STRATEGY FOR DETECTION AND LOCALIZATION OF EVIL-TWIN TRANSMITTERS IN WIRELESS NETWORKS

by

Payal Bhatia

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
May, 2010

Your file Votre référence
ISBN: 978-0-494-68631-7
Our file Notre référence
ISBN: 978-0-494-68631-7

To my father, Vijay Bhatia and mother, Veena Bhatia

Abstract

The boost in the use of wireless networks in our day-to-day world is phenomenal. Users need to have a confidence in communicating securely over the wireless medium. They want to be able to trust in the genuineness of a transmitting node. In this work, we examine an attack, called the evil-twin transmitter attack. In a wireless network comprising some receivers and a truth-teller transmitter, an attacker adds a malicious evil-twin transmitter to the network such that the evil-twin lies about its true identity and transmits like the truth-teller transmitter in the network. The truth-teller transmitter may be a malicious transmitter as well, but it is honest in that it doesn't lie about its identity. The evil-twin uses the identity of the truth teller and transmits at the same time as the truth-teller. The receivers are bound to get confused about the location of the honest transmitter.

We have described an algorithm to detect the wireless evil-twin transmitter attack as well as to localize the two transmitters. Our contributions with this work are:

1. We have simulated the use of directional antennas for determining whether a wireless network is under an evil-twin transmitter attack. The algorithm for detecting an evil-twin transmitter attack can be used independently, as well as in conjunction with a localization technique, depending on the problem scenario.

2. The previously devised Hyperbolic Position Bounding (HPB) mechanism is used to localize the two transmitters. We have also provided an alternative mechanism to localize the transmitter in case HPB fails to localize the transmitter.

The performance of the algorithm is tested using a simulation of a wireless network, the results of which are consistent over various scenarios. Directions for future work include determining which of the two transmitters is the truth-teller and the evil-twin.

Acknowledgements

I owe my deepest gratitude to my supervisors Prof. Michel Barbeau, and Dr. Christine Laurendeau, for their continuous support for the duration of my M.C.S. study. This work would not have been possible without them. Their encouragement was ever valuable to me and brought out the best in me. Their constructive feedback and extremely detailed comments not only made this thesis what it is presently, it also taught me the importance of attention to details.

I am very grateful to my parents, who have always trusted in my capabilities and have supported me through thick and thin. Their unconditional love always motivated me and kept me going. I would also like to thank my sister, Sonam and brother, Akash for making me feel positive when I was stressed, and for their cheering pranks. Sincere gratitude is also due to my dear friends in Ottawa - Mahesh, Naveen, Rujuta, Manya and Ranjit, who have been like family, and have guided me through a multitude of predicaments, ranging from technical to personal. Many thanks to my lab-mates Paul Boone, Oscar Ponce and Gimer Cervera for the much needed conversation breaks in between working, as well as for answering any questions I ever had.

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

Table of Contents

List of Figures

List of Acronyms

ACK Acknowledgement

AP Access Point

BS Base Station

CPP Central Processing Point

EIRP Effective Isotropic Radiated Power

GPS Global Positioning System

HPB Hyperbolic Position Bounding

ID Identity

LAN Local Area Network

MAC Medium Access Control

OBU On-Board Unit

RF Radio Frequency

RSS Received Signal Strength

SSID Service Set Identifier

TCP Transmission Control Protocol

TDOA Time Difference of Arrival

TOA Time of Arrival

WLAN Wireless Local Area Network

Chapter 1

Introduction

Security is an important aspect in wireless networks as they are becoming increasingly popular in our day-to-day world. With the advent of new technologies, their security also gets challenged everyday. Attackers devise new ways of disrupting networks and services as per their requirements. We need to ensure that parties involved in a communication transaction wirelessly are communicating securely. There are five key components of security: confidentiality, that is, the message remains secret to everyone except the communicating parties, integrity, that is, the message has not been tampered with, authentication, that is, the sender can be verified, non-repudiation, that is, the sender cannot deny having sent the message, and access control, that is, only an authorized recipient can read the message.

In this work, we examine an attack in wireless networks called the evil-twin transmitter attack. The attack model assumes a wireless network with few receivers and a truth-teller transmitter that does not lie about its identity. Another transmitter, called the evil-twin transmitter, is able to access the wireless network, and it sends messages in the network simultaneously with the truth-teller transmitter, in addition to using the identity of the truth-teller. The transmitters can be attackers, malicious insiders or malfunctioning nodes in the network. We do not assume any cooperation from the transmitting devices. The presence of the evil-twin in the network violates the security principles of authentication and non-repudiation, as its identity is the same as the truth-teller transmitter. We propose a solution for determining whether the wireless network is infiltrated by an evil-twin transmitter, and thereafter, determine the position of the truth-teller transmitter and its evil-twin in the network.

1.1 Motivation and Problem Statement

This work is inspired from the work done by Laurendeau and Barbeau in [20]. The Hyperbolic Position Bounding (HPB) mechanism was developed by them to localize a

malicious or malfunctioning transmitter in a wireless network, without assuming any co-operation from the transmitter. However, the HPB mechanism does not handle the scenario where there is another transmitter in the network transmitting at the same time and with the same ID as the legitimate transmitter. This could happen because all the receivers may not get the transmitted signals due to interference. Also, the receivers do not have a way of determining that the Received Signal Strength (RSS) values they get are from the same or different transmitter, thereby possibly causing incorrect results from HPB.

The evil-twin transmitter attack is a general form of the evil-twin Access Point (AP) attack. The evil-twin AP attack is increasingly common in Wi-Fi hotspots, and exploits common automatic access point selection techniques to trick a wireless client into associating with the malicious access point [4]. Be it evil-twins of access points or transmitters, or even persons in general, evil-twins have the potential to cause enormous harm to the item they are impersonating, as well as to the environment they are in. In a wireless network, the evil-twins can confuse the receivers about the actual location of truth-teller transmitters. If the evil-twins transmit malicious packets to the receivers using the identity of the truth-teller transmitter, they can also leave the receivers wondering whether to trust the truth-teller transmitter or not. The evil-twin transmitters can particularly be dangerous in a vehicular networks scenario, where they can cause accidents or impede traffic by broadcasting wrong traffic updates to the On-Board Units (OBUs). In a sensor network, an evil-twin could be gathering and sending corrupt or useless data, all with the ID of a sensor that has authorized access to the network.

The evil-twin can benefit from the inability of receivers in the network to correctly localize the truth-teller transmitter in its presence. For instance, if a sensor is malfunctioning in a sensor network and requires assistance, a localization algorithm could help in determining the position of the sensor. However, the presence of an evil-twin in the network can simply cause the localization algorithm to work erroneously. Emergency assistance to a cell phone user could never reach her if an evil-twin was functioning alongside and dismisses the need for assistance. The honest transmitter and the evil-twin could also be nodes cooperating with each other to disrupt the network.

1.2 Assumptions

The scenarios described in Section 1.1 help in identifying the need for detecting the presence of an evil-twin transmitter attack in a wireless network. We cannot assume any cooperation from a transmitting device, as the device may be incapable of cooperation or may be malicious in nature, therefore, will provide incorrect information regarding its whereabouts. Due to the presence of an evil-twin transmitter in the network, we also need to localize the truth-teller transmitter as well as its evil-twin. It must be noted that the truth-teller transmitter is honest only in that it doesn't lie about its identity. No assumptions are made in our attack model about the honest transmitter being uncorrupt. It is a possible scenario that the truth-teller transmitter and rogue transmitter are coordinating the evil-twin attack. Our attack model also assumes an outdoor environment. The receivers are authorized and trusted in the wireless network to which they belong. The receivers in the network have globally known position coordinates. Each receiver is equipped with a directional aerial called the four-square antenna. The receivers in the network are pre-configured to have the same orientation for their antenna, such that the antennas are aligned with each other. The wireless network has deployed some form of security mechanism so that the communications in the network are secure.

1.3 Summary of Contributions

Our contributions with this work are in the areas of detecting an evil-twin transmitter attack and localizing the transmitters in the network, while assuming no cooperation from the transmitters.

1. We have described the evil-twin transmitter attack, which can be extended to specific types of wireless networks including, but not limited to, Wi-Fi networks and vehicular networks. The evil-twin transmitter transmits messages using the truth-teller transmitter's ID, and at the same time as the truth-teller transmitter. We have simulated the use of directional antennas for determining whether a wireless network is under an evil-twin transmitter attack. The simulation area is divided into n equal-sized *zones*, and an algorithm calculates two potential zones that will most likely contain the transmitters. The algorithm for detecting an evil-twin transmitter attack

can be used independently, as well as in conjunction with a localization technique, depending on the problem scenario.

