Intrusion Detection in Gaussian Distributed Heterogeneous Wireless Sensor Networks

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

Abstract—Intrusion detection is one of the fundamental applications in wireless sensor networks (WSNs). Some applications require different detection capabilities at different areas in the deployment field. Gaussian distributed WSNs can fulfill such requirements and are widely deployed in practice. In addition, the presence of some high capability sensors leads to performance enhancement in term of intrusion detection probability. This makes it imperative to explore the intrusion detection problem in heterogeneous WSNs. This work is to examine the intrusion detection problem in a heterogeneous Gaussian distributed WSN theoretically and experimentally. A heterogeneous WSN model with distinct types of Gaussian distributed sensors is proposed, where both single-sensing detection and k-sensing detection models are employed. Based on this network model, the intrusion detection probabilities under various application scenarios are theoretically derived and experimentally validated by extensive simulations. This work is to provide guidelines in designing heterogeneous WSNs for intrusion detection.

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

I. INTRODUCTION

A Wireless Sensor Network (WSN) is a collection of small, cheap and low powered sensors which can automatically and dynamically form a network in ad hoc fashion [1]. In general, a WSN can be made up of identical sensors or distinct types of sensors. The sensors can be deployed around a pre-defined deployment point by a low-flying aircraft. The resulting WSN conforms to Gaussian distribution, i.e., Normal distribution. In a homogeneous WSN, all sensors have identical capability in terms of sensing range, transmission range, battery power, and processing power. On the other hand, in heterogeneous WSN, the presence of high capability sensors with larger sensing range or transmission range can increase the network performance [2]. However, the question of what type, and how many sensors should be introduced, and how much performance improvement can be achieved in WSN applications following Gaussian distribution remains unexplored. This work is to address this problem in a heterogeneous Gaussian distributed WSN.

Intrusion detection (i.e., object tracking) is one of the fundamental applications in WSNs, and is defined as a monitoring system for detecting an malicious intruder that is invading the network domain [3], [4], [5], [6]. In a heterogeneous WSN deployed for this purpose, different types of sensors are deployed in an area of interest to monitor the environmental changes caused by moving intruder(s), using optical, mechanical, acoustic, thermal, RF and/or magnetic sensing modalities [7]. In this way, possible intruder(s) approaching or traveling inside the deployment field can be detected by the WSN if it enters into the sensing range of one or multiple sensor(s).

Fig. 1 illustrates such a situation, where heterogenous sensors are deployed in a circular area \( A = \pi R^2 \) for protecting the central-located target represented by the red star. The intrusion detection application concerns how soon or how efficiently the intruder can be detected by the WSN [8]. As illustrated in Fig. 1, the intrusion distance is referred as \( D \) (e.g., \( D_1 \) and \( D_2 \)). It is defined as the distance between the point the intruder enters the WSN and the point the intruder is first detected by the WSN [3]. Obviously, intrusion distance is of central interest to a WSN for intrusion detection, and can be used to measure its performance. For instance, less intrusion distance represents better detection capability of a WSN. The main contributions of this work include:

- Develop a network model for analyzing intrusion detection problem for heterogeneous Gaussian distributed WSNs, employing both single-sensing detection and multiple-sensing detection models.
- Mathematically derive the intrusion detection probability with respect to various network parameters based on the
network model.

- Analyze the impact of various network parameters on intrusion detection probability in heterogeneous Gaussian distributed WSNs.

- Perform extensive simulations to validate the model and theoretical analysis.

The rest of this paper is organized as follows: Section II presents some related works. Section III describes the intrusion detection system analytical model. Section IV examines the intrusion detection probability in single-sensing and multisensing detection cases. Section V theoretically and experimentally analyzes the effects of various network parameters on the intrusion detection probability in Gaussian distributed WSNs. Finally, the paper is concluded in Section VI.

