in selecting critical parameters. For example, under the studied case, the number of required sensors can be determined from the figure to achieve certain detection probability, if the sensor type in terms of sensing range is given. For example, the threshold number of sensors are 150, 110, and 60 when the sensor's sensing range is 9, 11, and 15, respectively, for achieving above 0.9 three-sensing detection probability under the considered scenarios. The results help in selecting appropriate type and count of sensors for fulfilling desirable quality of service and minimizing the deployment cost.

4.3 Effect of the Deployment Deviation σ

In a Gaussian or truncated Gaussian-distributed WSN with fixed deployment point (i.e., $G = (0, 0)$) and a constant number of deployed sensors, deviation in the deployment affects the performance of intrusion detection. In exploring the effect of the deployment deviation σ, we set the intruder's starting distance, the number of deployed sensors, the sensing range, and the maximal allowable intrusion distance as $R = 80$, $N = 100$, $r_s = 20$, and $\xi = 30$, respectively.

Fig. 10 shows the intrusion detection probability of Gaussian and truncated Gaussian-distributed WSNs when the deployment deviations σ is varied for both one-sensing and three-sensing detections. The detection probability of Gaussian-distributed WSN improves when the deployment deviation increases from 0 to a certain threshold such as 40, then the detection probability decreases while the deployment deviation keeps increasing. This is due to the fact that when the deployment deviation grows from 0 to the threshold value, more sensors can be deployed around the starting point of the intruder to detect it sooner. However, when the deployment deviation keeps increasing beyond the threshold, the number of sensors deployed in

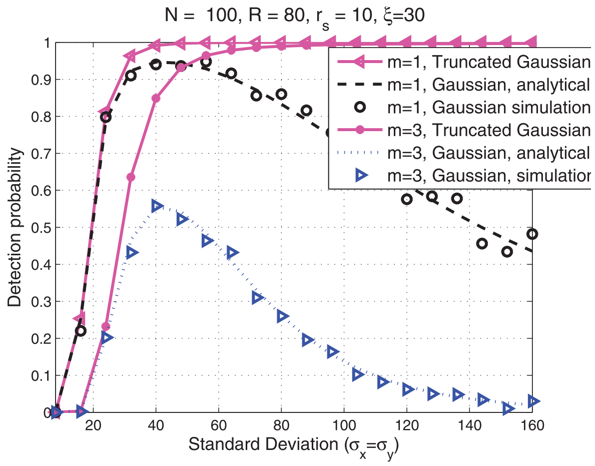

Fig. 10. Effect of deployment deviation σ on the detection probability in a Gaussian-distributed WSN $(\xi = 30)$.

the intrusion detection region decreases, which reduces the detection probability.

On the other hand, the detection probability of a truncated Gaussian-distributed WSN in both cases are observed to keep increasing until a threshold deviation is hit and stay constant after that, when the deviation is varied from low to high. In addition, the truncated Gaussian-distributed WSN outperforms the counterpart Gaussian-distributed WSN to a more significant extent when the standard derivation increases. It is because more sensors will be deployed outside the area of interest in a Gaussian-distributed WSN when the standard derivation increments further beyond the threshold. These observations confirm the necessity of examining the truncated Gaussian WSNs for intrusion detection applications.

Similar trend is observed in Fig. 11, which illustrates the immediate intrusion detection probability under the same network scenarios. However, Fig. 11 shows that in both one-sensing and three-sensing, the detection probability achieves its peak as the deviation equals to 55 for immediate detection, which is different from 40 where an intruder is allowed to travel some distance as shown in Fig. 10. It is because in immediate intrusion detection, the intruder has to be detected by enough sensors that are deployed close to the boundary. A larger deployment deviation results in more sensors being deployed close to the network boundary. The results suggest that there exists a threshold deviation in a Gaussian-distributed WSN for intrusion detection and it is related to the application requirements such as the maximum allowable intrusion distance ξ. We examine the impact of ξ on the network performance in Section 4.4.

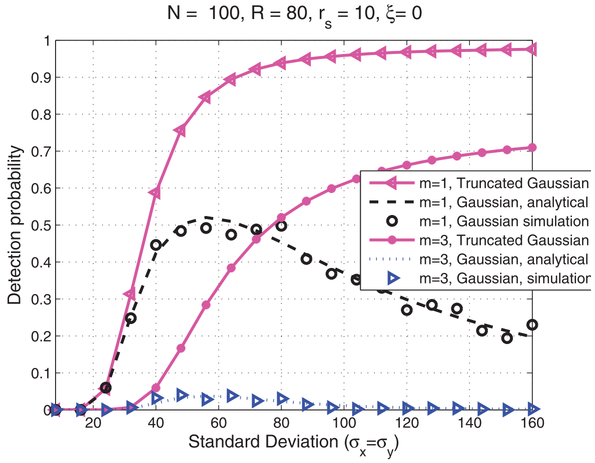

Fig. 11. Effect of deployment deviation σ on the immediate detection probability in a Gaussian-distributed WSN.

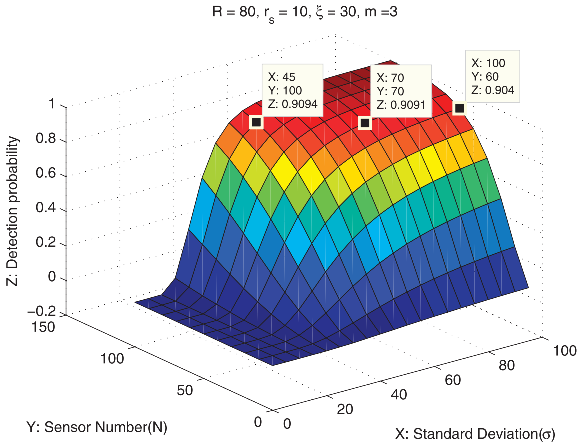

Fig. 12. Three-sensing detection probability of a truncated Gaussian-distributed WSN with varying ξ and N.