2. After a successful determination of an attack, we divide the RSS values received at the receivers into two pools and use the Hyperbolic Position Bounding (HPB) mechanism on each pool of RSS values to localize the two transmitters in the wireless network. An attempt was made to further improve the results of the localization mechanism. The area given by the HPB mechanism as the candidate area for a transmitter is intersected with the area of the potential zone to reduce the candidate area for localizing the transmitter. The outcome of the intersection is a candidate area that can range anywhere from 4% to 11% of the simulation area. If HPB fails to yield a candidate area for a transmitter, we use the area of the potential zone as the candidate area for that transmitter. This mechanism is termed the fallback mechanism.

We evaluate our algorithm for detecting the evil-twin transmitter attack and localizing the transmitters in a simulated environment, which replicates a real-world wireless network scenario. Our results over different scenarios are consistent, and provide confidence in the findings of our research.

1.4 Organization of Thesis

Chapter 2 reviews some information on the radio propagation models, workings of four-square antennas and the concepts of Hyperbolic Position Bounding (HPB), all of which are used to assist in solving our problem. Chapter 3 of the thesis gives an overview of the various attacks involving multiple transmitters in a wireless network setting, related work in localization techniques and the detection of uncooperative nodes and multiple transmitters. Chapter 4 introduces the problem and describes in detail our approach to detect an evil-twin transmitter attack. Chapter 5 provides an insight into the localization techniques we use to localize the transmitters in case an evil-twin transmitter attack is reported. Chapter 6 describes the metrics used to evaluate the performance of our algorithm and details the results obtained for the algorithm against those metrics in a simulated environment. Chapter 7 concludes the thesis and provides some directions for future work.

Chapter 2

Background

In this chapter we introduce the concepts that are used in our work. We outline some radio propagation models. We also describe the working of HPB and the Log-Normal Shadowing model, which are used by our algorithm to localize transmitters. We also describe the working of the four-square antenna, which is used by the receivers in the network to detect an attack.

2.1 Radio Propagation Models

Radio Frequency signals suffer a loss, called path loss, as they propagate through various media. When a signal passes through large obstacles, such as buildings and trees, large scale fading occurs. Since our work is on wireless networks, we will be considering the large scale path loss. Different models have been proposed for estimating the large scale path loss in an outdoor environment, probablistic and deterministic. The Okumura model predicts path loss based on transmitter and receiver antenna heights [29], but this is unsuitable for use for complex terrains [26]. The Okumura-Hata model [13] was established for urban areas, but was shown to work only within the frequency range of 150 - 1500 MHz. The Nakagami model [28] depends on the two parameters - the mean received power, and a fading parameter, both obtained through experiments for a known transmitter-receiver distance. Since the distance is unknown in our scenario, the values of the two parameters cannot be determined. The log-normal shadowing model [33] is simple, and used to estimate the distance between each receiver and the transmitter. This model is used by Hyperbolic Position Bounding (HPB), which is one of the tools our algorithm uses to estimate the transmitters' location. Section 2.2 describes the HPB and Section 2.2.1 describes the log-normal shadowing model, as used in HPB.

2.2 Hyperbolic Position Bounding

Hyperbolic Position Bounding (HPB), described by Laurendeau and Barbeau in [20], is a mechanism to compute a probable candidate area in which a transmitter may lie in Euclidian space. The algorithm doesn't assume any information about the transmitters except that they have an omni-directional antenna. Each receiver in the network is trusted and its location is known to other receivers. Each receiver is equipped with an omni-directional antenna and uses the Received Signal Strength (RSS) value to localize the transmitters. Using HPB for localization has a benefit over a lot of other localization algorithms in that it does not assume anything about the Effective Isotropic Radiated Power (EIRP) of the transmitters. The HPB algorithm uses a probabilistic path loss model and computes the maximum and minimum hyperbolas between all transmitter-receiver pairs. It is assumed that the transmitter lies in the area bounded by the intersection of all the hyperbola pairs, with a given confidence level. Section 2.2.1 describes the log-normal shadowing model used by HPB and Section 2.2.2 discusses in brief how HPB does location estimation.

2.2.1 Log-Normal Shadowing Model

The log-normal shadowing model allows for the calculation of the amount of path loss that a signal suffers over a known transmitter-receiver distance [33]. Rappaport's log-normal shadowing model predicts the amount of path loss at a given transmitter-receiver distance, based on a reference distance d_0 close to the transmitter, an average path loss $\overline{L}(d_0)$ at d_0 assuming free space propagation [11], a path loss exponent η depending on the propagation environment, and a random amount of signal shadowing X_σ with mean zero and standard deviation σ. Values for η and σ can be measured through experiments [9,22]. The following formula is used to calculate the path loss $L(d)$ (in dB):

$$L(d) = \overline{L}(d_0) + 10\eta log_{10}\frac{d}{d_0} + X_\sigma \tag{2.1}$$

2.2.2 Location Estimation

The minimum and maximum distances from a transmitter to a receiver are calculated using the log-normal shadowing model in [3, 24, 25] to construct an annulus around the

receiver, where the transmitter may be present. In contrast, HPB uses the relative distance difference between a pair of receivers and a transmitter, like the TDOA technique. Hyperbolas have the property that every point on the curve is at the same distance difference of the two foci. The minimum and maximum distance equations for an estimated range of EIRP values is proven in [19] to be:

$$d_k^- = d_0 \times 10^{\frac{\mathcal{P}^- - RSS_k - \overline{L}(d_0) - z\sigma}{10\eta}} \tag{2.2}$$

$$d_k^+ = d_0 \times 10^{\frac{\mathcal{P}^+ - RSS_k - \overline{L}(d_0) + z\sigma}{10\eta}} \tag{2.3}$$

Equations 2.2 and 2.3 calculate the minimum and maximum distances d_k^- and d_k^+ respectively, between the transmitter T and receiver R_k using the estimated EIRP interval $[\mathcal{P}^-, \mathcal{P}^+]$. There also exists a relationship between the path loss $L(d)$ and the EIRP and the RSS at a receiver R_k, as shown in Equation 2.4:

$$L(d) = EIRP - RSS_k \tag{2.4}$$

The minimum and maximum distance equations are derived directly from Equations 2.1 and 2.4.

If the difference in distance of a transmitter T to two receivers R_1 and R_2 is known, a hyperbola $H_{1,2}$ can be plotted, each point of which would be equidistant between R_1 and R_2. Since the HPB assumes no knowledge of the EIRP of the transmitter, it is not possible to calculate the exact distance difference, nor the exact hyperbola between a pair of receivers. Thus, HPB defines a candidate area bounded by two hyperbolas between each pair of receivers, such that one hyperbola is at the mimimum bound and the other is at the maximum bound of the distance difference range. The two hyperbolas $H_{1,2}^-$ and $H_{1,2}^+$ are defined such that $H_{1,2}^-$ is the minimum hyperbola and $H_{1,2}^+$ is the maximum hyperbola. The intersection of all the candidate areas determined in the previous step, computed by all receiver pairs, gives a relatively smaller area in which the transmitter is most likely located.

Figure 2.1 shows how HPB localizes a transmitter. The candidate area given by HPB in Figure 2.1 is about 11% of the simulation grid. The receivers R_1, R_2, R_3 and R_4 all compute their minimum and maximum distance differences with each other, forming minimum and maximum distance hyperbolas. The intersection of the hyperbolic area gives the candidate area for the location of the transmitter.

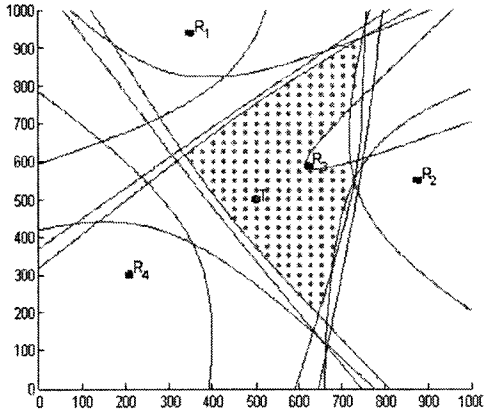

Figure 2.1: HPB with one transmitter.

We use HPB as part of our strategy to localize individual transmitters in the event of an evil twin attack.