II. RELATED WORK

As a critical problem in WSNs, intrusion detection attracts much attention from researchers. To date, prior works on intrusion detection of WSNs assume a network model following Poisson distribution [3], [7] [4], [9], [5], [6]. In [9], Ren et al. have investigated the tradeoff between the network detection quality (i.e., how fast the intruder can be detected) and the power conservation and network lifetime based on a homogeneous WSN model. Wang et al. [3] have examined the problem of intrusion detection for both homogeneous and heterogeneous Poisson distributed WSNs, and explore the impact of node heterogeneity on the quality of service of a WSN following Poisson distribution in terms of coverage [10] and intrusion detection probability [11]. In [7], Lazos et al. have studied a heterogeneous sensing model in a Poisson distributed WSN, where each sensor can have an arbitrary sensing range, and evaluated the mean free path until the intruder is first detected. However, Poisson distributed WSN can not provide differentiated detection capabilities for WSN applications such as intrusion detection. It is discovered in [8] that Gaussian distributed WSNs can provide differentiated detection capability at different locations for intrusion detection, where Wang et al. have investigated the intrusion detection problem in a homogeneous Gaussian distributed WSN with identical sensors. As heterogeneous WSNs with different types of sensor are more and more popular and desirable in practice, we aim to explore the intrusion detection problem in a heterogeneous Gaussian distributed WSN where distinct types of sensors are deployed. This work will measure how much better heterogeneous WSNs are than homogeneous WSNs for intrusion detection.

III. SYSTEM MODEL AND DEFINITIONS

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

A. Network Model

We consider a heterogeneous WSN consisting of $H$ types of sensors. A number of $N$ sensors are randomly and independently deployed in the deployment field following Gaussian distribution. The number of type $i$ sensors is $N_i$. Therefore $N = \sum_{i=1}^{H} (N_i)$. For simplicity of analysis, we first explore a heterogeneous WSN with two types of sensors as illustrated in Fig. 2, where two distinct types of sensors are deployed independently and follows Gaussian distribution and the red star represents the deployment point with coordinates of $(0, 0)$. Following Gaussian distribution, the probability density function (PDF) that a Type I sensor locates at point $(x, y)$ is given by:

$$f(x, y, \sigma_{x_1}, \sigma_{y_1}) = \frac{1}{2\pi\sigma_{x_1}\sigma_{y_1}} e^{-\left(\frac{x^2}{2\sigma_{x_1}^2} + \frac{y^2}{2\sigma_{y_1}^2}\right)} \quad \text{(1)}$$

and the PDF that a Type II sensor locates at point $(x, y)$ is given by:

$$f(x, y, \sigma_{x_2}, \sigma_{y_2}) = \frac{1}{2\pi\sigma_{x_2}\sigma_{y_2}} e^{-\left(\frac{x^2}{2\sigma_{x_2}^2} + \frac{y^2}{2\sigma_{y_2}^2}\right)} \quad \text{(2)}$$

where $\sigma_{x_1}$ and $\sigma_{y_1}$ denotes the deployment deviation of Type $i$ sensors along $x$-axis and $y$-axis respectively.

Then, the the PDF that a sensor (either type I or type II) locates at point $(x, y)$ is therefore given by:

$$f(x, y, \sigma_{x_1}, \sigma_{y_1}, \sigma_{x_2}, \sigma_{y_2}) = f(x, y, \sigma_{x_1}, \sigma_{y_1}) \ast f(x, y, \sigma_{x_2}, \sigma_{y_2}) \quad \text{(3)}$$

Here we assume $\sigma_{x_1} = \sigma_{y_1} = \sigma_1$, and $\sigma_{x_2} = \sigma_{y_2} = \sigma_2$. Then, Eq. (3) is reduced as:

$$f(x, y, \sigma_1, \sigma_2) = f(x, y, \sigma_1) \ast f(x, y, \sigma_2) \quad \text{(4)}$$

For simplicity of notation, $f(x, y, \sigma)$ is interchangeable with $f_{xy}(\sigma)$ in the rest of this paper. For instance, Eq. (4) can be referred as: $f_{xy}(\sigma_1, \sigma_2) = f_{xy}(\sigma_1) \ast f_{xy}(\sigma_2)$.

