University of Cincinnati

Date: 9/24/2012

I, Narendranad Katneni , hereby submit this original work as part of the requirements for the degree of Master of Science in Computer Science.

It is entitled:

Deployment Strategies and Mechanisms for Intrusion Detection In Wireless Sensor Networks.

Student's name: **Narendranad Katneni**

This work and its defense approved by:

Committee chair: Dharma Agrawal, DSc

Committee member: Yizong Cheng, PhD

Committee member: Yiming Hu, PhD

3034

Deployment Strategies and Mechanisms for Intrusion Detection In Wireless Sensor Networks

by

Narendranad Katneni

B.Tech. (Vellore Institute of Technology, Vellore, India) 2009

A thesis submitted in partial satisfaction of the
requirements for the degree of
Master of Science

in

Computer Science

in the

School of Computing Sciences and Informatics
of the
College of Engineering
of the
UNIVERSITY OF CINCINNATI, OHIO

Committee:
Dr. Dharma P Agrawal, Chair
Dr. Yizong Cheng
Dr. Yiming Hu

Fall 2012

Abstract

Wireless Sensor Networks (WSNs) play a big role in many real life scenarios and are used in a wide range of applications. That includes military, industrial and civilian security and this requires stability, performance and affordability of WSNs. Deployment schemes of sensors play an important role in the design of WSN and contribute to improving it's security. There are various deployment schemes that have their own strengths and weaknesses and each one suits best for a particular set of applications.

In this thesis, we focus particularly on "Intrusion Detection", which is an application of WSNs. We study the existing deployment schemes such as Uniform, Gaussian and identify their strengths and limitations. We then propose two new deployment techniques called Hybrid *Gaussian-Ring* Deployment and Reverse Gaussian Deployment. Hybrid *Gaussian-Ring* offers better border protection and network connectivity, whereas Reverse Gaussian performs better in protecting multiple facilities located within the area protected by the WSN.

Subsequently, we study about Regular Deployment schemes, their applications and their differences from the probabilistic deployment schemes. These are more useful when the area of deployment of WSN is more accessible and non-hostile. We then analyze the performance of various regular deployment schemes and establish which of these is best suited for intrusion detection.

To my parents and grandparents,

for their endless love.

Acknowledgments

I would like to sincerely thank my thesis committee Dr. Dharma P. Agrawal, Dr. Yizong Cheng, and Dr. Yiming Hu for giving me this opportunity and their abundant help and prolific suggestions. Special thanks to Dr. Agrawal for his time, patience and understanding. You take exceptional care of your students, not only at an academic level, but also at a personal level.

My gratitude to the members of Center for Distributed and Mobile Computing (CDMC) lab, current and former, for their co-operation and guidance whenever I needed help with my research work. Special thanks to Vaibhav and Hailong for showing great interest in working with me and mentoring me at every level. I'd be always grateful to you guys for encouraging me when the going got tough. I'd also like to thank all my friends at UC and elsewhere for making my time here fun and worthwhile.

Last but not the least, I'd like to thank my family, my parents Sasikala, Meghanad and my sister Deepti for staying with me through thick and thin and keeping trust in me. Without your support this accomplishment would not have been possible.

Contents

List of Figures

Chapter 1

Introduction

1.1 Wireless Sensor Networks

Security is a very important aspect in everybody's life. We need to have security for guarding our property (physical or digital) from unwanted intrusions or targeted attacks meant for stealing, compromising or destroying it. In some cases, such as in the military, it is of utmost importance to prevent intruders from succeeding in their task. Physically securing the property or location is not an option in every scenario. This leaves us with only choice of monitoring the area in question and detecting the intruders before any harm is caused.

If a particular location needs to be protected from intruders, it is preferable to monitor the general area surrounding this location so as to avoid any damage that can be caused even from a distance. The best way to avoid any damage due to these

intruders is to detect them using various Intrusion Detection techniques. Wireless Sensor Networks are widely used as an Intrusion Detection System.

Wireless Sensor Network (WSN) is a term used to denote a group of sensors than are deployed within or around a designated area to form a cooperative network connected wirelessly. These networks are typically deployed to observe and report particular phenomenon in the area where sensors are deployed. Each node in this WSN is a "sensor" that performs the actual sensing operations [1]. These nodes (sensors) are the building blocks for the WSN and may have capabilities such as sensing, data processing and communication (transmission and reception).

Sensors typically include transducer devices that can be used to sense various phenomenon such as movement, light, sound, heat etc. These sensors are deployed in the networks so that they cover an area, rather than just a particular point. In addition to this, there is a level of overlapping among these sensors in the network so as to ensure that the total area is covered and the sensed data can be propagated in multiple small one-hop transmissions [2].

A WSN need not necessarily have a regular shape or structure. This calls for robust WSN protocols to ensure that the random nature of the network doesn't hinder critical features such as data aggregation and synchronization of the sensor nodes.

The Wireless Sensor Networks usually comprise of a mix of various kinds of nodes. These includes basic sensing nodes which are simple but have limited power source

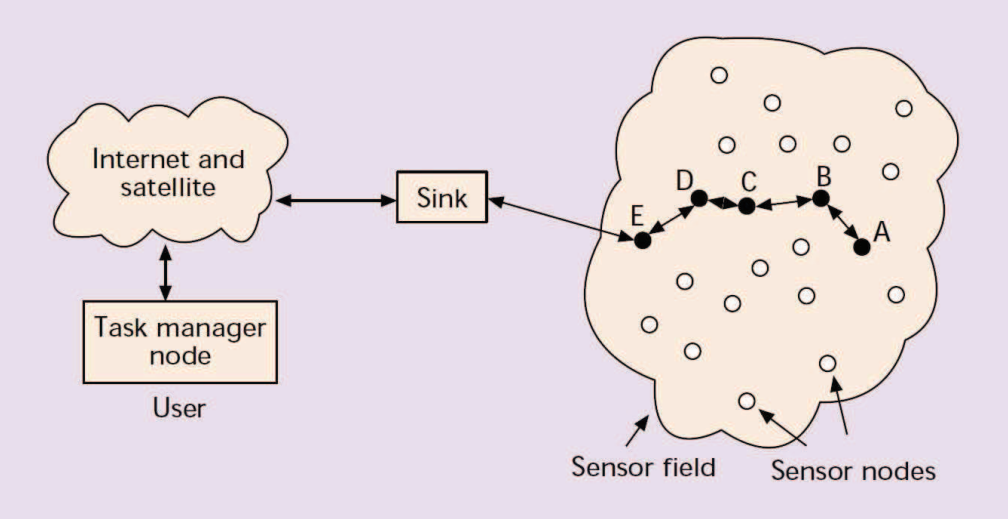


Figure 1.1: A simple Wireless Sensor Network. [2]

that is difficult to replace due to inaccessibility of sensor nodes. This means, they must be limited to perform the most basic of operations such as gathering raw data, data transmission and perform minor computations on-board so that they can reduce the amount of data transmitted and reduce redundancy. The data is propagated across the network based on the protocol being implemented in particular WSN. There are various types of these sensors which can be used for different sensor applications depending on what they can sense. A few examples of sensors are [3]:

- infrared sensors,
- acoustic sensors,
- electromagnetic sensors,
- optical sensors, and

- thermal sensors.

The other type of nodes in the WSN are usually the ones which have a power source and superior computational abilities. These are the nodes that aggregate all the data transmitted by the regular sensors and get information out of it. Such a node is called a Base Station (BS) and the network administrator is connected to them and thus has access to all the data and can generate reports or trigger actuators depending the scenario. The Base Station node, after being deployed, start working in tandem to gather data, process it and generate useful information.

1.1.1 Applications and uses of WSNs

Wireless sensor networks have some unique strengths such as low cost, small size of nodes which are pretty easy to manufacture, inherent distributed nature and ease of programming individual nodes to make the whole network work synchronously on user defined protocols. There are a lot of applications in this modern era of science and technology, that make use of these strength associated with WSNs [4].

WSNs in Military

One of the primary areas that highlight the importance of WSNs is their extensive use in military applications [5]. WSNs are almost perfectly tailored for various scenarios such as surveillance, intrusion detection [6], damage estimation, etc. Deployment of equipment for military applications such as those listed typically have

many constraints. For example, the deployment area might be inaccessible by foot in which case the equipment need to be deployed from the air. The adhoc nature of WSNs helps in this case as the sensors can be deployed from air and in bulk.

In addition to this, the distributed nature of the WSN can be advantageous in case of partial damage to the network. Mobile sensors or redeploying of sensors can repair the damaged network. Surveillance through sensors decreases the need of human beings to be involved in an actual battlefield thereby potentially saving many lives. WSNs can also be used by a military force to protect important locations by placing the sensors at strategic locations. This forms a virtual field of protection in that area and can help in detecting intruders. WSNs can also be used to survey the battlefield before and after military operations. They are also used for long distance attacks in guiding ammunition such as homing missiles.

WSNs in Environment

WSNs have various environmental applications too. Natural disasters such as forest fires or flood can be catastrophic to the environment and need to be handled efficiently. WSNs can be useful in these scenarios to estimate, limit, or even prevent the damage caused. In cases such as forest fires, it is practically impossible for fire fighters to actually go into the affected region. So, WSNs can be used to estimate the point of origin of the fire and also estimate the area actually on fire and the possible movement of the fire into other regions. This can help the authorities to

be better prepared and prevent causing further damage. WSNs can also be used to detect floods by deploying various types of sensors to gauge the rainfall and water level in water bodies [7].

WSNs can also be used to track the movement of various kinds of animals and birds. This can help researchers in finding out the migration patterns of a particular species or monitor the status and health of endangered species. WSNs are also used in observing large biodiversity to automatically collect data and helps the remote user to monitor and analyse the biocomplexity of that area [8]. There are also applications that use WSNs to analyze soil, greenhouse gases, and atmosphere in an agricultural area and thus help in the enrichment of agricultural output and also the health of the crop.

WSNs in Industry and at home

In addition to the military and environmental applications of WSNs, there are also a wide variety of Industrial and Home applications. WSNs are very useful in monitoring the health of large machinery where manual inspections and actuations are either too costly or dangerous. Hazardous and inaccessible parts of these machines can be equipped with a network of sensors to monitor cracks or unusal temperature and pressure and report them immediately to the technician in charge.

WSNs have also found their use in helping people with their home needs. These include sensors and actuators placed within domestic appliances to facilitate users to

manage their homes better. WSNs are used for domestic security by acting as intruder detection systems to detect burglars or strangers. WSNs can be easily programmed and efficiently deployed around the house and can be monitored by the residents from inside the house.

1.2 Limitations and Challenges involved in WSNs

Inspite of the widespread usage of WSNs in various areas, there are still some obvious limitations. It is very important that the challenges posed due to these limitations are well understood and handled effectively such that it won't effect the performance and usability of WSNs. Listed below are some of the limitations of WSNs, followed by the challenges that are posed due to these limitations.

1.2.1 Limitations

Sensor Lifetime

A typical sensor node has a battery with limited lifetime. The small size of the sensor and also the lack of constant power supply means that sensors need to be battery driven (small power source) which will gradually deplete based on the amount of work (sensing, transmitting) done. This limited power supply is used by the sensors for sensing, computation, and mostly for transmission of data. Once the battery is exhausted, the sensor dies out and the typical deployment scenarios of WSNs mean

that these batteries can't be replaced. Hence the administrator of the WSN needs to be aware that any large data communication overheads must be avoided, as much as possible.

Computational Power

Usually, the sensors are equipped with hardware to perform computations. But this hardware's capacity is kept limited because of the space and cost constraints and don't have high computational capacity of work stations or other kinds of wireless devices. So, the sensors cannot perform high intensity computations. Hence, complex cryptographic encryption techniques cannot be implemented on these sensors. Thus, adapting the perfect security mechanism in a WSN is very crucial to reduce the computational burden on the sensors and at the same time, keeping the network safe from malicious nodes or adversaries.

Connectivity and Compromise

Another limitation of WSNs is that they are usually deployed in hostile and remote areas where there is the threat of some nodes being destroyed or even worse, get compromised by adversaries. Sensors are typically deployed in bulk, but if a large number of sensors are destroyed then the WSN can get disconnected. This means that the network is separated into two or more parts which cannot communicate with each other. This leads to crucial data being lost and drastically reduces the performance

of the WSN.

