DETECTING THE EVIL TWIN ATTACK IN A SINGLE HOP WIRELESS NETWORK USING FOUR-SQUARE ANTENNAS

by

Melodie Carrington

A thesis submitted to
the Faculty of Graduate Studies and Research
in partial fulfillment of
the requirements for the degree of

MASTER OF COMPUTER SCIENCE

School of Computer Science

at

CARLETON UNIVERSITY

Ottawa, Ontario

April 18, 2011

Your file Votre référence
ISBN: 978-0-494-81618-9
Our file Notre référence
ISBN: 978-0-494-81618-9

To my mother, Sherille Carrington

Abstract

Recent technological advances have increased the prevalence of wireless networks in our society. Users can easily access the Internet at home, work, school or even while travelling. The ease of accessibility and mobility makes wireless networks a viable target for attackers. Compromised wireless networks allow attackers to eavesdrop on sensitive data such as passwords and credit card information. Attack detection schemes must identify when an attack is taking place, then mitigate this threat. Good detection solutions must have a high detection rate and low false positives.

In our work, we consider a general form of the evil twin attack, called the evil twin transmitter attack. In the evil twin transmitter attack, a malicious wireless node gains access to the network and uses the same identity as a legitimate wireless node. We aim to minimize this threat and localize the wireless nodes involved. Our contributions to this work are:

1. We describe two algorithms using four-square antennas at the receivers, which can be implemented in the most common deployment scenarios, such as a random or a regular grid networking environment, to detect an evil twin attack.

2. We propose two location estimation schemes that use the phase differences of the signal received at the four-square antenna, to determine the position of the wireless node. The accuracy of the phase comparison technique is dependent on the environmental noise.

3. Our simulation results demonstrate that our algorithms achieve a high rate of detection while maintaining low false positives and negatives.

Acknowledgements

I am grateful to my supervisor, Professor Michel Barbeau, who shared his expertise and research insight. The completion of this work would have not been possible without his enthusiam, guidance and feedback. I would like to thank my mum who has been my biggest supporter and encouraged me to go on this journey of self discovery. My mum provided a loving home and worked extremely hard to allow me to follow my dreams. My deepest gratitude goes to James Griffiths, whose love, motivation and support contributed to my work. In all my struggles, fears and frustrations, I could count on him to be there. Thanks to all my friends, the ones in Barbados and the ones I made in Canada. Thank you, Pryah, Tasha, Allison, Ryan, Raghad and Muhiji. Thank you for the emails, phones calls, discussions and much needed coffee breaks.

I would also like to thank the Organization of American States (OAS) and the Natural Sciences and Engineering Research Council (NSERC) for their financial support.

Contents

List of Tables

List of Figures

List of Abbreviations and Symbols

AOA	Angle of Arrival
AP	Access Point
BS	Base Station
CPP	Central Processing Point
DoS	Denial of Service
DNS	Domain Name Server
$EIRP$	Effective Isotropic Radiated Power
FN	False Negative
FNR	False Negative Rate
FP	False Positive
FPR	False Positive Rate
GPS	Global Positioning System
HPB	Hyperbolic Position Bounding
$HPB - LA$	Hyperbolic Position Bounding with Learning Ability
IP	Internet Protocol
LOS	Line-of-Sight
MAC	Medium Access Control
OBU	On-Board Unit
PSO	Particle Swarm Optimisation
$RARP$	Reverse Address Resolution Protocol
RF	Radio Frequency
RFF	Radio Frequency Fingerprinting
RSS	Received Signal Strength
SNR	Signal-to-Noise Ratio

$T-R$	Transmitter-Receiver
$TDOA$	Time Difference of Arrival
TN	True Negative
TNR	True Negative Rate
TOA	Time of Arrival
TOF	Time of Flight
TP	True Positive
TPR	True Positive Rate
$WiFi$	Wireless Fidelity
VPN	Virtual Private Network

Chapter 1

Introduction

Security is an important issue in wireless networks, however it is difficult to implement because anyone within range of the transmitter can connect to the network. In recent years, many schemes have been proposed to prevent network and service disruption [1, 2, 3]. To ensure security in a wireless network, some general features are desired:

- **Confidentiality:** Communication must be secured so that data is only visible to the communicating parties.
- **Integrity:** The message must not be changed during transmission.
- **Authentication:** Messages are sent by the verified sender rather than a malicious insider.
- **Non-repudiation:** The sender cannot deny having sent the message.
- **Access Control:** Only the intended recipient can view the message.

In a 2006 study conducted by Nicholson et al. in Chicago, it was found that 42% of 802.11 wireless networks had no security mechanisms [4]. In 2008, studies conducted in major cities showed that between 3% and 14% of 802.11 wireless networks were not

secure [5]. Even with security measures emplaced such as data encryption, attacks are still highly likely and there is a high risk of traffic being intercepted [6]. An attacker may disrupt a secure connection by launching a denial of service (DoS) or man-in-the-middle attack and manipulate the user into connecting to it [6, 7].

In public networks, hotspot providers delegate the responsibility of protecting the user's data on the transmission medium to the user. An attacker can easily gain access to the network, eavesdrop on traffic and read the user's confidential information [8]. One solution is that users may use a Virtual Private Network (VPN). However, it is still possible to gain information before a VPN connection is established [9].

The evil twin attack has been identified as an emerging threat in the security of wireless networks [7]. The malicious wireless node or *evil twin* gains access to the network and violates the security principles by eavesdropping on traffic. An evil twin attack can be easily deployed with few technical skills. A hacker simply needs a Wireless Fidelity (Wi-Fi) connection and a wireless card that acts as an Access Point (AP). The attacker then sets their own wireless network with the same name as the legitimate network. Several software applications are readily available to monitor and intercept traffic such as Kismet and Wireshark [10, 3]. In our work, we propose two evil twin detection schemes for a regular grid and a randomly distributed networking environment. Once an attack has been detected, the wireless nodes are localized.

1.1 Motivation and Problem Statement

The evil twin AP attack occurs when a client unknowingly connects to a rogue AP that has the same Service Set Identifier (SSID) as a legitimate AP. The malicious AP exploits the network by intercepting traffic. Typically, evil twin attacks are deployed near wireless

hot spots such as cafes, libraries and airports, where there is no need to authenticate users [7]. The evil twin may have a stronger signal or be in an area where the original network is inaccessible. Users are tricked into connecting to the rogue AP and give away their sensitive information. Often, users are still unaware of the attack after it has occurred. This attack is easy to launch but difficult to ascertain since it may be shut off at any time.

In our work, we consider a general form of the evil twin attack, called the evil twin transmitter attack. In the evil twin transmitter attack, a malicious wireless node gains access to the network and uses the same identity as a legitimate wireless node. Some examples of wireless nodes are wireless workstations and transmitters. Evil twins are a serious threat to wireless security [7], be it an AP or a wireless node. In a search and rescue situation, an evil twin can increase the difficulty of finding a person in a snowstorm. In a vehicular network, evil twins can broadcast incorrect traffic updates to the On-Board Units (OBU), resulting in accidents. Section 1.2 details the assumptions made in our model to detect and reduce the impact of the evil twin transmitter attack.

1.2 Assumptions

The attack model assumes a wireless network with several receivers and a truth-teller transmitter. The truth-teller transmitter is only honest in terms of it does not lie about its identity, which is handled by the error detection code. A malicious transmitter gains access to the network by impersonating and cloning the identity of the truth-teller transmitter. The malicious transmitter is the *evil twin* of the legitimate transmitter. No assumptions are made about the nature of the transmitters in the network, since it is possible that they are colluding to launch attacks. We assume that all transmitters have omni-directional antennas and are only able to send messages to the receivers that are one hop away. The receivers communicate securely with each other and will be confused by the presence of

the evil twin in the network. Depending on the signal strength of the transmitters at the receivers, they may be connected to the truth-teller transmitter, the evil twin or neither due to interference. Our mitigation approach to reduce the impact of an evil twin transmitter attack is described in Section 1.3.

1.3 Summary of Contributions

In our work, we focus on a problem pertaining to wireless network security: the identification of the evil twin transmitter attack and reducing the severity of the attack by localizing the transmitters involved. A secure wireless network must have a strong security monitoring system to prevent unauthorized access from malicious attacks and provide user security. Our mitigation approach for the evil twin transmitter attack encompasses these fundamental features of network security.

1. We described two detection algorithms that can be used in different network setups such as a randomly distributed and a regular grid network. The environment is divided into n zones where n receivers may be placed. In the regular grid environment, the receivers are perfectly aligned in a rigid setting which is disadvantageous in some cases. In the randomly distributed environment, the receivers are randomly placed within the zones. Once an attack is detected, we localize the malicious nodes.

2. We developed effective methods to pool the signals at each receiver to determine the corresponding transmitter. We proposed two location estimation schemes using the phase differences of the signal received, to pinpoint the position of the transmitter. These methods address localization using only one and multiple receivers.

3. The detection and localization schemes can be used independently of each other.

The performance of our algorithms is evaluated and the results demonstrate that our algorithms achieve a high detection rate while maintaining low false positives and negatives.

1.4 Organization of Thesis

Chapter 2 describes different approaches for location estimation and introduces different radio propagation models. Chapter 3 outlines the operation of the four-square antenna. Chapter 4 reviews existing work in the security of wireless networks and the localization of multiple uncooperative transmitters. Chapter 5 details the localization schemes using phase differences to determine the position of a transmitter. We also determine the location error of these techniques. Chapter 6 describes the countermeasures proposed for an attack in a random and regular grid environment. Chapter 7 describes the performance metrics and simulation setup of the network. We evaluate the performance of our algorithms and present the results. Chapter 8 concludes the thesis and describes possible directions for future work.

Chapter 2

Background

In this chapter, we discuss several principle location determination techniques that can detect the relative position of a target or a malicious node.

2.1 Location Determination Techniques

Wireless networks are frequently plagued with attacks, especially by rogue insiders [7]. The first step in reducing the impact of an attack is to find the location of the attacker and alert its neighbour nodes. An attacker may have multiple identities; however, its geographic position is unique. Locating its position may prevent subsequent attacks. The location of nodes in a wireless network can be discovered using self-localization or network-based techniques [11].

In self-localization, the nodes acquire their location through the aid of other nodes within the network. An example of self-localization is the Global Positioning System (GPS). The GPS receiver passively receives signals from the GPS satellites which transmits data that includes their location and the current time. The signals are transmitted at the same time and arrive at the receiver at slightly different times. The receiver can

then compute its position using trilateration. It is best to use four or more satellites to obtain the longitude, latitude and even elevation of the receiver, since a small timing error at the satellites may cause a large location error. Self-localization is useful, however it is not feasible in attack scenarios because attackers are uncooperative. Network-based techniques use other nodes within the network to determine the position of a node. An example of network-based localization is triangulation. Localization techniques need to operate independently of malicious or uncooperative nodes.

Many localization techniques have been proposed, using angulation, Received Signal Strength (RSS) and time, either individually or in combination [12, 13, 14]. Angular tracking determines the angle between the direction of propagation of an incident wave to a common reference point. Phased antennas are applicable to the angulation technique [12, 14, 15]. Examples of angular tracking are Angle of Arrival (AOA) and phase comparison monopulse. RSS is a measurement of the power received in a radio signal from the sender to receiver.

2.1.1 Angle of Arrival

AOA systems calculate the position of a node by measuring the angles of the received signals at multiple receivers. The intersection of the line-of-sight (LOS) paths pinpoints the location of the target node. We consider two AOA capable nodes in precise locations A and B, as shown in Figure 2.1. Each AOA node measures the angle of the signal received from the target node, with respect to its orientation. The angle of arrival is θ_A and θ_B. A line is drawn from each AOA node at the angle measured and the intersection of the lines is the position of the target node. The accuracy of the AOA technique is dependent on the noise and the multipath reflections [13, 16].

Geolocation of mobile phones is based on the principles of AOA. Multiple Base Sta-

tions (BSs) in a network receive signals from a mobile phone and the lines of bearing are calculated. The intersection of the projected azimuth lines results in an approximate location of the mobile phone user. Geolocation is useful in emergency situations, where the location of a mobile phone user may need to be estimated.

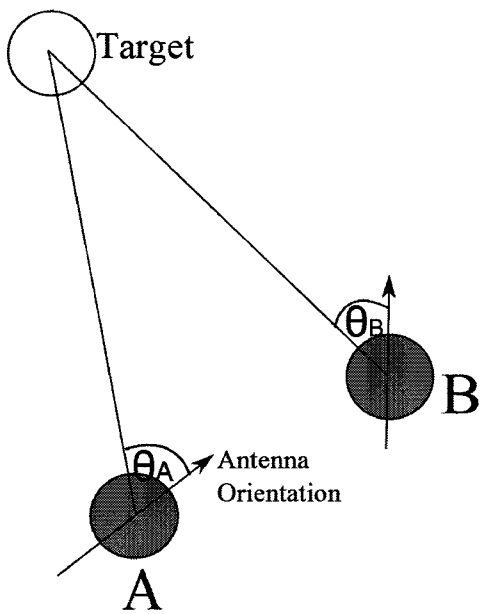


Figure 2.1: Angle of Arrival technique

2.1.2 Phase Comparison Monopulse

The phase comparison monopulse technique measures the phase difference of a signal from two or more antennas to estimate the direction of arrival. The antennas are usually separated a half-wavelength apart to reduce the electromagnetic interference, which is detrimental to an antenna's performance [17]. In this technique, the received signal at each antenna is of equal amplitude but different in phase. In Figure 2.2, the signal from transmitter T travels different path lengths, A, B, C and D. The baseline is the line connecting the two antennas, R_1 and R_2, and it has a length l. The intersection points of

the path length B and the baseline, and the baseline and the axis, are denoted by x and o, respectively. The distance between the points x and o is represented by c.

We use the law of cosines relating to the Pythagorean theorem to determine the phase angle θ in the two element array antenna. In triangle $T\hat{o}R_2$, α is equal to $\theta + \frac{\pi}{2}$.

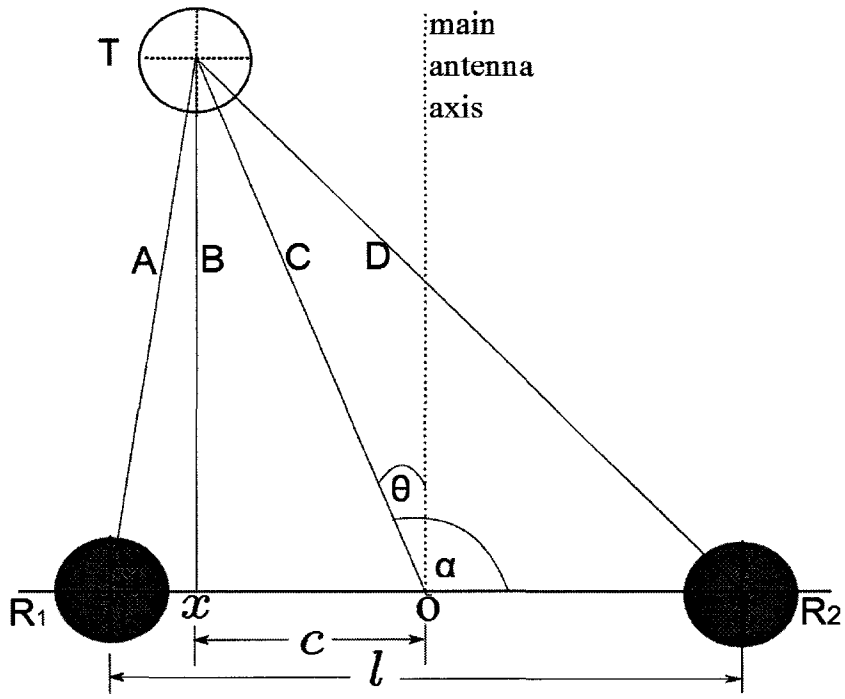


Figure 2.2: Phase Comparison with a two element array antenna

We consider the triangle $T\hat{x}R_2$ to determine the side length D. We have

$$\begin{aligned} D^2 &= B^2 + \left(\frac{l}{2} + c\right)^2 \\ &= (C^2 - c^2) + \left(\frac{l}{2}\right)^2 + \frac{2lc}{2} + c^2 \\ &= C^2 + \left(\frac{l}{2}\right)^2 + lc \end{aligned} \tag{2.1}$$

Using the law of sines, we know

$$\begin{aligned} \frac{c}{C} &= \cos(\pi - \alpha) \\ c &= C\cos\left(\frac{\pi}{2} - \theta\right) \\ &= C\sin(\theta) \end{aligned} \tag{2.2}$$

Substituting Eq. 2.2 in Eq. 2.1,

$$D^2 = C^2 + \left(\frac{l}{2}\right)^2 + lC\sin\theta \tag{2.3}$$

We consider the Taylor's Theorem, which states that for any function *f(x)* which has a point x centered around a base point a, can be expressed as:

$$\begin{aligned} f(x) &= f(a) + f'(a)(x-a) + \frac{f''(a)}{2!}(x-a)^2 \\ &\quad + \frac{f'''(a)}{3!}(x-a)^3 + \frac{f''''(a)}{4!}(x-a)^4 \\ &\quad + \ldots \qquad (2.4) \\ &= \sum_{n=0}^{\infty} \frac{f^{(n)}(a)}{n!}(x-a)^n \end{aligned} \tag{2.5}$$

where f' and f'' is the first and second derivative, and $f^{(n)}$ is the *nth* derivative [18]. We transform Eq. 2.3 into the form $(1+x)^n$ where $n = \frac{1}{2}$ and $x = \frac{l\sin\theta}{C}$. Assuming $l \ll D$,

$l \ll C$ and factoring out C^2, we get:

$$D^2 \approx C^2\left(1+\frac{l\sin\theta}{C}\right) \tag{2.6}$$

Then,

$$D \approx C\left(1+\frac{l\sin\theta}{C}\right)^{\frac{1}{2}} \tag{2.7}$$

Expanding Eq. 2.7 as a square root of the Taylor series with $a = 0$, we get

$$D \approx C\left(1+\frac{1}{2}\left(\frac{l\sin\theta}{C}\right)-\frac{1}{8}\left(\frac{l\sin\theta}{C}\right)^2+\frac{1}{16}\left(\frac{l\sin\theta}{C}\right)^3-\ldots\right) \tag{2.8}$$