2.3 Four-Square Antenna

An antenna converts electric currents and voltages into electromagnetic waves at the transmitter's end and vice versa at the receiver's end. Antennas can be categorized into two categories - omni-directional antennas and directional antennas. Omni-directional antennas receive and radiate equally well in all directions. The directional antennas, on the other hand, are the antennas which transmit and receive more power in one or several directions. The simplest and most common antenna is the dipole, showed in Figure 2.2. The electromagnetic waves get weaker as they travel through space due to the path loss. Engineers have tried to come up with ways such that interference can be reduced in antennas. For example, placing two antennas side by side at a distance of half the wavelength of the radio signal produces a fairly broad radiation pattern of the shape of the figure eight. This is called a two-antenna array. More types of radiation patterns, including narrower beam width, and elongated radiation patterns, can be achieved by adding more elements to an antenna array. Phased-array antennas are types of directional antennas and have been used to focus radar beams since the World War II [8].

A directional antenna has a direction of maximum radiation or reception. It focuses its

RF energy in that direction and improves the antenna's performance and also provides the benefit of discriminating against interference [21]. This increase in the signal strength in the direction of maximum radiation is termed the gain of the antenna. The radiation pattern of an antenna is the measure of the angular dependence of the radiated or received power. The omni-directional antennas have a circular radiation pattern pertaining to the fact that equal energy is distributed in all directions, whereas the directional antennas have a pattern determined by the gain at each angle. There are numerous kinds of directional antennas, all producing different types of radiation patterns. Depending on the need of the problem that one is trying to address, the antenna needs would be different. A few types of directional antennas are dipole antenna, loop antenna, Yagi antenna and four-square antenna. To illustrate the differences between the various radiation patterns available, Figures 2.2 and 2.4 show the physical structures, and Figures 2.3 and 2.5 show the radiation pattern of the dipole and loop antennas respectively.

For our work, a phased-array antenna (or directional antenna) called the four-square antenna is used [32]. Figure 2.6 shows the physical structure of the four-square antenna. Also, it is possible to see from the radiation pattern (Figure 2.7) that each antenna element is focusing its energy in one main direction. The antenna has four different elements, each an antenna in itself. Figure 2.7 shows the radiation pattern for one element of the four-square antenna [21]. Figure 2.8 shows the radiation pattern of the four-square antenna when the radiation pattern of each individual element is combined together. When the four-square antenna receives a signal, each of the elements registers the RSS value it gets. Since the angle of arrival of the signal is different for each of the elements, the gain at each element is different. The maximum RSS value is registered as the RSS value of the four-square antenna. The four different elements in the antenna can help determine the direction of the incoming signal and the direction of maximum gain is registered as the direction of the incoming signal for the four-square antenna. Our goals are to be able to get a signal from as far as possible and to be able to determine its direction, both of which can be achieved with a four-square antenna.

All the receivers in our work are equipped with a four-square antenna. An omni-directional antenna would give us the RSS value. The benefit of using a four-square antenna is that in addition to the RSS value registered at each of the receivers, we now are

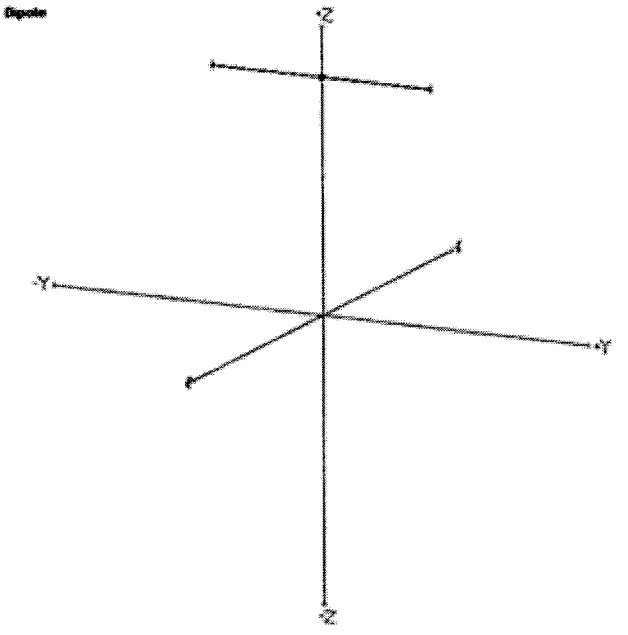

Figure 2.2: Physical structure of a dipole antenna.

also aware of the direction in which the receiver is getting the signal. This additional information about the direction of the incoming signal is going to help us in detecting the presence of an evil-twin attack.

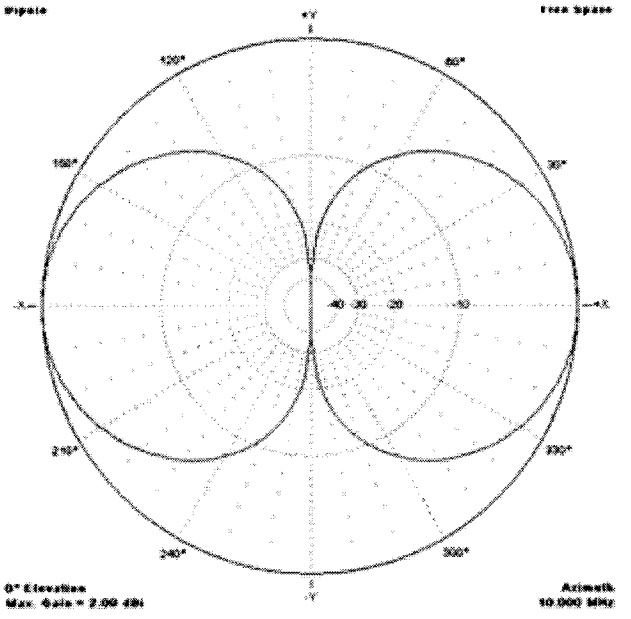

Figure 2.3: Radiation pattern of a dipole antenna.

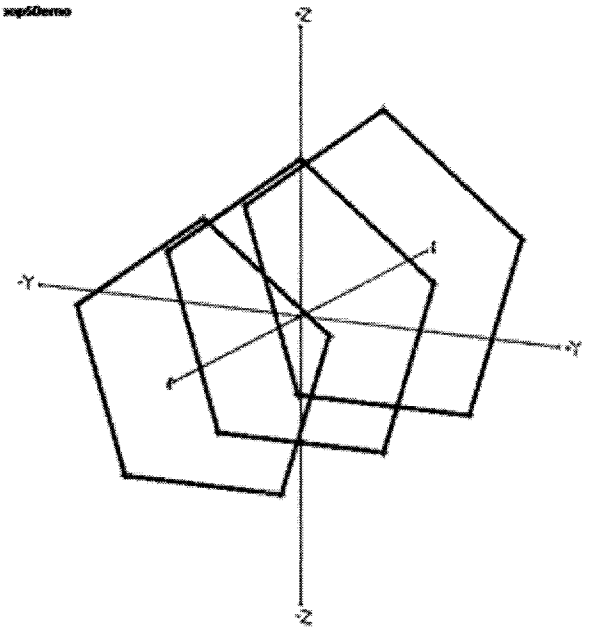

Figure 2.4: Physical structure of a loop antenna.

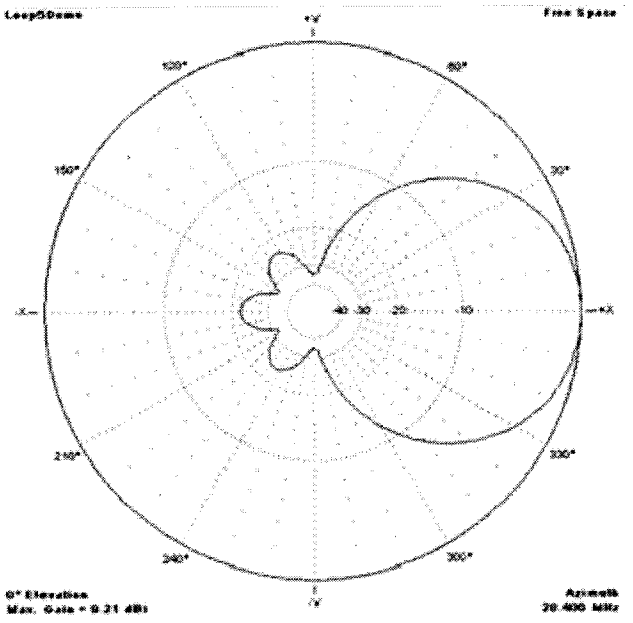

Figure 2.5: Radiation pattern of a loop antenna.