In some cases the sensors might be compromised and might be stealing important information or feeding wrong information into the WSN, trying to disrupt it's functionality. This is a possible scenario and it is a challenge for the researchers to devise a robust and resilient security mechanism.

1.2.2 Challenges

The above mentioned limitations pose some serious challenges for researchers and it is very important that appropriate measures are taken to overcome them. One of them is the design challenge of scalability [2] and flexibility of the WSN. The communication and authentication protocols must be designed in such a way that adding new nodes or changing the topology of the WSN should not disturb the stability of the system. Another design challenge posed by WSNs is that the sensors share the load of transmission as much as possible to avoid putting more burden on a few nodes and thus forcing them to quickly use up their power source.

A naive solution to counter these limitations would be to deploy a very large amount of sensors. But, this solution is not practical because of the cost involved and also the challenge in deploying such a large number of sensors. Thus, one of the important WSN design challenges for researchers is to intelligently deploy the sensors in such a way that they maximize the productivity of the network, minimize the cost and at the same time overcome the limitations of WSNs to provide a robust

framework.

1.3 Purpose of this study

Wireless Sensor Networks play a big part in many real-life scenarios and are used extensively for a wide spectrum of applications. Two of those are military, civilian security and this calls for a constant improvement on the stability, performance and affordability of WSNs. We consider that deployment of sensors is an important aspect in the design of a WSN and can definitely contribute to improving the security of WSN. Various types of deployment schemes are possible and there is surely no single schemes that works best for all applications or scenarios. Each scheme has it's own strengths and weaknesses and it is up to the people deploying the network to select a better suited scheme for their particular requirements.

In this thesis, in Chapter 2, we focus on a particular type of security issue, i.e., intrusion by an external aggressor and explore various deployment schemes that can be considered for such a scenario. We study the existing proposals such as Poisson deployment, Gaussian deployment and identify that each have their own strengths and limitations. Subsequently, in Chapter 3 we propose a novel technique called Hybrid *Gaussian-Ring* Deployment which offers better border protection and network connectivity as compared to the existing deployment schemes in Chapter 2. In Chapter 4, we propose another scheme called Reverse Gaussian Deployment which works better in protecting multiple facilities located within the area covered by the

WSN.

There are also many applications of WSNs which satisfy the criteria for using Regular Deployment schemes. This means that for these specific applications, the area is easily accessible and not hostile, Regular deployments are preferable over the aforementioned probabilistic schemes. Thus, we explore the various kinds of Regular deployment schemes and analyze and compare the performance of each of them in Chapter 5. Finally, Chapter 6, summarizes the results and discuss topics for future research.

Chapter 2

Background and Preliminaries

2.1 Intrusion

In this chapter, we look into intrusions in Wireless Sensor Networks (WSNs) and how these affect the performance of the network. Then, we will look into how proximity of intruders to the network can facilitate topological attacks and later we assert the importance of good deployment schemes in avoiding these types of attacks. We also delve into the previous work done on deployment schemes.

2.2 Types of Intrusion attacks

Since WSNs are usually placed in the open and hostile environment, they are vulnerable to attacks. Therefore, it is important to understand the types of attacks that could be typically used on a WSN.

There are two types of damages caused by intruders on the WSN. One way is to attack the network physically and destroy or capture some of the nodes. Here, the aggressor (intruder) tries to sabotage the sensor hardware [9]. These types of attacks can be prevented by sensing the intruder early with the means of audio [2] [10] or motion sensing.

Another way intruders attack a WSN is to logically influence it. As, this is an intelligent way to attack the network, the intruder doesn't physically destroy the nodes and tries to damage the data being captured and aggregated by the sensors. There are various ways in which this is achieved as explained by Karlof et al. [11]. Such an he attack might be performed by denial of service by flooding the network with garbage data [12]. A few other logical attacks are wormhole attacks [13], sinkhole attacks [14], Sybil attack [15], selective forwarding, spoofing information [11], etc. These attacks cause a topological distortion by confusing the normal sensor nodes about the location of their neighbors and is able to portray a false network structure and hierarchy to other nodes [16].

2.2.1 Protection against Intrusion

A WSN needs to be protected from these kinds of attacks by employing various well discussed countermeasures. Some of these countermeasures are to have a strong encryption schemes in place to avoid data manipulation and loss. There are also working models of routing mechanisms that make use of the unique properties of a WSN

to detect and avoid malicious nodes [17]. So, the typical intrusion detection systems combine the techniques of intrusion prevention, strong ecryption/authentication and robust routing to provide security to WSNs.

2.2.2 Proximity/Topological Intrusion attacks

It can be noted from the above intrusions and detection schemes that the proximity of the intruder to the WSN topology is very crucial. Both physical or logical attacks require close access to one or more sensors nodes. Thus, it is important to make sure that proximity access of the WSN nodes to the intruder must be prevented or in the worst case detected soon enough.

2.2.3 Need for Good Deployment Schemes

So, the question is where do deployment schemes come into the picture? Inspite of the above mentioned intrusion detection schemes, there is still scope for ways to better protect the WSN by intelligently placing the nodes in the network. This should help the network to carry on it's designated functionality and at the same time facilitate better intrusion detection without any big cost or time overhead. In the next two sections, we'll look at the various kinds of WSN deployment schemes.

2.3 Wireless Sensor Network Deployments

2.3.1 Probabilistic Deployments

In this section, we discuss previous work done on sensors using various deploying techniques in WSNs. Some of the earliest work is done by Dousse et al. [18] wherein they focus on finding the delay in detecting an intrusion when the sensors are deployed randomly in a particular area. The authors in [18] identified the importance of detecting an intruder in a WSN and also highlighted the need for the WSN being well connected to facilitate a successful detection of intrusion and subsequent alert generated by the Base Station (BS) or sink node. Hence, we can deduce that the coverage and connectivity are two very important aspects for Intrusion detection in a WSN. This further supports the fact that the technique of deployment of sensors in WSN is as critical as the detection and communication methods in the Intrusion Detection System (IDS).

Wang et al. [19] analyzed the performance of Intrusion detection in WSNs by varying the network parameters such as node density, sensing range, etc. and finding the resulting effect on the intrusion detection probability and maximum distance travelled by the intruder before eventual detection. The effect of transmission range on the connectivity to the BS of the WSN is also studied.

Further work took off from this point and significant contribution is made by Wang et al. [20] to estimate the performance of Intrusion detection in WSNs when

the sensor nodes are deployed following a Uniform Random scheme. This is done by deploying sensors at a particular density in a given area ensuring that the total area is uniformly covered with sensor nodes. Performance evaluation is done based on the techniques proposed in Xiaodong. This type of sensor deployment is very useful when the threat is from the borders, which is usually the case.

Later, Wang et al. [21] analyzed another technique in which the the sensor nodes are deployed in a 2-D Bivariate Gaussian distribution. The authors of [21] claim that this type of distribution ensures that there is added protection to the center of the WSN where the Base Station(BS) is located and has an ease of deployment as compared to Uniform. Further study is done in [22] on the effects of using a heterogeneous mix of sensor nodes (use of few high performance sensors) in the Gaussian deployment. However, this deployment strategy might not be effective if the intrusion is from the border as the boundary has very sparse distribution of sensor nodes and any kind of detection usually takes a long time. The intruder can cause significant harm during that period.

Considering the fact that each of these deployments have their own advantages and disadvantages, we modeled our system to follow a hybrid deployment strategy that makes use of the advantages of both Gaussian and Uniform distribution to ensure faster detection by better protection at the border while, at the same time, being real cost effective.

2.3.2 Deterministic Deployments

In this section we look into Deterministic or Regular Gaussian Deployment schemes and their applications in various real-world scenarios. Unlike probabilistic deployment schemes which are typically used in hostile and inaccessible areas, deterministic deployments can be used in applications where the location of each and every sensor can be pre-meditated. Gao et al. [23] show that probabilistic deployments can be inefficient and costly in these scenarios. This is further asserted by Gajbhiye et al. [24]. There are three types of Regualar deployments namely, Square, Hexagon and Triangle. The performance of these three schemes under various communication protocols is well documented as seen in [25], [26], [27] . However, the lack of a proper performance analysis of these regular deployments in Intrusion Detection encouraged us to perform a comparison of the efficiency of Intrusion Detection in Square, Hexagon and Triangle WSNs.

Chapter 3

Hybrid *Gaussian-Ring* Deployment

3.1 Introduction

In this section, we look at how specific deployment of sensor nodes affects security of the network with respect to an external attack where the intruder aims to physically penetrate through the area protected by or monitored by the network. These classes of WSNs are typically surveillance or data aggregation networks where sensor nodes are deployed to monitor a pre-specified area. It is vital that malicious mobile intruders are promptly detected by the network, before a serious attack can be launched or a node is compromised [28].

The sensing range of these sensors are much smaller than the transmission range. Therefore, even a fully connected network in terms of transmission coverage may have significant gaps or regions in the network where there is little or no sensing

coverage, making the network highly susceptible to intruders. Clearly, a large sensor deployment can provide adequate sensing coverage for a quick detection of intruders. However, this is neither a cost effective nor practical way to deploy sensors. A number of studies have analyzed many realistic probabilistic deployments of sensors such as Uniform, Gaussian and Poisson distributions that estimate the detection probability of an intruder attacking the network.

Uniform and Gaussian deployments each have their own advantages and disadvantages. A uniform deployment works well for intruders that attacks from the boundary of the area under protection, but it can suffer from the energy hole problem [29] and can not provide extra protection to sensitive areas within the network. The Gaussian deployment can address the energy hole problem and can provide differentiated intrusion detection capabilities around the network and provide additional protection to key areas within the network. However, they are very susceptible to attacks from the boundary of the network. An intruder entering the boundary of the network, can travel a significant distance before being detected. Therefore, these two schemes can not satisfy the security requirements of different applications.

We propose a hybrid deployment scheme to take advantage of both the Uniform and Gaussian deployments. Our scheme can satisfy security requirements of a broader class of applications that can not tolerate intrusions from the boundary of the network and require differentiated detection capabilities within the network. An example of this application would be to protect a military installation in a hostile environment.

The installation may require high detection capabilities for a number of regions within the base, but also can not tolerate any infiltration at the perimeter either. This can be easily adopted by 3-D aerial space as well.

In this section, we propose a probabilistic hybrid *Gaussian-Ring* deployment and provide the network deployment parameters that are better suited for applications that requires differentiated intrusion capabilities and border protection.

3.2 Hybrid *Gaussian-Ring* Deployment Strategy for Intrusion Detection

In this section, we propose our hybrid deployment strategy for intrusion detection [30]. Combining the benefits of Gaussian and Uniform deployment strategies, we introduce an analytical model for coverage and connectivity of hybrid deployed WSN. To elaborate our proposed method, we would like to review the existing models for Gaussian and Uniform strategies. Then, we present an analysis of hybrid *Gaussian-Ring* deployment strategy.

3.2.1 Random Distribution Network

Consider that a large number of intrusion detection sensors (N) are being deployed uniformly and independently in a two-dimensional geographical region D, and the BS is at the center. Location of sensors could be modelled as a stationary 2-D Poisson

point process [31]. Denote the number of sensors in field D as $N(D)$, which follows the Poisson distribution:

$$P(N(D) = k) = \frac{(\lambda|D|^k e^{-\lambda|D|})}{k!}, \tag{3.1}$$

where λ is the density of Poisson point process, $|D|$ is the area of region D. Liu et al. [31] show that for such a randomly deployed sensor network in a two-dimensional infinite plane, the probability f_a that a point is covered by at least one sensor is as follows:

$$f_a = 1 - e^{-\lambda\pi r_s^2}, \tag{3.2}$$

where λ is the node density and r_s is sensing range of each sensor node. Also, Bettstetter in [32] showed a relationship between the sensor transmission range r_c and the network connectivity as:

$$r_c \geq \sqrt{\frac{-\ln(1 - p^{1/n})}{\rho\pi}}, \tag{3.3}$$

where p is the probability that no sensor node in the WSN is isolated, n is the total number of sensor nodes deployed in the large area A satisfying $A \gg r_c^2\pi$, and $\rho = n/A$ is the node density.