B. Sensing and Detection Model

An idealized unit disk sensing model is assumed for both types of sensors, their sensing coverage is assumed to be
circular and symmetrical and determined by their sensing range(s). To be specific, Type I sensors are assumed to be equipped with a larger sensing range of \(r_{s1}\), and Type II sensors have a smaller sensing range of \(r_{s2}\), i.e., \(r_{s1} > r_{s2}\).

Based on this sensing model, both single-sensing detection and multiple-sensing detection are studied in this work. Single-sensing detection provides a worst-case guarantee on intrusion detection, in which the intruder can be successfully detected by a single sensor. On the other hand, in the multiple-sensing detection model, the intruder should be collaboratively detected by at least \(k\) sensors to enhance fault tolerance and reduce false alarms [7] or is required to provide specific service such as positioning [12]. For instance, the location of an intruder should be calculated from at least three sensors’ sensing data [13].

**C. Evaluation metrics**

In order to evaluate the quality of intrusion detection in WSNs, we define two metrics as follows [3]:

- **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 \(\xi\); \(\xi > 0\)) 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 \(\xi\)) specified by WSN applications.

**IV. INTRUSION DETECTION IN A HETEROGENEOUS GAUSSIAN DISTRIBUTED WSN**

In this section, we present the analysis of intrusion detection in a heterogeneous Gaussian distributed WSN. We derive the detection probability for single-sensing and \(k\)-sensing detection scenarios.

**A. Single-sensing Detection**

In order to analyze the intrusion detection probability in a heterogeneous Gaussian distributed WSN, we build a Cartesian coordinate system as illustrated in Fig. 3, based on the network model. Without loss of generality, \((0,0)\) is set as the location of the target point (i.e., the deployment point). \((R,0)\) 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 start point is set, the corresponding Cartesian coordinate system can be built accordingly.

In order for the intruder to be detected by the WSN, it has to enter into the sensing range of any sensor(s). Suppose the intruder can travel in the WSN with distance of \(D = \xi\) before being sensed by any sensor(s). This intrusion distance and the sensors’ sensing range actually determine the *intrusion detection area* [3], as illustrated in Fig. 3. The intrusion detection area is an oblong area and consisting of one rectangle area \(S_r\) and two half disk \(S_s\). To be specific, the intrusion detection area for Type I sensors with sensing range \(r_{s1}\) is given by:

\[
S_{1D} = 2 \cdot D \cdot r_{s1} + \pi r_{s1}^2,
\]

and for Type II sensors with sensing range \(r_{s2}\) is given by:

\[
S_{2D} = 2 \cdot D \cdot r_{s2} + \pi r_{s2}^2.
\]

Then, if any Type I sensor(s) locate in the area of \(S_{1D}\), the intruder can be detected within intrusion distance \(D\); or if any Type II sensor(s) locate in the area of \(S_{2D}\), the intruder can also be sensed. In view of this, given maximal allowable intrusion distance \(D = \xi\), there should be at least one Type I sensor resides in \(S_1\) or at least one Type II sensor locates in the area \(S_2\) to detect the intrusion within \(\xi\), under single-sensing detection model.

Let \(p_{1i}\) be the probability that a Type \(i\) sensor deployed in the rectangle area \(S_r = 2\xi r_{s1}\), \(p_{1c}\) be the probability that a Type \(i\) sensor resides in the left half disk \(S_{1l} = \pi r_{s1}^2\), and \(p_{1r}\) be the probability that a Type \(i\) sensor resides in the right half disk \(S_{1r} = \pi r_{s1}^2\).

Based on the given Gaussian distributed WSN, \(p_{1i}\) can be derived as:

\[
p_{1i} = \int_{-\xi}^{R} \int_{-r_{s1}}^{r_{s1}} f_{xy}(\sigma_1) dy dx,
\]

where \(R - \xi < x \leq R\).