Only the first two terms in the parentheses are significant, so the equation reduces as follows:

$$D \approx C\left(1+\frac{l}{2C}\sin\theta\right) \tag{2.9}$$

Similarly,

$$A \approx C\left(1-\frac{l}{2C}\sin\theta\right) \tag{2.10}$$

The phase difference Φ, in degrees, between two antennas is calculated by:

$$\Phi = \frac{2\pi(A-D)}{\lambda} = \frac{2\pi l\sin\theta}{\lambda} \tag{2.11}$$

where λ is the wavelength, l is the distance between the two antennas and θ is the direction

of arrival. If the transmitter is located on the main antenna axis, the phase difference is equal to 0°. The signal-to-noise ratio (SNR) indicates the amount of noise a signal experiences. A ratio of 1:1 indicates there is more signal than noise. The smaller the ratio, the more the signal is influenced by the noise. SNR greatly affects the phase comparison technique; however, Mahafza summarizes the implementation of the sum and difference channels to increase the accuracy of the phase comparison monopulse [19]. Two or more simultaneous beams received at the antennas are compared. The sum and difference channels, represented by Σ and Δ in Eqs. 2.12 and 2.13, are the addition and subtraction of the two signals S_1 and S_2 in the antennas.

$$\Sigma(\Phi) = S_1 + S_2 \tag{2.12}$$

$$\Delta(\Phi) = S_1 - S_2 \tag{2.13}$$

The signals have similar amplitude, but differ by a phase of Φ. Therefore, the sum and difference channels are expressed as:

$$\Sigma(\Phi) = S_2(1 + e^{-\jmath\Phi}) \tag{2.14}$$

$$\Delta(\Phi) = S_2(1 - e^{-\jmath\Phi}) \tag{2.15}$$

The phase error E is the ratio of the difference and sum signals, this is represented by Eq. 2.16, which is purely imaginary.

$$\frac{\Delta}{\Sigma} = \frac{(1 - e^{-j\Phi})}{(1 + e^{-j\Phi})} = j\tan\left(\frac{\Phi}{2}\right) \tag{2.16}$$

Then, the modulus of the error signal is

$$E = \tan\left(\frac{\Phi}{2}\right) \tag{2.17}$$

2.1.3 RSS Tracking

Radio Frequency (RF) signals attenuate as they propagate through an environment due to several factors such as reflection, refraction and multipath, resulting in a location estimation error [20]. Nevertheless, RSS measurements can be taken easily in numerous applications, which makes RSS tracking a desirable technique. RSS-based localization algorithms can be categorized as signature dependent or geometric. Signature dependent techniques collect RSS measurements during an offline training phase. This technique is generally used in indoor environments because it has fewer environmental fluctuations. The location of a transmitter is determined by matching the measurement to the existing collection [21]. The geometric RSS-based technique estimates the location using the strength of the signal and the Euclidean space. Laurendeau and Barbeau investigated the combination of RSS values and Hyperbolic Position Bounding (HPB) to localize transmitters [22]. This method utilized a probabilistic geometric path loss model, in addition to the maximum and minimum hyperbolas between a transmitter and receiver pair to estimate a location in which a transmitter may lie.

It is proven that the collaboration of localization techniques with RSS can improve

their performance [12, 14, 20]. Malhotra et. al. evaluated the performance of the combination of RSS and AOA localization using directional antennas in different network deployments [14]. The deployment scenarios are when the anchor and target antennas are aligned, unaligned and if the target antenna is omni-directional. The semi-directional antennas are arranged in a square layout and triangulate the cooperative target node by measuring the RSS values and determining the radial distance. The AOA and the calculated distance can be used to pinpoint the location of the antenna. This technique may be improved by averaging the radial distance from several antennas.

2.1.4 Time-Based Tracking

Time of Arrival (TOA), or Time of Flight (TOF), measures the round trip time for a message to be received from a transmitter to a receiver. Another time-based localization system is Time Difference of Arrival (TDOA). TDOA calculates the time difference for a message to be received by several synchronized receivers. Transmitters and receivers need to be synchronized, since inaccurate times result in an incorrect location estimation. A GPS receiver calculates its position by timing the arrival of signals received from the GPS satellites. Sastry et al. proposed a localization verification scheme called Echo protocol [23]. The protocol uses a prover and verifier node. The prover node requests access to the network and the verifier node may either accept or reject the prover node based on the time elapsed between the signals sent and received, and if it determines the prover node to be in a certain region of interest.

2.2 Radio Propagation Models

Friis described the power received at an antenna, given the transmitting antenna is at r distance away [24]. This is represented by:

$$P_R = P_T G_T G_R \left(\frac{\lambda}{4\pi}\right)^2 \left(\frac{1}{r}\right)^\eta \tag{2.18}$$

where P_R and P_T is the power received and transmitted, G_R and G_T is the gain received and transmitted, λ is the wavelength of the signal and η is the path loss exponent. When $\eta = 2$ models the behaviour of a signal in free space with no obstacles and the power received at the antenna is proportional to the inverse square of the distance [25, 26]. This free space model is unrealistic and real environments can be modelled using an empirically determined path loss exponent. The path loss exponent is the rate of an attenuated signal as it propagates through space and varies with the propagation environment. The more obstacles the environment has, the higher the path loss loss exponent.

Different theoretical and empirical models have been proposed to predict the behaviour of radio wave propagation in outdoor and indoor environments. The Okumura-Hata model is suitable for urban areas and calculates the transmitter and receiver heights using path loss [27]. Another propagation model is the two-ray ground model which is more accurate than the free space model [28]. This model takes into account the direct and reflected paths while introducing the antenna heights and is represented by:

$$P_R = \frac{P_T G_T G_R h_t^2 h_r^2}{d^4} \tag{2.19}$$

where P_R and P_T is the power received and transmitted, G_R and G_T is the gain received and transmitted, h_t and h_r are the transmitter and receiver heights, and d is the distance between the antennas. The Nakagami model predicts the received power based on a fading

parameter m which is determined from a series of experiments [28]. When m is equal to 1 represents a non-LOS communication, typically known as a Rayleigh distribution. As the fading parameter increases, it resembles a free space environment. Another predictive model is the log-normal shadowing model, which determines the path loss a signal experiences as it travels a transmitter and receiver (T-R) distance [26], as described in Section 2.2.1. We use the log-normal shadowing model in our work.

2.2.1 Log-Normal Shadowing

We model the behaviour of the signal in a real environment using the log normal shadowing model. The log-normal shadowing model calculates the path loss $L(d)$ a signal experiences as it travels a known T-R distance [26],

$$L(d) = \overline{L}(d_0) + 10\eta \log\left(\frac{d}{d_0}\right) + X_\sigma \tag{2.20}$$

where d_0 is the reference distance closest to the transmitter, $\overline{L}(d_0)$ is the average path loss at d_0, η is the path loss exponent and X_σ is a Gaussian distributive random variable with zero mean and standard deviation σ (dB). Variations of the path loss exponents and standard deviations commonly studied environmental cases, are shown in Table 2.1 [25].

Table 2.1: Path Loss Exponents and Standard Deviation for Different Environments

Environment	Path Loss Exponent	Standard Deviation (dB)
Free Space	2	0
Urban Area Cellular Radio	2.7 - 3.5	10 - 14
Shadowed Urban Cellular Radio	3 - 5	11 - 17
In building line-of-sight	1.6 - 1.8	4 - 7
Obstructed in building	4 - 6	5 - 12
Obstructed in factories	2 - 3	6 - 9

Chapter 3

The Four-Square Antenna

In this chapter, we describe the operation of the four-square antenna. This antenna uses its directional properties to detect an evil twin attack and localize the transmitters involved. We show how the location determination approaches discussed in Chapter 2, relate to the four-square antenna.

3.1 The Operation of the Antenna

The four-square antenna consists of four identical antennas positioned on the corners of a square with a one-quarter wavelength side. This low profile antenna makes it practical to be used in commercial and military applications [29]. Our work is based on the conventional four-square antenna as shown in Figure 3.1 [30]. Each element is connected with an individual feed line to the center of the array and is driven with equal amplitude and in-phase excitation to produce beams on the xz and yz planes. Figure 3.2 shows the physical structure of the antenna. Figure 3.3 shows the radiation pattern of an element in the antenna. Four beams are created along the feed line and formed in the xy plane, obtaining 360° azimuth coverage, as shown in Figure 3.4.

An antenna's performance is measured by its radiation pattern and gain [30]. The gain

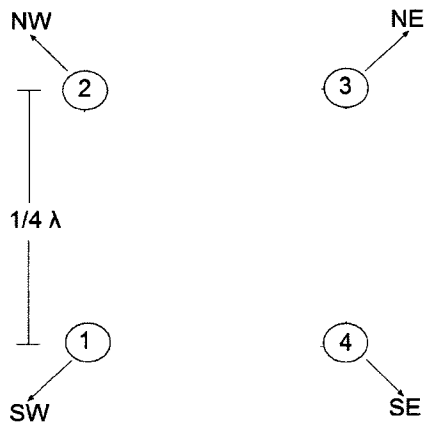


Figure 3.1: The conventional Four-Square antenna

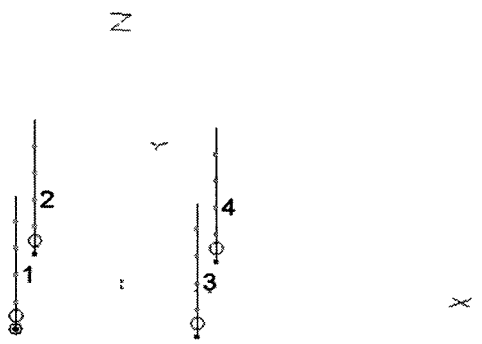


Figure 3.2: The Physical Structure of the Four-Square Antenna

of an antenna is the direction of the maximum radiated energy. The radiation pattern is the distribution of the energy received or radiated in the angular regions. The four-square antenna is categorized as a directional antenna. A directional antenna radiates or receives energy in a desired direction, which is the direction of maximum radiation or reception. This improves the antenna's efficiency by increasing the gain in a region when transmitting, and reducing the noise when the antenna is receiving [31]. Some examples of directional antennas are the loop, parabolic and Yagi antennas. The radiation pattern of an element in the four-square antenna is similar to a dipole over a ground plane [32]. Figure 3.5 shows the radiation pattern of a dipole. An omni-directional antenna radiates or receives energy

equally in all directions and is unable to determine the direction of the received signal. In our work, we use the four-square antenna because of its directionality and the gain received is dependent on the angle of the incoming signal.

On reception of a signal, each element in the four-square antenna registers a RSS value. The gain of each element in the four-square antenna is dependent on the angle of arrival and is similar to a cardioid shaped function, with a maximum gain G_{max} and exponent m $\geq$1:

$$G(\theta) = G_{max}\left(1 + \cos\left(\theta\right)\right)^m = G_{max}\left(\cos^2\left(\frac{\theta}{2}\right)\right)^m \tag{3.1}$$

where θ is the angle of arrival and m is the directivity of the antenna. Larger values of m result in a more directive antenna [33]. The importance of using the four-square antenna is that in addition to registering the signal, the antenna is able to determine the direction of arrival of the incoming signal.

A variety of strategies have been employed to steer the beams in the four-square array in a desired direction. One strategy uses a hybrid coupler to provide equal amplitude and current with a phase difference of 90° [34]. Christman modified this model to produce an eight direction of fire four-square element [35]. The array fires from the diagonals and the sides of the square by varying the phase angle of the current. Devoldere describes a mathematical approach to steer a beam by having absolute control of the magnitude and phase of the current in the elements [31].

3.2 Range Estimation with the Four-Square Antenna

It is possible to estimate the distance of a transmitter from a receiver given the power of the transmitter and the attenuation model. For example, a free space radio signal is

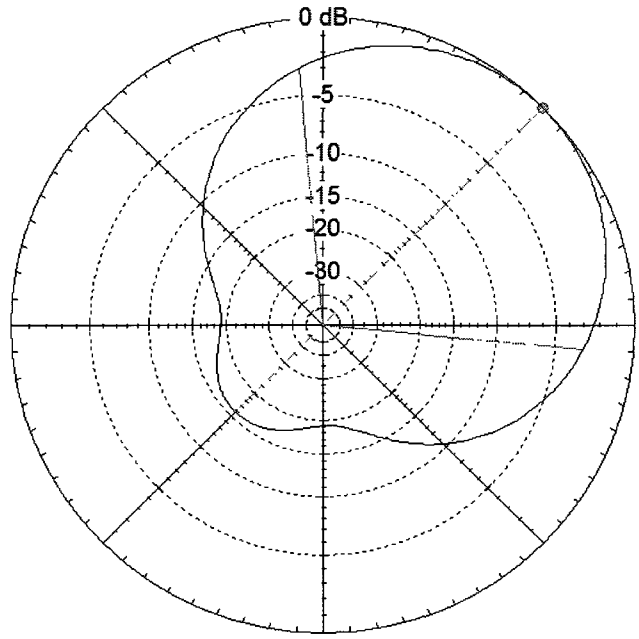


Figure 3.3: Radiation Pattern of an Element within the Four-Square Antenna

transmitted from a node and reduced by a factor of $\frac{1}{r^2}$ when it reaches the receiving node at r distance away [15]. Lateration, as described by Hightower and Borriello, calculates the position of the transmitter based on distance measurements from multiple receivers [15]. Each element in the four-square antenna receives signals from the target antenna. Let P_T and G_T denote the transmitted power and gain at the target antenna, P_R and G_R denote the maximum received power and the gain received at the four-square antenna. The path loss exponent is known and the estimated distance r of the target transmitter from the four-square antenna can be calculated using Eq. 2.18. Figure 3.6 shows the range-based technique with four-square antennas at the receivers. Each receiver estimates the distance from the target antenna. The intersection of the distance measurements pinpoints the location of the target antenna. The received power fluctuates due to several propagation factors, resulting in inaccurate distance estimation [36, 25].

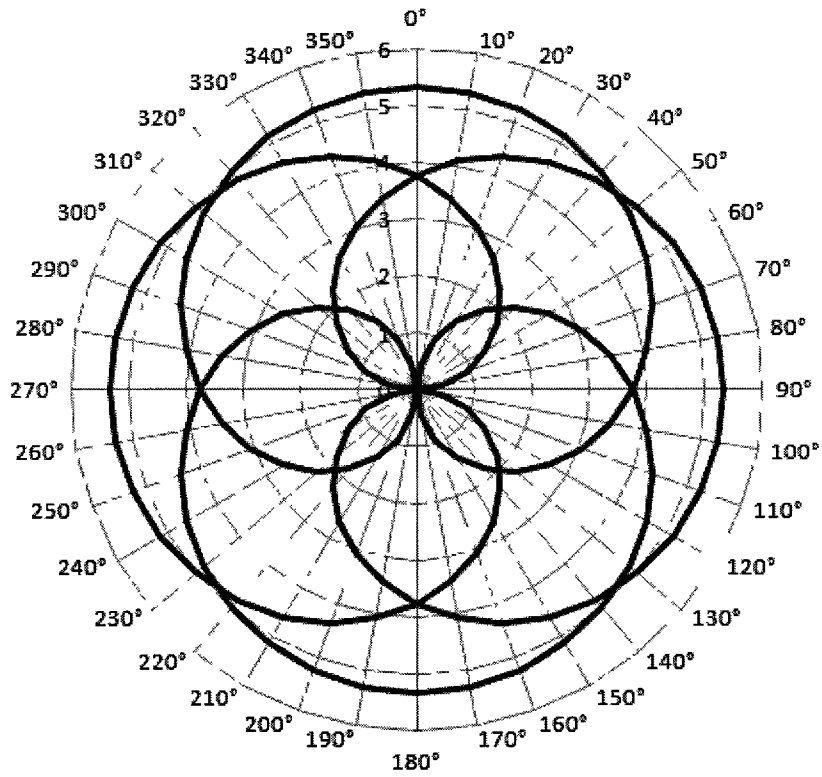


Figure 3.4: The Clover-Shaped Radiation Pattern of the Four-Square Antenna

3.3 Hyperbolic Position Estimation

HPB, described by Laurendeau and Barbeau in [37], is a localization scheme which estimates the probabilistic maximum and minimum distance between the T-R. Each pair of receivers in the environment calculates the maximum and minimum distance from the transmitter and the corresponding hyperbolas are constructed. The location of the transmitter is bounded in the intersection of the hyperbolas. The smaller the candidate area, the easier it is to pinpoint the transmitter. El Sayr introduces the HPB with Learning Ability (HPB-LA) system, which improves the accuracy of the HPB mechanism by determining the best receiver pairs to use to locate a transmitter in the offline phase. Bhatia uses the directionality of the four-square antenna in combination with the HPB technique to detect a malicious transmitter [38].

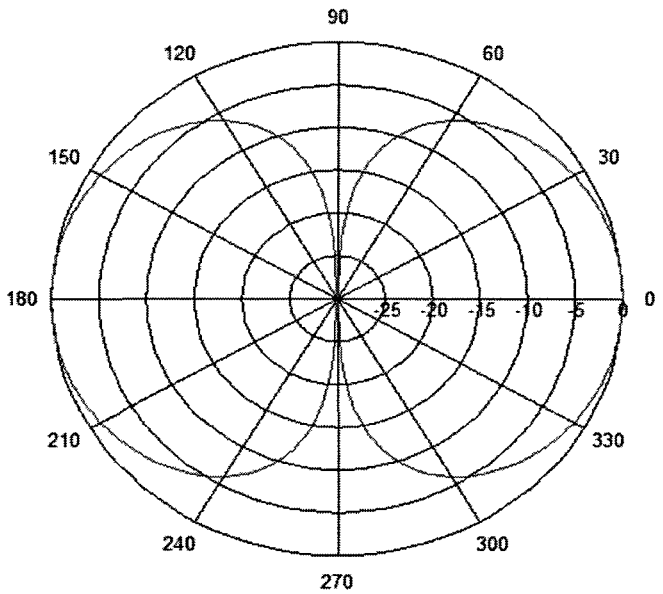


Figure 3.5: Radiation Pattern of a Dipole

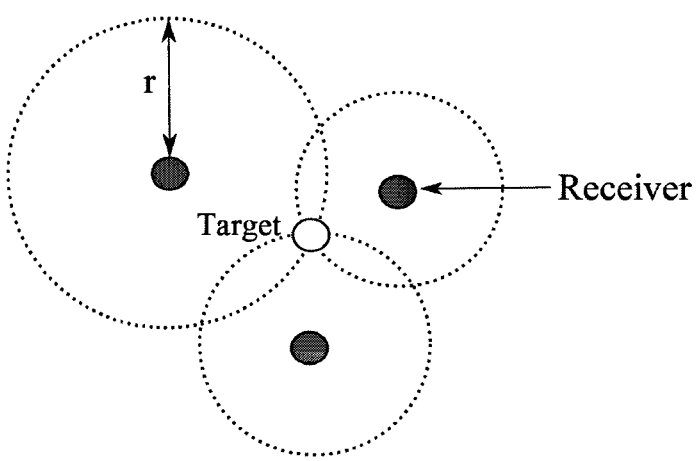


Figure 3.6: Lateration Technique with the Four-Square Antenna.