3.2.2 Gaussian Distribution Network

Now, we consider that a network with N intrusion detection sensors are deployed in a two-dimensional plane following two-dimensional Gaussian distribution as:

$$f(x, y) = \frac{1}{2\pi\sigma_x\sigma_y} e^{-\frac{(x - x_i)^2}{2\sigma_x^2} + \frac{(y - y_i)^2}{2\sigma_y^2}}, \tag{3.4}$$

where (x_i, y_i) is the position of BS, σ_x and $\sigma_y$are the standard deviations for x and y axes. To simplify the analysis, let BS position $x_i = 0, y_i = 0$, and we use only the Gaussian distribution with $\sigma_x = \sigma_y$ considered in the analysis of [33]. For the scenario with a $\sigma_x \neq \sigma_y$ distribution, result could be derived in the same way, but are not included here. Then we call Gaussian distribution network with $\sigma_x = \sigma_y$ as Gaussian distribution network for short and 2D Gaussian distribution probability function can be presented as:

$$f(x, y) = \frac{1}{2\pi\sigma^2} e^{-\frac{x^2 + y^2}{2\sigma^2}}. \tag{3.5}$$

To analyze Gaussian distribution network, it is modeled as a disk as is done in [33]. The disk with radius R is divided into multiple annuli as shown in Fig.4.2, and the center of disk is at the origin of XY plane, where the BS is located. The width of annuli is r_c, which is the transmission range of sensor node. Annuli are marked from 1 to k where $k = \lceil R/r_c \rceil$. Then, any sensor node with distance d to sink node always falls inside ith annuli of disk if d satisfies $(i-1) \times r_c < d \leq i \times r_c$. Further more, any sensor in annulus i can communicate with sensors in annulus $i-1$ in one-hop manner. Since the network follows a Gaussian distribution, inner annuli sensor node density ρ_r is larger than outer annuli node density.

Although Eq. (4.14) is proposed for a uniform random distribution, we apply this model to calculate the network connectivity in each annulus after an appropriate annuli division of the whole region. This means that in an annulus i, as long as annulus width $r_c \ll R$, distribution of sensor nodes is approximated as a uniform

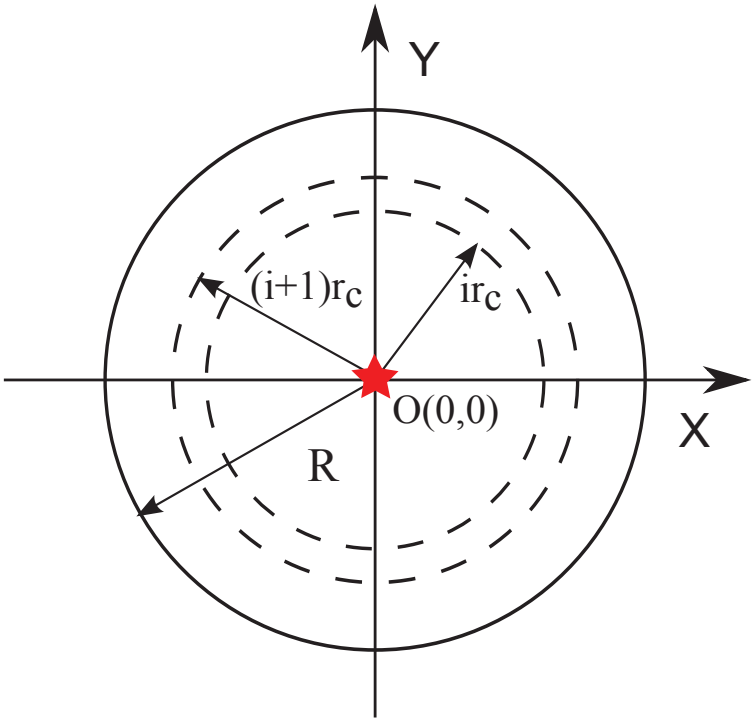


Figure 3.1: Disk Annuli Division of Network

distribution. Rewriting Eq. (4.14) for annulus i as:

$$P_c^i \geq (1 - e^{-\rho_i^r \pi r_c^2})^{N_i}, \tag{3.6}$$

where N_i is number of sensors within the annulus i and ρ_i^r is ith annulus node density. When the deployed target region and radio transmission range r_c are given, Eq. (3.6) indicates the relation between the connectivity probability and the number of deployed sensors. If the network connectivity requirement is satisfied in the outermost annulus k with N_k sensor nodes, then the network can guarantee connectivity of the network, as all inner annuli of Gaussian distributed network have a higher node density than the outermost annulus. Assuming the network connectivity requirement

is P_c^* and we need at least N_k^* sensor nodes in annulus k satisfying:

$$P_c^k \geq (1 - e^{-\rho_k^r \pi r_c^2})^{N_k^*} = P_c^*. \tag{3.7}$$

3.2.3 Hybrid *Gaussian-Ring* Deployment Network

To detect intrusion for border and center area of monitored region, we propose that WSNs are deployed in a hybrid manner, called *Gaussian-Ring*, mixing Gaussian and uniform distribution. Assume area of monitored region is A and we have a WSN with N wireless sensors, with transmission range r_c and sensing range r_s, for intrusion detection. We use notation N_g to denote the number of sensors for Gaussian deployment and N_u for the number of sensors following uniform deployment. The sink node or the BS is assumed to be located at the center of the region, whose location is set as origin of plane $O(0, 0)$ and whole region is divided into multiple annulus as shown in Fig. 4.2. N_g sensors are deployed over the whole region following Gaussian distribution, satisfying connectivity probability P_c^*, for better protection of the central area of the whole monitored region. Furthermore, based on annuli division of monitored region, N_u sensors are uniformly distributed in annulus k, i.e., the outermost ring, satisfying coverage requirement P_s^* and connectivity requirement P_c^*, to protect border area. Since connectivity of annulus k of Gaussian distributed network is guaranteed, the uniform deployment network is also connected by sensors in annuli 2 through $(k - 1)$ with the BS at the center.

Uniform Deployment Network in Annulus k

Coverage of WSN depends on uniformly distributed network and coverage probability P_s can be calculated based on Eq. (4.12) as:

$$P_s = 1 - e^{-N_u \pi r_s^2 / A_k}, \tag{3.8}$$

where A_k is the area of annulus k. r_s depends on the sensing capability of the sensor and once r_s is set, coverage probability would increase when more sensor nodes are deployed in a given area. Assume the coverage requirement as P_s^*(e.g., 95%). To guarantee the network coverage in annulus k, we need at least N_u^* sensors satisfying:

$$P_s = 1 - e^{-N_u^* \pi r_s^2 / A_k} = P_s^*. \tag{3.9}$$

Eq. (3.9) provides a theoretical support to optimize the cost of WSNs while meeting the coverage requirement at the same time.

Suppose connectivity requirement of uniformly deployed WSN network is P_c^* and the minimal number of sensor nodes to guarantee connectivity is N_u^{**}. Connectivity of sensor nodes in annulus k could be calculated by Eq. (4.14), and we could find the minimal number of sensors for uniformly deployed WSN in annulus k as:

$$N_u = \min\{N_u^*, N_u^{**}\}. \tag{3.10}$$

Gaussian distributed Network

To guarantee the connectivity requirement, P_c^*, of Gaussian distributed WSN, we need at least $N_{g_k}^*$ sensors deployed inside annulus k. Then, the whole network,

including both uniform and Gaussian network, are connected. We have N_{g_k} out of N_g sensors deployed in annulus k expressed as:

$$N_{g_k} = N_g \times P_k, \tag{3.11}$$

where P_k is the probability that a sensor node is in the kth annulus of Gaussian distributed WSN. Based on the probability that a sensor node is in the ith annulus P_i derived in [33]:

$$\begin{aligned} P_i &= \int_{(i-1)r_c}^{ir_c} \frac{1}{2\pi\sigma^2} e^{\frac{-l^2}{2\sigma^2}} 2\pi l dl \\ &= e^{-\frac{(i-1)^2 r_c^2}{2\sigma^2}} - e^{-\frac{i^2 r_c^2}{2\sigma^2}}, \end{aligned} \tag{3.12}$$

we have:

$$P_k = e^{-\frac{(k-1)^2 r_c^2}{2\sigma^2}} - e^{-\frac{k^2 r_c^2}{2\sigma^2}}. \tag{3.13}$$

According to Eq. (3.7), the connectivity of Gaussian distributed network P_c should satisfy:

$$P_c \geq P_c^k \geq (1 - e^{-\rho_k^r \pi r_c^2})^{N_{g_k}^*} = P_c^*. \tag{3.14}$$

Based on the above analysis, we obtain a relation between N_g and the connectivity requirement P_c^* as:

$$N_g \times P_k = N_{g_k} \geq N_{g_k}^*. \tag{3.15}$$

To obtain the value of σ and N_g, optimization algorithm need to be applied similar to [33]. Details of the optimization is out of scope of this work. We notice that optimized parameter impact only the lifetime of WSNs, but not the comparison of

different strategies. Thus, only a simplified method to estimate σ is applied in our simulation to illustrate the performance of our proposed hybrid deployment strategy. The formula:

$$(1 - e^{-R^2/2\sigma^2}) = 99\%, \tag{3.16}$$

ensures that 99% of the sensors deployed using Gaussian (with σ Standard Deviation) fall in the region with Radius R. By rearranging the equation we can calculate σ for a given R.

3.3 Simulation

Based on aforementioned model, we simulated the Hybrid *Gaussian-Ring* Deployment technique for Intrusion detection and obtained very encouraging results. The simulation set up, evaluations metrics and their analysis are discussed below.

3.3.1 Setup

Our simulation set up considers a circular area A of radius 500 units in which the WSNs are deployed. The sensor nodes deployed have the transmission (r_c) and sensing ranges (r_s) of 100 and 10 units respectively which are close to the ranges of typical sensors. The intruder attacks from a random point on the boundary of the circular area A. Two types of attacks are simulated:

Border to Center

The intruder enters through a random point on the boundary and heads straight to the center of the circle.

Border to Border

The intruder enters through a random point on the boundary and leaves through another random point, travelling through the area in a straight line.

The metrics used for the performance analysis are:

1) Intrusion Distance

The total distance the intruder covered before being detected by the WSN.

2) Sensors Alerted

The number of sensors that are alerted by the intruder when it is inside the WSN.

The Hybrid *Gaussian-Ring* Deployment has sensors uniformly distributed (N_u) in the outermost Annulus (thickness r_c) with sufficient density to ensure atleast P_s^* (90%) coverage. In addition to this, using Gaussian distribution, sensors are deployed assuming the center of circle A as the mean and Standard Deviation σ as calculated by Eq. (3.16). The number of sensors being deployed in a Gaussian distributed WSN

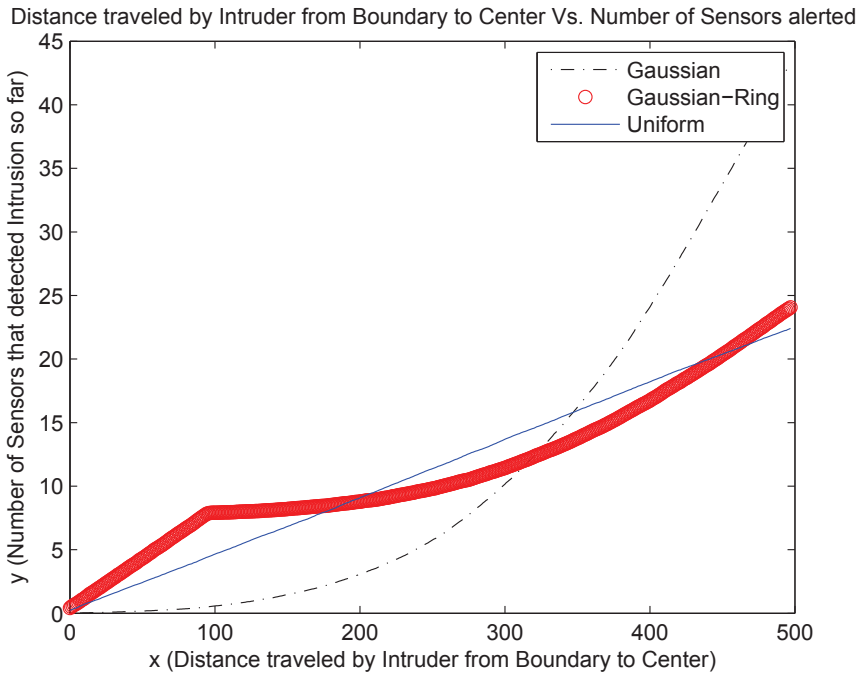


Figure 3.2: Intrusion Distance vs. Sensors Alerted in Border to Center Scenario

is calculated using Eq. (3.14) and Eq. (3.15) to ensure 90% connectivity.