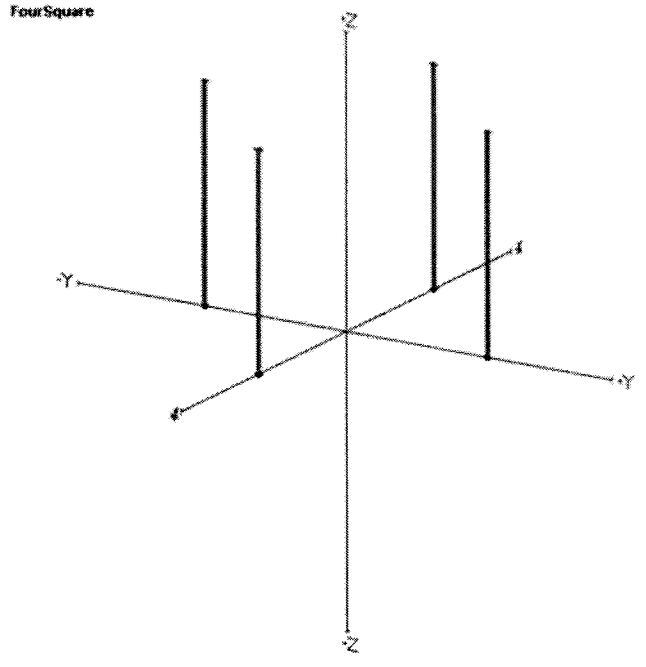

Figure 2.6: A four-square antenna.

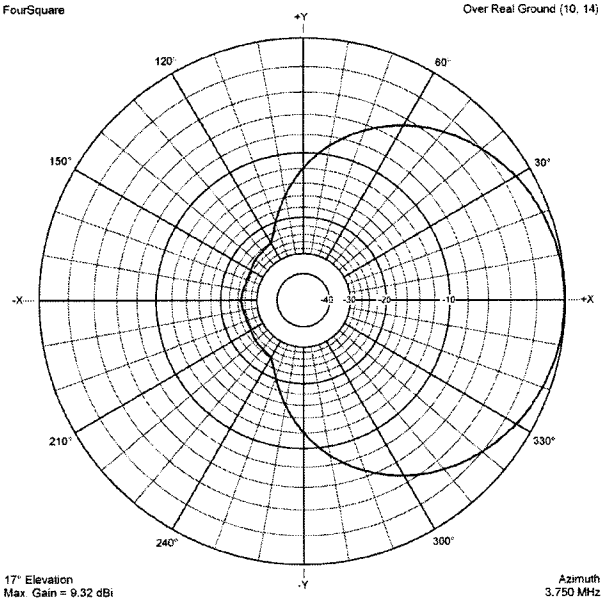

Figure 2.7: Radiation pattern of an element of the four-square antenna.

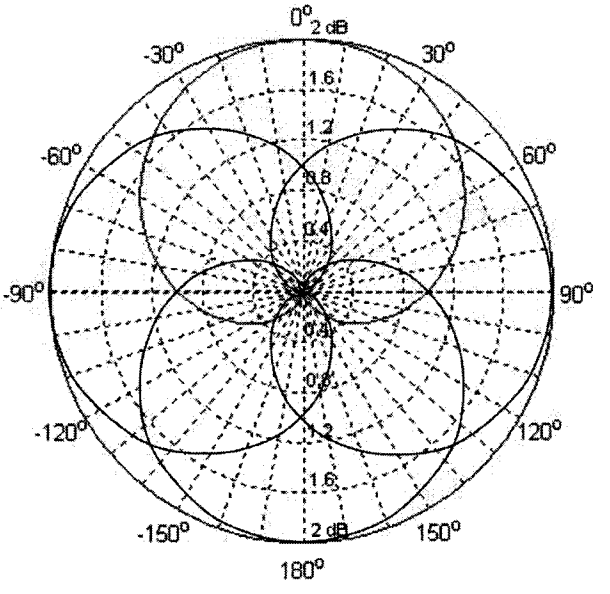

Figure 2.8: The clover shaped radiation pattern of a four-square antenna.

Chapter 3

Related Work

We present the existing work that has been done in the same area as our problem. Section 3.1 provides a few different types of attacks in a wireless setting, all involving multiple transmitters/adversaries, including a detailed discussion of the evil-twin attack, which is the prime focus of this work. Our first goal is to detect an evil-twin attack in a wireless network. Section 3.2 mentions a few techniques that have been previously devised to localize uncooperative nodes in a wireless network. Section 3.3 details previous work that has been done in relation to detecting multiple transmitters in a network and then localizing them. Since we are dealing with two transmitters in a wireless network as well, it was important to look at previous work done involving multiple transmitters.

3.1 Attacks in Wireless Networks Involving Multiple Transmitters

There are a number of different types of attacks that can be launched in a wireless network. We are particularly interested in the attacks in wireless networks involving multiple transmitters. The following sections describe a few types of attacks that are related to the attack scenario in our work in that they have more than one malicious nodes in the network or an instance of identity spoofing.

3.1.1 Wormhole Attack

A wormhole attack is an attack that is typical to wireless networks, particularly wireless sensor networks. In a multi-hop wireless network, an attacker can continue to receive packets from its neighbours, and *tunnel* them to another node in the network. Tunneling in the network gives an added advantage of faster communication and better connectivity in the network. However, the attacker can also exploit the network by choosing to not forward the packets once it receives them, thus launching a denial-of-service attack. The two ends of the wormhole or the two attackers in the network can also eavesdrop on the network and

maliciously drop packets or launch a man-in-the-middle attack [17]. In ad hoc networks, where nodes are trying to identify their neighbours, a wormhole attack can cause a lot of commotion. Although this attack is not directly related to our attack model, it gives an example of multiple adversaries in the network.

3.1.2 MAC Address Spoofing

Media Access Control (MAC) addresses are used as a unique identifier in wireless LAN networks. The MAC address can be spoofed by attackers to masquerade their presence in a network in which they are not authorized, or to access the network with a MAC address that has more privileges. A MAC address can also be spoofed by an attacker to be able to read packets over the network. Few techniques to spoof MAC addresses are shown by Cardenas in [6] and Wright in [41].

3.1.3 Evil-Twin Attack

The evil-twin attack is a further specialization of the spoofing attacks, and is also called the rogue Access Point (AP) attack. An evil-twin is a rogue Wi-Fi AP that has been set up by an attacker in a Wi-Fi network to eavesdrop on the information in the network. The evil-twin access point is setup by attackers close to hotspots, so that they can dupe users into connecting to the internet through their evil-twin access point. The evil-twin AP can also be setup on a secure network without authorization and can be used to perform a man-in-the-middle attack. In a man-in-the-middle attack, the attacker typically makes an individual connection with two parties intending to communicate with each other, makes them believe that they are privately and securely talking to each other, but in reality, the attacker not only has the capability of reading the messages, but also of altering the messages and then passing them on. The attackers do not need any high-end equipment for conducting the evil-twin attack - a laptop with a wireless card and a few programming skills is all it takes. At times, the evil-twins are setup close to the users so that the signal of the evil-twin access point is stronger than the actual hotspot, giving them all the more reason to connect to it. The attacker can capture all the users' transactions over the Internet using various tools like WireShark [30] and use them in combination with tools that can decode packets to disclose clear-text passwords. The attacker can setup the evil-twin access point so that

it resembles the original AP, i.e. both have the same characteristics like MAC address, Service Set Identifier (SSID), etc. Evil-twin APs are difficult to trace, as they can be turned off at the will of the attacker. Since they are identical to the honest APs, it is also harder to differentiate between the two. Section 3.3 mentions some work that has been done in the detection of evil-twins or rogue APs.

We have tried to solve a more generalized version of the evil-twin attack, which we term as evil-twin transmitter attack. In our work, we have a truth-teller transmitter, which may be malicious in nature, but doesn't lie about its position. There is also the *evil-twin* of the truth-teller transmitter, which not only impersonates the identity of the truth-teller transmitter, but also transmits at the same time as the truth-teller transmitter. Contrary to spoofing attacks, where at least one transmitter is good in nature, our work doesn't make any assumptions about the *goodness* of any transmitter in the network. Our work is not specific to Wi-Fi networks only; it can be extended to any type of wireless network.