Chapter 4

Related Work

We review existing literature relevant to our area of research. It is important to detect spoofing attacks and localize the attackers involved. Several attack scenarios are discussed, specifically the evil twin attack, which is the focus in our paper. Section 4.1 describes different types of attacks. Section 4.2 details previous work for detecting and localizing multiple transmitters.

4.1 Attacks in Wireless Networks

Most wireless networks employ strict security features; however, they are still vulnerable to attacks [6]. A malicious wireless node can sniff packets in the coverage area and disrupt the connection by launching a DoS or man-in-the-middle attack [6, 7]. Mai et. al. categorised a rogue AP into four classes: improperly configured, unauthorised, phishing and compromised AP [39]. Improperly configured APs may appear rogue because of a small configuration mistake. Unauthorised APs gain access to the network without authorisation. Phishing APs attempt to acquire sensitive information. A compromised AP is a malicious insider or an AP that has been hacked.

Security breaches can be prevented if we can detect and locate the attackers from gain-

ing unauthorised access. We describe some attacks related to our work and the detection and localization of these attacks.

4.1.1 Wormhole Attack

In a simple wormhole attack, an attacker deploys two transceivers in a network to create a tunnel. The malicious nodes gain access to the network and eavesdrop on the packets being transmitted in the coverage area. The packets are tunneled from one intruder node to the other. The tunnel affects routing and connectivity in the network because it is seen as a shortcut. The collusion of the intruder nodes may create dropped packets, a DoS or a man-in-the-middle attack. Wormhole attacks are difficult to detect because attackers can break or connect the tunnel at any time.

Hu and Evans presented a localization technique utilizing directional antennas to prevent wormhole attacks [2]. The antenna has n zones and obtains the zone in which the maximum signal is received. This zone is used to communicate with the transmitter. The technique employs three protocols: Directional, Verified and Strict Neighbour Discovery. The first protocol chooses an announcer, which broadcasts to all nodes. If a node is a neighbour of the announcer, the node uses the Verified Neighbour Discovery protocol, otherwise the message is ignored. An attacker can trick the announcer that a distant node is its neighbour. The second protocol, Verified Neighbour Discovery, prevents this vulnerability. An announcer node may only accept the neighbour node if it is determined to be legitimate by the verifier node. The verifier node is a node located in a zone which has the least probability to be affected if a wormhole is near the announcer. The Strict Neighbour Discovery protocol protects against the Worawannotai attack. The Worawannotai attack occurs when nodes are unable to hear each other but have a verifier node that can hear both nodes. If the nodes are out of range, the protocol ensures that the verifier region is

empty. The technique described by Hu and Evans has satisfactory performance and introduces small overhead; however, it prevents some legitimate links from being established [2].

4.1.2 MAC Spoofing

Medium Access Control (MAC) spoofing is a technique which modifies the address of a node, hence allowing a malicious device to impersonate other devices in a network. The attacker can easily read packets and launch other attacks. MAC spoofing is a serious threat and various countermeasures have been employed to minimize its effect [40, 41]. Radio Frequency Fingerprinting (RFF) has been studied to detect MAC spoofing specifically [40]. RFF, employed by Hall et al., is a technique that can identify a transceiver based on a transient portion of the signal it generates [40]. Before deployment of the network, the transceiver profiles of the networking devices are stored in a database. As signals are detected, feature extraction is introduced and the fingerprint of the signal is compared to the profiles stored in the database. If the transceiver print is not in the database, the signal is ignored else the information is retrieved. Profiles can be updated to take into consideration transceiver aging and the environmental conditions. Cardenas described several techniques to prevent MAC spoofing such as installing a firewall and Reverse Address Resolution Protocol (RARP) [41]. RARP maps a MAC address to an Internet Protocol (IP) address. An attack will be detected if there are multiple IP addresses assigned to a single MAC address.

4.1.3 Evil Twin Attack

The evil twin attack occurs when a rogue AP that appears to be legitimate, gains access to the network. The rogue AP exploits the network by intercepting traffic. The most common evil twin attacks are launched at wireless hot spots and impersonate a legitimate

provider [7]. The client or operating system connects to a familiar network associated by the name or the RSS. The malicious node is now capable of sniffing client information. The evil twin attack can cause security breaches in a highly secured network [6], as the attacker can implement a DoS attack and force the client to connect to it. Evil twin attacks are difficult to ascertain since they can be turned off an any time.

Several countermeasures have been proposed for this attack [38, 42, 43]. Bhatia uses a hyperbolic localization scheme with four-square antennas to detect an evil twin attack and localize the transmitters involved [38]. Several software systems are available which monitor the RF signals collected from the APs and compares the RFF with an authorized list [44, 42, 43]. However, some of these systems have a high percentage of claiming a legitimate AP as a rogue [7].

In our work, we consider a general form of the evil twin attack, called the evil twin transmitter attack. A wireless malicious node gains access to the network and uses the same identity as a legitimate wireless node. The wireless network consists of several receivers and a truth-teller transmitter. The truth-teller transmitter is only honest in terms of it does not lie about its identity. A malicious transmitter gains access to the network by impersonating the truth-teller transmitter. No assumptions are made about the nature of the transmitters in the network, since it is possible that they are colluding to launch attacks.

4.2 Detecting and Localizing Multiple Transmitters

The detection of a malicious node or an attack is difficult and expensive, specifically to detect them simultaneously. Yang et al. defined a system to detect spoofing attacks, identify the number of attackers, and localize the multiple adversaries using a cluster-based

technique [21]. The cluster analysis identifies the attack by monitoring the RSS to determine the location which is characterised by the dimensional signal space. The work in [21] assumes an indoor environment. Nelson et al. focus on locating multiple transmitters within a set geographic area using Particle Swarm Optimization (PSO) [45]. PSO uses a cost function and searches the area for the location of the transmitter that minimizes the function.

Shetty et al. focus on another approach, utilizing traffic characteristics to detect a malicious node [46]. The principle of this method is when a rogue AP accesses the network, the traffic from the attacker will be more than a legitimate node in the network. If it exceeds beyond a pre-defined threshold, then the device is an attacker. Han et al. measures the round trip time between the user and Domain Name Server (DNS) to detect a rogue AP [47].

4.3 Summary

Section 4.1 detailed different types of attacks related to our work. We reviewed the literature related to the evil twin attack, which is the focus in our paper. Section 4.2 discussed techniques employed to localize multiple attackers and adversaries.

Chapter 5

Location Estimation Using the Four-Square

We describe the implementation model of the four-square antenna, which can provide angular and diversity information for location sensing. We also determine the location estimation error of the techniques using one and two four-square antennas.

5.1 Location Estimation Algorithms

We implement a model of the four-square antenna using the phase comparison technique as described in Section 2.1.2. We consider four elements in the antenna *1, 2, 3* and *4* in a Northeast-Southwest and Northwest-Southeast direction, as shown in Figure 5.1. Each pair of elements in the four-square antenna has an axis, which is perpendicular to its baseline. The baseline is the line connecting the two elements. The element pairs can be in a vertical, horizontal or diagonal configuration, such as pairs *1-2*, *1-4* and *2-4*. The phase differences and angles of the element pairs are positive, if measured anticlockwise from the main antenna axis and negative, if measured clockwise. The other side of the axis

mirrors the signs of the phase differences from the main antenna axis. The phase angles fluctuate between 90° and −90°. Figure 5.10 and 5.11 show the expected phase differences and phase angles for each element pair as a function of the azimuth of the transmitter with no environmental noise.

Figure 5.1 shows the axis of the element pair *2-3* and the signs of the phase differences recorded in relation to the main antenna axis. If a wireless node is located at 90° to the receiver, the node resides on the element pairs *2-3* and *1-4* axes and the phase differences of 0° will be recorded. It will be determined that the transmitter either lies in two possible directions: 90° or 270° from the receiver. This poses a problem since we need to determine the true bearing and location of the transmitter. Figure 5.2 shows the phase angle between the element pair *2-4*. The axis of the element pair *2-4* is perpendicular to its baseline and runs along the element pair *1-3*. Then phase angle θ is the direction of the signal at the axis of the element pair *2-4*.

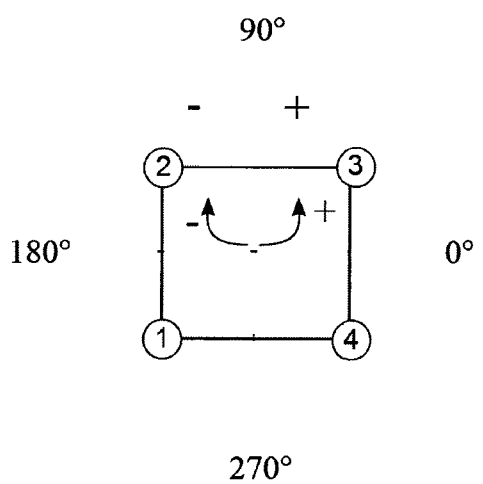


Figure 5.1: The Axis of the Element Pair *2-3*

The direction of propagation of the radio signal received at an antenna is affected by the environmental noise [19]. We assume the phase is influenced by an additive Gaussian noise which has a normal distribution of $X \sim \mathcal{N}(\mu, \omega^2)$. The random variable X is distributed

normally with mean μ and variance ω^2. The Gaussian distribution has the property that 95% of the measurements lie within the plus/minus standard deviation of the mean. For example, if the standard deviation of the noise is $\frac{\pi}{8}$, then 95% of the samples will lie in the interval $(\frac{-\pi}{4}, \frac{\pi}{4})$ of the true azimuth.

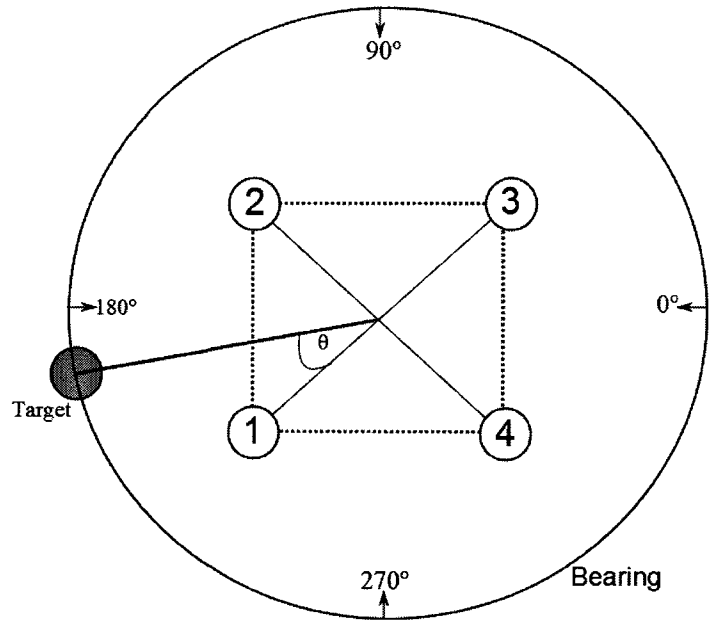


Figure 5.2: Implementation Model of the Four-Square Antenna with the Phase-Comparison

5.1.1 Localization Using Multiple Four-Square Antennas

The phase differences at each element pair is recorded and the phase angle is calculated. To determine the location of the transmitter, at least two independent azimuth angles must be measured from the receivers. The intersection of the lines drawn from the two azimuths yields the approximate location of the target node. If three four-square antennas receive a signal from the target node, this will increase the accuracy and show the probable location of the transmitter.

On reception of a signal, the four-square antenna registers the RSS and phase differences. The phase angles are calculated from the phase differences. A phase angle θ corresponds to two possible azimuths $Azimuths_{i,j}$ of the transmitter at each element pair i and j. This poses a problem since we need to determine the true bearing of the transmitter. The investigation of the behaviour of the phase angles as the transmitter cycles around the receiver reveals that the comparison of the set of azimuths from the two element pairs *1-3* and *2-4* yields the true bearing. The differences of the azimuths of the element pairs *1-3* and *2-4* are calculated. The difference or similarity represents the azimuths closeness in terms of degrees. The average of the azimuths which relate to the minimum difference is chosen as the true bearing. The intersection of two or more azimuth lines from the receivers will determine the coordinates of the transmitter.

Figure 5.11 shows the similarity comparison algorithm. The element pairs *1-3* and *2-4* have the set of azimuths 40° and 50°, 50° and 220° respectively. The comparison of the azimuths 50° and 50°, will yield a similarity of 0°, which will be the minimum value. The location of the transmitter will be determined to be at a bearing of 50° from the receiver.

5.1.1.1 Direction Finding via Azimuthal Similarity Comparison

The phase differences are measured at each receiver and the corresponding phase angles are calculated. If the element pair *2-3* has a phase angle of 0°, the transmitter resides at an azimuth of 90° or 270° from the receiver. If an element pair *3-4* has a phase angle of 0°, the transmitter lies along the azimuth of 0° or 180° from the receiver. A phase angle relates to two possible bearings $Azimuths_{i,j}$ at each element pair i and j. This poses a problem since we have to determine the exact bearing of a transmitter from the receiver.

We establish a relationship between the phase angle θ and the two possible azimuths

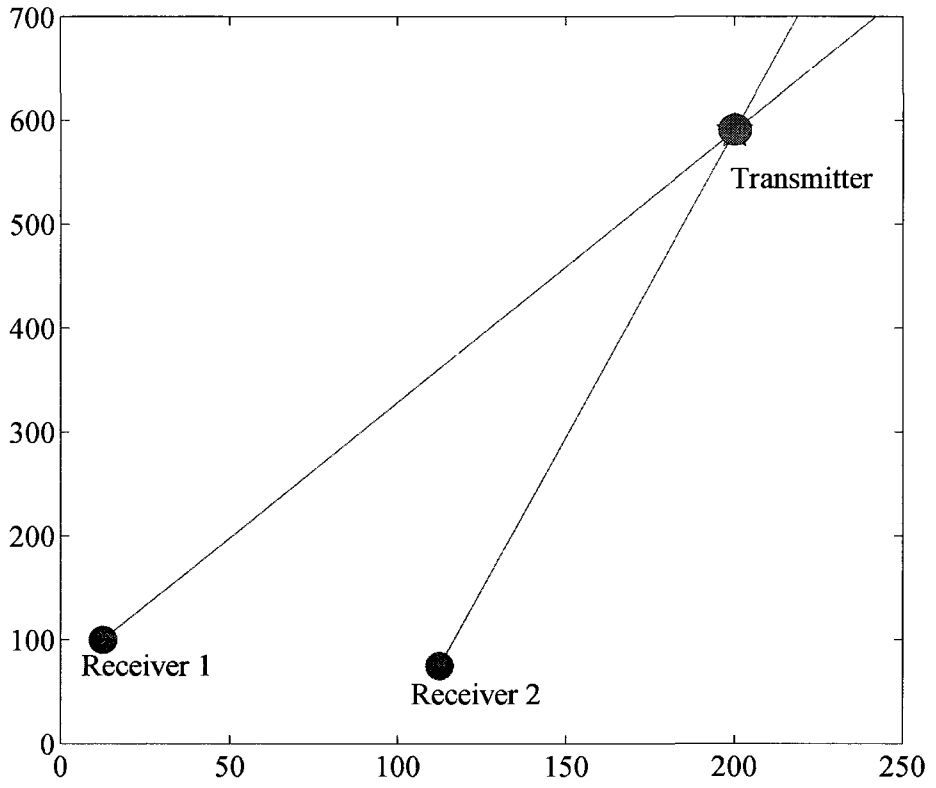


Figure 5.3: Localization of a Transmitter Using Two Four-Square Antennas

$Azimuths_{i,j}$ of the transmitter for each element pair i and j. The set of equations are:

$$Azimuths_{1,2} = \left\{ \theta, 180 - \theta \right\} \tag{5.1}$$

$$Azimuths_{1,3} = \left\{ 135 - \theta, 315 + \theta \right\} \tag{5.2}$$

$$Azimuths_{1,4} = \left\{ 90 + \theta, 270 - \theta \right\} \tag{5.3}$$

$$Azimuths_{2,3} = \left\{ \ 90 - \theta, 270 + \theta \ \right\} \tag{5.4}$$

$$Azimuths_{2,4} = \left\{ \ 225 + \theta, 45 - \theta \ \right\} \tag{5.5}$$

$$Azimuths_{3,4} = \left\{ \ 180 + \theta, -\theta \ \right\} \tag{5.6}$$

Algorithm 1 determines the relative position of the transmitter by comparing the similarity of the possible azimuths of the element pairs *1-3* and *2-4*, which have a common reference point at the midpoint of the four-square antenna. The azimuth range is between 0° and 360°. *Similarity* will refer to the absolute difference between the two azimuth measurements. There are six element pairs for a receiver and the variable *count* keeps track of how many pairs have been processed. The element pairs are *1-2*, *1-3*, *1-4*, *2-3*, *2-4* and *3-4*. The phase angles and the two azimuths of each element pair *i-j* in the receiver are calculated and stored in $PhaseAngles_{count}$, $Az_{count,1}$ and $Az_{count,2}$.

We use the element pairs *1-3* and *2-4* to determine the bearing of the transmitter from the receiver, which corresponds to the variable *count* at *2* and *5*. The array *Bearing* stores the azimuths of the element pairs *1-3* and *2-4*. We compare and calculate the similarity of these azimuths. An azimuth calculated using one element pair is compared with the two azimuths calculated using a different element pair.