\(p_{1c}\) can be calculated as:

\[
p_{1c} = \int_{-\xi}^{R} \int_{-r_{s1}}^{r_{s1}} \int_{\sqrt{x^2 + (x-R)^2}}^{\sqrt{x^2 + (x-R)^2} + \xi} f_{xy}(\sigma_1) dy dx,
\]

where \(R - \xi - r_{s1} < x < R - \xi\).

\(p_{1r}\) can be given by:

\[
p_{1r} = \int_{R}^{R + r_{s1}} \int_{-r_{s1}}^{r_{s1}} f_{xy}(\sigma_1) dy dx,
\]

where \(R < x < R + r_{s1}\).
Then, the probability \( p^i_\xi \) that a Type \( i \) sensor is deployed in the intrusion detection area \( S^i_\xi \) with respect to the maximal intrusion distance \( \xi \), can be computed as:

\[
p^i_\xi = p^{i1}_\xi + p^{i2}_\xi.
\]  

(10)

Note that the probability that the intruder can be detected by a Type I sensor within the maximal intrusion distance \( \xi \), is equivalent to the probability that there is at least one Type I sensor located in the corresponding intrusion detection area \( S^1_\xi \). The probability that no Type I sensor located in the area \( S^1_\xi \) is:

\[
P^1_\xi[n] = 0|n \in N_1, l(n) \in S^1_\xi] = (1 - p^{11}_\xi)^{N_1},
\]  

(11)

where \( z(n) \) represents the number of sensors, and \( l(n) \) represents the location of \( n_{th} \) sensor.

Similarly, the probability that no Type II sensor located in the area \( S^2_\xi \) is:

\[
P^2_\xi[n] = 0|n \in N_2, l(n) \in S^2_\xi] = (1 - p^{22}_\xi)^{N_2}.
\]  

(12)

Then, the probability that no sensor (either Type I or Type II) located in the intrusion detection area \( S^1_\xi \) or \( S^2_\xi \) can be derived as:

\[
P^1_\xi[n] = 0|n \in N, l(n) \in S^1_\xi \cup S^2_\xi] = (1 - p^{11}_\xi)^{N_1} \times (1 - p^{22}_\xi)^{N_2}.
\]  

(13)

Therefore, the probability that there is at least one sensor that within its intrusion detection area specified by the maximum intrusion distance \( D = \xi \), and is able to detect the intruder can be expressed as:

\[
P^1_\xi[D \leq \xi] = 1 - \prod_{i=1}^{2} P^1_\xi[n] = 0|n \in N_i, l(n) \in S^i_\xi] = 1 - (1 - p^{11}_\xi)^{N_1} \times (1 - p^{22}_\xi)^{N_2}.
\]  

(14)

Note that this result can be extended to more complex WSN system with \( H \) types of different sensors as follows:

\[
P^H_\xi[D \leq \xi] = 1 - \prod_{j=1}^{H} P^j_\xi[n] = 0|n \in N_i, l(n) \in S^j_\xi] = 1 - \prod_{j=1}^{H} (1 - p^{j1}_\xi)^{N_i},
\]  

(15)

where \( p^{j1}_\xi \) is the probability that a Type \( j \) sensor resides in its intrusion detection area \( S^j_\xi \) with respect to \( \xi \).

**B. Multiple-sensing Detection**

According the definition of \( k \)-sensing detection, at least \( k \) sensors has to be deployed in the intrusion detection area for jointly detect the intruder successfully. These \( k \) sensors can be any combination of Type I and Type II sensors. For instance, in 2-sensing detection model, these 2 sensors can be 1) two Type I sensors, 2) two Type II sensors, or 3) one Type I sensor and one Type II sensor.