3.2 Localizing Uncooperative Nodes

Localization of nodes in a wireless network can be done using either self-localization techniques or network-based techniques [19]. In self-localization techniques, the wireless node learns its own position with the help of other trusted nodes in the network. An example of a wireless node performing self-localization is a GPS. It uses the Time of Arrival (TOA) technique to compute its distance to various satellites, and performs trilateration on other satellites' positions to calculate its own position. Moses *et. al.* [27] and Barbeau *et. al.* [2] provided self-localization techniques for sensor networks to determine sensors' positions.

Although self-localization techniques offer good results, it is not feasible to use them in cases where there is a malicious node in the network. A malicious node, in addition to performing some attack on the network, may also try to hide or lie about its identity in the network. Therefore, for detecting the presence of a malicious node in the network we cannot rely on the information provided by the malicious node, and need to devise other ways of calculating its position. This is where the network-based localization techniques come in handy. A lot of research that has been done in determining the location of a node using a network-based technique assumes that the node being localized participates in its

localization. Following is a brief discussion of a few types of network-based localization techniques.

Triangulation is a technique that uses two receivers' coordinates along with the angle of arrival of the received signal to calculate the location of the transmitter. Triangulation requires the receivers in the network to be equipped with directional antennas, to be able to determine the angle of arrival.

The TOA and the TDOA mechanisms are time-based mechanisms for calculating location of the transmitter. The former calculates the transmitter-receiver distance using the round-trip time taken by messages between the transmitter and the receiver, whereas the latter uses the difference in time taken by a message to reach two different receivers, and plots a hyperbola with receiver coordinates at the foci. Both mechanisms require cooperation from all participating nodes, as they require the clocks to be synchronized. The hardware for clock synchronization is difficult to install and maintain [31]. With TOA, the transmitter must return the message to complete the round-trip. Some work based on the TOA technique is presented by Brands and Chaum [5] and Sastry *et. al.* [35]. The work presented by Thaeler *et. al.* [38] and Ho and Chan [15] are examples of the TDOA technique.

There are also the RSS-based localization algorithms. The RSS-based localization schemes gained popularity due to their capability of being measured easily. The signature dependent techniques depend on RSS signalprints that have been obtained during an offline training phase. To estimate the location of a transmitter or access point, the RSS received is matched with the already existing set of signalprints, and the location is based on the similarity between the two [1, 10, 18, 42]. These signature based schemes are able to produce acceptable results only in indoor environments, as the parameters affecting the path loss have a low variation indoors. The technique relies on the cooperation of the target node, which is not an assumption in our threat model. Another drawback of this scheme is the effort that is needed to collect the initial training data.

The second type of the RSS-based localization algorithms, the geometric RSS-based schemes like [25] and [24], determine the node's location based on the signal strength of the received message. The schemes proposed in [25] and [14] assume that the transmitting node transmits at the same EIRP as the other nodes in the network and [43] fails to take

into consideration the signal strength variations between receivers. Further, [3] use a probabilistic geometric RSS-based technique to construct annuli whose non-empty intersection most likely contain the transmitter. The HPB mechanism described in [20] enhances [2], by assuming no information about the EIRP of the transmitter, and suggesting the use of hyperbola pairs instead of annuli, thus reducing the area containing the transmitter.

3.3 Detecting and Localizing Multiple Transmitters

The work in [17] provides a mechanism to detect the wormhole attacks mentioned in Section 3.1.1 by adding a *leash* - geographical or temporal, to each packet in the network. Directional antennas have been deployed to detect wormhole attacks by Hu and Evans in [16], which suggests the use of directional antennas for our problem as well. Wang and Bhargava [39] suggested using RSS to estimate distances between two nodes to determine if the packet had been tunneled or not.

Described here are a few techniques that have been developed over time to mitigate the effects of the MAC address spoofing attack described in Section 3.1.2. Existing work has been done in networks that involve more than one transmitter or more than one adversary. Yang *et. al.* [42] provide an algorithm for detecting spoofing attacks in a wireless network with multiple adversaries, determining the number of attackers and localizing the multiple adversaries using cluster analysis. The clustering algorithm does a pattern matching and based on that, detects an attack and determines the number of adversaries. However, the method uses the signalprints technique, which is effective for indoor environments only. Authors in [10] initiated the use of matching the signalprints for spoofing detection, and [36] modeled the RSS values using a Gaussian mixture model, which was a result of antenna diversity. A diversity scheme is a scheme used to improve the reliability of a message signal, by using two or more communication channels with different characteristics. Chen *et. al.* in [7] use K-means cluster analysis to detect spoofing attacks in WLANs and ZigBee networks. Unlike [42], the other algorithms are just limited to detecting one spoofing attack in the network. The work in [42] cannot be used to solve our problem, as our attack model does not assume an indoor environment.

In term of detecting and localizing malicious APs in cases of evil-twin attacks, the authors in [12] propose a time based mechanism to differentiate between a legitimate AP and

a rogue AP. The mechanism calculates the round trip time between the user and the DNS server, and determines whether the AP is legitimate or not. Rogue AP detection is a two step process: discovering an AP, and determining whether the AP is malicious or not. Some techniques used to discover an AP involve RF scanning and AP scanning. Some techniques used to identify rogue APs compare the AP's characteristics against a pre-configured authorized list of APs. A few other effective techniques, like [37] uses traffic characteristics to detect a rogue AP, and [40] analyzes TCP ACK-pairs to detect a rogue AP. Roth *et. al.* [34] provide a simple strategy in defending against evil-twin APs, which results in having the users gain trust in the access point they are connected to. However, this solution involves having hardware supports including the ability to display two color lights on the routers, and an additional switch on the wireless device in hotspots.

3.4 Summary

Section 3.1 briefly discussed about the types of attacks that are related to our attack model. Our attack scenario is the closest to the evil-twin attack in terms of characteristics, thus we call our attack scenario the evil-twin transmitter attack. Section 3.3 described some ideas that have been put forward to deal with attacks that were similar to ours in behaviour, and Section 3.2 detailed a few techniques that have been described for localizing transmitters in different situations. We were inspired to test the directional antenna, particularly the four-square antenna as part of the solution to detecting the evil-twin transmitter attack in the wireless network. We have used the HPB mechanism described in detail in the previous chapter to localize the transmitters after an attack is detected. The next chapter will describe our algorithm for identifying the evil-twin transmitter attack in the network.

Chapter 4

Detecting the Evil-Twin Transmitter Attack

We introduce our mechanism to detect an evil-twin transmitter attack in a wireless network. The directional antenna's property of being able to determine the direction of an incoming signal is used extensively to detect that a system is under an evil-twin transmitter attack.

4.1 The Attack Model

The attack model assumes a wireless network with some receivers, each equipped with a four-square antenna, and a truth-teller transmitter, equipped with an omni-directional antenna. The truth-teller transmitter that is part of the network may be a malicious transmitter, but it doesn't lie about its identity. An attacker trying to launch an evil-twin transmitter attack in this wireless network gains access to the network and adds a malicious transmitter to the network. The attacker's transmitter has an omni-directional antenna and avoids being detected by using the same MAC address as the truth-teller transmitter and by sending signals at the same time as the truth-teller transmitter. The attacker's transmitter is called the *evil-twin* of the honest transmitter. The term *evil-twin* is borrowed from the concept of the evil-twin attack, explained in Section 3.1.3. Furthermore, no assumption about the EIRPs of either transmitter is made by the receivers.

In our attack scenario the receivers and the transmitters are placed outdoors. The receivers are authorized and trusted in the wireless network and communicate securely with each other. The receivers in the network have globally known position coordinates and are equipped with four-square antennas. The antennas of the receivers are aligned with each other using a common reference direction. The wireless network is secure and its nodes are authorized and authenticated for any communication in the network.

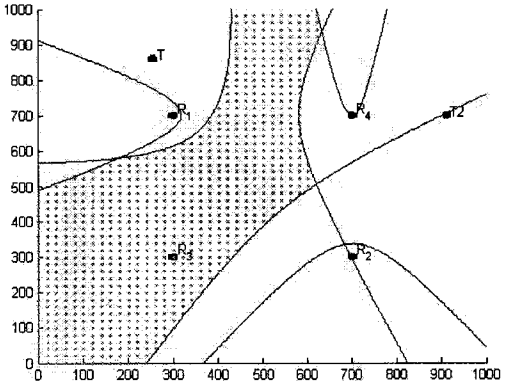

Figure 4.1: HPB with two transmitters

If the receivers in the network are trying to find the location of the truth-teller transmitter, then they will get confused by the presence of the evil-twin transmitter. Thus, they will provide inaccurate results for the localization of the truth-teller transmitter. Figure 4.1 shows how HPB gets confused and fails to localize the transmitters correctly when two transmitters are present in the network. The area size given by the algorithm is large, and neither of the transmitters lie in the candidate area. Therefore, we need to detect if the system is under an evil-twin transmitter attack before being able to correctly localize the transmitters.