A problem may arise: if 357° and 4° are compared, it will have a similarity of 353°, which is incorrect as it is determined not to be relatively close in terms of their angular direction. It should have a difference of 7°. This problem is handled by finding the min-

imum azimuth in *Bearing*. The azimuths of the element pair, which correspond to the minimum azimuth, is modified by adding an angle of 360°. *Similarity* is the difference of the azimuths' element pairs. The difference of the azimuths in terms of degrees, is calculated by subtracting 360°.

The function *abs* makes all values positive. The minimum difference in *Similarity* is calculated, and its index *NewIndex* is stored. The *AverageAzimuth* of the four-square antenna can be determined from the azimuths associated with the minimum similarity. The intersection of two or more lines drawn along the azimuths of the receivers will determine the coordinates XY of the transmitter.

The location of a transmitter may be found by simple triangulation or the least squares approach. In the least squares approach, the azimuth $AverageAzimuth_n$ from each receiver is used in an equation binding the locations of the receivers to the transmitter [48].

$$X - x_n = (Y - y_i) \cdot \tan(90 - AverageAzimuth_{1,n}) \tag{5.7}$$

where $\begin{bmatrix} X & Y \end{bmatrix}$ and $\begin{bmatrix} x & y \end{bmatrix}$ are the coordinates of the transmitter and the receiver. The receiver will estimate the position of the transmitter using the system of equations below.

$$A \cdot c^T = b \tag{5.8}$$

where A= $\begin{bmatrix} 1 & -\tan(90 - AverageAzimuth_1) \\ 1 & -\tan(90 - AverageAzimuth_2) \\ \vdots & \vdots \\ 1 & -\tan(90 - AverageAzimuth_n) \end{bmatrix}$, c= $\begin{bmatrix} X & Y \end{bmatrix}$ and

$$\text{b}=\begin{bmatrix} x_1 & -y_1 \tan(90 - AverageAzimuth_1) \\ x_2 & -y_2 \tan(90 - AverageAzimuth_2) \\ \vdots & \vdots \\ x_n & -y_n \tan(90 - AverageAzimuth_n) \end{bmatrix}.$$

Therefore, the estimated position is

$$c = ((A^T A)^{-1} A^T b)^T \tag{5.9}$$

5.1.2 Localization Using One Four-Square Antenna

In the localization using one four-square antenna method, all possible angle of arrivals at each element pair are calculated using the phase differences. The intersection points of the azimuth lines for each combination of element pairs are estimated. The intersection point which has the maximum distance from the centre of the four-square antenna is chosen as the location of the transmitter.

We describe the method using one receiver to localize a transmitter in Algorithm 2. The four-square antenna is an antenna array which has the ability to use the signal received at each element to locate a wireless node. The phase $PhaseDifference_{i,j}$ of each element pair $i - j$ is registered and the phase angle $PhaseAngles_{i,j}$ is calculated. The phase angle corresponds to two possible directions from the midpoint of the element pair's axis, as shown in Figure 5.4. The array *Angles* stores all phase angle combinations of the horizontal and vertical element pairs in the four-square antenna.

The function *CalculateAllIntersection* calculates the intersection points for each combination of element pairs in *Angles*. There are two azimuths for each element pair, this means at most there will be four intersection points for one combination. However, some of the azimuth lines may be parallel, coincident or have no intersection point, resulting

Algorithm 1 Calculate the transmitter's location

```
for n = 1 to N receivers do
  count =0
  for i = 1 to 3 do
    for j = i + 1 to 4 do
      Register PhaseDifference_count
      Calculate PhaseAngles_count
      Calculate Az_{count,1}, Az_{count,2}
      count = count + 1
    end for
  end for
```

$$Bearing = \begin{bmatrix} Azimuths_{5,1} \\ Azimuths_{5,2} \\ Azimuths_{2,1} \\ Azimuths_{2,2} \end{bmatrix}$$

```
  Index ⟵ Calculate the index which has the minimum azimuth in Bearing
  if (Index ≤ 2) then
    Bearing_1 = Az_{5,1} + 360°
    Bearing_2 = Az_{5,2} + 360°
  else
    Bearing_1 = Az_{2,1} + 360°
    Bearing_2 = Az_{2,2} + 360°
    Bearing_3 = Az_{5,1}
    Bearing_4 = Az_{5,2}
  end if
  Similarity_1 = Bearing_1 − Bearing_3
  Similarity_2 = Bearing_1 − Bearing_4
  Similarity_3 = Bearing_2 − Bearing_3
  Similarity_4 = Bearing_2 − Bearing_4
  Similarity = Similarity − 360
  Similarity = abs(Similarity)
  [Value, NewIndex] = min(Similarity)
  AvgAzimuth_n ⟵ Calculate the average of the azimuths associated with the
  NewIndex of the minimum similarity calculated
end for
XY ⟵ Calculate the intersection using the average azimuth of the four-square antennas
```

in null values. For example, we compare the phase angles of element pairs *1-4* and *2-3*. The intersection points for the azimuth lines of the element pairs are calculated, and a set of possible intersection points are returned. The coordinate with the maximum distance from the middle of the four-square antenna is chosen and stored in the variable $PossibleCoordinates_a$. The variable a is the number of element pair combinations. The function *CalculateAllIntersection* is repeated for each element pair combination, resulting in a set of possible intersections points *PossibleCoordinates*.

In the function *CalculateIntersection*, the coordinates with the maximum distance from the middle of the four-square antenna is chosen from the set *PossibleCoordinates*. The four-square antenna has a low profile therefore some of the intersection points may be located in the antennas layout, as shown in Figure 5.4. This is minimised by choosing the intersection point with the maximum distance from the receiver.

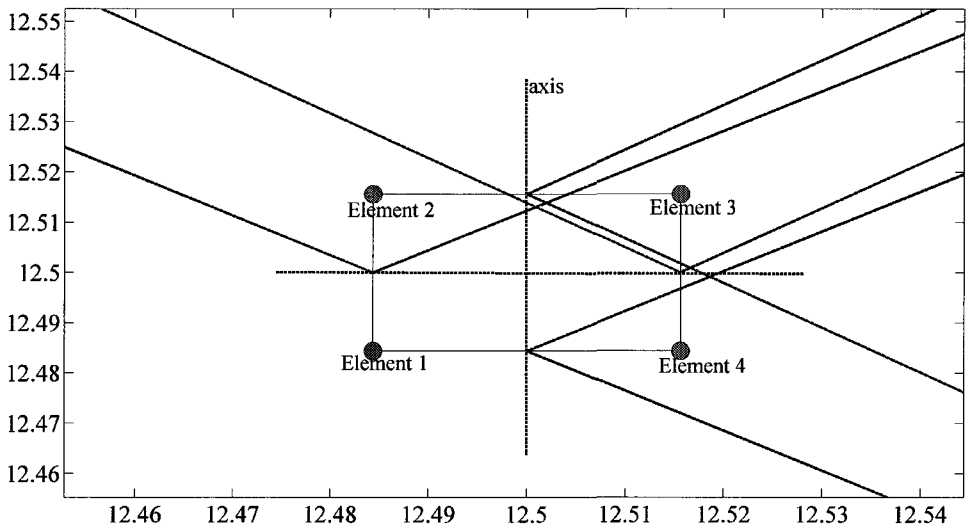


Figure 5.4: Angle of Arrivals Possibilities at Each Element Pairs' Axis in the Receiver

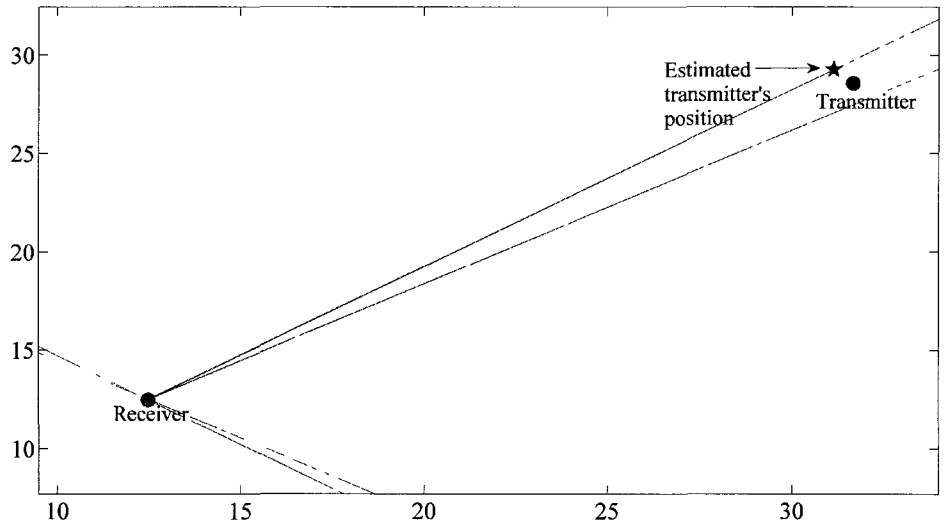


Figure 5.5: Localization Using One Four-Square Antenna

5.2 Performance Evaluation

Two receivers operating in the 2.4 GHz frequency range, are placed in an environment with no prior knowledge of the location and activity of the transmitter. The power received is greater than the sensitivity of the receiver. The sensitivity of a receiver is the minimum tolerable signal strength that a receiver can detect. Each receiver has a random amount of noise. The performance metrics of the algorithm are the percentage of locations identified successfully and the location error. The percentage of locations identified successfully is the number of locations identified divided by the total number of tries. In some cases, the receivers may fail to identify a location when the azimuth lines are parallel or coincident. Location error R_{error} is the distance between the estimated and actual location of the transmitter, divided by the distance between the axis of the receiver and the actual transmitter's position [14]. The location error is defined as:

$$R_{error} = \frac{\sqrt{(x_{estimated} - x_{actual})^2 + (y_{estimated} - y_{actual})^2}}{\sqrt{(x_{axis} - x_{actual})^2 + (y_{axis} - y_{actual})^2}} \tag{5.10}$$

Algorithm 2 Calculate the transmitter's location using one receiver

for $i = 1$ to 3 **do**
  for $j = i + 1$ to 4 **do**
    Register $PhaseDifference_{ij}$
    Calculate $PhaseAngles_{ij}$
  end for
end for

$$Angles = \begin{bmatrix} PhaseAngle_{1,2} & PhaseAngle_{3,4} \\ PhaseAngle_{1,4} & PhaseAngle_{2,3} \\ PhaseAngle_{1,2} & PhaseAngle_{1,4} \\ PhaseAngle_{1,2} & PhaseAngle_{2,3} \\ PhaseAngle_{3,4} & PhaseAngle_{1,4} \\ PhaseAngle_{3,4} & PhaseAngle_{2,3} \end{bmatrix}$$

for $a = 1$ to 6 **do**
  $PossibleCoordinates_a \longleftarrow CalculateAllIntersection(Angles_{a,1}, Angles_{a,2})$
end for
$Coordinates \longleftarrow CalculateIntersection(PossibleCoordinates)$
return Coordinates

where $x_{estimated}, y_{estimated}$ are the coordinates of the estimated position of the transmitter, x_{actual}, y_{actual} are the coordinates of the actual transmitter's location and x_{axis}, y_{axis} are the coordinates of the receiver.

5.2.1 Results of the Localization Using Two Four-Square Antenna

The results of Algorithm 1 are presented in this section with a confidence level of 95%, as shown in Appendix A. Figure 5.6 shows that Algorithm 1 effectively determines the azimuth of the transmitter from the receiver. The angle function is the angle between the receivers and the transmitter. For example, if the transmitter is located between the receivers, the angle function is 180°, as shown in Figure 5.7. If the transmitter is directly located to the left or right of both receivers, the angle function is 0°. Algorithm 1 fails to locate the position of the transmitter when the angle function is 0° and 180° because the azimuth lines are parallel or coincident, as shown in Figure 5.7. The transmitter is suc-

cessfully localized 99.9% of the time when the transmitter is not on the receivers' baseline. The receivers' baseline is the line connecting the two receivers.

Figure 5.8 shows the location error in different noisy environments. Small angles are more affected by noise than large angles [13]. An angular error of 5° will affect a small angle function of 10° more than a large angle of 75°. The smaller the angle function, the larger the location error. When the angle function is greater than 25°, the location error decreases. A large amount of environmental noise results in a higher location error.

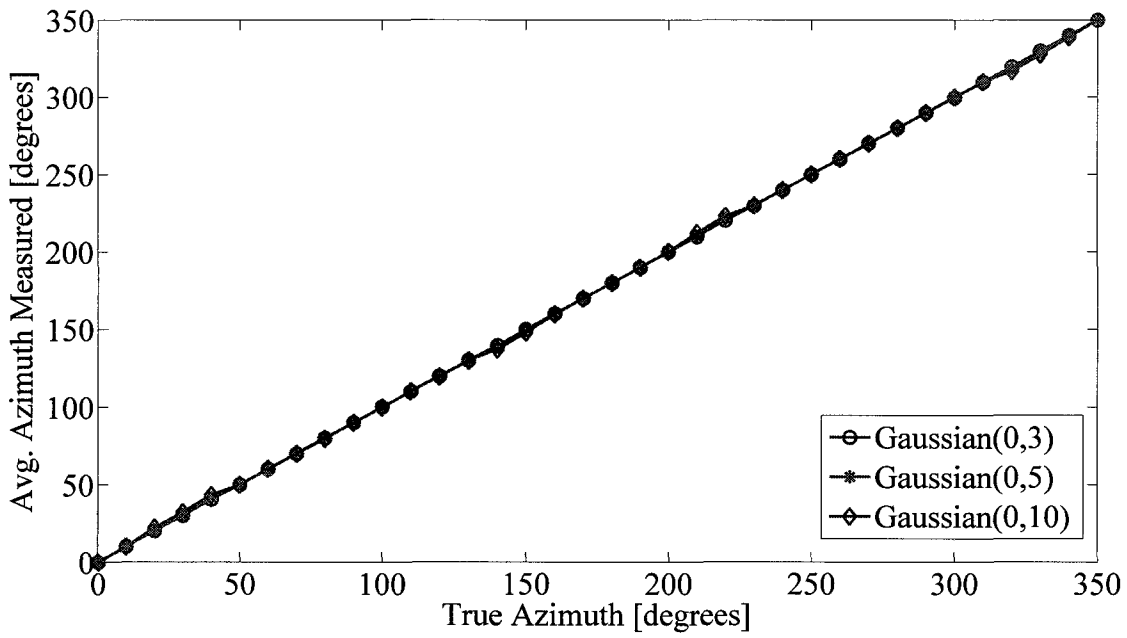


Figure 5.6: Performance of Algorithm 1

5.2.2 Results of the Localization Using One Four-Square Antenna

The results of Algorithm 2 are presented in this section with a confidence level of 95%, as shown in Appendix A. Algorithm 2 is robust, as the wireless node is localized 100% of

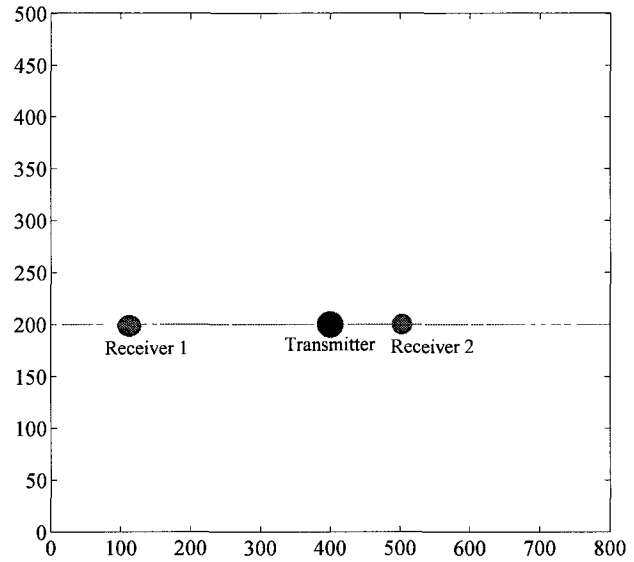


Figure 5.7: Failure to Identify the Location of the Transmitter at an Angle Function of 180°

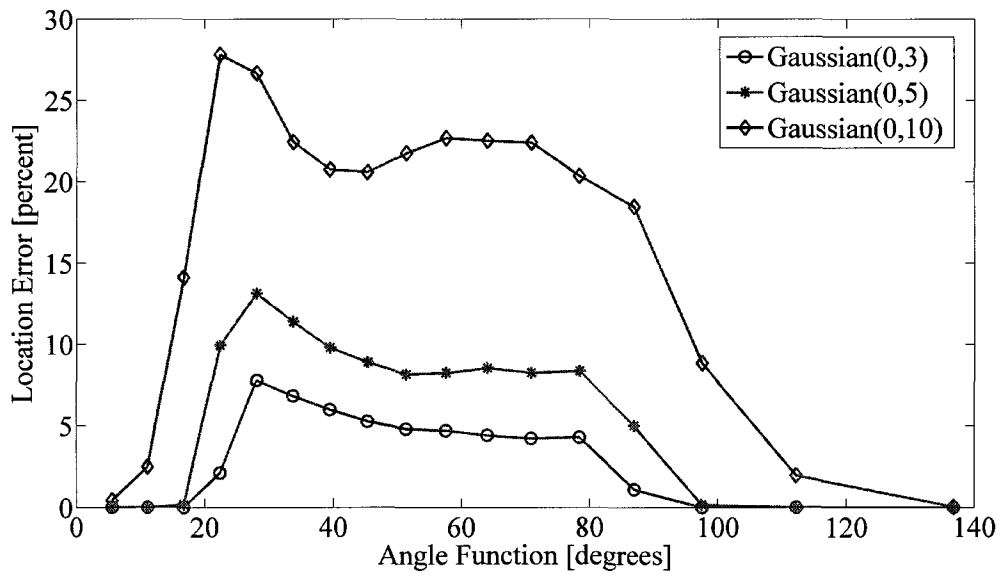


Figure 5.8: Location Error Using Two Four-Square Antennas

the time, independent of the noise and the angle function. The angle function is the angle between the receiver and the transmitter, and the transmitter and the North landmark. The North landmark is located to the North of the receiver at the end of the wireless

environment and is used to facilitate the comparison of the two methods by way of the angle function value.