Furthermore, the number of deployed sensors also plays an important role in the threshold deviation for fulfilling certain detection probability. Fig. 12 depict the three-sensing detection probabilities of a truncated Gaussian-distributed WSNs when standard deviation varies from 0 to 100 and the number of sensors changes from 0 to 150. It is clear that the threshold standard deviation for a WSN to achieve certain detection probability varies when the sensor number changes. For instance, the threshold deviation is 45, 70, and 100 to achieve 0.9 detection probability when the sensor number is 100, 70, and 60, respectively. It is also observed that there exists a threshold sensor count, e.g., 60 shown in the considered case, below which the network cannot achieve desirable intrusion detection probability.

4.4 Effect of the Maximal Allowable Intrusion Distance ξ

Different applications may have different tolerance on the intruder in the WSN by specifying different maximal allowable intrusion distance ξ. In order to explore the effect of maximal allowable intrusion distance on the detection probability in a given Gaussian-distributed WSN, we fix the intruder's starting distance, the deployment standard deviation, the number of deployed sensors, and the sensing range as $R = 80$, $\sigma = 25$, $N = 100$, and $r_s = 10$, respectively.

Fig. 13 shows the intrusion detection probability with respect to different maximal allowable intrusion distances ranging from 0 to 70 in both single-sensing and multiple-sensing detections. The figure shows that the intrusion detection probability increases by enlarging the maximal allowable intrusion distance. This is because a larger maximal allowable intrusion distance leads to a larger intrusion detection region, which further results in a higher probability that the intruder can be detected by enough sensors (e.g., three sensors for three-sensing detection). This

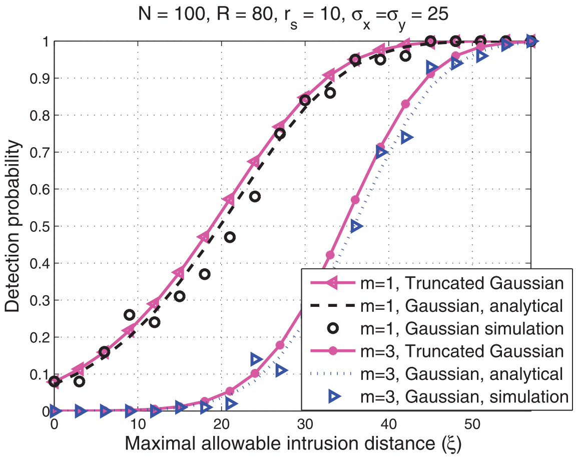

Fig. 13. Effect of the maximal allowable intrusion distance (ξ) on the detection probability in a Gaussian-distributed WSN.

confirms our argument that the maximum allowable intrusion distance plays a critical role in determining the detection probability of a WSN and its sensor deployment strategy. Moreover, we plot the corresponding detection probability of the counterpart truncated Gaussian-distributed WSNs as well. The small increase on the detection probability results from the fact that we set a relatively small deviation as 25 in this analysis.

Fig. 14 demonstrates the detection probability of a WSN with truncated Gaussian distribution when the application requires m-sensing detection. Specifically, m varies from 1 to 5 and the standard deviation σ changes from 5 to 100 in the analysis. It is apparent that the application requirement m impacts the threshold deviation to significant extent for achieving certain given detection probability. Under the studied scenarios, 0.94 detection probability can be achieved if the threshold deviation is 30, 50, and 100 for one-sensing, three-sensing, and five-sensing detection, respectively. Moreover, Fig. 15 illustrates the detection probability when ξ is varied from 0 to 150 and the standard deviation σ is changed from 5 to 100. It can be observed that, to achieve near one detection probability, the threshold deviation is 70, 60, 40, and 30 when $\xi = 5, 25, 55$, and 95, respectively. In other words, the threshold deviation is jointly impacted by the application requirements in terms of maximum allowable intrusion distance ξ and m-sensing detection.

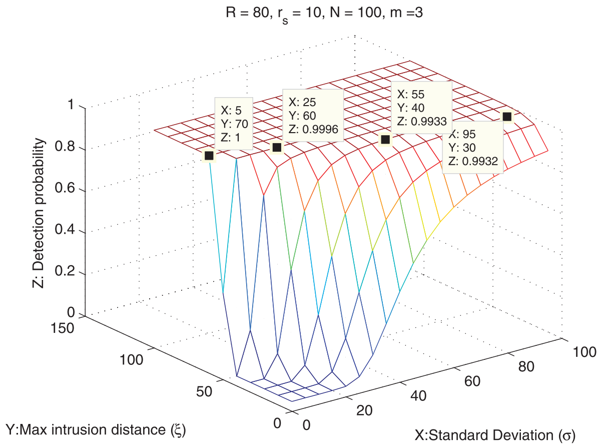

Fig. 15. Three-sensing detection probability of a truncated Gaussian-distributed WSN with varying ξ and σ.

4.5 Effect of the Intruder's Starting Distance R

The intruder's starting distance R to its target also impacts the intrusion detection probability and we examine this by setting the number of deployed sensors, the deployment standard deviation, the sensing range, and the maximal allowable intrusion distance as $N = 100$, $\sigma = 25$, $r_s = 10$, and $\xi = 30$, respectively.