The level of connectivity P_c^* is varied from 60% to 90% to get a wide range of values for total Number of Sensors deployed, $N = N_u + N_g$. The simulation is run for 3 different deployments of sensors: Gaussian, Uniform and Hybrid *Gaussian-Ring*, and the average of 1000 runs is used to enhance the accuracy of our results. We used Network Simulator in Java to perform the simulations.

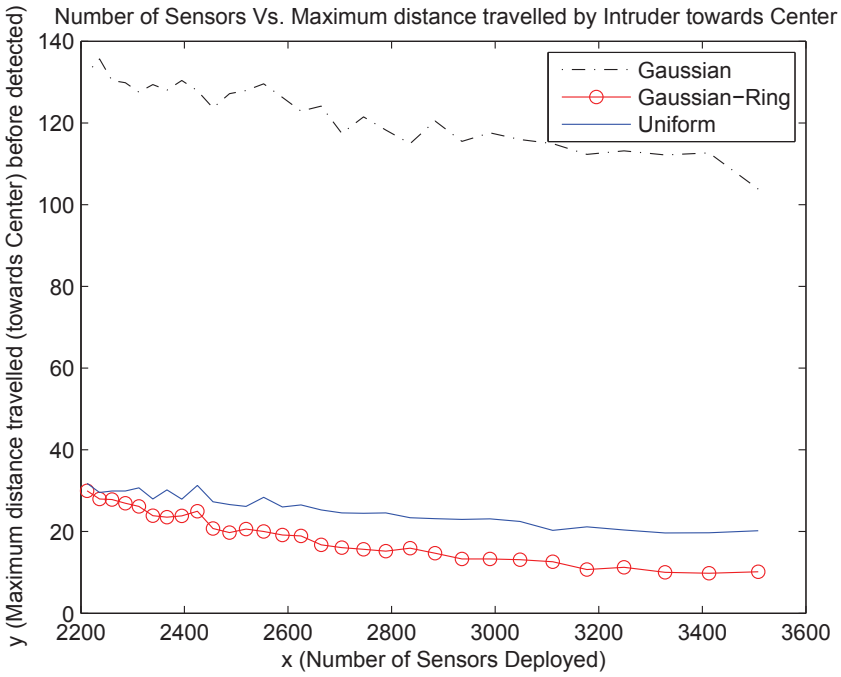


Figure 3.3: Intrusion Distance (Border to Center) vs. Number of Sensors

3.3.2 Analysis of Results

From Fig.(3.2), we can see that, in an Border to Center scenario, Hybrid *Gaussian-Ring* performs better than the other two in detecting intrusion very early. The X-axis represents the distance travelled by the intruder towards the center and the Y-axis represents the sensors that are alerted by the time the intruder reaches that point. So, it basically represents how quickly the intrusion is detected and how many sensors are alerted in the process. It can be observed from the figure that *Gaussian-Ring* has got a higher value at the start, which means the intruder is detected near the border itself and this reinforces our design with a better secured border protection.

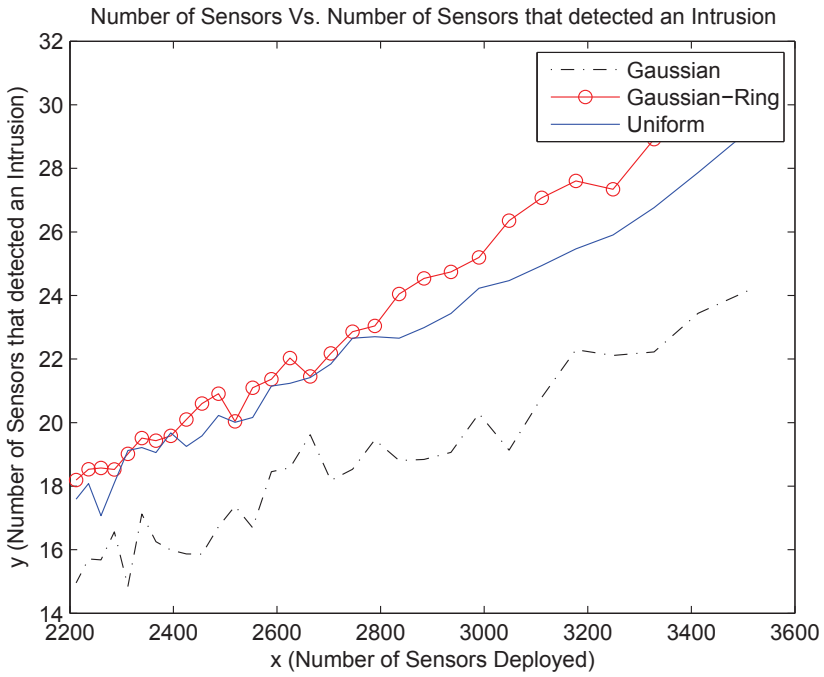


Figure 3.4: Sensors Alerted (Border to Center) vs. Number of Sensors

In Fig. (3.3), in an Border to Center scenario, we show the total number of sensors deployed vs. the maximum distance the intruder can travel before it is detected. We also see that Gaussian performs very badly as it has a large percent of its available sensor nodes near the center. Hence, it can't detect intrusions until the intruder is very close to the center. On the other hand, Uniform performs better than Gaussian. But, *Gaussian-Ring* again comes out as having the best return for the same cost ($N = N_u + N_g$). It can be observed that as the number of sensors increases, *Gaussian-Ring* gives improved performance and with sufficiently large number of sensors, can provide almost instant detection, whereas Gaussian and Uniform need a large number of sensors to provide a similar performance.

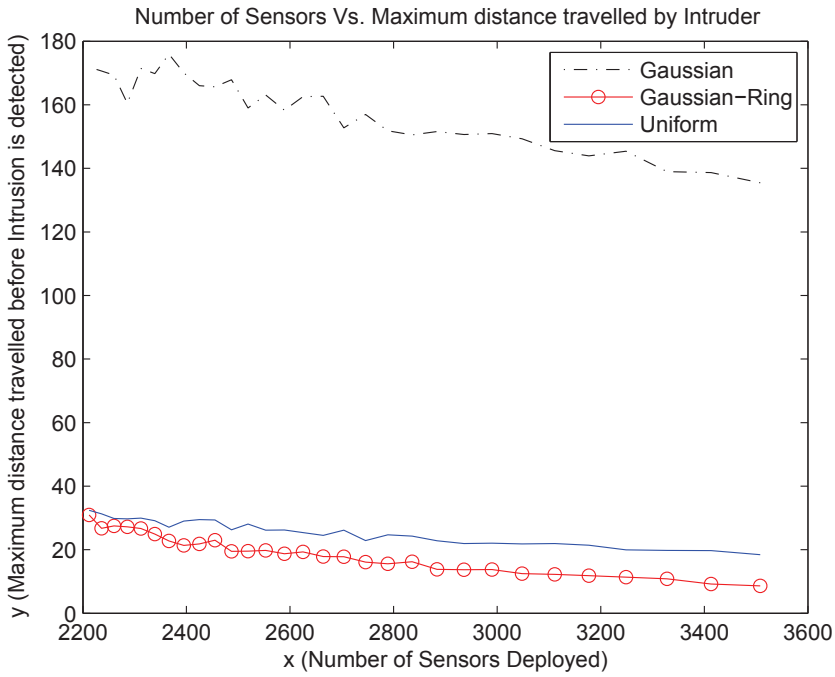


Figure 3.5: Intrusion Distance (Border to Border) vs. Number of Sensors

In Fig. (3.4) and Fig. (3.5), we compare the performance of three deployments in an Border to Border scenario. Fig. (3.4) shows the number of sensors that detect intrusion vs. the number of sensor nodes used. *Gaussian-Ring* performs similar to Uniform scheme for smaller number of sensors, but eventually improves as the number of sensors is increased.

Similarly, Fig. (3.5), plots the maximum distance travelled by the intruder before it is detected vs. the total number of sensors deployed. Gaussian shows poor results as the intruder is allowed to roam in the protected area for too long before detected (due to the sparsely populated nature of border in Gaussian deployed WSNs). But, once again *Gaussian-Ring* does better than both Gaussian and Uniform due to denser

borders.

3.4 Conclusion

There is a lot of scope for further improvements that can be done to the Hybrid *Gaussian-Ring* Deployment Technique such as using Heterogeneous sensors or having multiple concentric rings of protection. We plan to consider these in our future work.

Finally, we conclude that in all the four scenarios that are critical for border protection, secure center (BS) and at the same time requiring well connected networks, our novel Hybrid *Gaussian-Ring* Deployment strategy outperforms both the Uniform and Gaussian Deployment techniques in terms of quicker detections and the number of sensor alerted in the scheme. Our idea of a hybrid approach combining two existing deployment strategies succeeds in matching their underlying characteristics and also negates their respective weaknesses.

Chapter 4

Reverse Gaussian Deployment

4.1 Introduction

In the previous chapters, we discussed about various deployment strategies for Intrusion detection in WSNs that are popular and widely used. These include Gaussian, Poisson and our proposed Hybrid-Gaussian Ring Deployment. In this chapter, we propose a modification of the Gaussian Deployment scheme and call it Reverse Gaussian Deployment. We provide the design model of this deployment and then compare its performance against the existing techniques.

4.2 Reverse Gaussian Distributed Deployment

In this section, we consider the deployment of a WSN in a two-dimensional monitored area and derive the probability distribution function (PDF) of the two-

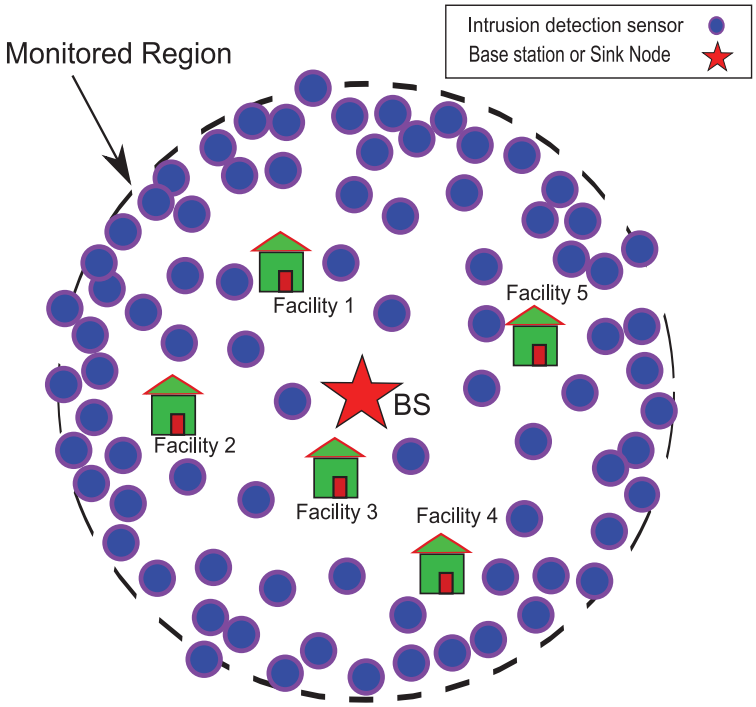


Figure 4.1: Reverse Gaussian distributed WSN for intrusion detection

dimensional Reverse Gaussian distribution $f(x, y)$ using the two-dimensional Gaussian distribution $g(x, y)$ [34].