Figure 5.9 shows the location error of Algorithm 2. As the transmitter moves away from the axis of the receiver, the location error fluctuates and four peaks are observed. The axis of the receiver is at 0°, 90°, 180° and 270°, which relates to the angle function of 180°, 59°, 0° and 59°, respectively. When the transmitter is close to an axis of the element pair, the location error increases. A good location estimate of the wireless node is obtained when the node is at least 10° from the axis of an element pair. A small phase angle calculated at an element pair is greatly affected by noise, resulting in a large location error estimate.

The environmental noise affects the location error. The average location error of the noise with the standard deviation 3, 5 and 10 dBm is 3%, 6% and 15%, respectively, when two receivers are used to localize a transmitter. A higher location error was experienced for the second method, where one four-square antenna was used for localization. The location error is 5%, 8% and 16% for the Gaussian noise 3, 5 and 10 dBm, respectively. Localization using two receivers fails to determine a position for the transmitter when it has an angle function of 0° or 180°. A higher degree of accuracy is obtained when multiple receivers are introduced. In our work, we use multiple receivers to localize transmitters. However, in cases where only one receiver detects a signal from a wireless node, we can fallback on Algorithm 2.

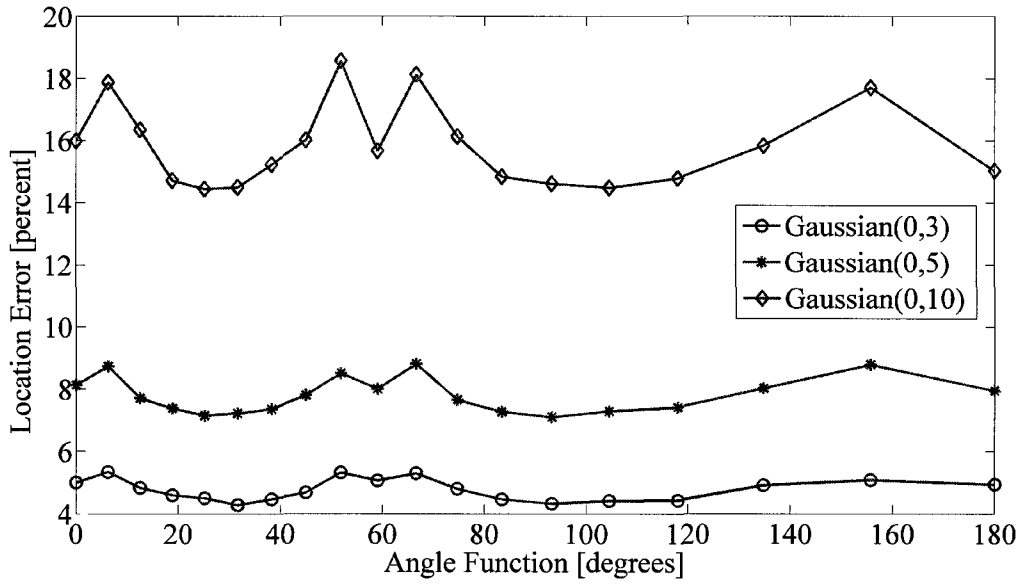
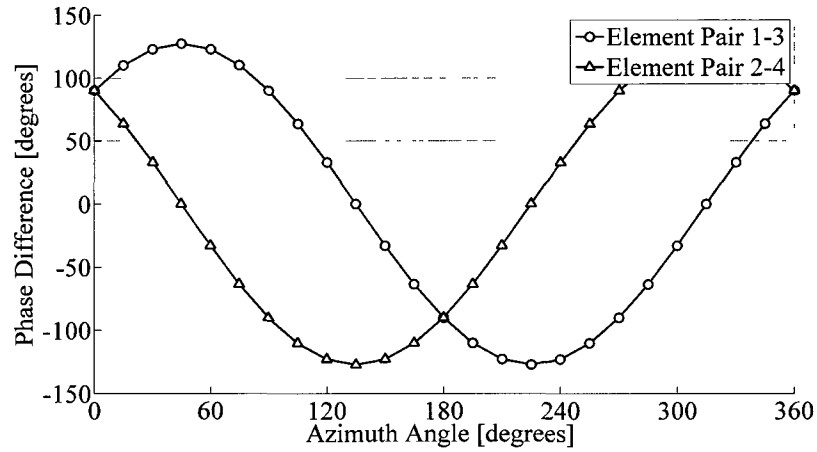
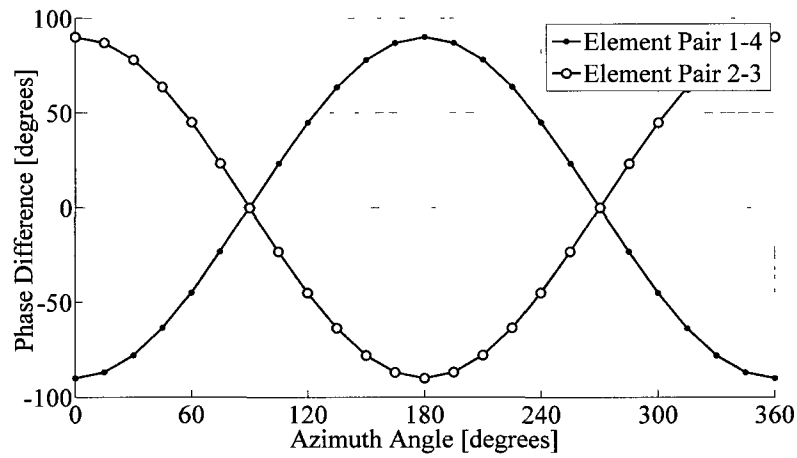


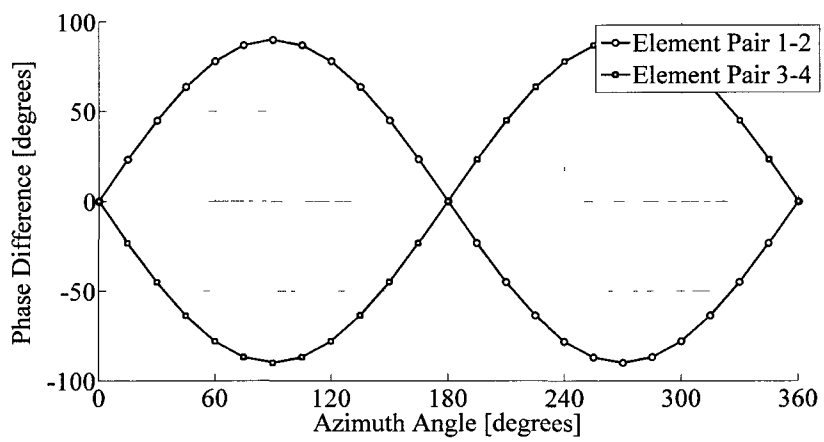
Figure 5.9: Location Error Using One Four-Square Antenna



(a) Phase Difference of the diagonals of the Four-Square Antenna

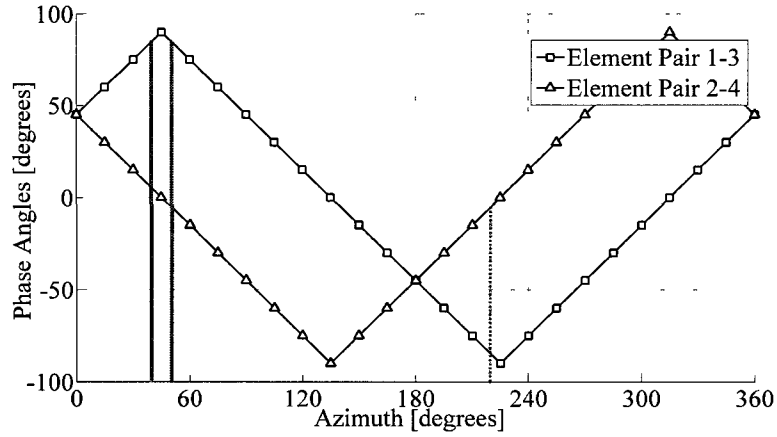


(b) Phase Difference of the Horizontals of the Four-Square Antenna

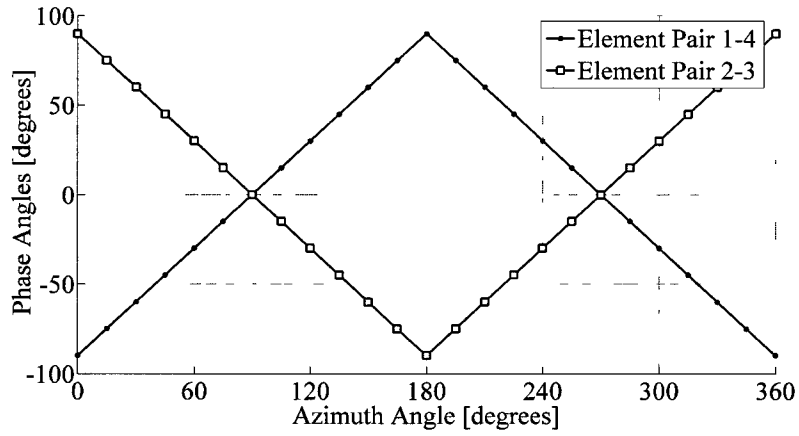


(c) Phase Difference of the Verticals of the Four-Square Antenna

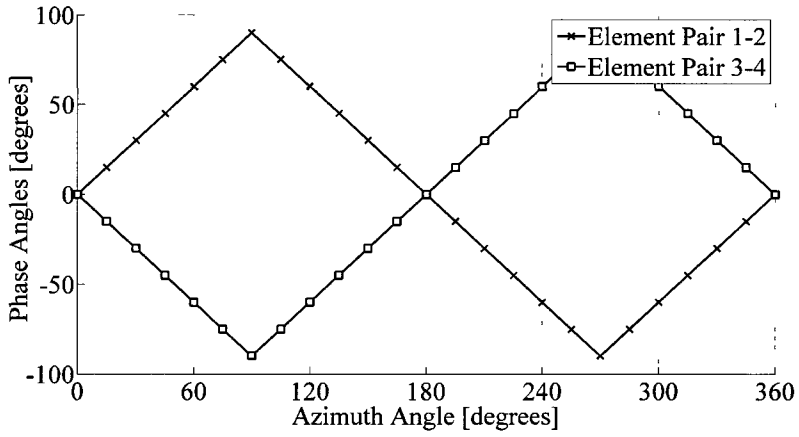
Figure 5.10: Phase Difference of the Four-Square Antenna



(a) Phase Angles of the Diagonals of the Four-Square Antenna



(b) Phase Angles of the Horizontals of the Four-Square Antenna



(c) Phase Angles of the Verticals of the Four-Square Antenna

Figure 5.11: Phase Angles of the Four-Square Antenna

Chapter 6

Defeating the Evil Twin Attack

In the evil twin transmitter attack, a rogue wireless node gains access to the network and eavesdrops on the traffic. Wireless networks are susceptible to evil twin attacks as they are easy to launch, but difficult to ascertain. Existing solutions on evil twin attacks consider monitoring RF waves from each node, or using a hyperbolic localization scheme to detect the rogue node [38, 42, 43]. We propose two evil twin detection schemes for different network layouts: a regular grid and a randomly distributed environment. The four-square antenna uses its directional properties to detect an evil twin attack and then probabilistically locate the positions of the transmitters.

6.1 The Attack Model

Our attack model assumes an outdoor wireless network with several receivers that monitor the phase differences of the signal detected. The receivers have four-square antennas and communicate securely with each other. The location of each receiver deployed in the network is known. A truth-teller transmitter resides in the network and does not lie about its identity, which is handled by the error detection code. An attacker or *evil twin* gains access

to the network by using the same identity and transmits information at the same time as the truth-teller transmitter. The receivers have no prior knowledge of the transmitting power and the location of the transmitters. We assume that the transmitters are equipped with omni-directional antennas and are only able to send messages to the receivers that are one hop away.

The receivers will be confused by the presence of the evil twin in the network and may be connected to the truth-teller transmitter, the evil twin or neither due to interference. For a signal to be detected at a receiver, the RSS of a signal must be within the dynamic range of the receiver. The dynamic range is the ratio of the minimum and maximum tolerable signal a receiver can handle. If two signals are received within the dynamic range, the signals interfere and nothing is recorded. If strong and weak signals are received, and the weak signal is not within dynamic range, the stronger signal is registered. The sensitivity of a receiver is the minimum tolerable signal strength a receiver can detect.

6.2 Partitioning the Wireless Environment

The environment is divided into n zones where n is always a perfect square. The zone is a section of the grid, as shown in Figure 6.2(a). The number of receivers deployed in the network, is equivalent to the number of zones. In our work, we use 9 zones and 9 receivers. In the regular grid environment, the receivers are aligned in a rigid structure and are placed in the middle of the zones as shown in Figure 6.2. The zones are numbered I, II, III, IV, V, VI, VII, VIII and IX. In the randomly distributed network, the receivers are randomly placed, as shown in Figure 6.6.

Each receiver has a four-square antenna and is capable of registering the RSS and using the phase differences of the element pairs to calculate the azimuth of the signal received.

The azimuth corresponds to the sector in which the antenna receives a signal. The sector is a quadrant of the four-square antenna, as shown in Figure 6.1. Sectors 3, 2 , 1 and 4 are between 0° and 90°, 90° and 180°, 180° and 270°, 270° and 360°. Each zone is divided into four sub-zones. In Zone I, the sub-zones are 1, 2, 7 and 8, as shown in Figure 6.2(b). The sub-zones are numbered 1 to 36. The regular grid algorithm has been specifically designed for the four-square antenna, with the four sectors corresponding to the four elements of the antenna. If a receiver *R1* detects a signal from a transmitter in sector 1, the transmitter may lie in sub-zones 7, 13, 19, 25 or 31. If a receiver *R1* detects a signal from sector 3, the transmitter may lie in in sub-zones 2, 3, 4, 5 or 6. In the random algorithm, the directional properties of the four-square antenna is used to determine the azimuth of the transmitter.

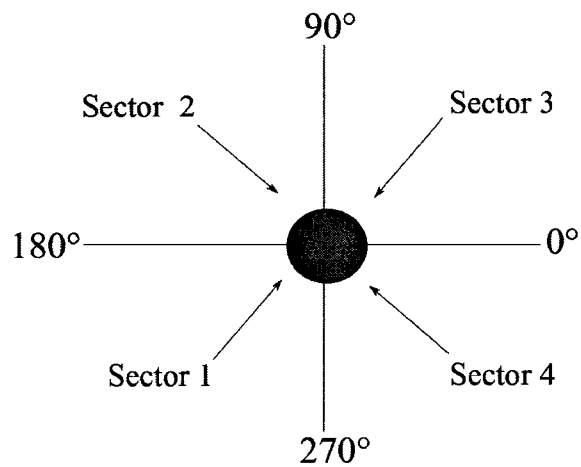


Figure 6.1: The Sectors of a Receiver

6.3 Detection Algorithm for a Regular Grid Network

On reception of a signal, a receiver registers the RSS value and the phase differences. This information is collectively used at the Central Processing Point (CPP) to determine if the network is under attack, and if true, then the transmitters are localized. The CPP uses the

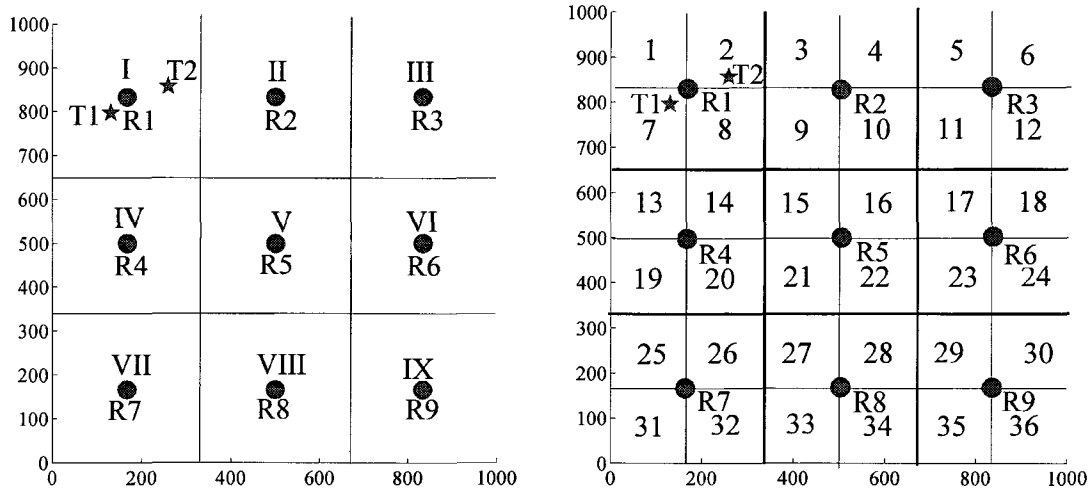


Figure 6.2: Wireless Environment Partitioned into (a) Zones and (b) Sub-Zones

phase differences from each receiver to determine the incoming signal which corresponds to the sector in which the transmitter may lie. The sectors of the receivers in the same row and column are compared. If the sectors and the sub-zones are overlapping, this information is consistent with one transmitter residing in the environment and the system declares the network is safe. For example, if receivers R_1 and R_2 register a signal from a transmitter T_1 in sector 1, the system is declared to be not under attack, as shown in Figure 6.3(a). The sub-zones are overlapping and the information from the receivers is consistent with one transmitter residing in the wireless environment. An evil twin transmitter attack is detected if there is conflicting information about the location of the transmitter. For example, if the receiver R_1 registers a signal from a transmitter T_1 in sector 1 and the receiver R_2 registers a signal from a transmitter T_2 in sector 2, the system is declared to be under attack, as shown in Figure 6.3(b).