4.2 Challenges

The detection of the evil-twin transmitter attack is difficult. Once an attacker is able to gain access to the network, the identity it forges cannot be traced back to the attacker's real identity because the attacker is using another transmitter's credentials while transmitting signals. The ability of the evil-twin transmitter to send messages simultaneously as the truth-teller transmitter is another challenge in identifying that the network is under an evil-twin transmitter attack. Therefore, the scheme proposed by Han *et.al.* in [12] using time difference to differentiate between the evil-twin AP from its honest counterpart becomes unusable in our scenario.

4.3 Partitioning the Receiver Area

As part of the solution, each receiver in the network is equipped with a four-square directional antenna. As previously mentioned in Section 2.3, the four-square antenna is capable of detecting what direction the signal is being received from. We assume that each of the transmitters (i.e. truth-teller as well as the malicious transmitter) in the network is equipped with an omni-directional antenna. The entire area is divided into n zones. The number n is always a perfect square, and the number of receivers m present in the area satisfies the following equation:

$$m = (\sqrt{n} - 1)^2 \tag{4.1}$$

The m receivers are placed such that they are present on the inner most corners of the n zones. For this work, we use 9 zones and 4 receivers in the network. The entire setup is shown in Figure 4.2. Each of the receivers is equipped with a four-square antenna. This means that the receiver is capable of determining which direction it is getting the signal from. The transmitters' EIRPs are unknown to the receivers. Each receiver records the RSS values of signals that it receives. Each receiver also calculates the *sector* in which it gets every signal. A sector is different from a zone. A sector is a quadrant in which each receiver gets its signal. A zone is a part of the grid, and used to locate the transmitters. The 1st quadrant of an XY plane is referred to as the Sector 1, the 2nd quadrant is the Sector 2, the 3rd quadrant is the Sector 3 and the 4th quadrant is the sector 4. A quadrant is defined to be any of the four areas into which a plane is divided by the reference axes X and Y in a Cartesian coordinate system, with the receiver at the origin. The quadrants of the receiver are designated first, second, third, and fourth, counting counterclockwise from the area in which both coordinates are positive.

The sectors for the receiver R_1 are shown in the Figure 4.3. For example, considering the settings showing in Figure 4.4, if the receiver R_1 receives a signal from zones II, III, V or VI, it is considered to be in its sector 1. If the receiver R_1 receives a signal from zones I or IV, it receives in the sector 2, and so on. In Figure 4.4, if receiver R_2 receives in sector 3, the transmitter T_2 must lie in zones VII or VIII in the grid. Alternatively, if receiver R_3 receives a signal from sector 3, the transmitter can potentially lie in zones IV or VII.

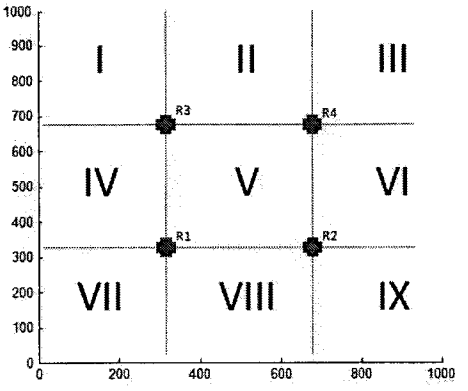

Figure 4.2: The area is divided into 9 zones and the 4 receivers are placed at the innermost corners.

4.4 Detecting Multiple Transmitters

For two transmitters, a receiver will have up to two RSS values and two sectors. If the receiver receives both the signals from the same sector and if both values fall in the dynamic range of the receiver, the signals interfere, and nothing is recorded, else only the louder value is registered. The dynamic range of a receiver is defined as the range of signal levels over which it can operate. If a strong and a weak signal is transmitted for a receiver, the receiver only hears the stronger signal if the weaker signal is not in the dynamic range of the receiver. The length of the dynamic range of a receiver is fixed, but the dynamic range values depend on the strength of the stronger signal. Also, if either of the RSS values is beyond the sensitivity level of the receiver, it is not registered. Sensitivity of a receiver is the minimum signal strength that the receiver is capable of receiving.

After each receiver registers the RSS values and their respective sectors, the next step is to divide the pool of RSS values such that each pool corresponds to one transmitter. With the information about sectors, each receiver calculates a set of *potential* zones in which the transmitter(s) may possibly lie.

Each receiver then sends its set of potential zones Z_i to a Central Processing Point (CPP), which is responsible for taking the individual information from the receivers, and

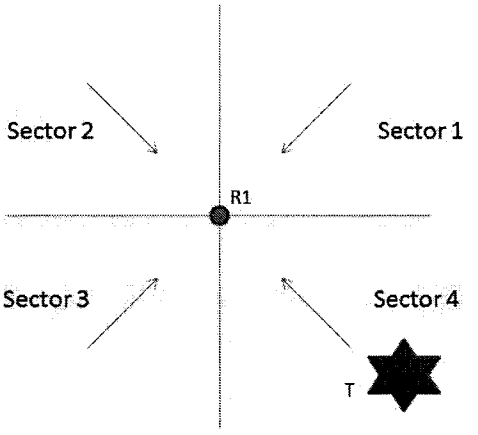

Figure 4.3: The sectors for receiver R_1.

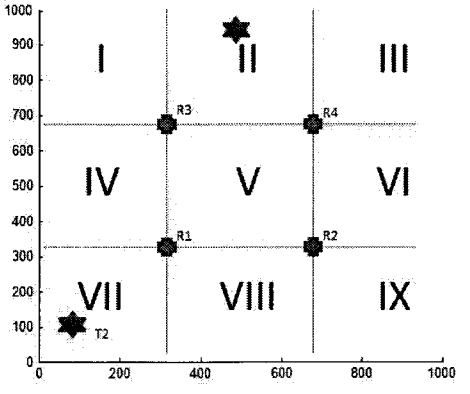

Figure 4.4: A possible setup of the transmitters in the network.

processing it to output a list of zones in which the transmitters must potentially lie in accordance to the pattern in which the messages are received. The CPP performs an intersection of the sets of potential zones it receives, and calculates a set Ω that contains the zones common to all receivers.

$$\Omega = \bigcap_{i=1}^{m} Z_i \tag{4.2}$$

If the number of elements in the set Ω is one, it is declared that the system is not under attack, and there is just one transmitter in the network, which is the honest transmitter. Otherwise, an attack is reported. If the number of elements in the set Ω is more than two, only the two most frequently occurring zones remain in the set Ω. With the processing done above, we have two zones in the area in which the transmitters are present. After detection of an attack, our next aim is to localize the two transmitters within the frequently occurring zones.

Algorithm 1 describes the steps for identifying an attack. The RSS and *sector* values are recorded by each receiver. Then, each receiver calculates its $PotentialZones$, which is a set of zones where the transmitter(s) may lie for the receiver to receive in the manner it does. The $PotentialZones$ set is calculated using the *sector* or reception of signal and the coordinates of the zones. An intersection of all $PotentialZones$ sets yields the common zones set Ω. If the number of elements in the set Ω is 1, then *no attack* is reported. If it is more than two, then we scale down the number of common zones in set Ω to the most frequently occurring two zones. When the set Ω has two elements in it, an attack is reported.

Algorithm 1 $Identify\_Attack$

for $i = 1$ to N receivers **do**
  Register $rss1$, $rss2$, $sector1$, $sector2$
  global Ω
  if $sector1 == sector2$ **then**
    Choose non-interfering RSS values
  end if
  Calculate Potential Zones Z_i
end for
Calculate $\Omega = \bigcap_{i=1}^{n} Z_i$
if $\mid \Omega \mid == 1$ **then**
  return (-1)
  //No Attack is Detected
else if $\mid \Omega \mid > 2$ **then**
  for $j = 1$ to M zones **do**
    for $k = 1$ to N receivers **do**
      if $j \in Z_k$ **then**
        C[j] = C[j] + 1
      end if
    end for
  end for
  $\Omega = \{Index\ of\ max(C), Index\ of\ 2^{nd}\ max(C)\}$
end if
return (1)
//Attack is Detected

Chapter 5

Localizing Transmitters

This chapter introduces the mechanism that we use to localize the transmitters in a wireless network. The directional antenna's property of being able to determine the direction of an incoming signal is used extensively to detect that a system is under an evil-twin transmitter attack. Once the Algorithm 1 explained in Chapter 4 reports an attack, the next step is to localize the transmitters in the wireless network. The HPB mechanism described in Section 3.2 is used to localize the transmitters one at a time. If HPB fails for any of the transmitters, an alternate fallback mechanism described in Section 5.2 is used. The algorithm localizes both transmitters in the network, regardless of the nature of the transmitter. However, determining which out of the two transmitters in the wireless network is the evil-twin is out of the scope of the present work.