The two-dimensional Gaussian distribution is:

$$g(x,y) = \frac{1}{2\pi\sigma_x\sigma_y} e^{-\left(\frac{(x-\mu_x)^2}{2\sigma_x^2}+\frac{(y-\mu_y)^2}{2\sigma_y^2}\right)}, \tag{4.1}$$

where σ_x and σ_y are the standard deviations for x and y axis respectively, and μ_x and μ_y are the mean for x and y axis respectively. The BS or sink node is situated at the central point (0, 0). Thus, the means μ_x and μ_y are both 0. In this work, we only consider the scenario that the standard deviations across both the dimensions are equal and independent of each other ($\sigma_x = \sigma_y = \sigma$). For scenario $\sigma_x \neq \sigma_y$

distribution, result could be derived in the same way and are not included in this chapter. Thus, we rewrite the 2D Gaussian distribution PDF as:

$$g(x,y) = \frac{1}{2\pi\sigma^2} e^{-\left(\frac{x^2+y^2}{2\sigma^2}\right)}. \tag{4.2}$$

From the probability point of view, a Reverse Gaussian distributed WSN contains more sensor nodes far away from the BS than closer to the BS, which is opposite to the 2D Gaussian distributed WSN. Thus, the PDF of 2D Reverse Gaussian distribution can be derived from the upside down curve of the 2D Gaussian distribution:

$$-g(x,y) = -\frac{1}{2\pi\sigma^2} e^{-\left(\frac{x^2+y^2}{2\sigma^2}\right)}. \tag{4.3}$$

To guarantee the probability is always non-negative in the PDF, we scale the PDF by its height of the peak which is $\frac{1}{(2\pi\sigma^2)}$ and we have:

$$f(x,y) = \frac{C}{2\pi\sigma^2} - \frac{C}{2\pi\sigma^2} e^{-\left(\frac{x^2+y^2}{2\sigma^2}\right)}, \tag{4.4}$$

where C is a constant used to adjust the Reverse Gaussian distribution based on different sizes of the WSN. The Reverse Gaussian distribution must satisfy a constraint that the cumulative probability of the whole monitored area must be 100%. Assume the radius of the area covered by WSN be R. To satisfy the coverage constraint,

we can calculate cumulative probability of Reverse Gaussian distribution over the monitored area as:

$$f(x,y) = \iint C * \left[\frac{1}{2\pi\sigma^2} - \frac{1}{2\pi\sigma^2} e^{-\left(\frac{x^2+y^2}{2\sigma^2}\right)} \right] dxdy. \tag{4.5}$$

To satisfy the PDF constraint, constant C can be expressed by:

$$\begin{aligned} C &= \frac{1}{\iint [\frac{1}{2\pi\sigma^2} - \frac{1}{2\pi\sigma^2} e^{-\left(\frac{x^2+y^2}{2\sigma^2}\right)}] dxdy} \\ &= \frac{2\sigma^2}{R^2 + 2\sigma^2(e^{-R^2/2\sigma^2} - 1)}. \end{aligned} \tag{4.6}$$

Then, Eq. (4.4) depicts the PDF of a 2D Reverse Gaussian distribution.

4.3 Coverage and Connectivity of Reverse Gaussian Distributed WSN

In this section, we discuss the coverage and connectivity of the Reverse Gaussian distributed WSN. Coverage and connectivity are two fundamental constraints for the sensor deployment. Without considering these two constraints, the performance of any WSN would be less than satisfactory.

To analyze coverage and connectivity, we first divide the whole WSN into multiple annuli as is done in demin. Multiple annuli in the circular WSN area with radius R

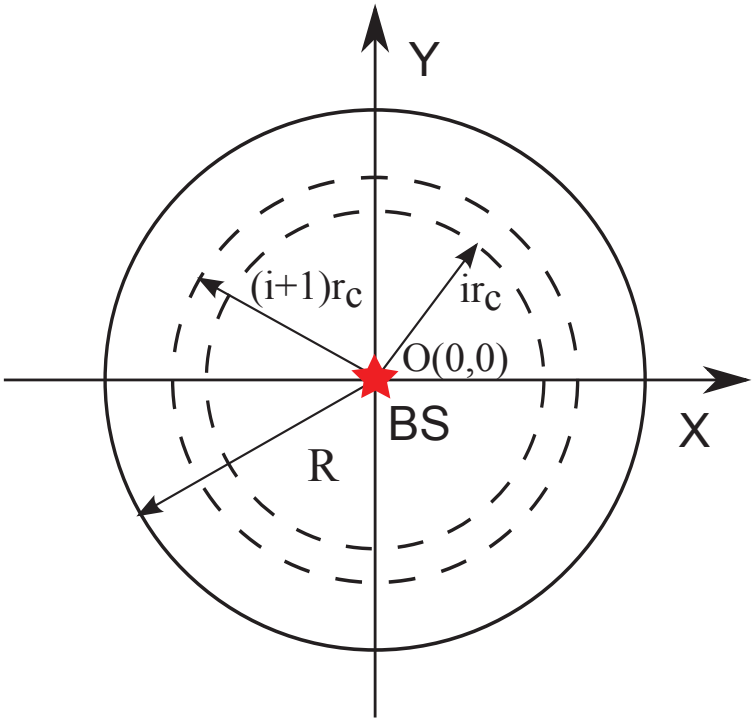


Figure 4.2: Disk Annuli Division of *Circular WSN*

is shown in Fig. 4.2, and the center of disk is at the origin of XY plane, where the BS or the sink node is located. The width of annuli is r_c, which is adjusted equal to the transmission range of each sensor node. Annuli is marked from 1 to k where $k = \lceil R/r_c \rceil$. Then, any sensor node with distance d to the sink node always falls inside ith annuli of disk if d satisfies $(i-1) \times r_c < d \leq i \times r_c$. Our original Reverse Gaussian distributed WSN has various sensor nodes densities for different locations, which makes analysis very complicated. By dividing a WSN into multiple concentric annuli, sensor nodes distributed in each annulus can be approximated as uniformly distributed, as long as the annulus width $r_c \ll R$. Then, the coverage and

the connectivity analysis can be performed for individual annulus since sensor nodes density is approximated to be the same inside each annulus.

Assume that the number of sensor nodes in annulus i is N_i and the total number of sensor nodes in the WSN is N. Then, with disk annuli modeling, we have the relation between N_i and total number N as:

$$N_i = N \times P_i, \tag{4.7}$$

where P_i is the probability that a sensor node is in the ith annulus of WSN and can be calculated by:

$$P_i = F_i - F_{i-1}, \tag{4.8}$$

where F_i indicates a cumulative distribution function (CDF) of two-dimension Reverse Gaussian distribution over a circular area, whose radius is $i \times r_c$. It is clear that F_i is the volume enclosed by XY plane and Gaussian distribution function $f(x, y)$. Since $f(x, y) = f(-x, y) = f(x, -y) = f(-x, -y)$, $f(x, y)$ is symmetric to X, Y axis. The whole volume enclosed by $f(x, y)$ boundary is four times of the volume in the first octant (X^+, Y^+, Z^+) . Then we can compute F_i as:

$$\begin{aligned} F_i &= 4F_i^{(X^+,Y^+,Z^+)} \\ &= 4\int_0^{ir_c}\int_0^{\sqrt{(ir_c)^2-x^2}} \frac{C}{2\pi\sigma^2} - \frac{C}{2\pi\sigma^2}e^{-(\frac{x^2+y^2}{2\sigma^2})}dxdy. \end{aligned} \tag{4.9}$$

Using a polar coordinates transformation, we have:

$$F_i = \int_0^{ir_c} \int_0^{\frac{\pi}{2}} \frac{2C}{\pi\sigma^2} r - \frac{2C}{\pi\sigma^2} e^{-(\frac{r^2}{2\sigma^2})} r dr d\theta$$
$$= C\frac{i^2 r_c^2}{2\sigma^2} - C + Ce^{-\frac{i^2 r_c^2}{2\sigma^2}}. \tag{4.10}$$

From Eqs. (4.8) and (4.10), we have:

$$P_i = C[\frac{r_c^2(2i-1)}{2\sigma^2} + e^{-\frac{i^2 r_c^2}{2\sigma^2}} - e^{-\frac{(i-1)^2 r_c^2}{2\sigma^2}}]. \tag{4.11}$$

With Eq. (4.11), we can calculate the number of sensor nodes in ith annulus N_i, given σ and N using Eq. (4.7). N_i is applied to verify the coverage and connectivity.

4.3.1 Coverage of Reverse Gaussian Distributed WSN

For such a randomly deployed WSN in a two-dimensional infinite plane, Liu et al. [31] show that the probability f_a that a point is covered by at least one sensor as follows:

$$f_a = 1 - e^{-\lambda\pi r_s^2}, \tag{4.12}$$

where λ is the node density and r_s is the sensing range of each sensor node. Since after network division, the sensor node deployment can be approximated as uniform distribution. Thus, Eq. (4.12) can be utilized for individual annulus of our Reverse Gaussian distributed network directly and minimal number of sensor nodes for intrusion detection in a given annulus can be estimated. Since our aim of Reverse Gaussian

scheme is to protect multiple facilities located in a given region, the outermost annulus k would be deployed with the maximum number of sensor nodes. Given coverage requirement P_s^*, we should deploy at least N_k^* sensors at the annulus k to guarantee the coverage probability P_s to satisfy:

$$P_s \geq 1 - e^{-\frac{N_k^* r_s^2}{r_c^2(2k-1)}} = P_s^*. \tag{4.13}$$

4.3.2 Connectivity of Reverse Gaussian Distributed WSN

Consider a random uniform distributed network, a relationship between the sensor transmission range r_c and the network connectivity is shown in range as:

$$r_c \geq \sqrt{\frac{-\ln(1-p^{1/n})}{\rho\pi}}, \tag{4.14}$$

where p is the possibility that no sensor node in the network is isolated, n is the total number of sensor nodes deployed in the large area A, satisfying $A \gg r_c^2\pi$, and $\rho = n/A$ is the node density. To satisfy the connectivity constraint P_c^*, connectivity probability in each annulus should all be larger than the minimum required. We can rewrite Eq. (4.14) for annulus i as:

$$P_c^i \geq (1 - e^{-N_i^*/(2i-1)})^{N_i^*} = P_c^*, \tag{4.15}$$

where N_i^* is the least number of sensor nodes needed in the annulus i.

4.4 Simulation Results

4.4.1 Simulated Scenario Setting

We considers a circular monitored area A in which the WSNs are deployed. The BS is located at the center and facilities are randomly deployed within the area A under protection. The attacks from the intruders originate from any random point on the border of the monitored region. The simulation is run for the three different deployments of Gaussian, Uniform, and Reverse Gaussian distributions. Two types of attacks are simulated:

Border to Center

The intruder enters through a random point on the border and heads straight to the center (BS) of the circle.

Border to Facility

The intruder enters through a random point on the border and tries to reach to a certain facility using the shortest path.

In the Reverse Gaussian deployment, we deploy sufficient sensor nodes to ensure at least P_s^* (90%) coverage at the outermost annulus of the region. Also, the connectivity probability in each annuli is verified using Eq. (4.15) to ensure 90% connectivity. The same number of sensor nodes are deployed for the Gaussian and Uniform distribution

as well in order to compare their performances. The simulation framework used was Java, with each scenario run for 1000 trials. The metrics used for the performance analysis are:

1) Intrusion Distance

The total distance the intruder travelled before being detected by the WSN.

2) Number of Sensors

The number of sensors that are triggered by the intruder.

For our simulations, the area under consideration is of radius $R = 500m$, this area is protected by a WSN with sensor nodes of transmission range $50m$. The total number of sensors deployed vary from 1000, 1200, 1400, 1600, 1800, 2000, to 2200 sensor nodes. Intrusion distance, which is the key metric for intrusion detection application is measured in our simulations for all three deployments.