The CPP compares information from the receivers in the same row or column. Algorithm 3 describes the procedure used to identify an evil twin attack. On reception of a signal, each receiver records the RSS and phase differences of the signal. The CPP calculates the direction of the signal and its sector using the phase differences, defined

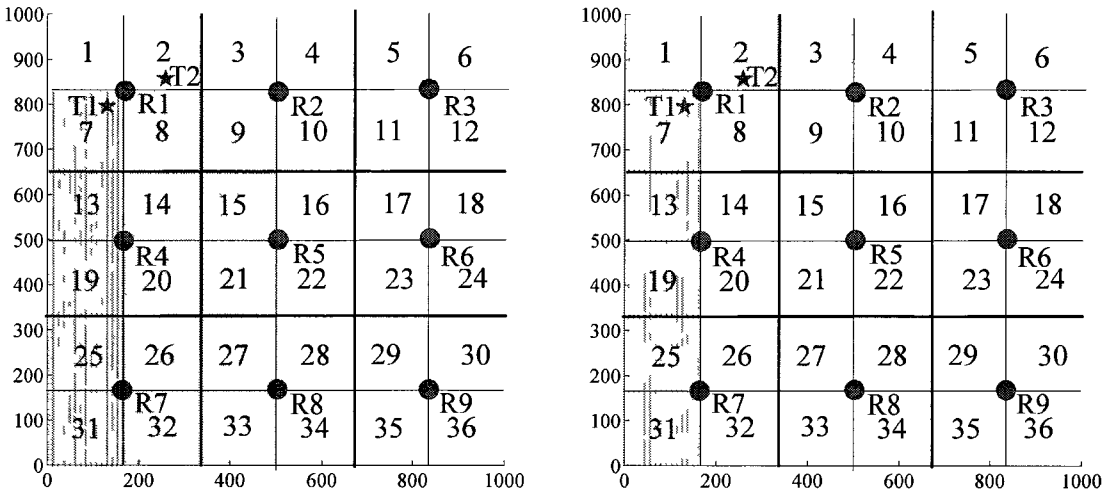


Figure 6.3: Wireless Environment when (a) No Attack is Detected (Overlapping Sub-Zones) and (b) An Attack is Detected (Conflicting Sub-Zones)

in Algorithm 3 as *AvgAzimuth* and *sector*, respectively. The variable *Receivers* store the receivers that detect a signal and the variable *ETA* monitors if the system is under attack. The function *size* determines the number of receivers that detect a signal and stores this value in the variable *Size*. The receivers in each row and column in the environment are analysed. The receivers in row 1 are: R_1, R_2 and R_3; in row 2 are: R_4, R_5 and R_6; in row 3: R_7, R_8 and R_9. The receivers in column 1 are: R_1, R_4 and R_7; in column 2 are R_2, R_5 and R_8; in column 3 are: R_3, R_6 and R_9. If receivers R_1, R_2, R_6 and R_7 detect a signal, then the sectors of the receivers in the row R_1 R_2 and column R_1 R_7 are compared. The system is unable to perform any comparison with receiver R_6 as there are no nearby receivers that detect a signal. Each receiver $Receiver_i$ and the corresponding sector $Sector_i$ in a row is compared to other receivers $Receiver_j$ and their $Sector_j$ in the same row. Each receiver $Receiver_i$ and the corresponding sector $Sector_i$ in a column is compared to other receivers $Receiver_j$ and their $Sector_j$ in the same column. When the sub-zones or sectors of the receivers being compared do not overlap, as shown in Figure 6.3(b), the system declares an evil twin transmitter attack and the variable *ETA* is set to 1. The receivers in-

volved are identified as a conflicting pair. If there is no conflict, the system is declared safe.

Algorithm 3 Identify Evil Twin Attack

```
for i = 1 to N receivers do
  Register RSS_i, AvgAzimuth_i, sector_i
end for
Receivers = [ R_1  R_2  ...  ... ]
Sector = [ sector_1  sector_2  ...  ... ]
ETA = 0
[Row, Size] = size(Receivers)
for i = 1 to Size do
  for j = 2 to Size do

    if Receivers_i & Receivers_j are in the same row then
      if Sector_i == 1 & Sector_j == 3||Sector_i == 2 & Sector_j == 3||
        Sector_i == 3 & Sector_j == 4||Sector_i == 1 & Sector_j == 2||
        Sector_i == 1 & Sector_j == 4||Sector_i == 2 & Sector_j == 4||
        Sector_i == 4 & Sector_j == 2||Sector_i == 3 & Sector_j == 1||
        Sector_i == 2 & Sector_j == 1 then
        ETA=1
      end if
    end if
    if Receivers_i & Receivers_j are in the same column then
      if Sector_i == 1 & Sector_j == 3||Sector_i == 2 & Sector_j == 4||
        Sector_i == 2 & Sector_j == 3||Sector_i == 3 & Sector_j == 1||
        Sector_i == 4 & Sector_j == 2||Sector_i == 1 & Sector_j == 4||
        Sector_i == 2 & Sector_j == 1||Sector_i == 3 & Sector_j == 2||
        Sector_i == 3 & Sector_j == 4 then
        ETA=1
      end if
    end if
  end for
end for
return ETA
```

6.3.1 Dividing the Receivers into Pools

When the system detects an evil twin transmitter attack, the system divides the receivers into two pools to determine which receivers are detecting a signal from the transmitters T_1 and T_2. The first pool consists of the receivers detecting a signal from a transmitter and the second pool is made up of the receivers detecting a signal from the other transmitter. We use the method described in Section 5.1.2, localization using one four-square antenna, to pinpoint the location of the transmitter from each receiver. A cluster of the possible locations of the transmitter means that the receivers are detecting a signal from the same transmitter, as shown in Figure 6.4. The clustering algorithm requires that each coordinate be compared to other coordinates, to determine which coordinates are close or within a certain distance d_c. Coordinates within the distance d_c are determined to be from one transmitter. The system calculates the intersection point of the azimuth lines from the set of receivers, which have been determined to be receiving a signal from the same transmitter. The receivers excluded are determined to be from the second transmitter and the intersection point of the azimuth lines is calculated. Multiple receivers improve the accuracy of localizing the transmitter.

If the environment has an unknown amount of noise, the system might be unable to detect two distinct clusters of points. We then analyse the conflicting pairs. For example, if there is only one conflicting pair R_1R_2, the receiver R_1 receives a signal from a transmitter T_1 and the receiver R_2 receives a signal from another transmitter T_2. Then receiver R_1 is placed in one pool and receiver R_2 is placed in the other pool. Localization using one four-square antenna can then be used to estimate the positions of the transmitters. Multiple conflicting pairs can also be divided into two pools. For example, receivers R_1 and R_9 detect a signal from a transmitter T_1 in sector 2, and the receiver R_3 registers a signal from a transmitter T_2 in sector 3. The conflicting pairs are R_1R_3 and R_3R_9. The system analyses the first conflicting pair, the receiver R_1 is placed in one pool and the receiver

R_3 in the other. The receiver R_9 is placed in the first pool since it is determined to be in conflict with the receiver R_3, which is in the second pool. If there are multiple receivers in a pool, the transmitters can be localized using multiple four-square antennas, as described in Section 5.1.1. If there is only one receiver in a pool, the transmitter may be localized using one four-square antenna, as described in Section 5.1.2.

We described a regular grid system that can be used to detect an evil twin attack. The disadvantages of this model is that antennas have to be aligned in a rigid pattern, therefore we propose an evil twin detection system for a random-based networking environment.

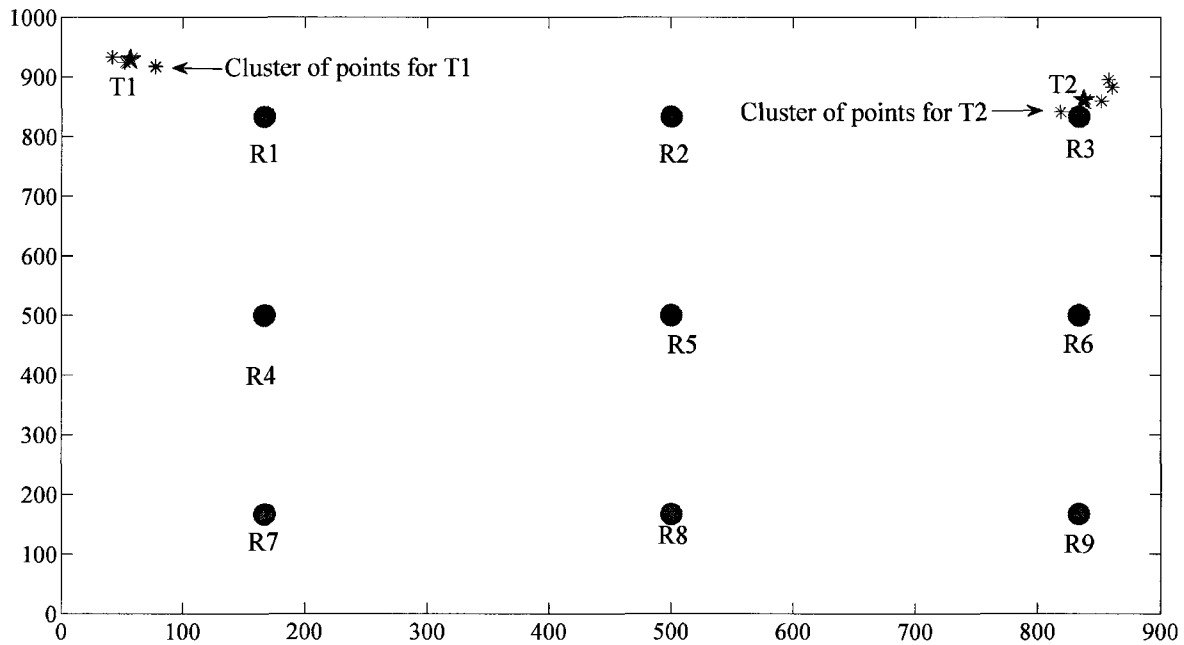


Figure 6.4: A Cluster of Points for Each Transmitter

6.4 Detection Algorithm for a Randomly Distributed Environment

The receivers are randomly placed in each zone throughout the environment. Each receiver registers the RSS value and the phase differences of the signal it receives. This information is sent to the CPP, which performs computations on each set of phase difference received to determine the direction of the signal at each receiver. A receiver pair is two receivers that detect a signal. All possible intersection points are calculated using the azimuth lines of the receiver pairs. If the CPP is unable to compute an intersection point for a receiver pair, this results in a null value and the system declares an evil twin transmitter attack as it senses there is more than one transmitter in the network. If the CPP is able to attain values for all intersection points, the system assumes that there is only one transmitter residing in the environment and there is no threat.

Figure 6.5 and 6.6 show the detection system in the two states: no attack and attack detected. In Figure 6.5, the intersection point of the azimuth lines of the receiver pair R_1R_2 is calculated and determined to be a value. The system declares the network is safe. In Figure 6.6, the CPP calculates the intersection points of the azimuth lines for the receiver pairs such as R_2R_3, R_2R_6, R_3R_6, R_6R_8. Some of the receiver pairs such as R_1R_2, R_1R_3 and R_1R_6, fail to disclose values when the intersection points of the azimuth lines are calculated. The system interprets this information as more than one transmitter residing within the environment.

In some cases, the receivers register signals from both of the transmitters in the environment and attains values for all intersection points of the azimuth lines for the receiver pairs. This results in a false negative, as shown in Figure 6.7. We extend the algorithm to handle this problem, when the lines of azimuths for the receivers pairs intersect with values. If the receivers are detecting a signal from one transmitter, this set of intersection

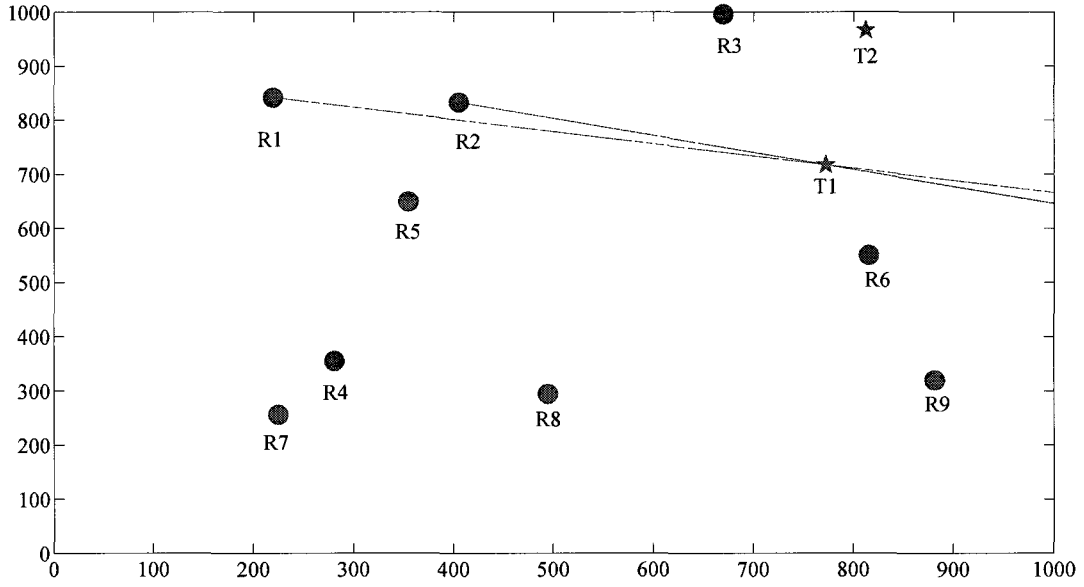


Figure 6.5: Detection System Declares the Network is Safe

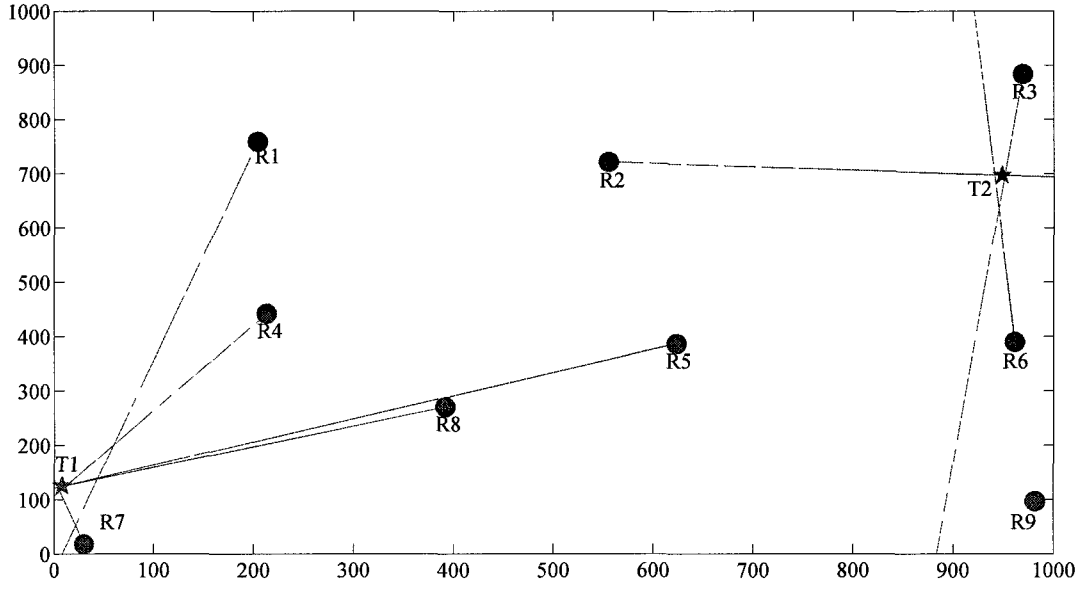


Figure 6.6: Detection System Declares an Attack

points will be within a certain distance from each other. We set the maximum distance between the coordinates as d_r. If the distance between the intersection points exceeds the

distance d_r, the CPP determines that it is under attack and the receivers are detecting signals from more than one transmitter. Figure 6.7 shows the system will now detect the threat, whereas without the extension to the algorithm, the system would have failed. Figure 6.8 is a flowchart of the detection system for a randomly distributed environment.

When the detection system is aware of an attack, it must pool the azimuths of the

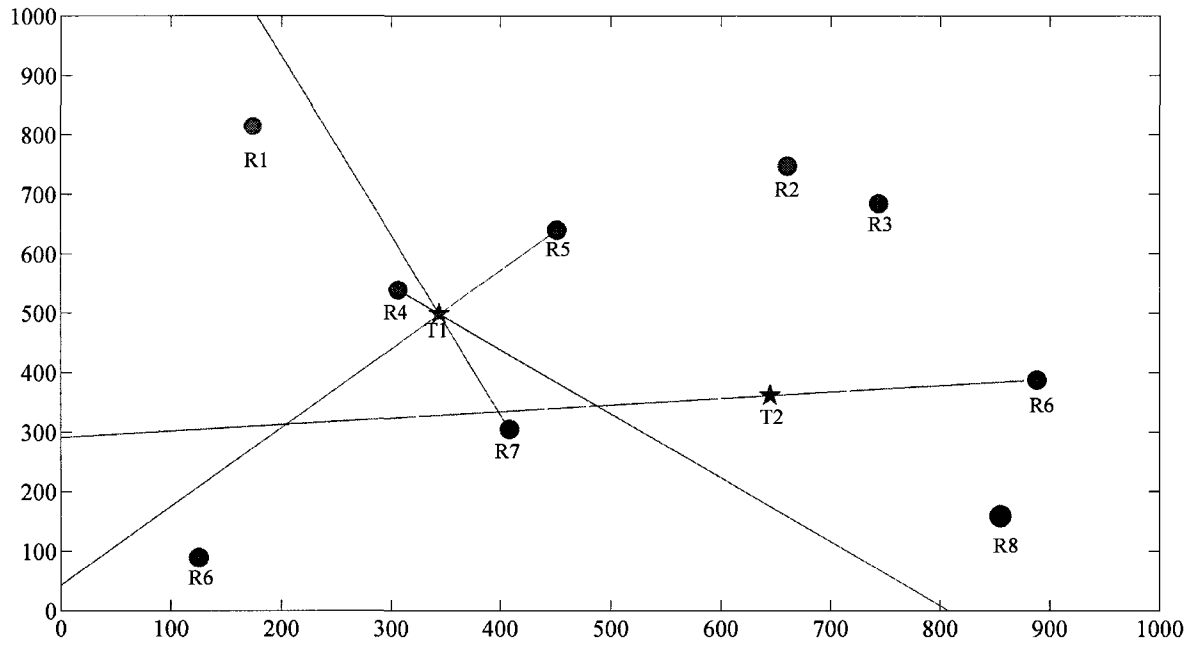


Figure 6.7: CPP Declares the System is not under Threat without the Extension of the Algorithm

receivers to determine which receivers are detecting a signal from the transmitters T_1 and T_2. Localization using each receiver is used to determine the possible coordinates of the transmitters. We use a clustering algorithm to pool the coordinates of the transmitters T_1 and T_2, as described in Section 6.3.1. The coordinates within a defined range d_c are related to one transmitter. The excluded coordinates are related to the other transmitter. If there are multiple receivers in a pool, the transmitters are localized using multiple four-square antennas as described in Section 5.1.1. If there is only one receiver in a pool, the transmitter may be localized using one four-square antenna as described in Section 5.1.2.