Eq. (10) gives the probability that a Type \( i \) sensor resides in the intrusion detection area \( S^i_\xi \) with respect to the maximal intrusion distance \( \xi \). Then, the probability that \( j \) Type I sensors locate in the area \( S^1_\xi \) can be derived as:

\[
P_k[z(n) = j|n \in N_1, l(n) \in S^1_\xi] = \binom{N_1}{j} (p^{11}_\xi)^j(1-p^{11}_\xi)^{(N_1-j)}.
\]  

(16)

The probability that \( (m-j) \), where \( (j \leq m \leq k) \), Type II sensors locate in the area \( S^2_\xi \) is given by:

\[
P_k[z(n) = m-j|n \in N_2, l(n) \in S^2_\xi] = \binom{N_2}{m-j} (p^{22}_\xi)^{m-j} \times (1 - p^{22}_\xi)^{(N_2-m+j)}.
\]  

(17)

For simplicity of notation, we let \( P^1_k(j) \) and \( P^2_k(m-j) \) represent \( P_k[z(n) = j|n \in N_1, l(n) \in S^1_\xi] \) and \( P_k[z(n) = m-j|n \in N_2, l(n) \in S^2_\xi] \) respectively for Eq. (16) and (17).

Then, the probability, denoted as \( P_k[m] \), that there are exactly \( m \) sensors that can sense the intruder within \( \xi \) is given by:

\[
P_k[m] = P_k[z(n) = m|n \in N, l(n) \in S^1_\xi] = \sum_{j=0}^{m} P^1_k(j) \times P^2_k(m-j),
\]  

(18)

where these \( m \) sensors can be any combination of \( j \) Type I sensors and \( m-j \) Type II sensors, where \( (0 \leq j \leq k) \).

If \( m < k \), the intruder can NOT be successfully detected in \( k \)-sensing detection model, where at least \( k \) should be in the intrusion detection area to jointly detect the intruder. Therefore, \( P_k[m|m \geq k] \) is the probability that the intruder can be sensed by at least \( k \) sensors in the given WSN to detect the intruder, and \( P_k[m|m \geq k] \) can be further represented as:

\[
P_k[m|m \geq k] = 1 - P_k[m|m < k] = 1 - \sum_{m=0}^{k} P_k[m] = 1 - \sum_{m=0}^{k} \left[ \sum_{j=0}^{m} P^1_k(j) \times P^2_k(m-j) \right].
\]  

(19)

Then, the probability that there are at least \( k \) sensors deployed in the area \( S^2_\xi \) to detect the intruder within maximal
intrusion distance $\xi$ can be derived as:

$$P_k[D \leq \xi] = P_k[m|m \geq k] = 1 - \sum_{m=0}^{k-1} \sum_{j=0}^{m} P^1_k(j) * P^2_k(m-j)$$

$$= 1 - \sum_{m=0}^{k-1} \left\{ \sum_{j=0}^{m} \binom{N_1}{j} (p^1_\xi)^j (1-p^1_\xi)^{N_1-j} \right\} \binom{N_2}{m-j} (p^2_\xi)^{m-j} (1-p^2_\xi)^{N_2-m+j} \right\}.$$  \hspace{1cm} (20)

### V. Analysis and Simulation Validation

In this section, we explore the effects of various network parameters on the intrusion detection probability theoretically and experimentally. To be specific, theoretical analysis is done by using MATLAB R2007a, and simulations are done by developing a WSN simulator in C++. Unless otherwise specified, the system parameters in both theoretical and simulation analysis are listed in Table I. All simulation results shown here are the average of 1000 simulation runs. It is observed that the simulation results match the analytical results pretty well, which validates the correctness of our proposed model and theoretical derivation.

#### A. Effect of the Number of Type I Sensors: $N_1$

Fig. 4 illustrates the effect of the number of Type I sensors on the intrusion detection probability of the given heterogeneous Gaussian distributed WSN under both 1-sensing detection and 3-sensing detection model, where we set $r_{s1} = 30$ and $\sigma_1 = 15$. It is clear that the simulation results match pretty well with the analytical results.

It should be noted that we also plot the analytical and simulation results in homogeneous case, where the sensing range of Type I sensors is reduced to the sensing range of Type II sensors as $r_s_1 = r_s_2 = 10$, in contrast to the performance of heterogeneous WSNs. From the figure, we can see that by introducing some high capability sensors, e.g., Type I sensors, the intrusion detection probability increases dramatically, as compared to the gradual increase in homogeneous case. Further, the detection probability under 3-sensing detection is much smaller than 1-sensing detection, given the same network parameters. It is because 3-sensing detection pose a much more strict requirement on the WSN to perform intrusion detection. This can be used to select the right number of heterogeneous sensors for WSN deployment given application requirements.