Fig. 16 illustrates one-sensing and three-sensing detection probability of a Gaussian and a truncated Gaussian-distributed WSN by varying the intruder's starting distance R from 0 to 120. It can be observed from the figure that the detection probability decreases with increasing R. This is because less sensors are deployed in an area that is farther away from the deployment point (i.e., the intruder's target point) in a Gaussian or truncated Gaussian-distributed WSN. When the intruder starts from a point far away from its target, fewer sensors are deployed in the intrusion detection region and hence decreases the detection probability. Fig. 16 also demonstrates that the intruder can be detected with high probability, even if the starting point of

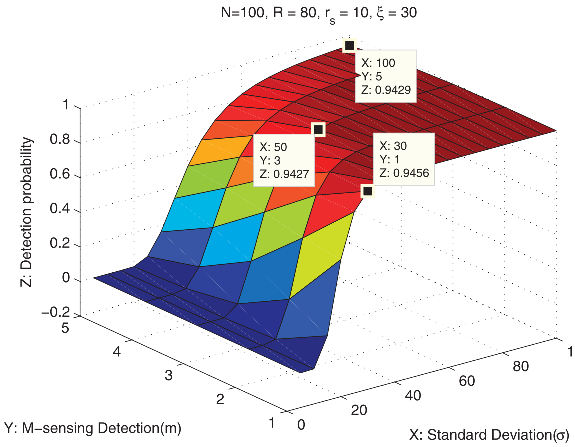

Fig. 14. Single-sensing detection probability of a truncated Gaussian-distributed WSN with varying ξ and N.

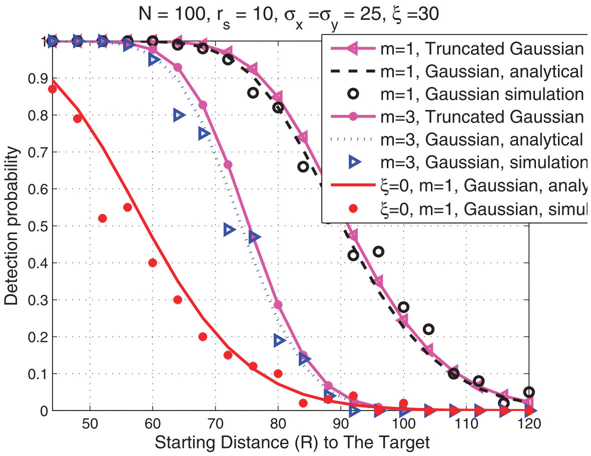

Fig. 16. Effect of intruder's starting point (at distance R to the center) on the detection probability in a Gaussian-distributed WSN.

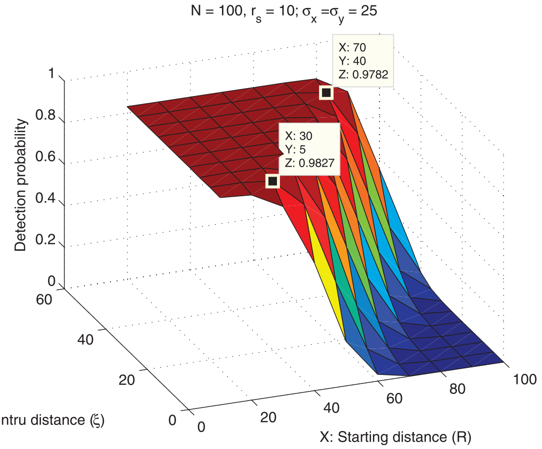

Fig. 17. Three-sensing detection probability of a truncated Gaussian-distributed WSN with varying ξ and R.

the intruder is close to the target. For instance, the detection probability reaches 1 in one-sensing detection when $R < 60$. The detection probability in three-sensing detection can reach 1 when $R < 50$. It is because, in a WSN following Gaussian or truncated Gaussian distribution more sensors are deployed around the deployment point, i.e., the intruder's target. This results in higher detection probability when the intruder starts from a point closer to its target.

Fig. 17 depicts the three-sensing detection probability of a WSN following truncated Gaussian distribution with varying R and ξ. From the figure, it is clear that when the intruder starts at a distance closer to the target, e.g., $(30 < 70)$ and the maximum intrusion distance is smaller (e.g., $5 < 40$), it will be detected by the Gaussian-distributed WSN with very high probability of about 0.98. This confirms the effectiveness of Gaussian-distributed WSNs for intrusion detection when applying to realistic scenario that smaller maximum intrusion distance is allowed if the intruder starts at a position closer to the hot spot.

These observations support the effectiveness of Gaussian-distributed WSN for intrusion detection from two perspectives. First, it can protect the target effectively when the intruder starts from a position inside the *FoI* and close to the target point, whereas a uniform-distributed WSN may fail. Second, it provides differentiated detection probability in the *FoI* such as enhanced detection probability in the area close to the target and reduced detection probability in the area far way from the target. However, when the intruder starts from a point far way from the target such as the network boundary when $R \geq 100$, the detection probability of a Gaussian-distributed WSN drops dramatically and can barely detect the intruder. This makes it necessary to investigate and compare the Gaussian and uniformly distributed WSNs in order to provide guidelines for network deployment and configuration for intrusion detection.

5 Gaussian-Distributed WSNs versus Uniform-Distributed WSNs

In order to investigate and compare the intrusion detection capability of a Gaussian-distributed WSN with its counterpart uniform WSN, we formulate the intrusion detection probability in a uniformly distributed WSN based on the methodology we used in analyzing the Gaussian-distributed WSN.

Theorem 3. *Let $\overline{p_m}[D \leq \xi]$ be the probability that the intruder is detected within the maximal allowable intrusion distance ξ in m-sensing detection model in a uniformly and randomly distributed WSN with N sensors and sensing range r_s. $\overline{p_m}[D \leq \xi]$ is formulated as*

$$\overline{p_m}[D \leq \xi] = \begin{cases} 1 - (1 - \overline{p_\xi})^N, & m = 1, \\ 1 - \sum_{i=0}^{m-1} \binom{N}{i} (1 - \overline{p_\xi})^{(N-i)} * \overline{p_\xi}^i, & m > 1. \end{cases} \tag{12}$$

where $\overline{p_\xi} = \frac{2\xi r_s + \pi {r_s}^2}{A}$.