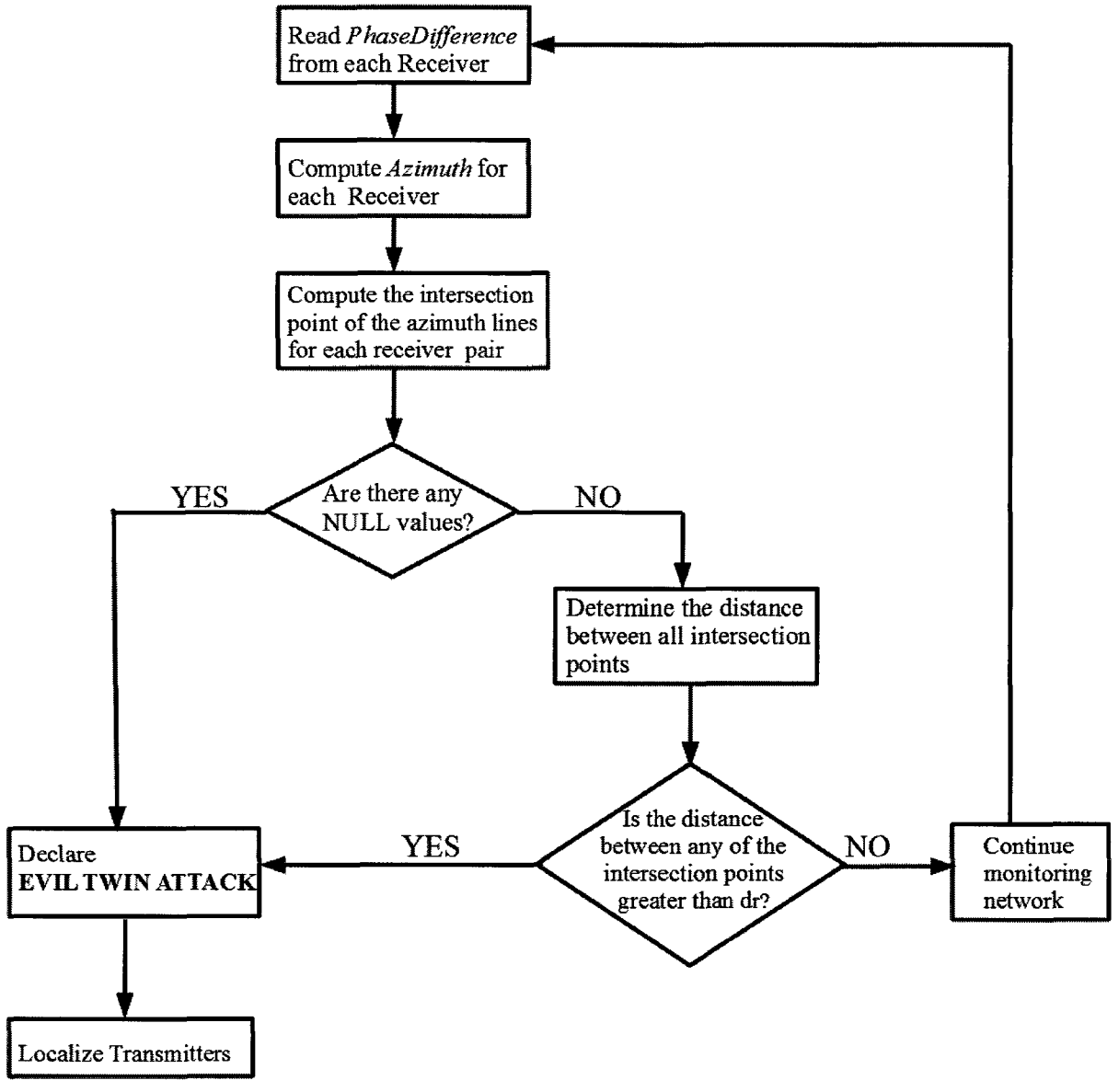


Figure 6.8: Detection System for a Randomly Distributed Environment

Chapter 7

Simulation

We discuss our simulation setup and evaluate the performance of the evil twin transmitter attack schemes in a regular grid and a randomly distributed network structure. When an attack is declared, the system localizes the transmitters involved. The simulation is performed under real world scenarios. The performance of our algorithms is compared to another evil twin detection scheme.

7.1 Simulation Setup

The environment is a 1000 x 1000 m^2 grid with 9 zones and 9 receivers. The receivers are operating in the 2.4 GHz frequency range and have no prior knowledge of the location or the activity of the transmitters. In the regular grid environment, the receivers are perfectly aligned in the middle of each zone and their locations are known. For each test run, the receivers are randomly placed in each zone for the randomly distributed environment. This random placement is chosen by chance with a uniform distribution. We use the parameter values obtained by Liechty et al. to model a real world environment, where the reference distance d_0 is one meter, the path loss exponent η is 2.76 and the standard deviation σ is 5.62 dB [49]. The maximum gain of each element in the antenna is 8 dBi

and the directivity parameter m is set to 1.

Each receiver simulates a random amount of signal shadowing and noise for each test run and for each transmitter. The noise generated in the environment has a zero mean and a standard deviation of 1.96 dBm [13], and is added to each phase measurement to simulate errors. The dynamic range of the receiver is 20 dB and the receiver sensitivity is set to -93 dBm. The Equivalent Isotropically Radiated Power (EIRP) of the transmitters is 33 dBm. The parameter value d_c was determined through a series of experiments by averaging the distance between a cluster of points and is set to 100 meters. The parameter d_r is set to 100, 120, 160 and 180 metres for the noise with a standard deviation of 1.96, 3, 5 and 10 dBm respectively. Experiments are conducted 1400 times with a confidence level of 95%, as shown in Appendix A.

7.2 Performance Metrics

Our algorithms monitor the signal detected at each receiver and analyse the information to determine if the system is under attack. Once an attack is detected, the system localizes the transmitters involved. True Positive (TP) occurs when a true attack is correctly reported. False Positive (FP), also known as a false alarm, occurs when an attack is incorrectly reported. True Negative (TN) occurs when a true non-attack is correctly reported, whereas a False Negative (FN) occurs when a non-attack is incorrectly reported. The performance metrics calculated from these are: True Positive Rate (TPR), False Positive Rate (FPR), True Negative Rate (TNR) and False Negative Rate (FNR), as shown in Eqs. 7.1 -7.4.

$$TPR = \frac{\text{TP}}{\text{TP} + \text{FN}} = \frac{\#\text{correctAttacks}}{\#\text{Attacks}} \tag{7.1}$$

$$TNR = \frac{\text{TN}}{\text{TN} + \text{FP}} = \frac{\#\text{correctNon-Attacks}}{\#\text{Non-Attacks}} \tag{7.2}$$

$$FPR = \frac{\text{FP}}{\text{FP} + \text{TN}} = 1 - TNR \tag{7.3}$$

$$FNR = \frac{\text{FN}}{\text{FN} + \text{TP}} = 1 - TPR \tag{7.4}$$

A TPR of 100% means that the system identifies all actual positives whereas a TNR of 100% means that the test recognizes all actual negatives. The TPR and TNR aids us in gauging the performance of the algorithms. The FPR is the rate of non-attacks incorrectly identified as attacks, whereas the FNR is the rate of attacks incorrectly identified as non-attacks. The overall accuracy of the system is an indicator of the performance, as shown in Eq. 7.5.

$$Accuracy = \frac{\text{TP} + \text{TN}}{\text{TN} + \text{FN} + \text{TP} + \text{FP}} = \frac{\#\text{correctAttacks}+\#\text{correctNon-Attacks}}{\#\text{Attacks}+\#\text{Non-Attacks}} \tag{7.5}$$

7.3 Results for the Regular Grid Network

Table 7.1 shows the environmental noise greatly affects the rate of false negatives. All of the attacks identified by the system are true positives. The average FPR and FNR is 0% and 7.37%, respectively. Both transmitters are localized each time an attack is detected. Our algorithm detects an evil twin attack with no false positives, and the false negative rate is greatly influenced by the noise level in the environment. The system correctly identifies attacks with a TPR of 92.63%, and non-attacks with a TNR of 100%.

We delve further into evaluating the performance of the algorithm by partitioning the environment into zones. The noise level in the environment is 1.96 dBm. Figure 7.1 shows the rate of false negatives in relation to the proximity of the transmitters involved in the attack. The distance between the transmitters is measured as the number of zones apart. For example, if both transmitters are located in Zones I, the number of zones apart is 0. If the transmitters are in Zones I and IV, the number of zones apart is 1.

Table 7.1: The Rate of False Positives and Negatives in a Regular Grid Environment

Noise Level [dBm]	FPR [percent]	FNR [percent]
1.96	0	7.04
3	0	7.21
5	0	7.88
10	0	7.34
Average	0	7.37

Each time an attack is detected, it is a true positive and both transmitters are localized. The system has difficulty in detecting an attack when the transmitters are in the same zones, due to the overlapping sub-zones being consistent with one transmitter, resulting in a false negative. Therefore, a higher false negative rate is presented when the transmitters reside in the same zones than in different zones. Collectively, the system declares a non-attack and an attack with an average accuracy of 100% and 88.19% respectively, as shown in Figure 7.1.

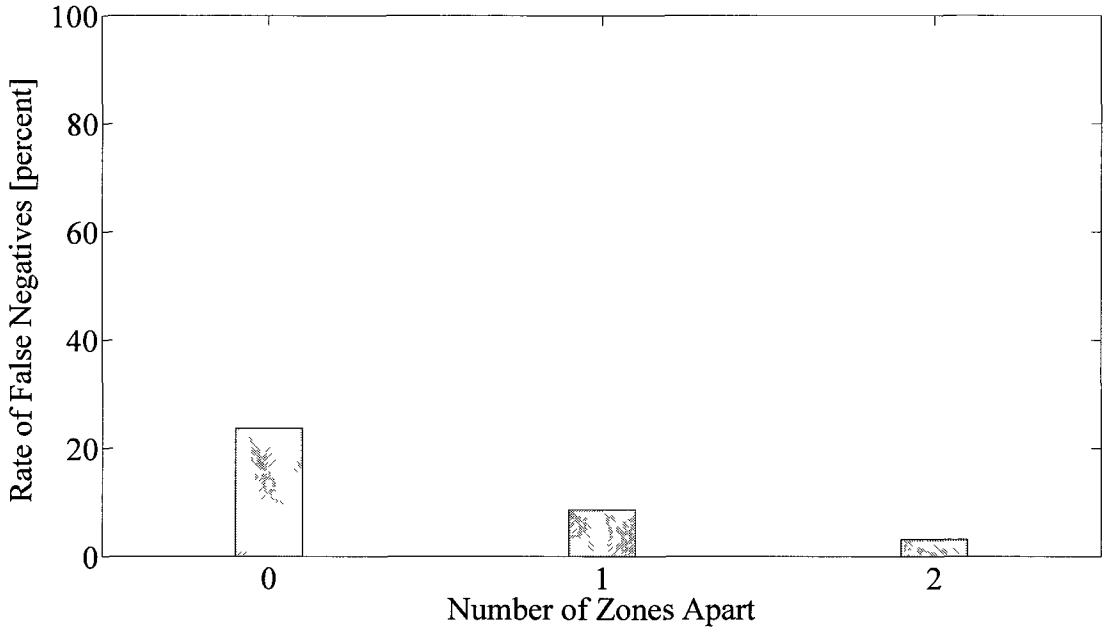


Figure 7.1: The Rate of False Negatives in a Partitioned Regular Grid Environment

7.4 Results for the Randomly Distributed Network

We simulate our algorithm described for a random-based network and measure the rate of detection in different noisy environments, and when the transmitters involved in an attack are a certain distance apart. Our algorithm performs considerably well in different noisy environments, as shown in Table 7.2. The increase of noise in the environment introduces more false positives. The rates of false positives and negatives have an average of 17.48% and 3.51% in the different environments.

We evaluate the performance of a partitioned environment for the random-based algorithm. The standard deviation of the noise in the environment is 1.96 dBm. Figure 7.2 shows the rates of false positives and negatives in relation to the proximity of the transmitters involved in the attack. When the transmitters are in different zones, there

is a high probability that the lines of intersection will yield null values, resulting in more attacks being identified. However, the rate of false positives increases because of the noise in the environment, as shown in Figure 7.2. Overall the system has low false positives and negatives, with an average of 15.64% and 5.93% respectively. Both transmitters are sucessfully localized, each time an attack is detected.

Table 7.2: The Rates of False Positives and Negatives in a Randomly Distributed Environment

Noise Level [dBm]	FPR [percent]	FNR [percent]
1.96	14.86	3.51
3	14.53	4.64
5	17.60	2.90
10	22.93	2.98
Average	17.48	3.51

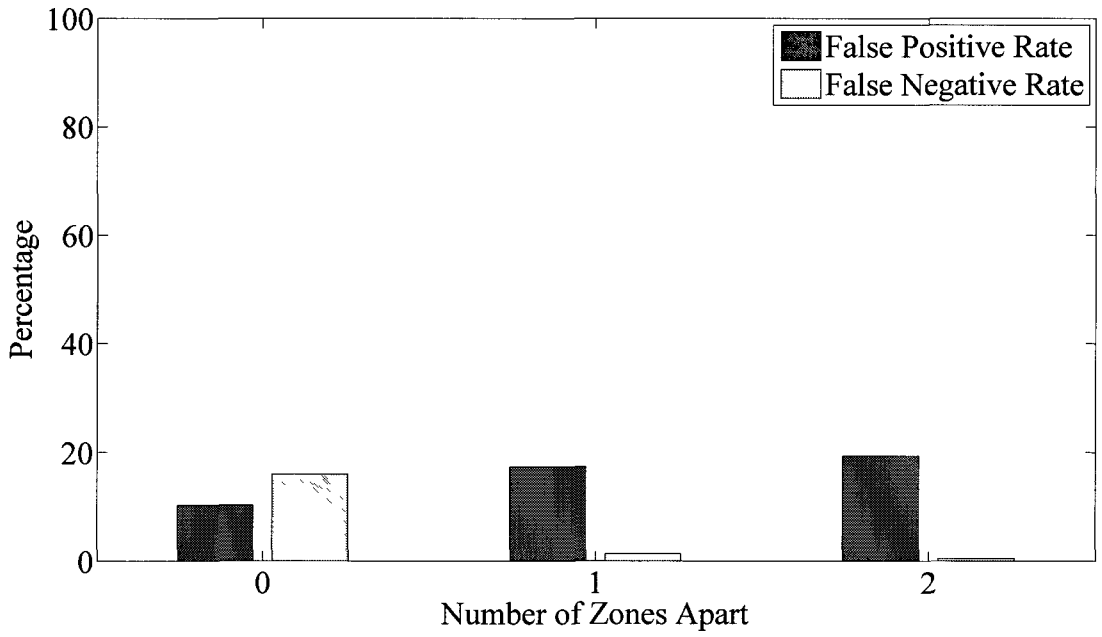


Figure 7.2: The Rates of False Negatives and False Positives in a Partitioned Randomly Distributed Environment

7.5 Comparison of the Regular Grid and the Randomly Distributed Algorithms

We compare the effectiveness of the regular and random algorithms in correctly identifying if an attack has taken place or not. Figure 7.3 compares the accuracy of the different noisy environments. Figure 7.4 shows the overall accuracy of the algorithms in relation to the proximity of the transmitters. The overall accuracy takes into account the number of true attacks and non-attacks identified by the system. The randomly distributed and regular grid systems have an average accuracy of 95% and 94.08% in the different noisy environments. In a partitioned environment, the randomly distributed and regular grid systems have an average accuracy of 94.18% and 90.73%, respectively. The randomly distributed algorithm performs better than the regular grid algorithm because it has a lower false negative rate and identifies more true attacks. In addition, the random algorithm has fewer network constraints as the receivers are randomly placed in the zones.