From Fig. 4.3, we can see that the Reverse Gaussian scheme performs better than the other two scheme, for the Border to Center scenario. The X-axis represents the number of sensor nodes being deployed and the Y-axis represents the intrusion distance. It represents how quickly the intrusion is detected in the area under consideration. It can be observed from the figure that the Reverse Gaussian deployment consistently shows a lower intrusion distance with the varying total number of sensors deployed. Since the Gaussian distribution only provides better security around

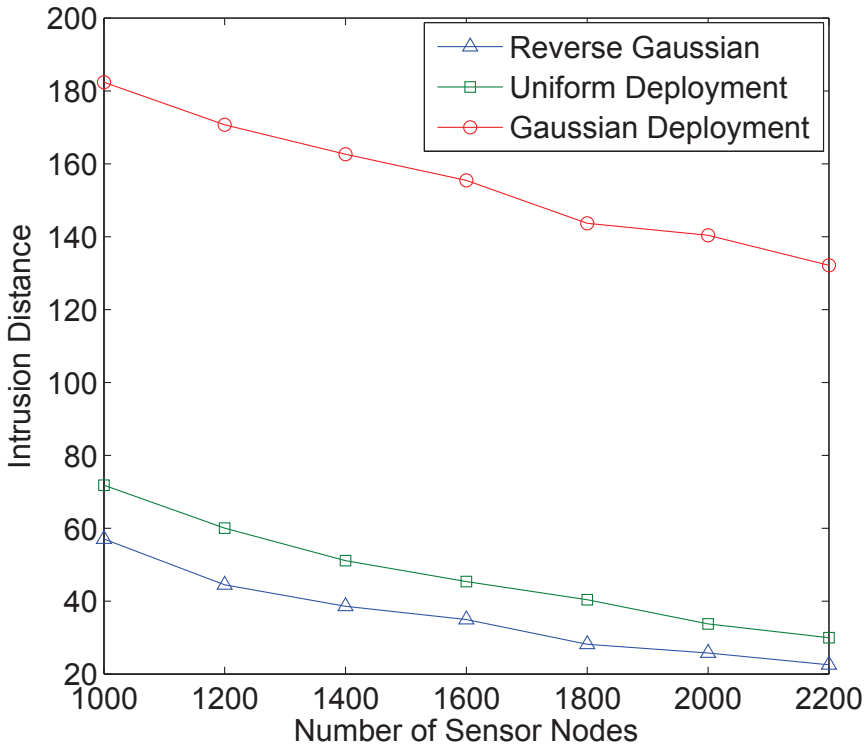


Figure 4.3: Number of Deployed Sensors vs. Intrusion Distance (Border to Center)

center, the intrusion distance is much higher than Reverse Gaussian and Uniform deployment schemes. The simulation shows that our proposed Reverse Gaussian deployment provides better security than the other two schemes, for these set of attacks in the whole monitored area.

Fig. 4.3 also illustrates that the Reverse Gaussian scheme has excellent protection for multiple facilities located inside the monitored region. When the facility is located near the border region, the Reverse Gaussian scheme can still detect intrusions very quickly before the intruder reaches the important facilities. The Uniform scheme

has a worse performance as compared to the Reverse Gaussian scheme in terms of border region protection and the Gaussian scheme can barely provide any protection for facilities near the Border.

Another key metric to test the performance of the intrusion detection system, is to measure the number of sensor nodes triggered during the intrusion attack, while the intruders move towards the targets. Multiple detections causes redundancy and helps guard against false accusations by single sensors in the system. The measure of the total triggered sensors is also useful in estimating the real-time damage caused by intrusion. The next set of simulations measure this metric against attacks to the outermost facility.

In Fig. 4.4 and 4.5, we compare the performance of three deployments in a Border to Facility scenario. The monitored region radius is set as $R = 500m$ and homogeneous sensors with $r_s = 50m$ are deployed into the region. The whole region is divided into 10 annuli. X-axis of these two figures shows the ith annulus where the outermost facility is located and Y-axis represents the number of sensors that detect an intrusion. Fig. 4.4 shows the results for 1000 sensor nodes deployed into the monitored region for the three schemes. The Reverse Gaussian performs better in the region from annulus 5 to annulus 10, but for all inner annuli, Uniform and Gaussian distribution schemes work better. In Fig. 4.5, we deploy 2200 sensor nodes into the given region. Once again, Reverse Gaussian scheme performs better in annuli $4 - 10$ than the other two schemes. It is clear that for the same investment, the Reverse

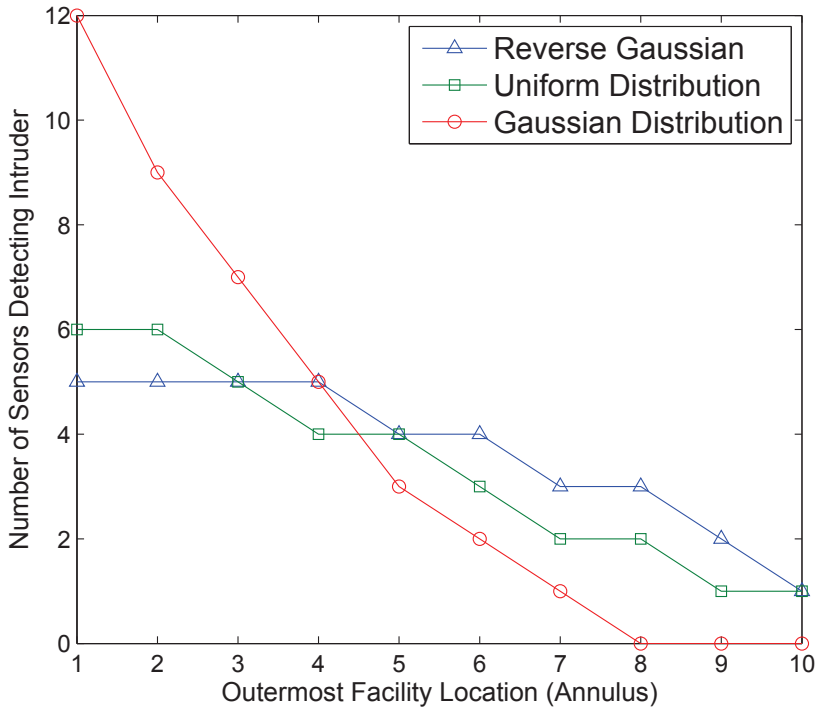


Figure 4.4: Facility Location vs. number of sensors (1000 sensor nodes)

Gaussian does better than both Gaussian and Uniform in term of protecting multiple facilities, especially facilities located in the border region.

The limitations of the Reverse Gaussian deployment scheme are also analyzed. First, the Reverse Gaussian scheme provides good protection for intrusion starting from the border area. Aerial attacks, such as paratrooper attacks, which can start from any point within the area to be monitored are not handled very well by this scheme, especially if the attacks begin near the center of the area. However, this kind of attack is a lot bolder and very different from covert ground attacks from the border, which are the class of attacks we consider in this paper. Secondly, the energy hole

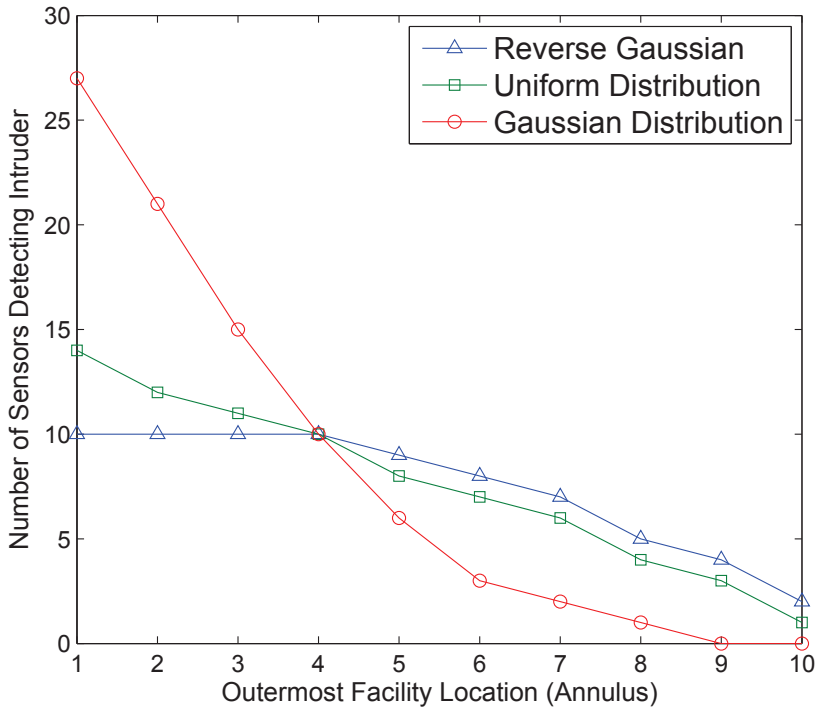


Figure 4.5: Facility Location vs. number of sensors (2200 sensor nodes)

problem may compromise the network lifetime when the intrusion attacks are very frequent. Therefore, The Reverse Gaussian can provide better intrusion detection capabilities for ground attacks from the border.

4.5 Conclusion

We propose a novel Reverse Gaussian distribution deployment for intrusion detection. In order to provide a higher level of security for the whole monitored area, sensor nodes are deployed randomly following a Reverse Gaussian distribution, where

more sensor nodes are deployed at the border for intrusion detection purposes and an adequate number of sensor nodes are deployed near the center of the region to satisfy network connectivity constraint. With the same investment, the Reverse Gaussian scheme provides faster detection compared to Gaussian and Uniform distribution schemes, for intrusion attacks from the border that target multiple facilities.

Chapter 5

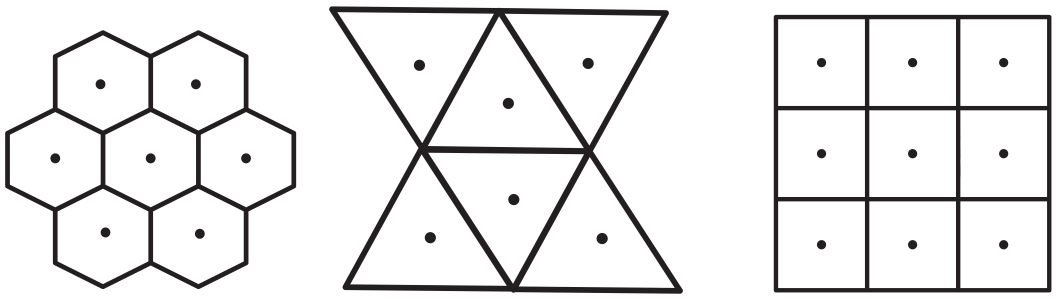
Regular Deployment

5.1 Introduction

The previously discussed Gaussian, Random and Hybrid deployment techniques are probabilistic schemes which can be facilitated by aerial deployment. These deployment schemes can be extremely useful in cases when the area is not accessible or hostile. But it is not recommended to use probabilistic deployment schemes in all scenarios. They typically have redundancy in terms of coverage and also require no structural planning whatsoever. In scenarios where the deployment area is accessible and sensors can be placed at pre-determined locations (accessible, friendly territory), the efficiency and cost of the network is not optimal when using probabilistic schemes [23]. So, in these cases, a deterministic regular deployment could provide better performance.

In this chapter, we will be discussing about the other type of deployment schemes, i.e. Deterministic Deployment or Regular Deployment as they are generally called. As the name suggests, regular deployment schemes have an inherent *pattern* of sensor nodes which scale over the area of interest. A particular type of regular deployment has the each sensor deployed at a particular pre-determined location and this pattern stays uniform across the whole network. Such a scheme provides better throughput per sensor in a given area and are also make the WSN easily scalable and more flexible.

Regular deployments scheme for WSNs are used for different kind of applications as compared to their probabilistic counterparts. This application dependent approach is explained in detail by Gajbhiye et al. [24]. Due to their uniform structure, they are mostly used in scenarios where the deployment area is easily accessible and non-hostile. In these cases, it is easy to place each sensor in its designated spot and also make any changes or replacements in case of damage or power drain. Typical applications would be similar to planned military or civilian projects where the area is available for survey and the deployment and maintenance of the network can be planned. An example of such kind of application would be deployment of a WSN on the wings of an aircraft to detect cracks during flights. It is not advisable to use probabilistic deployments in this scenario because regular deployments typically perform better and if circumstances are favourable, they should be preferred. Zhang et al. verify in [35] that regular deployments are cheaper and need lower node density



(a) Hexagon Topology (b) Triangle Topology (c) Square Topology

Figure 5.1: The three types of regular deployments.

to achieve the same throughput.