Proof. Derived in (7),

$$\begin{aligned} p_\xi = & \int_{R-\xi}^{R} \int_{-r_s}^{r_s} f'_{xy}(\sigma) dy dx \\ & + \int_{R-\xi-r_s}^{R-\xi} \int_{-\sqrt{r_s^2-(x-R+\xi)^2}}^{\sqrt{r_s^2-(x-R+\xi)^2}} f'_{xy}(\sigma) dy dx \\ & + \int_{R}^{R+r_s} \int_{-\sqrt{r_s^2-(x-R)^2}}^{\sqrt{r_s^2-(x-R)^2}} f'_{xy}(\sigma) dy dx \end{aligned}$$

is the probability that a sensor is deployed within the intrusion detection region S_ξ with an area of $2\xi r_s + \pi {r_s}^2$ in the Gaussian-distributed WSN where $f'_{xy}(\sigma)$ varies at different points. However, in a uniformly distributed WSN, the PDF for point (x, y) to be deployed with a sensor remains the same all over the entire *FoI* and $f(x, y) = \frac{1}{A}$. Therefore, replacing $f'_{xy}(\sigma)$ with $f(x, y)$ in the expression of p_ξ yields the probability that a sensor is deployed in the intrusion detection region S_ξ as $\overline{p_\xi} = \frac{2\xi r_s + \pi {r_s}^2}{A}$. Following the same procedure in proving Theorems 1 and 2, we can prove Theorem 3 as $\overline{p_1}[D \leq \xi] = 1 - (1 - \overline{p_\xi})^N$ and $\overline{p_m}[D \leq \xi] = 1 - \sum_{i=0}^{m-1} \binom{N}{i} (1 - \overline{p_\xi})^{(N-i)} * \overline{p_\xi}^i$ for single sensing and multiple sensing detections, respectively, where $\overline{p_\xi} = \frac{2\xi r_s + \pi {r_s}^2}{A}$, in a uniformly distributed WSN with the same number and type of deployed sensors. □

In the following discussions, we compare the performance of a Gaussian-distributed WSNs with a uniform-distributed WSN for intrusion detection by setting the area of FoI as $A = 100 \times 100$ $(-50 < X < 50, -50 < Y < 50)$, the sensing range as $r_s = 10$, the deployment deviation as $\sigma_x = \sigma_y = 30$, unless otherwise specified.

5.1 Comparison on the Effect of the Number of Sensors

Fig. 18 illustrates the results on detection probability for the uniform and (truncated) Gaussian-distributed WSNs under three-sensing detection when the number of deployed sensors is varied from 10 to 200. The detection probability for all of the cases increases with the increase of the number of sensors N. In addition, two important observations are illustrated in Fig. 18. First, when the distance of the intruder's starting point is changed from $R = 50$ to $R = 30$, the detection probability in the uniform-distributed WSN remains the same, but the detection probability in the (truncated) Gaussian-distributed WSN

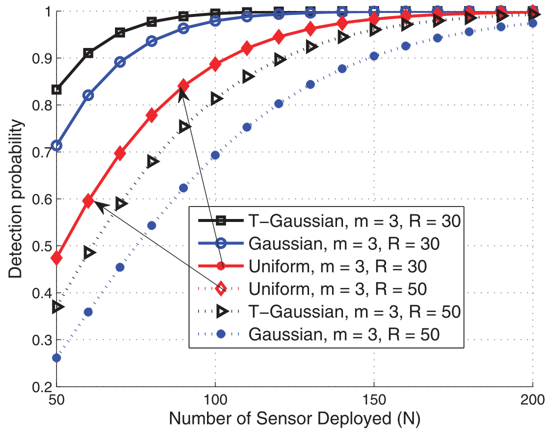

Fig. 18. (Truncated) Gaussian versus uniform distribution.

changes dramatically. This validates our intuition that a WSN following uniform distribution provides uniform detection capability in its deployment field, while the (truncated) Gaussian-distributed WSNs can provide location-related detection capability.

Another important observation from Fig. 18 is that neither the (truncated) Gaussian-distributed WSNs nor the uniform-distributed WSNs are always better than the other ones. For instance, when the intruder's starting point is close to the network boundary and far way from the target, i.e., $R = 50$, the uniform-distributed WSN outperforms the Gaussian-distributed WSN. On the other hand, when the intruder's starting point is far away from the network boundary and close to the target, i.e., $R = 30$, the (truncated) Gaussian-distributed WSN performs better than the uniform-distributed WSN.

These observations make it imperative to examine the effects of the intruder's starting distance on the detection probability in comparing (truncated) Gaussian-distributed WSNs with uniform-distributed WSNs.

5.2 Comparison on the Effect of the Intruder's Starting Distance

Fig. 19 illustrates the effect of the normalized intruder's starting distance R_{norm} in terms of network radius $\sqrt{A}/2$ on the detection probability of WSNs following a uniform distribution and a Gaussian distribution under both one-sensing detection and three-sensing detections. R is varied from 5 to 50 and the normalized R_{norm} is varied from 0.1 to 1.