#### B. Effect of the Sensing Range of Type I Sensors: $r_{s1}$

Fig. 5 illustrates the effects of varying Type I sensors’ sensing range $r_{s1}$ on the detection probability in heterogeneous Gaussian distributed WSNs, where the sensing range of Type II sensor remains $r_{s2} = 10$. We observe that regardless the sensing detection models, the theoretical formula agrees with the simulation outcomes. In addition, the detection probability improves with the increasing of the Type I sensors’ sensing range, under all the sensing-detection models, including 1-sensing detection, 3-sensing detection, and 5-sensing detection. In addition, increasing $k$ poses the requirement to enlarge

### TABLE I

**SYSTEM PARAMETERS**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>$(R, 0)$: the start point of the intruder</td>
<td>$(80, 0)$</td>
</tr>
<tr>
<td>$D_{max}$: the start point of the intruder</td>
<td>30</td>
</tr>
<tr>
<td>$N_2$: the number of Type II sensors</td>
<td>50</td>
</tr>
<tr>
<td>$\sigma_2$: the deployment deviation of Type II sensors</td>
<td>25</td>
</tr>
<tr>
<td>$r_{s2}$: the sensing range of Type II sensors</td>
<td>10</td>
</tr>
<tr>
<td>$N_1$: the number of Type I sensors</td>
<td>$0 \sim 100$</td>
</tr>
<tr>
<td>$\sigma_1$: the deployment deviation of Type I sensors</td>
<td>$10 \sim 50$</td>
</tr>
<tr>
<td>$r_{s1}$: the sensing range of Type I sensors</td>
<td>$10 \sim 50$</td>
</tr>
</tbody>
</table>

---

Fig. 4. Effect of number of Type I sensors on the detection probability in homogeneous and heterogeneous Gaussian distributed WSNs

Fig. 5. Effect of sensing Range of Type I sensors on the detection probability in heterogeneous Gaussian distributed WSNs
the sensing range of the Type I sensors or using more powerful Type I sensors for keeping the required detection probability. To be specific, to provide almost surely detection probability of 1, the sensing range of type I sensors should be at least 30, 35, and 40 for 1-sensing detection, 3-sensing detection, and 5-sensing detection respectively. This can be used to select the right type of sensors for WSN deployment given application requirements.

C. Effect of the Deployment Deviation of Type I Sensors: $\sigma_1$

Fig. 6 evaluates the detection probability with different deployment deviations of Type I sensors, in homogeneous and heterogeneous WSN under 3-sensing detection and 5-sensing detection. In the simulation, we set $r_{s1} = 30$, and $N_1 = 50$. It can be seen from the figure that, there is an optimum deployment deviation that leads to the highest detection probability for all the cases. For example, in the given heterogeneous WSN for 5-sensing detection, the deployment deviation of 30 results in the maximal detection probability, while the deployment deviation of 45 leads to the peak detection probability for homogenous case. This can be used to help in selecting critical parameters in network deployment for optimal performance without increasing the network investment for a Gaussian distributed WSN.

VI. CONCLUSION

In this paper, we address the problem of intrusion detection in a heterogeneous WSN model, where $H(H \geq 2)$ types of sensor are deployed randomly and independently, conforming to Gaussian distribution. This model can be reduced to a homogeneous WSN as a special case. Based on this model, we theoretically and experimentally explore the intrusion detection probability in terms of the network parameters, under both single-sensing detection and multiple-sensing detection models. Theoretical analysis is validated by extensive simulation results in comparing homogeneous and heterogeneous WSNs with varying network parameters. This work can be used to direct the real deployment of WSNs engaged in intrusion detection or related WSN applications using heterogeneous sensors.

REFERENCES