Given that the area in which we are deploying the Wireless Sensor Network is accessible, the deterministic regular deployments are very convenient to plan because the position of each node is pre-set. This reduces the cost of the network (lesser nodes required) to cover the same area when compared to probabilistic deployments. In addition to that, the encryption and communication mechanisms are simpler to design, thus improving the maintainability and predictability of the WSN.

5.1.1 Structure of Regular Deployments

As the name Regular deployment suggests, the nodes in these deployments are placed such that they form polygonal structures as seen in Figure 5.1. These tiny shapes formed by the nodes are the building blocks of large Regular WSN that span over the whole area of interest. The cells shown in the figure contain a sensor node and it's imperative that cell size be determined in such a way that each node can

communicate with the nodes in it's adjacent cells. For example, a node in the triangle topology must be able to communicate with it's three adjacent nodes, unless it is a boundary node, in which case there will be less number of adjacent nodes. Depending on which of the three regular deployments is chosen, the WSN is planned and deployed in such a way that the nodes cover the complete area and at the same time maintain the rigid structure throughout the network thus facilitating better performance, easier maintenance and reduced cost compared to probabilistic deployment schemes.

There are three types of regular deployments: Square (Grid), Hexagon and Triangle. In the Figure 5.1, each dot indicates a sensor and it is surrounded by 6 other nodes, thus giving it a hexagonal shape. Each node in the hexagon is placed such that it has connectivity with all of it's neighbours. Similarly, the triangle and square topology are also a cluster of the respective polygonal shapes.

5.2 Regular Deployment Strategies for Intrusion Detection

Beutel et al. [36] describe various real-world applications of regularly deployed WSNs and also enumerate potential problems encountered during this task. A few techniques are proposed to pinpoint failures and find out their root cause. Despite these potential issues, WSNs with regular topology still succeed in maximizing network lifetime as illustrated by Tian et al. [37]. Now, these regular deployments can

also be used in WSNs for Intrusion detection if the conditions are favourable (non-hostile, accessible environment etc.). A lot of analysis has been done by researchers on how efficient regular deployments are as compared to random deployments [38] and how regular deployments strategies can be improved for better communication strategies [39] [26].

But, there is an evident lack of research done on how these three deployment schemes fare when pitted against each other for a particular set of applications. In previous chapters, we have seen how attacks by intruders on WSN can be catastrophic on it's lifetime and performance. We think, it is important to have a good idea on how each regular deployment fares a given scenario, for Intrusion Detection. Hence, in this chapter, we will set up simulation of Intrusion attacks on various regular deployed WSNs and find out which of them is a better choice, i.e., which deployment offers the best protection against intruders.

5.3 Simulation

Below are the details of the setup, results and analysis of the simulations various intrusion attacks on Wireless Sensor Networks that are deployed using Regular Strategies. It should be noted that here the simulations are performed and comparison of performance is done only among the regular deployments [35].

5.3.1 Setup

The simulation setup is similar to the setups from the previous chapters as we consider a circular area A of radius 500 units in which the WSNs are deployed. The TelosB mote platform (IEEE 802.15.4 compliant) which is an open source wireless sensor module and has a programmable USB interface is the model for the nodes in our simulation. real-life sensors used in applications can have a varying degree of transmitting range depending on the about of power that is packed into its battery. Thus, in our simulation, we chose three scenarios where the transmission range is 20, 40 and 80 units respectively. This ensures that we cover a wide range of real-life application that may profit from this performance analysis. Similarly, the sensing range is assumed to be 10 units which is typically the case with a real-life sensor. This sensing range doesn't affect the power consumption as much as transmission range does, so we considered a single value for this in all 3 scenarios. The intruder attacks from a random point on the boundary of the circular area A and leaves through another random point, travelling through the area in a straight line.

The metrics used for the performance analysis are:

1) Intrusion Distance

The total distance the intruder covered before being detected by the WSN.

2) Sensors Alerted

The number of sensors that are alerted by the intruder when it is inside the WSN.

The nodes for these 3 deployments are plotted by starting from the center and then spawning neighbouring nodes layer by layer until the 500 units radius area is completely covered. Using the geometrical properties of each of the 3 polygons, nodes are plotted accordingly.

The transmission range (r_c) is varied from low (20 units) to medium (40 units) and then to high (80 units). The simulation is run for 3 different deployments of sensors: Square, Hexagon and Triangle, and the average of 1000 runs is used to enhance the accuracy of our results. We used Network Simulator in Java to perform the simulations.

5.3.2 Analysis of results

In Figure 5.2, we can see the three groups of results that give an idea of how well the deployment schemes work relative to each other. Initially, the transmission range (r_c) is 20 units and we can see that Hexagon deployment has a lowest value on the Y-Axis (Intrusion Distance[ID]). This shows that hexagon detects the intruder quicker than the other two schemes. As the transmission range is increased to 40 and then to 80 it can clearly be seen that hexagon still outperforms square and triangle topologies.

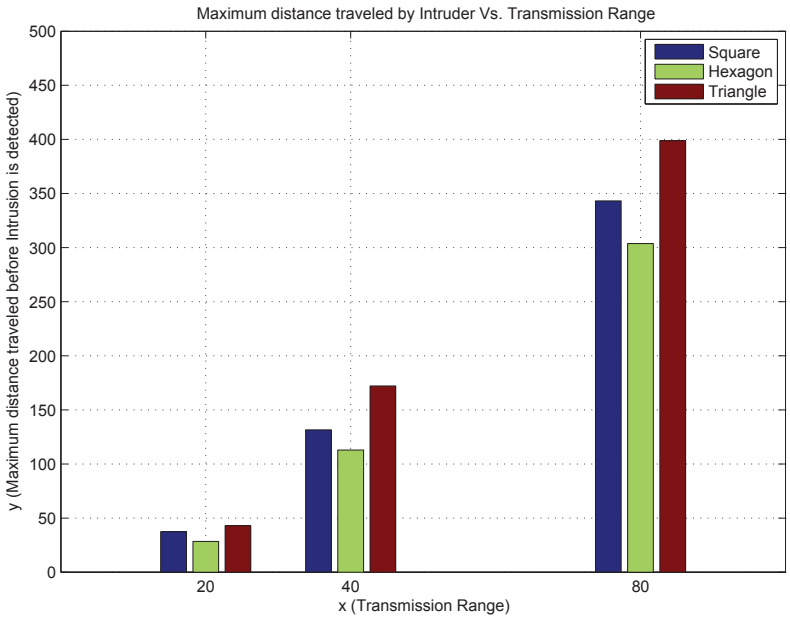


Figure 5.2: Maximum distance traveled by Intruder Vs. Transmission Range

This is because hexagon topology has a tightly knit structure, thus has more nodes in the area and as a result has highest coverage. Square topology has a relatively relaxed structure and thus it performs second best ahead of triangle topology, which has a high ID value.

Figure 5.3 show a bar graph of transmission range versus the total number of Sensors Alerted while the intruder is within the network. It is again clearly evident that hexagon deployment scheme has a higher number of intrusion detections within the same area. This is again due to the structure of the deployment scheme.

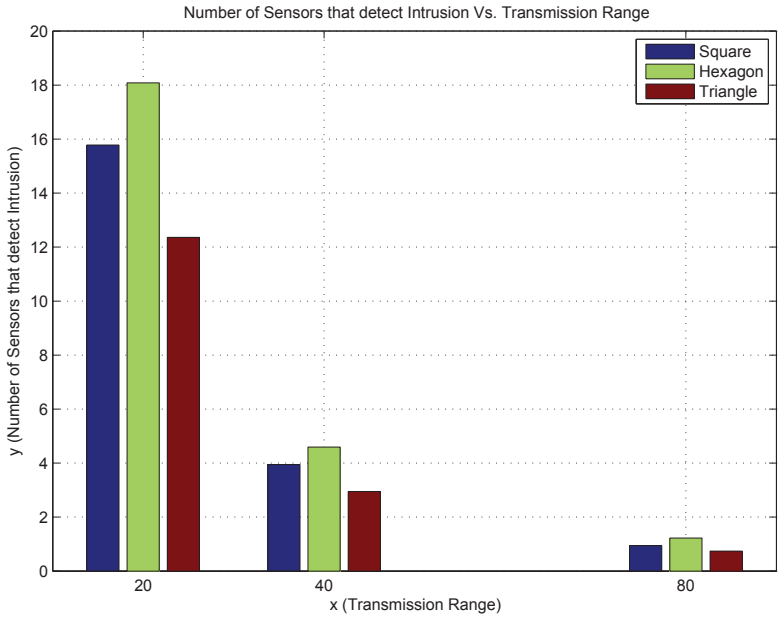


Figure 5.3: Number of Sensors that detect Intrusion Vs. Transmission Range

5.4 Conclusion

In this chapter, we describe various Regular Deployment schemes and their applications where Regularly deployed WSNs can be used. Due to the lack a good comparison study to determine which scheme has better performance, we design a simulation to do the same. The performance of the three Regular deployment schemes, Square, Hexagon and Triangle, in a scenario of Intrusion in a WSN are compared. As it can be seen from the result bar graphs, hexagon performs better in detection intruder when used to deploy in an area covered by the WSN.

Chapter 6

Conclusion and Future Work

6.1 Conclusion

In Chapter 1, a brief introduction to Wireless Sensor Networks (WSNs) is given and its components and basic functionalities are explained. A wide range of applications that can use WSNs are studied and a few examples are given. The limitations of WSN corresponding to it's hardware and basic design are given and we then looked into the challenges that are posed due to these limitations. Then, in section 1.3, we look at how security is an important aspect in WSN applications and thus highlighting the importance of the deployment schemes used for these WSNs.

In Chapter 2, we did a background study on the various topics relevant to this purpose of study. First we explored what "Intrusion" is and then listed the types of Intrusion attacks that are possible. We looked into the research work done on

how a WSN can be protected from Intrusion and found why avoiding the intruder to reach the proximity of the sensors is crucial in preventing attacks. Thus, we assert the need for good deployment schemes in the WSN to avoid these proximity attacks. Further we look at various deterministic and probabilistic deployment schemes that we previously proposed and how each have their own advantages and disadvantages in various scenarios.

We proposed a new deployment scheme called Hybrid *Gaussian-Ring* Deployment in Chapter 3. We introduced the need for this scheme and identified the application scenarios where it can be effective. We then looked into the analytical design models of Random and Gaussian deployment schemes and introduced the analytical design model for our proposed deployment scheme. A simulation is setup to simulate the intrusion attacks on all three deployment schemes under similar conditions and parameters. The results are then plotted and the performance of the three schemes are analyzed based on the same metrics and found out that Hybrid *Gaussian-Ring* Deployment detects an intruder faster and also provides better multiple detections compared to Random and Gaussian deployments.

Another novel scheme, Reverse Gaussian Deployment, is proposed and its applications are described in Chapter 4 . We then explained the analytical model of this deployment scheme. This model shows how the coverage and connectivity of the WSN can be guaranteed while deploying the sensors in Reverse Gaussian deployment. A simulation setup similar to the previous scenario is taken and intrusion attacks are

simulated on Random, Gaussian and Reverse Gaussian deployment. The results are then analysed and we found that the performance of Reverse Gaussian is again better when considering the same metrics, thus validating our analytical model.

In Chapter 5 we described the Regular Deployment schemes. We also detailed how these schemes have a different application set when compared to Probabilistic schemes like Gaussian, Hybrid or Reverse Gaussian. A few applications that use WSNs with sensors deployed using Regular deployment schemes are looked into. We observed that a good comparison of performance among these Regular deployment schemes is lacking and proposed a simulation setup to do the same. The objective of the simulation and subsequent analysis of results is to estimate which of the regular deployment schemes performs best in a scenario of intrusion detection in a homogeneous WSN of fixed area. Our analysis proved that Hexagon deployment schemes performs better than Square and Triangle deployments in detected an intruder moving into the network.