From Fig. 19, we observe that the detection probability in a uniformly distributed WSN keeps constant when the starting point $(R, 0)$ of the intruder is varied for both one- and three-sensing detections. This is due to the fact that uniformly distributed WSNs provide the same node density all over the *FoI*. In other words, it does not matter where the intruder enters the WSN domain and the number of sensors located in the intrusion detection region S_ξ is expected to be the same in a uniform-distributed WSN. On the other hand, in a (truncated) Gaussian-distributed WSN, the detection probability drops gradually at the increase of the intruder's starting distance R under both one and three-sensing detection cases. The underlying reason is that, in (truncated) Gaussian-distributed WSNs the further the intruder's starting point is away from the center, the fewer sensors are deployed in the corresponding intrusion detection region S_ξ. Furthermore, we observe that there exists a threshold on the ratio of the starting distance R of the intruder to the network radius $\sqrt{A}/2$. Below the threshold, (truncated) Gaussian-distributed WSNs outperform uniform-distributed WSNs and vice versa. Note that the ratio indicated by Gaussian-distributed WSNs is different from that of the truncated Gaussian-distributed WSNs.

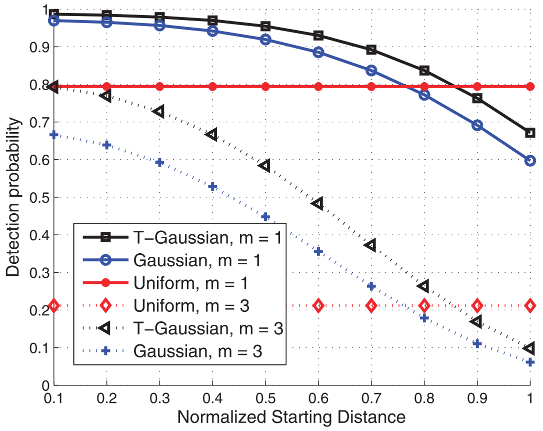

Fig. 19. (truncated) Gaussian versus uniform distribution on normalized intruder's starting distance.

5.3 Comparison on the Effect of Maximal Allowable Intrusion Distance

It is also desirable to investigate the effect of the maximal allowable intrusion distance. Fig. 20 demonstrates the results for both uniform and (truncated) Gaussian-distributed WSNs under both one-sensing and three-sensing detections.

From the figure, with an increase in the maximal allowable intrusion distance ξ, detection probability increases for all the cases. In addition, we discover that there also exists a threshold in the maximal allowable intrusion distance that can be used as a reference in selecting appropriate deployment strategy for intrusion detection applications with different tolerance of the intruder, i.e., ξ. In brief, when using a WSN for intrusion detection, the deployment strategy should be carefully selected according to the given application's requirements (i.e., ξ) and the

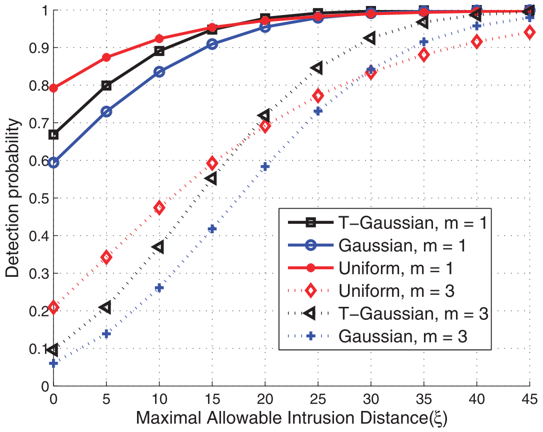

Fig. 20. Gaussian versus uniform distribution on maximal allowable intrusion distance.

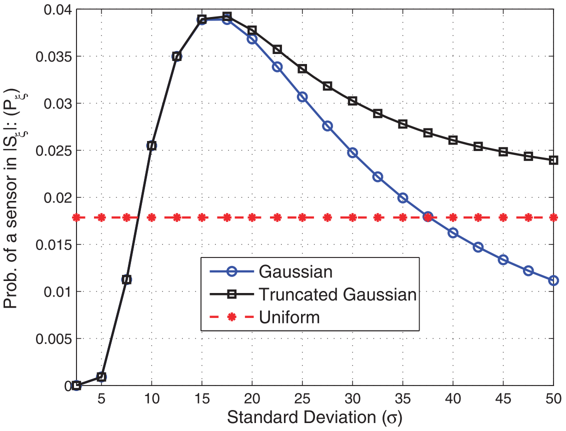

Fig. 21. Probability of a sensor being deployed in the intrusion detection region S_ξ of Gaussian, truncated Gaussian, and uniform-distributed WSNs with varying σ.

intruder's approaching strategy (i.e., R). More specifically, if the intruder can only enter the network from a position that is far away from the center and exceeds the threshold computed from Theorems 1, 2, and 3, sensors should be deployed following a uniform distribution. Otherwise, a Gaussian deployment strategy should be employed.

It is worth noting that another way to determine which distribution is the best in a given situation is to compare the probability of deploying a sensor inside the effective intrusion detection region S_ξ, i.e., p_ξ, p'_ξ, and $\overline{p_\xi}$ for Gaussian, truncated Gaussian, and uniformly distributed WSN, respectively. For example, if $p_\xi > \overline{p_\xi}$, a WSN admitting a Gaussian distribution surpasses that following a uniform distribution, and vice versa. Fig. 21 compares the probability of a sensor in S_ξ, i.e., p_ξ in the three considered WSNs.

6 Related Works

Intrusion detection (sometimes refers to target detection or object detection/tracking) as a surveillance problem of practical importance in WSNs [8] has received considerable attention in the literature. Aiming at effectively detecting the presence of an intruder and conserving network resources, researchers have been studying the problem from both practical and theoretical perspectives under different constraints and assumptions [10], [15], [11], [12], [16], [26], [20], [27], [28], [29].