5.1 Using HPB to Localize the Transmitters

After an attack in the network is detected, we localize the two involved transmitters. The set Ω calculated from Equation 4.2 contains two zones. After the computation, the CPP divides the set of RSS values into two pools, such that one pool contains the RSS values our algorithm presumes to be generated from one transmitter and the second pool contains the RSS values presumed to be generated from the other transmitter. Next, the HPB mechanism is used to construct the hyperbolas at the minimum and maximum bounds of the probable distance difference range between each transmitter and each pair of receivers in the network. The details of the HPB algorithm to estimate the position of transmitter in a wireless network are given in Section 2.2.

For example, consider the grid shown in Figure 5.1 simulating a wireless network. Algorithm 1 detects an attack in the network and calculates the potential zones. After that, the RSS values are separated into two separate pools, and we run HPB on the first set of

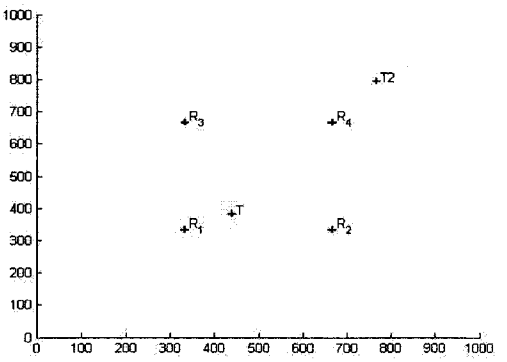

Figure 5.1: Example simulation grid.

RSS values generated. HPB is able to localize the transmitter. The candidate area given by HPB is depicted in Figure 5.2.

A further enhancement of the algorithm has been done. As seen from the Figure 5.2, the candidate area given by HPB is quite large. In addition to this candidate area, we have additional information of the zone in which the transmitter might lie, for the receivers to get the signal from certain sectors. This additional information of the potential zone can help to further minimize the candidate area size. We take an intersection of the candidate area given by HPB and the area covered by the potential zone identified by the Algorithm 1 to give us a smaller area to locate the transmitter. The lesser the candidate area size for a transmitter, the easier it is to pin-point the transmitter. Figure 5.3 shows a tremendous decrease in the candidate area for localizing the transmitter T. The candidate area in Figure 5.2 is about 27% of the grid whereas the candidate area shown in Figure 5.3 is about 4% of the total grid.

There are cases in which HPB yields a null area for the location of a transmitter. In other words, HPB fails to give a candidate area for the transmitter. This could be due to the HPB not being able to form sufficient hyperbolas between the receiver pairs, which in turn, could be a result of either interference due to two transmitters' signals at one or more receivers, or due to incapacity of a receiver to receive an signal if the RSS value is not within the dynamic range of the receiver. Our algorithm provides a fallback mechanism to calculate the area in cases where HPB fails.

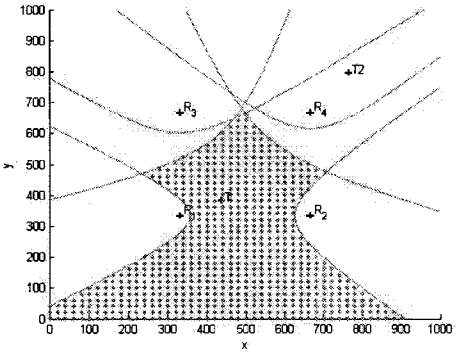

Figure 5.2: HPB localized transmitter T.

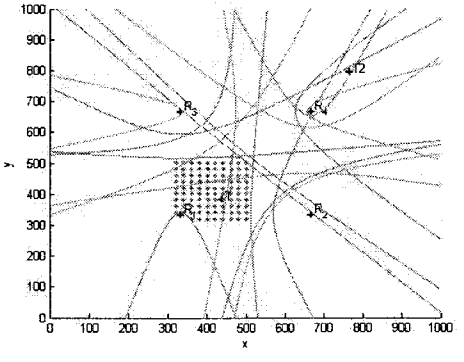

Figure 5.3: Candidate area is reduced when area of HPB and area of zone are intersected.

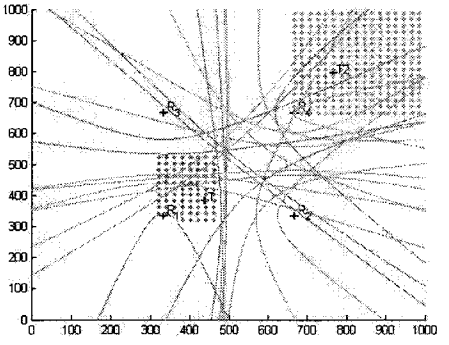

Figure 5.4: Fallback mechanism used to localize transmitter T_2.

5.2 The Fallback Mechanism

We have an alternate mechanism to calculate a candidate area in cases where HPB is not able to localize the transmitter or the intersection of the area given by HPB and the zone is empty. We use the additional information of the potential zone that we calculated previously. Since we have a potential zone already calculated for the presence of the transmitter, we use that zone's area as the estimated candidate area for the location of the transmitter. The area size is $1/n^{th}$ the size of the whole grid, where n is the number of zones in the grid. For example, when $n = 9$, which is also the case in the simulation grid shown in Figure 5.1, the fallback mechanism gives us a candidate area of approximately 11% of the entire grid for the transmitter. Figure 5.4 shows a candidate area calculated using the fallback mechanism when HPB was unable to localize the transmitter T2.

The localizing algorithm uses the methods described Sections 5.1 and 5.2 to localize one transmitter after the other in the event of an evil-twin attack. At a given time, HPB or fallback or the intersection of HPB and fallback can be used to localize the transmitter. It could also be that in the same scenario of an evil-twin attack one transmitter is localized using the intersection of HPB and zone's area, and the other one is localized using the fallback mechanism. Figure 5.4 shows a case where a combination of HPB and fallback is able to localize both transmitters after an attack has been detected. Figure 5.5 shows a case where the fallback mechanism is used both times to localize the transmitters after HPB has failed.

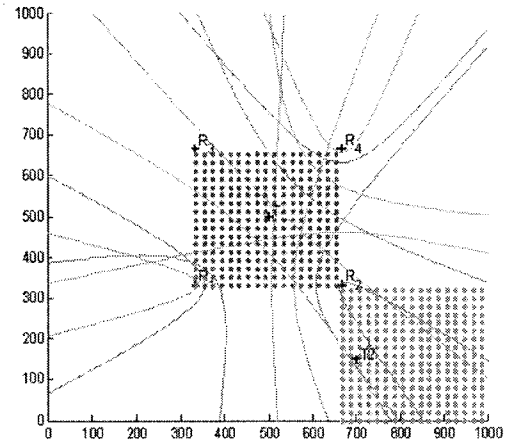

Figure 5.5: Fallback mechanism used to localize transmitters.

5.3 The Localization Algorithm

The Algorithm 2 describes the steps for localizing the transmitters. The $RSSPool(1)$and $RSSPool(2)$ are calculated based on the potential zones set Ω calculated in Algorithm 1. The function *HPB(RSSPool)* takes a pool of RSS values computed by the CPP and computes the minimum and maximum distance hyperbolas for each pair of receivers according to the algorithm specified in [20]. If the HPB gives a candidate area, it is intersected with the area of the potential zone computed by CPP to give a smaller candidate area. The area of the potential zone is given by the function $coordinates$, which takes the zone number as an argument, and gives the coordinates covered by the zone. If the HPB fails to give a candidate area or if the transmitter is not found in the intersection, then only the fallback mechanism $coordinates(potentialZone)$ is used, and that returns the coordinates of the zone the transmitter lies in, as the candidate area.