7.6 Performance Comparison with Another Evil Detection Scheme

In this section, the performance of our regular grid algorithm is compared to an evil twin detection scheme described by Bhatia in [38]. Bhatia proposed a regular grid algorithm and investigated the rates of true positives and false negatives in relation to the proximity of the transmitters involved in the attack [38]. The algorithm has a true positive and false negative rates of 53% and 47% respectively, when transmitters are in the same zone. When the transmitters are in different zones, the true positive rate is 100%. In our regular grid algorithm, the rates of true positives and false negatives are 76% and 24% respectively,

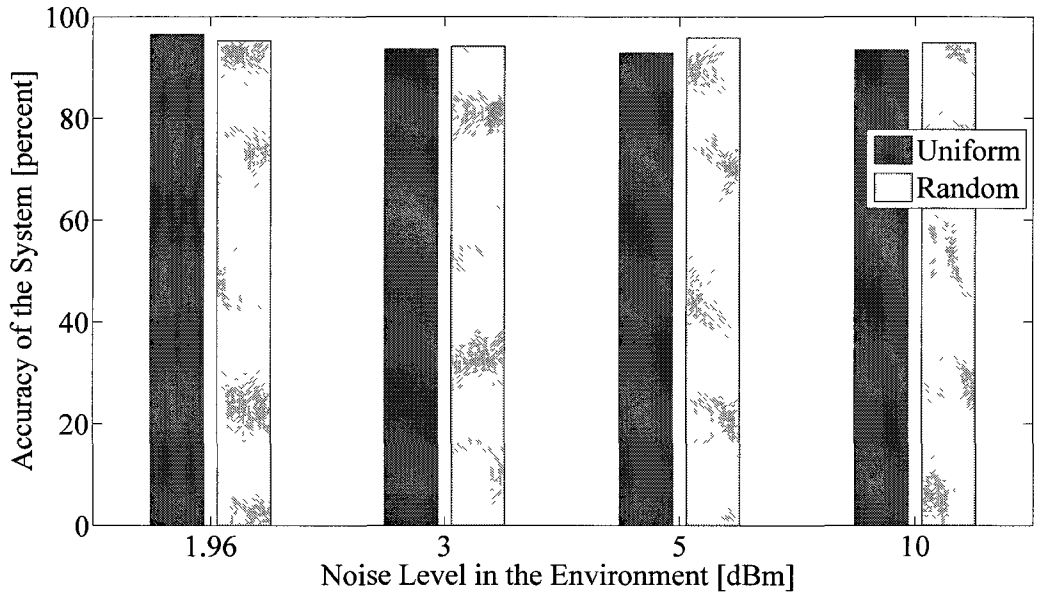


Figure 7.3: The Accuracy of the Regular Grid and Random Distributed Algorithms in Different Noisy Environments

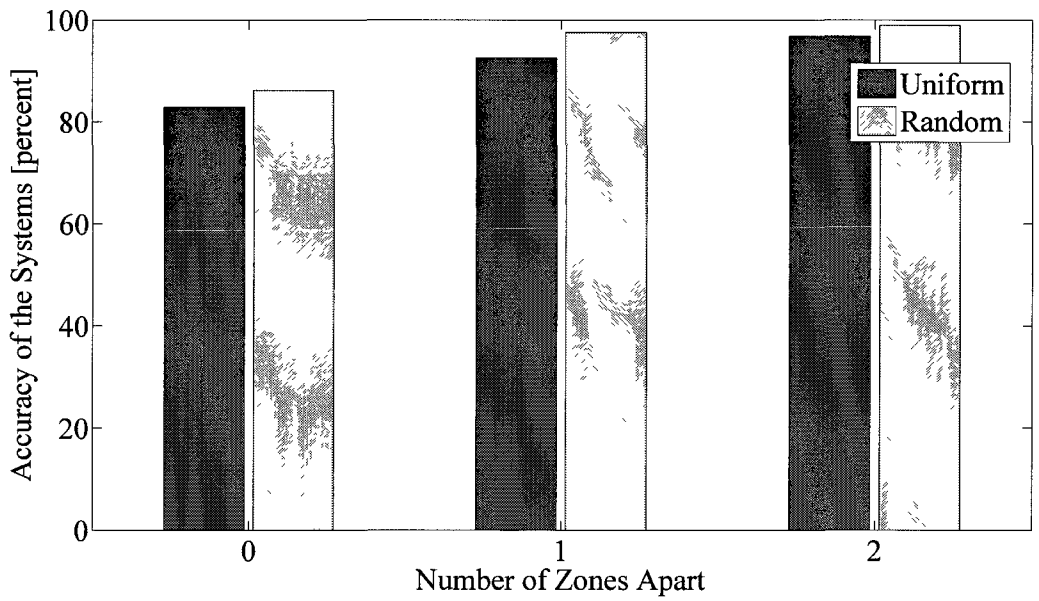


Figure 7.4: The Accuracy of the Regular Grid and Randomly Distributed Algorithms in Relation to the Proximity of the Transmitters

when transmitters are in the same zones. In different zones, the rate of true positives is 94%.

In the evil twin detection scheme proposed by Bhatia, both transmitters are localized 74% of the time [38]. Once an evil twin attack has been declared in our algorithms, both transmitters are localized 100% of the time. Our algorithm exhibits better performance overall than Bhatia [38]; however, our simulation utilizes more receivers. In addition to our regular grid algorithm, we proposed a randomly distributed algorthm where the receivers are randomly placed in the environment, thereby reducing restrictions on the placement of the receivers. We are unable to compare the performance of the randomly distributed algorithm with the algorithm proposed by [38] as the structure of the network differs.

7.7 Summary

In this chapter, we evaluated the performance of our algorithms to detect the evil twin attack. In the regular grid algorithm, the receivers must be placed in a rigid, defined structure which may be disadvantageous in some cases. In the randomly distributed algorithm, the receivers are placed randomly within the environment. Overall, the systems performed well and achieved a low false positive and negative rate. The randomly distributed and regular grid systems have an average accuracy of 95% and 94.08% in the different noisy environments. In a partitioned environment, the randomly distributed and regular grid systems have an average accuracy of 94.18% and 90.73%, respectively.

Chapter 8

Conclusion and Future Work

We described two algorithms using four-square antennas at the receivers, which can be implemented in different network structures. The detection schemes can be used in the most common deployment scenarios, such as a randomly distributed or a regular grid networking environment. In the regular grid networking environment, the receivers are perfectly aligned in in a rigid, defined structure, whereas in the randomly distributed environment the receivers are placed randomly. We introduce the evil twin attack mechanisms with minimal assumptions about the EIRP of the transmitters and their cooperativeness. Once an attack is detected, we evaluate the direction of each signal received to probalistically locate the position of an attacker.

The localization techniques using one and multiple four-square antennas are presented in Chapter 5. We evaluated the location error for the methods proposed and their trade-offs. Our evil twin attack detection schemes are described in Chapter 6 and proposed for the two common deployment scenarios in a networking environment. The performance of the algorithms are evaluated in Chapter 7. Section 8.1 summarizes the work presented and highlights our contributions. We also provide recommendations for future work in Section 8.2.

8.1 Contributions

We approached the threat of the evil twin attack by implementing two algorithms for different network scenarios. We made no assumptions about the nature of the transmitters, which may be involved in a coordinated or uncoordinated attack to gain access to network. Each receiver experiences a random amount of noise and signal shadowing, making our simulation a realistic model of the real world scenario. The receivers have no prior knowledge of the transmitting power of the transmitters.

In the regular grid system, we declare an attack when there is conflicting information about the location of the transmitters. In the random-based system, we define two test scenarios to detect an attack: if the set of intersection points have any null values and secondly, if the range of the intersection points exceed a certain distance. Once an attack is declared, the systems localize the transmitters using the proposed localization schemes for a four-square antenna described in Chapter 5. The proposed localization schemes can locate a transmitter with one or multiple receivers using the phase differences of the signal received. The detection and localization schemes can be used independently of each other and is able to detect multiple evil twin attacks at a time.

Our attack detection schemes achieve a high detection rate while maintaining a low false positive and negative rates. The randomly distributed and regular grid systems have an average accuracy of 95% and 94.08% in the different noisy environments. In a partitioned environment, the randomly distributed and regular grid systems have an average accuracy of 94.18% and 90.73%, respectively.

8.2 Future Work

In our work, we made an assumption about the directional pattern of the transmitters while tackling the evil twin attack. We assume the transmitters involved are omni-directional antennas. Omni-directional antenna radiates or receives power equally in one plane. Directional antennas radiates or receives power in a certain direction. Our algorithm may be applicable to directional transmitters as it does not rely on the RSS to determine the position of the transmitter. Only if the RSS value is beyond the sensitivity level, there is interference or the signals are within the dynamic range of the receiver, it is not registered at the receiver. However, the directionality of the transmitter affects the rate of detection in the algorithms proposed.

An area of promising research is to determine the performance of our algorithms in a multi-hop system. We assumed a single hop communication where the transmitters sent data directly to the receivers. In a multi-hop communication system, the transmitters are able to send data to the receivers using other transmitters.

Another improvement to our algorithms, is the ability to identify which transmitter(s) are involved in the evil twin attack. When the transmitters are in close proximity, the rate of detection decreases. It is highly unlikely in a coordinated attack, that transmitters will be placed close to each other; however, our algorithms needs to be able to handle this case effectively.

8.3 Summary

In this chapter, we discuss our contributions and highlight possible extensions to our work. The algorithms for the regular grid and the randomly distributed network scenario are presented and both algorithms exhibit good performance while detecting the evil twin

transmitter attack. The randomly distributed algorithm performs better than the regular grid algorithm because it has a lower false negative rate and identifies more true attacks. In addition, the random algorithm has fewer network constraints as the receivers are randomly placed in the zones.

Bibliography

[1] J. Douceur. The Sybil Attack. In *Peer-to-Peer Systems: Proceedings of the First International Workshop (IPTPS)*, volume 2429, pages 251–260. Springer Berlin / Heidelberg, 2002.

[2] L. Hu and D. Evans. Using Directional Antennas to Prevent Wormhole Attacks. In *Network and Distributed System Security Symposium, NDSS 2004. The Internet Society.*, pages 131–141, 2004.

[3] A. Orebaugh, G. Ramirez, J. Burke, L. Pesce, J. Wright, and G. Morris. *Wireshark and Ethereal Network Protocol Analyzer Toolkit.* Syngress Publishing, 4th edition, Feb. 2007.

[4] A. Nicholson, B. Noble, Y. Chawathe, D. Wetherall, and M. Chen. Improved Access Point Selection. In *In MobiSys*, pages 233–245, 2006.

[5] RSA. The Wireless Security Survey of London. Tech. Rep DEC-TR-506, The Security Division of EMC, Oct 2008.

[6] M. Barbeau. Assessment of the True Risks to the Protection of Confidential Information in the Wireless Home and Office environment. In *Proceedings of the 2010 IEEE International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, WOWMOM '10, pages 1–6, Washington, DC, USA, 2010. IEEE Computer Society.

[7] Y. Song, C. Yang, and G. Gu. Who is Peeping at Your Passwords at Starbucks? To Catch an Evil Twin Access Point. In *Dependable Systems and Networks (DSN), 2010 IEEE/IFIP International Conference on*, pages 323–332, June 2010.

[8] M. Barbeau. Beware the Rogue Access Points and Web Traffic Hijacking, Feb 2011. http://ve3emb.wordpress.com/2011/02/15/beware-the-rogue-access-points-and-web-traffic-hijacking/.

[9] AirDefense. Wi-Phishing and Evil Twins at Hotspots- How to secure your mobile workforce. *IEEE Transactions on Antennas and Propagation*, pages 1–7, 2007.

[10] Kismet. http://www.kismetwireless.net/.

[11] C. Laurendeau. *Location Tracking Mitigation for Honest Nodes and Location Estimation for Honest Nodes and Location Estimation for Unccoperative Nodes in Wireless Mobile Networks.* PhD thesis, Carleton University, 2009.

[12] C. Yang, S. Bagchi, and W.J. Chappell. Location Tracking with Directional Antennas in Wireless Sensor Networks. In *Microwave Symposium Digest, 2005 IEEE MTT-S International*, page 4 pp., Dec 2005.

[13] D. Niculescu and B. Nath. Ad hoc Positioning System (APS) using AOA. In *INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies*, volume 3, pages 1734 – 1743, 30 2003.

[14] N. Malhotra, M. Krasniewski, C. Yang, S. Bagchi, and W. Chappel. Location Estimation in Ad-Hoc Networks with Directional Antennas. In *Distributed Computing Systems, 2005. ICDCS 2005. Proceedings. 25th IEEE International Conference on*, pages 633 –642, 10-10 2005.

[15] J. Hightower and G. Borriello. Location Sensing Techniques. Technical Report UW-CSE-01-07-01, University of Washington, Computer Science and Engineering, July 2001.

[16] M. Barbeau, E. Kranakis, D. Krizanc, and P. Morin. Improving Distance Based Geographic Location. In *Proceedings of the 3rd International Conference on AD-HOC Networks and Wireless (ADHOC-NOW'04)*, pages 22–24. Springer Verlag, 2004.

[17] K. Solbach and S. Angenendt. Four-Square Phased Array for Multi-Beam Applications using Novel Matrix Feed. In *Radar Conference, 2007. EuRAD 2007. European*, pages 358 –361, Oct 2007.

[18] D. Parkhurst. *Introduction to Applied Mathematics for Environmental Science.* Springer, 1st edition, 2006.

[19] B. Mahafza. *Radar Systems Analysis and Design using Matlab*, chapter 11. Chapman and Hall, 1st edition, 2000.

[20] C. Hekimian-Williams, B. Grant, X. Liu, Z. Zhang, and P. Kumar. Accurate Localization of RFID tags using Phase Difference. In *RFID, 2010 IEEE International Conference on*, pages 89 –96, April 2010.

[21] J. Yang, Y. Chen, W. Trappe, and J. Cheng. Determining the Number of Attackers and Localizing Multiple Adversaries in Wireless Spoofing Attacks. In *INFOCOM 2009, IEEE*, pages 666 –674, 19-25 2009.

[22] C. Laurendeau and M. Barbeau. Hyperbolic Location Estimation of Malicious Nodes in Mobile wifi/802.11 Networks. In *Local Computer Networks, 2008. LCN 2008. 33rd IEEE Conference on*, pages 600 –607, 14-17 2008.

[23] N. Sastry, U. Shankar, and D. Wagner. Secure Verification of Location Claims. In *2nd ACM Workshop on Wireless Security (WiSe)*, pages 1–10, 2003.

[24] H. Friis. A Note on a Simple Transmission Formula. In *Proceedings of the IRE*, volume 34, pages 254–256, May 1946.

[25] J. Liberti and T. Rapport. *Smart Antennas for Wireless Communications: IS-95 and Third Generation CDMA Applications.* Prentice Hall, 1999.

[26] T. Rapport. *Wireless Communications Principles and Practice.* Prentice Hall, 2nd edition, 2001.

[27] I. Schneider, F. Lambrecht, and A. Baier. Enhancement of the Okumura-Hata Propagation Model using Detailed Morphological and Building Data. In *Personal, Indoor and Mobile Radio Communications, 1996. PIMRC'96., Seventh IEEE International Symposium on*, volume 1, pages 34 –38, 1996.

[28] A. Kuntz, F. Schmidt-Eisenlohr, O. Graute, H. Hartenstein, and M. Zitterbart. Introducing Probabilistic Radio Propagation Models in OMNeT++ Mobility Framework and Cross Validation Check with NS-2. In *Proceedings of the Simutools '08*, pages 1–7, March 2008.

[29] S. Suh, W.L. Stutzman, and W.A. Davis. Low-profile, Dual-polarized Broadband Antennas. In *Antennas and Propagation Society International Symposium, 2003. IEEE*, volume 2, pages 256 – 259, June 2003.

[30] American Radio Relay League. *The ARRL Antenna Book: The Ultimate Reference for Amateur Radio Antennas, Transmission Lines and Propagation.* CRC Series: Modern Mechanics and Mathematics. ARRL, 21st edition, 2007.

[31] J. Devoldere. *ON4UN's Low Band DXing.* ARRL, 4th edition, 2005.

[32] C. Buxton. *Design of a Broadband Array Using the Foursquare Radiating Element.* PhD thesis, Virginia Polytechnic Institute and State University, 12 June 2001.

[33] G. Giorgetti, S. Maddio, A. Cidronali, S.K.S. Gupta, and G. Manes. Switched Beam Aantenna Design Principles for Angle of Arrival Estimation. In *Wireless Technology Conference, 2009. EuWIT 2009. European*, pages 5–8, Sept 2009.

[34] N. Kuga and H. Arai. A Flat Four-Beam Switched Array Antenna. *Antennas and Propagation, IEEE Transactions on*, 44(9):1227 –1230, Sep 1996.

[35] A. Christman. A Four Square with Eight directions of Fire. *National Contest Journal*, pages 1–4, March/April 2004.

[36] W. Xiao, Y. Sun, Y. Liu, and Q. Yang. TEA: Transmission Error Approximation for distance estimation between two Zigbee devices. In *Networking, Architecture, and Storages, 2006. IWNAS '06. International Workshop on*, page 8 pp., 2006.

[37] C. Laurendeau and M. Barbeau. Insider Attack Attribution using Signal Strength-based Hyperbolic Location Estimation. *Security and Communication Networks*, 1(4):337–349, 2008.

[38] P. Bhatia. Strategy for Detection and Localization of Evil-Twin Transmitters in Wireless Network. Master's thesis, Carleton University, June 2010.

[39] L. Ma, A. Teymorian, and X. Cheng. Rap: Protecting Commodity Wi-Fi Networks from Rogue Access Points. In *Qshine*, pages 1–7, 2007.

[40] J. Hall, M. Barbeau, and E. Kranakis. Enhancing Intrusion Detection in Wireless Networks using Radio Frequency Fingerprinting. In *In Proceedings of the 3rd IASTED International Conference on Communications, Internet and Information Technology (CIIT*, pages 201–206, 2004.

[41] E. Cardenas. MAC Spoofing - An introduction. pages 11–13, August 2003.

[42] Airmagnet. http://airmagnet.com/.

[43] Netstumbler. http://www.netstumbler.com.

[44] Inssider. http://www.metageek.net/products/inssider/.

[45] J.K. Nelson, M.U. Hazen, and M.R. Gupta. Global Optimization for Multiple Transmitter Localization. In *Military Communications Conference, 2006. MILCOM 2006. IEEE*, pages 1 –7, 23-25 2006.

[46] S. Shetty, M. Song, and L. Ma. Rogue Access Point Detection by Analyzing Network Traffic Characteristics. In *Military Communications Conference, 2007. MILCOM 2007. IEEE*, pages 1 –7, 29-31 2007.

[47] H. Han, B. Sheng, Q. Li C.C Tan, and S. Lu. A Measurement Based Rogue AP Detection Scheme. In *INFOCOM 2009, IEEE*, pages 1593 –1601, 19-25 2009.

[48] P. Kulakowski, J. Vales-Alonso, E. Egea-López, W. Ludwin, and J. García-Haro. Technical Communication: Angle-of-arrival Localization based on Antenna Arrays for Wireless Sensor Networks. *Comput. Electr. Eng.*, 36:1181–1186, November 2010.

[49] L. C. Liechty. Path Loss Measurements and Model Analysis of a 2.4 GHz Wireless Network in an Outdoor Environment. Master's thesis, Georgia Institute of Technology, 2007.

[50] T. A. Williams D. R. Anderson, D. J. Sweeney. *Statistics for Business and Economics.* South-Western College, 10th edition, 2008.

Appendix A

A.1 Sample Size

We must determine how large the sample size should be to obtain results which reflect the population for a given level of accuracy. The sample size n is calculated using the following equation:

$$n = \frac{Z^2 * \text{p} * (1\text{-p})}{c^2} \tag{A.1}$$

where Z is the critical value of a specific confidence level, p is the proportion of the population making a choice and c is the confidence interval or the margin of error. The confidence level represents how true the percentage of a population lies with in the confidence interval [50].