Many works investigate this problem under various metrics and assumptions [9], [10], [16]. Arora et al. [8] defined the system models and examine the intrusion detection problem in the context of a security scenario called *A Line in the Sand* by quantitatively analyzing the effect of network unreliability on application performance, assuming that the nodes are deployed with uniform density and subject to some local variations. Wang et al. [9] provide a unifying approach in relating the intrusion detection probability with respect to various network settings. They assume a random WSN with uniform node density and disk sensing model. Given an intruder that moves on a straight line, they derived the probability of detecting the intruder within a predefined distance. Based on a Poisson approximation of uniform sensor distribution, Wang et al. [36] analytically compared its performance to that of a Gaussian distributed WSN. Dousse et al. [10] analyze the delay in intrusion detection, which is defined as the first contact time when the intruder hits the sensing range of a sensor belonging to the large sensor cluster. The key result in this work demonstrates a significant gap in the delay between the first contact time with a sensor and the first contact time with the large connected sensor cluster in a random WSN with uniform node density. Cao et al. [30] derive analytical formulas for detection probability and the mean delay in a uniformly distributed WSN with tunable system parameters such as node density and sleep duty cycle. They consider both stationary intruder and mobile intruder that moves on a straight line at a constant speed. Lazos et al. [21] formulate the intrusion detection problem as a line-set intersection problem and derive analytic formulas of the intrusion detection probability until a target is detected in a random WSN with uniform node density. Most recently, Medagliani et al. [31] propose an engineering toolbox which contains a set of models for describing the probability of missed detection, the alert transmission latency, and the energy consumption to optimally configure a given WSN for a variety of quality of service requirements. This work adopts and extends the analytical framework used in [21] and assumes a linear intrusion path. Different from adopting a linear path, Wang et al. [25], [32] propose a Sine-curve mobility model that can simulate different intrusion paths by adjusting its features (amplitude, frequency, and phase) and examine the interplays between network settings and the intruders mobility patterns. It is found that an intruder following a Sine-curve intrusion path can be more beneficial than following a straight-line path as the probability of being detected can be decreased, however with a side effect of reducing intrusion progress toward the destination to some extent. In other words, the straight-line path provides the maximum possible intrusion progress toward the destination when the moving distance is fixed.

Other works study the intrusion detection problem under energy, cost, and detection accuracy constraints. Ren et al. [15] examine the tradeoff between the network detection quality (i.e., how fast the intruder can be detected) and the network lifetime, and propose three wave sensing scheduling protocols to achieve the bounded worst case detection probability. Wang et al. [33] propose a two-level cooperative and energy-efficient detection algorithm to reduce the energy consumption rate of a WSN by limiting the number of sensors in operation through a face-aware routing and wake-up mechanism. Based on multiple-sensing detection, data aggregation and fusion techniques are employed to improve the detection accuracy and false-tolerance of WSN systems. Guerriro et al. [34] employ a Bayesian framework to exploit prior knowledge such as the target's location for data fusion in WSN. They derive the closed form for the Bayesian detector and show the performance improvement over the Scan statistic without using extra sensor observations. Zhu et al. [35] propose a binary decision fusion rule that reaches a global decision on the target detection by integrating local decisions made by multiple sensors. They derive the fusion threshold using Chebyshev's inequality without assuming a priori probability of target presence that ensure a higher hit rate and lower false alarm rate compared to the weighted averages of individual sensors. Moreover, Liu et al. [16] take the node mobility into consideration and present a strategy for fast detection by illustrating that a mobile WSN improves its detection quality due to the mobility of sensors.

In this paper, we address the problem of intrusion detection from another angle by examining a Gaussian-distributed WSN and comparing its performance with a uniformly distributed WSN. We have investigated such a problem by modeling, analysis, and simulations, under both single-sensing and multiple-sensing detections. The analytical results are shown to match with the simulation outcomes, validating the correctness of this work. A preliminary version of this work was presented in conference [23]. We extend it by considering the truncated Gaussian-distributed WSNs; comparing the intrusion detection performance of a random WSN with a Gaussian, a truncated Gaussian, a uniform distribution under the same application scenarios; illustrating how two network variables affect the detection probability together; and discussing the practical implication of the results. This work provides the comprehensive insights into the intrusion detection problem in a randomly distributed WSN following a Gaussian, truncated Gaussian, or uniform distribution and compares their performance in a bounded field of interest.

7 Conclusion

This paper examines the intrusion detection problem in a (truncated) Gaussian-distributed WSN by characterizing intrusion detection probability with respect to the application requirements and network parameters theoretically and by simulations. Furthermore, the performance of intrusion detection in a Gaussian-distributed WSN is compared with a uniformly distributed WSN and a truncated Gaussian-distributed WSN from the perspectives of network settings, application requirements, and intruder's approaching strategy. This work can be used to guide the selection of an appropriate random sensor deployment strategy and help in the design of a WSN and determining critical parameters for intrusion detection.

References

[1] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A Survey on Wireless Sensor Networks," *IEEE Comm. Magazine,* vol. 40, no. 8, pp. 102-114, Aug. 2002.

[2] K. Sohraby, D. Minoli, and T. Znati, *Wireless Sensor Networks: Technology, Protocols, and Applications.* John Wiley and Sons, Inc., 2007.

[3] J.N. Al-Karaki and A.E. Kamal, "Routing Techniques in Wireless Sensor Networks: A Survey," *IEEE Wireless Comm.,* vol. 11, no. 6, pp. 6-28, Dec. 2004.

[4] S. Tilak, N.B. Abu-Ghazaleh, and W. Heinzelman, "A Taxonomy of Wireless Micro-Sensor Network Models," *ACM Mobile Computing and Comm. Rev.,* vol. 6, no. 2, pp. 28-36, Apr. 2002.

[5] A. Agah, S. Das, K. Basu, and M. Asadi, "Intrusion Detection in Sensor Networks: A Non-Cooperative Game Approach," *Proc. Third IEEE Int'l Symp. Network Computing and Applications (NCA '04),* pp. 343-346, 2004.