We can conclude that we achieved the purpose of this work by researching various deployment schemes to improve Intrusion Detection in Wireless Sensor Networks and proposing new schemes and assert the importance by backing it with a performance analysis.

6.2 Future Work

There exists a lot of scope for future work in this field and we present a few ideas of what can be done to Intrusion Detection in WSNs.

One of the ways to enhance the connectivity and coverage of the WSN is to introduce **Heterogeneous Sensors**. That means, there'll be a mix of regular sensors and a few high performance sensors which have higher transmission and sensing capabilities and better battery lifetime. This might drastically improve the intrusion detection potentials of the the Hybrid *Gaussian-Ring* and Reverse Gaussian deployment. A better model can be investigated to accommodate the heterogeneous network and the results can be compared to Random, Gaussian deployments and even the homogeneous counterparts. Another modification in the proposed deployments can be done by using a few **Mobile Relay** nodes along with the regular sensors. These mobile relay nodes can have some limited mobility but can greatly contribute to the one-hop connectivity and hence energy consumption of the WSN.

An improvement over the Hybrid *Gaussian-Ring* deployment could be to have multiple concentric rings (similar to a **Bimodal Gaussian Distribution**) of uniformly deployed sensors over the underlying Gaussian distribution. That is, rather than having just one "Ring" at the boundary, there can be multiple rings, within a particular distance from each other. This might help in providing something similar to multiple layers of protection for the center (BS) of the WSN and also add to the connectivity of the network as a whole.

We used a simplified method in this thesis to estimate the value of Standard Deviation(σ) for the Gaussian deployment in Section 3.2.3. But, an **optimization algorithm** can be developed to find out the best value of σ for a given Gaussian deployment in a region with Radius R.

Although not unique to this work, a **power scheduling** mechanism can be implemented in the proposed techniques. Advantages of power scheduling in WSNs are widely discussed and we believe implementing it in our deployment schemes will help improve the lifetime of the WSN and thus increasing the productivity and reducing the cost.

Bibliography

[1] S. Tilak, N. B. Abu-Ghazaleh, and W. Heinzelman, "A taxonomy of wireless micro-sensor network models," *SIGMOBILE Mob. Comput. Commun. Rev.*, vol. 6, no. 2, pp. 28–36, Apr. 2002. [Online]. Available: http://doi.acm.org/10.1145/565702.565708

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

[3] M. Winkler, K.-D. Tuchs, K. Hughes, and G. Barclay, "Theoretical and practical aspects of military wireless sensor networks," *Journal of Telecommuncations and Information Technology*, pp. 37 –45, 2008. [Online]. Available: http://www.itl.waw.pl/czasopisma/JTIT/2008/2/37.pdf

[4] T. Arampatzis, J. Lygeros, and S. Manesis, "A survey of applications of wireless sensors and wireless sensor networks," in *Intelligent Control, 2005. Proceedings of the 2005 IEEE International Symposium on, Mediterrean Conference on Control and Automation*, June 2005, pp. 719 –724.

[5] S. H. Lee, S. Lee, H. Song, and H. S. Lee, "Wireless sensor network design for tactical military applications: remote large-scale environments," in *Proceedings of the 28th IEEE conference on Military communications*, ser. MILCOM'09. Piscataway, NJ, USA: IEEE Press, 2009, pp. 911–917. [Online]. Available: http://dl.acm.org/citation.cfm?id=1856821.1856955

[6] I. Onat and A. Miri, "An intrusion detection system for wireless sensor networks," in *Wireless And Mobile Computing, Networking And Communications, 2005. (WiMob'2005), IEEE International Conference on*, vol. 3, Aug. 2005, pp. 253 – 259 Vol. 3.

[7] "Automated local evaluation in real time." [Online]. Available: http://www.alertsystems.org/

[8] A. Cerpa, J. Elson, M. Hamilton, J. Zhao, D. Estrin, and L. Girod, "Habitat monitoring: application driver for wireless communications technology," in *Workshop on Data communication in Latin America and the Caribbean*, ser. SIGCOMM LA '01. New York, NY, USA: ACM, 2001, pp. 20–41. [Online]. Available: http://doi.acm.org/10.1145/371626.371720

[9] A. Becher, E. Becher, Z. Benenson, and M. Dornseif, "Tampering with motes: Real-world physical attacks on wireless sensor networks," in *Proceeding of the 3rd International Conference on Security in Pervasive Computing (SPC*, 2006, pp. 104–118.

[10] D. Moore, "Demonstration of bird species detection using an acoustic wireless sensor network," in *Local Computer Networks, 2008. LCN 2008. 33rd IEEE Conference on*, oct. 2008, pp. 730 –731.

[11] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," in *Sensor Network Protocols and Applications, 2003. Proceedings of the First IEEE. 2003 IEEE International Workshop on*, may 2003, pp. 113 – 127.

[12] A. Wood and J. Stankovic, "Denial of service in sensor networks," *Computer*, vol. 35, no. 10, pp. 54 – 62, oct 2002.

[13] Y.-C. Hu, A. Perrig, and D. Johnson, "Wormhole attacks in wireless networks," *Selected Areas in Communications, IEEE Journal on*, vol. 24, no. 2, pp. 370 – 380, feb. 2006.

[14] I. Krontiris, T. Giannetsos, and T. Dimitriou, "Launching a sinkhole attack in wireless sensor networks; the intruder side," in *Networking and Communications, 2008. WIMOB '08. IEEE International Conference on Wireless and Mobile Computing,*, oct. 2008, pp. 526 –531.

[15] J. Newsome, E. Shi, D. Song, and A. Perrig, "The sybil attack in sensor networks: analysis & defenses," in *Proceedings of the 3rd international symposium on Information processing in sensor networks*. New York, NY, USA: ACM, 2004, pp. 259–268. [Online]. Available: http://doi.acm.org/10.1145/984622.984660

[16] Y. Zhou and Y. Fang, "Defend against topological attacks in sensor networks," in *Military Communications Conference, 2005. MILCOM 2005. IEEE*, Oct. 2005, pp. 768 –773 Vol. 2.

[17] J. Deng, R. Han, and S. Mishra, "A performance evaluation of intrusion-tolerant routing in wireless sensor networks," in *Proceedings of the 2nd international conference on Information processing in sensor networks.* Berlin, Heidelberg: Springer-Verlag, 2003, pp. 349–364. [Online]. Available: http://dl.acm.org/citation.cfm?id=1765991.1766015

[18] O. Dousse, C. Tavoularis, and P. Thiran, "Delay of intrusion detection in wireless sensor networks," in *Proceedings of the 7th ACM international symposium on Mobile ad hoc networking and computing.* New York, NY, USA: ACM, 2006, pp. 155–165. [Online]. Available: http://doi.acm.org/10.1145/1132905.1132923

[19] X. Wang, Y. Yoo, Y. Wang, and D. Agrawal, "Impact of node density and sensing range on intrusion detection in wireless sensor networks," in *Computer Communications and Networks, 2006, ICCCN 2006, Proceedings.15th International Conference on*, Oct. 2006, pp. 323 –327.

[20] Y. Wang, X. Wang, B. Xie, D. Wang, and D. Agrawal, "Intrusion detection in homogeneous and heterogeneous wireless sensor networks," *Mobile Computing, IEEE Transactions on*, vol. 7, no. 6, pp. 698 –711, June 2008.

[21] Y. Wang, W. Fu, and D. Agrawal, "Intrusion detection in gaussian distributed

wireless sensor networks," in *Mobile Adhoc and Sensor Systems, 2009. MASS '09. IEEE 6th International Conference on*, oct. 2009, pp. 313 –321.

[22] Y. Wang, "Intrusion detection in gaussian distributed heterogeneous wireless sensor networks," in *Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE*, Dec. 2009, pp. 1 –6.

[23] Y. Gao, K. Wu, and F. Li, "Analysis on the redundancy of wireless sensor networks," in *WSNA '03: Proceedings of the 2nd ACM international conference on Wireless sensor networks and applications.* New York, NY, USA: ACM, 2003, pp. 108–114.

[24] P. Gajbhiye and A. Mahajan, "A survey of architecture and node deployment in wireless sensor network," in *Applications of Digital Information and Web Technologies, 2008. ICADIWT 2008. First International Conference on the*, aug. 2008, pp. 426 –430.

[25] X. Liu and M. Haenggi, "The impact of the topology on the throughput of interference-limited sensor networks with Rayleigh fading," in *Sensor and Ad Hoc Communications and Networks, 2005, IEEE SECON 2005, 2005 Second Annual IEEE Communications Society Conference on*, 2005, pp. 317–327.

[26] S. Narayanan, J. H. Jun, V. Pandit, and D. Agrawal, "Proportionally fair rate allocation in regular wireless sensor networks," in *Computer Communications*

Workshops (INFOCOM WKSHPS), 2011 IEEE Conference on, Apr. 2011, pp. 549 –554.

[27] R. Rajagopalan and P. Varshney, "Connectivity analysis of wireless sensor networks with regular topologies in the presence of channel fading," *IEEE Transactions on Wireless Communications*, vol. 8, no. 7, pp. 3475–3483, 2009.

[28] A. Tanenbaum, C. Gamage, and B. Crispo, "Taking sensor networks from the lab to the jungle," *Computer*, vol. 39, no. 8, pp. 98 –100, aug. 2006.

[29] D. Agrawal and Q.-A. Zeng, *Introduction to Wireless and Mobile Systems*. Cengage Learning, 2010. [Online]. Available: http://books.google.es/books?id=Jekcmjdw5DIC

[30] N. Katneni, V. Pandit, H. Li, and D. Agrawal, "Hybrid Gaussian-Ring Deployment for Intrusion Detection in Wireless Sensor Networks," in *IEEE International Conference on Communications*, Ottawa, Canada, 2012.

[31] B. Liu and D. Towsley, "A study of the coverage of large-scale sensor networks," in *2004 IEEE International Conference on Mobile Ad-hoc and Sensor Systems,*, Oct. 2004, pp. 475 – 483.

[32] C. Bettstetter, "On the minimum node degree and connectivity of a wireless multihop network," in *Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing*, ser. MobiHoc

'02. New York, NY, USA: ACM, 2002, pp. 80–91. [Online]. Available: http://doi.acm.org/10.1145/513800.513811

[33] D. Wang, B. Xie, and D. P. Agrawal, "Coverage and lifetime optimization of wireless sensor networks with gaussian distribution," *IEEE Transactions on Mobile Computing,*, vol. 7, no. 12, pp. 1444 –1458, Dec. 2008.

[34] H. Li, V. Pandit, N. Katneni, and D. Agrawal, "A Reverse Gaussian Deployment Strategy for Intrusion Detection in Wireless Sensor Networks," in *IEEE International Conference on Communications*, Ottawa, Canada, 2012.

[35] H. Zhang and J. C. Hou, "Is deterministic deployment worse than random deployment for wireless sensor networks?" in *INFOCOM 2006. 25th IEEE International Conference on Computer Communications. Proceedings*, April 2006, pp. 1–13.

[36] J. Beutel, K. Rmer, M. Ringwald, and M. Woehrle, "Deployment techniques for sensor networks."

[37] H. Tian, H. Shen, and M. Roughan, "Maximizing networking lifetime in wireless sensor networks with regular topologies," in *PDCAT '08: Proceedings of the 2008 Ninth International Conference on Parallel and Distributed Computing, Applications and Technologies*. Washington, DC, USA: IEEE Computer Society, 2008, pp. 211–217.

[38] S. Panichpapiboon, G. Ferrari, and O. Tonguz, "Sensor networks with random versus uniform topology: Mac and interference considerations," in *Vehicular Technology Conference, 2004. VTC 2004-Spring. 2004 IEEE 59th*, vol. 4, May 2004, pp. 2111 – 2115 Vol.4.

[39] G. Mergen and L. Tong, "Stability and capacity of regular wireless networks," *IEEE Transactions on Information Theory*, vol. 51, no. 6, pp. 1938–1953, 2005.