[6] A. Agah, S. Das, and K. Basu, "A Game Theory Based Approach for Security in Wireless Sensor Networks," *Proc. IEEE Int'l Conf. Performance, Computing, and Comm.,* pp. 259-263, 2004.

[7] V. Giruka, M. Singhal, J. Royalty, and S. Varanasi, "Security in Wireless Sensor Networks," *Wireless Comm. and Mobile Computing,* vol. 8, no. 1, pp. 1-24, 2008.

[8] A. Arora, P. Dutta, S. Bapat, V. Kulathumani, H. Zhang, V. Naik, V. Mittal, H. Cao, M. Demirbas, and M. Gouda, "A Line in the Sand: A Wireless Sensor Network for Target Detection, Classification, and Tracking," *Computer Networks,* vol. 46, no. 5, pp. 605-634, 2004.

[9] Y. Wang, X. Wang, B. Xie, D. Wang, and D.P. Agrawal, "Intrusion Detection in Homogeneous and Heterogeneous Wireless Sensor Networks," *IEEE Trans. Mobile Computing,* vol. 7, no. 6, pp. 698-711, June 2008.

[10] O. Dousse, C. Tavoularis, and P. Thiran, "Delay of Intrusion Detection in Wireless Sensor Networks," *Proc. MobiHoc,* 2006.

[11] H. Kung and D. Vlah, "Efficient Location Tracking Using Sensor Networks," *Proc. IEEE Wireless Comm. and Networking Conf.,* vol. 3, pp. 1954-1961, Mar. 2003.

[12] C.-Y. Lin, W.-C. Peng, and Y.-C. Tseng, "Efficient In-Network Moving Object Tracking in Wireless Sensor Networks," *IEEE Trans. Mobile Computing,* vol. 5, no. 8, pp. 1044-1056, Aug. 2006.

[13] K. Chakrabarty, S. Iyengar, H. Qi, and E. Cho, "Grid Coverage for Surveillance and Target Location in Distributed Sensor Networks," *IEEE Trans. Computers,* vol. 51, no. 12, pp. 1448-1453, Dec. 2002.

[14] G.T.K. Xu and H. Hassanein, "On the Robustness of Grid-Based Deployment in Wireless Sensor Networks," *Proc. Int'l Wireless Comm. and Mobile Computing Conf. (IWCMC),* pp. 1183-1188, July 2006.

[15] 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 Trans. Parallel and Distributed Systems,* vol. 18, no. 3, pp. 334-350, Mar. 2007.

[16] B. Liu, P. Brass, O. Dousse, P. Nain, and D. Towsley, "Mobility Improves Coverage of Sensor Networks," *Proc. MobiHoc,* 2005.

[17] D. Wang, B. Xie, and D.P. Agrawal, "Coverage and Lifetime Optimization of Wireless Sensor Networks with Gaussian Distribution," *IEEE Trans. Mobile Computing,* vol. 7, no. 12, pp. 1444-1458, Dec. 2008.

[18] C.-f. Hsin and M. Liu, "Network Coverage Using Low Duty-Cycled Sensors: Random & Coordinated Sleep Algorithms," *Proc. Third Int'l Symp. Information Processing in Sensor Networks,* pp. 433-442, 2004.

[19] S. Banerjee, C. Grosan, A. Abraham, and P. Mahanti, "Intrusion Detection on Sensor Networks Using Emotional Ants," *Int'l J. Applied Science and Computations,* vol. 12, no. 3, pp. 152-173, 2005.

[20] L. Lazos, R. Poovendran, and J.A. Ritcey, "Probabilistic Detection of Mobile Targets in Heterogeneous Sensor Networks," *IPSN '07: Proc. Sixth Int'l Conf. Information Processing in Sensor Networks,* pp. 519-528, 2007.

[21] L. Lazos, R. Poovendran, and J. Ritcey, "Analytic Evaluation of Target Detection in Heterogeneous Wireless Sensor Networks," *ACM Trans. Sensor Networks,* vol. 5, no. 2, article 18, 2009.

[22] X. Bai, Z. Yun, D. Xuan, W. Jia, and W. Zhao, "Pattern Mutation in Wireless Sensor Deployment," *Proc. IEEE INFOCOM,* pp. 1-9, 2010.

[23] Y. Wang, W. Fu, and D.P. Agrawal, "Intrusion Detection in Gaussian Distributed Wireless Sensor Networks," *Proc. Sixth IEEE Int'l Conf. Mobile Ad Hoc and Sensor Systems,* 2009.

[24] Y. Li, Y. Song, Y. Zhu, and R. Schott, "Deploying Wireless Sensors for Differentiated Coverage and Probabilistic Connectivity," *Proc. IEEE Wireless Comm. and Networking Conf. (WCNC),* pp. 1-6, 2010.

[25] Y. Wang, Y. Leow, and J. Yin, "A Novel Sine-Curve Mobility Model for Intrusion Detection in Wireless Sensor Networks," *Wireless Comm. and Mobile Computing,* 2011.

[26] T. Clouqueur, K.K. Saluja, and P. Ramanathan, "Fault Tolerance in Collaborative Sensor Networks for Target Detection," *IEEE Trans. Computers,* vol. 53, no. 3, pp. 320-333, Mar. 2003.

[27] E. Yanmaz and H. Guclu, "Stationary and Mobile Target Detection Using Mobile Wireless Sensor Networks," *Proc. IEEE INFOCOM,* 2010.

[28] M. Zhu, S. Ding, Q. Wu, R.R. Brooks, N.S.V. Rao, and S.S. Iyengar, "Fusion of Threshold Rules for Target Detection in Wireless Sensor Networks," *ACM Trans. Sensor Networks,* vol. 6, pp. 18:1-18:7, Mar. 2010.

[29] T. Wimalajeewa and S.K. Jayaweera, "Impact of Mobile Node Density on Detection Performance Measures in a Hybrid Sensor Network," *IEEE Trans. Wireless Comm.,* vol. 9, no. 5, pp. 1760-1769, May 2010.

[30] Q. Cao, T. Yan, J. Stankovic, and T. Abdelzaher, "Analysis of Target Detection Performance for Wireless Sensor Networks," *Proc. First IEEE Int'l Conf. Distributed Computing in Sensor Systems,* pp. 276-292, 2005.

[31] P. Medagliani, J. Leguay, V. Gay, M. Lopez-Ramos, and G. Ferrari, "Engineering Energy-Efficient Target Detection Applications in Wireless Sensor Networks," *Proc. IEEE Int'l Conf. Pervasive Computing and Comm. (PerCom),* pp. 31-39, 2010.

[32] Y. Wang, Y.K. Leow, and J. Yin, "Is Straight-Line Path Always the Best for Intrusion Detection in Wireless Sensor Networks," *Proc. Int'l Conf. Parallel and Distributed Systems,* pp. 564-571, 2009.

[33] G. Wang, M.Z.A. Bhuiyan, and L. Zhang, "Two-Level Cooperative and Energy-Efficient Tracking Algorithm in Wireless Sensor Networks," *Concurrency and Computation: Practice and Experience,* vol. 22, pp. 518-537, Mar. 2010.

[34] M. Guerriero, L. Svensson, and P. Willett, "Bayesian Data Fusion for Distributed Target Detection in Sensor Networks," *IEEE Trans. Signal Processing,* vol. 58, no. 6, pp. 3417-3421, June 2010.

[35] M. Zhu, S. Ding, Q. Wu, R. Brooks, N. Rao, and S. Iyengar, "Fusion of Threshold Rules for Target Detection in Wireless Sensor Networks," *ACM Trans. Sensor Networks,* vol. 6, no. 2, article 18, 2010.

[36] Y. Wang, F. Li, and F. Fang, "Poisson versus Gaussian Distribution for Object Tracking in Wireless Sensor Networks," *Proc. Second Int'l Workshop Intelligent Systems and Applications (ISA),* pp. 1-4, 2010.

Yun Wang received the BS degree in computer science and engineering from Wuhan University, Hubei, China, in 2001. She received the PhD degree in computer science and engineering from the University of Cincinnati, Ohio, in 2008. She is currently an assistant professor in the Department of Computer Science and Information Systems at Bradley University, IL. She has been a faculty member at the Southern Illinois University Edwardsville (2008-2011). Her research interests include Network Modeling and Analysis, Performance Evaluation and Optimization, Wireless ad hoc and Sensor Networks, and Wireless Mesh Networks. She has published research works in *IEEE Transactions on Mobile Computing* and *IEEE Transactions on Parallel and Distributed Systems*. She has been a technical program committee member of many international conferences and a technical reviewer of many international journals and conference proceedings in her field.

Weihuang Fu received the BS degree in communications engineering and the MS degree in communication and information systems from Zhejiang University of Technology, China, in 2002 and 2005, respectively, and the PhD degree in computer science and engineering from the University of Cincinnati, OH, in 2010. He joined Cisco Systems, Inc., in 2010. He has been a technical program committee member of many international conferences and a technical reviewer of numerous international journals and conference proceedings. His research interests include next-generation network architectures, wireless multihop networks, mobile communication systems, etc.

Dharma P. Agrawal (M'74-F'87-LF'11) is the Ohio Board of Regents Distinguished Professor in the School of Computing Sciences and Informatics and the founding director for the Center for Distributed and Mobile Computing at the University of Cincinnati, OH. He was a visiting professor of ECE at the Carnegie Mellon University, on sabbatical leave during the autumn 2006 and winter 2007 Quarters. He has been a faculty member at the N.C. State University, Raleigh, NC (1982-1998) and the Wayne State University, Detroit (1977-1982). His current research interests include energy efficient routing and information retrieval in Sensor and Mesh networks, QoS in integrated wireless networks, use of smart multibeam directional antennas for enhanced QoS, various aspects of sensor networks including environmental monitoring and secured communication in ad hoc and sensor networks. His coauthored textbook on*Introduction to Wireless and Mobile Systems*, third edition published by Cengage Corp. has been adopted throughout the world and revolutionized the way the course is taught. His second coauthored textbook entitled, *Ad hoc and Sensor Networks*, second edition has been published by World Scientific. He has served as an editor of the *IEEE Computer magazine*, the *IEEE Transactions on Computers*, and the *International Journal of High Speed Computing*. He is an editor for the *Journal of Parallel and Distributed Systems*, *International Journal on Distributed Sensor Networks*, *International Journal of Ad Hoc and Ubiquitous Computing (IJAHUC)*, *International Journal of Ad Hoc and Sensor Wireless Networks*, and *Journal of Information Assurance and Security*. He has been the program chair and general chair for numerous international conferences and meetings. He has received numerous certificates and awards from the IEEE Computer Society. He was awarded a "Third Millennium Medal," by the IEEE for his outstanding contributions. He has also delivered keynote speech for five international conferences. He also has five patents and 23 patent disclosures in wireless networking area. He has served as a fulbright senior specialist for duration of five years. He has been appointed as the founding editor-in-chief of the *Central European Journal of Computer Science,* Versita. He has graduated 62 PhDs and 51 MS students and has also been named as an ISI Highly Cited Researcher in computer science. He is a winner of 2008 Harry Goode Memorial award from the IEEE Computer Society and 2011 Award for Excellence in Mentoring of Doctoral Students, University of Cincinnati. He is a life fellow of the IEEE, a fellow of the ACM, the AAAS, and WIF.