Algorithm 2 $Localize\_Transmitters$

Calculate $RSSPool(1)$, $RSSPool(2)$

//$RSSPool(1)$ and $RSSPool(2)$ are calculated based on the two zones in Ω

for $i = 1$ to $\mid \Omega \mid$ **do**

$HPBArea(i)$ = $HPB(RSSPool(i))$

//HPB(RSS) method calculates the coordinates of the candidate area based on the RSS pool

if $HPBArea(i)$!= ϕ **then**

Calculate $candidateAreaCoordinates(i)$ = $HPBArea \bigcap coordinates(\Omega(j))$

else

Calculate $candidateAreaCoordinates(i)$ = $coordinates(\Omega(j))$

//coordinates(zone) gives the coordinates of the zone where one transmitter lies

end if

end for

return $(candidateAreaCoordinates)$

Chapter 6

Simulation and Test Results

This chapter presents the simulation setup and experimental results we obtained for detecting the wireless evil-twin attack and localizing transmitters in the wireless network. The simulation environment is modeled such that it reflects real world scenarios. The details of the simulation setup are presented in Section 6.1. Various scenarios were tested in the simulation environment and different metrics were gathered. They are detailed in the Section 6.2 along with the test results.

6.1 Simulation Setup

The algorithm is evaluated by simulating random locations of the transmitter and its evil-twin in a 1000 x 1000 m^2 grid such that all combinations of the zones are tested. Therefore, there are 45 possible combinations in which the two transmitters can be placed in the zones. The receivers are always placed at the innermost corners of the zones in the grid. The algorithm holds for any number of zones in the grid, as long as the number is a perfect square and satisfies Equation 4.1. The test scenarios described here, however, assume four receivers, and therefore nine zones. The whole area is divided into nine equal sized zones. The scenario assumes that the four receivers in the wireless network are operating in the 2.4 GHz frequency range. For each of the 45 combinations, the HPB algorithm is executed 1000 times with a confidence level of 95%. The loss parameters η and σ are taken from experiments conducted by Liechty *et. al.* [22, 23] at 2.4 GHz and are also used in [20]. The value of η is 2.76 and σ is 5.62.

The simulation runs in two phases - one is the setup phase and the other is the Attack Detection and Localization Phase. In the setup phase, the RSS values are simulated at each receiver using the log-normal shadowing model. The EIRP of the transmitters in this case is chosen to be 30 dBm. For each execution and for each transmitter, each receiver simulates a random amount of signal shadowing along a log-normal distribution curve with

mean zero and standard deviation η. Each receiver also adds the receiver gain G_R at the angle at which it is receiving the RSS value. The signal shadowing and the gain are added to the receiver simulated RSS value. The dynamic range of the receivers is chosen to be 20 dB and the sensitivity of the receivers is chosen to be -83 dBm. The dynamic range value chosen is towards the lower end of the range values for dynamic range for WLAN cards. The sensitivity of WLAN cards is between -73 to -91 dBm, but the chosen value of -83 dBm is the sensitivity value of the Dell Wireless 1350 (802.11 b/g) miniPCI card at 18 Mbps.

In the Attack Detection and Localization Phase, the algorithm detects an evil-twin transmitter attack using the Algorithm 1. In case of an attack, the transmitters are localized with Algorithm 2, using the RSS values generated at each receiver, without knowledge of the EIRP or gain.

6.2 Test Results

The performance of our algorithms is measured along three metrics: the percentage of times an attack was detected correctly, the success rate of localization of transmitters, and the candidate area size as a percentage of the entire simulation grid. These metrics are gathered for each run of the algorithm. The receivers are placed in the grid as shown in Figure 4.2.

Results were gathered for two types of scenarios. The first one, presented in Section 6.2.1, is the scenario where either HPB or the fallback mechanism is used to localize the transmitters. The second one, presented in Section 6.2.2, is the scenario in which an intersection of the candidate area given by HPB and the area covered by the potential zone is taken to reduce the candidate area size.

6.2.1 Results With HPB or Fallback

In this scenario, only one of the localization mechanism - HPB or, if that fails, the fallback mechanism is used to localize the transmitters, as presented in the Algorithm 2. The results of a simulation of 1000 runs are presented in this section.

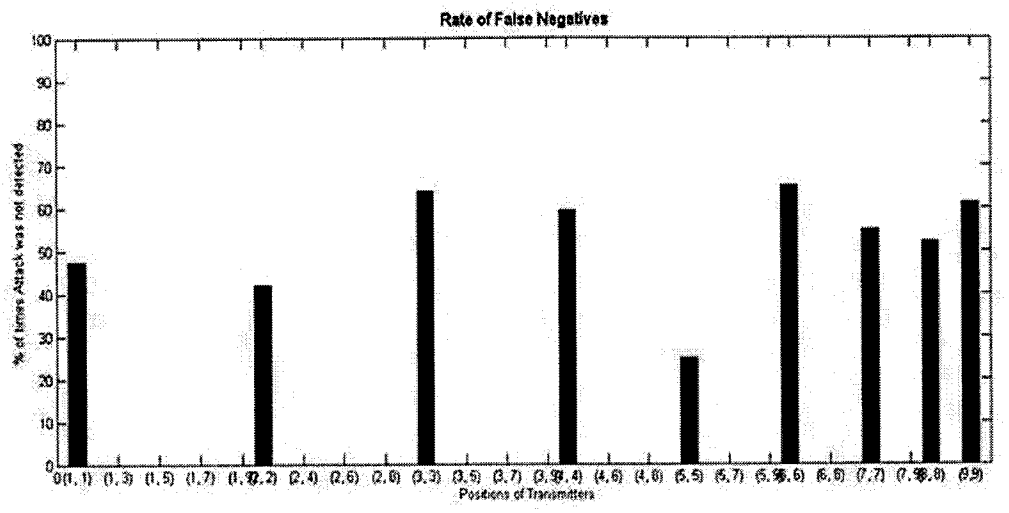

Figure 6.1: Rate of false negatives.

Figure 6.1 illustrates the rate of false negatives while detecting whether the network is under attack at different transmitter locations. The x-axis in the graph shows the zones in which the two transmitters are present. For example, (1, 2) means transmitter T is in zone I, and transmitter T2 is in zone II. We can see from the Figure 6.1, an attack is being detected in all cases in which the transmitters are in different zones. That is, the rate of false negatives is 0%, and the rate of true positives is 100% when the transmitters are in different zones. However, when the transmitters are in the same zone, the rate of false negatives on an average is 47% and the rate of true positives is 53%.

The success rate of localization of transmitters calculates the percentage of times both transmitters are correctly localized by the algorithm, only one of the transmitters is correctly localized, and neither is correctly localized. Both the transmitters are correctly localized with an average success rate of 62% and at least one of the transmitters is correctly localized with an average success rate of 83%. The algorithm calculates the correct zones for both the transmitters on an average of 92% of the time when the transmitters are in different zones, and 43% of the time when the transmitters were in the same zone. Figure 6.2 shows the correctness of zones as a function of the positions of the two transmitters.

In terms of the candidate area size, Figure 6.3 gives the average percentage area for both transmitters when they are located in the same zone. The average candidate area size

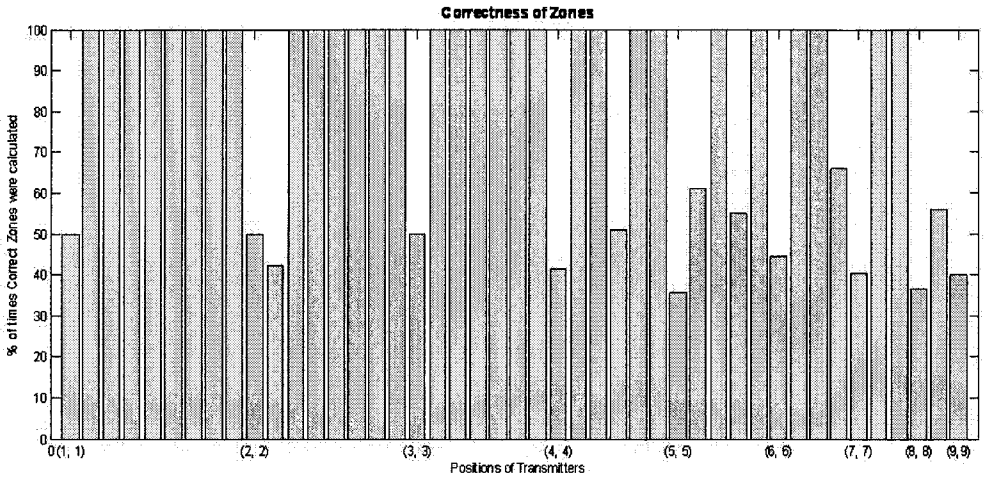

Figure 6.2: Correctness of zones.

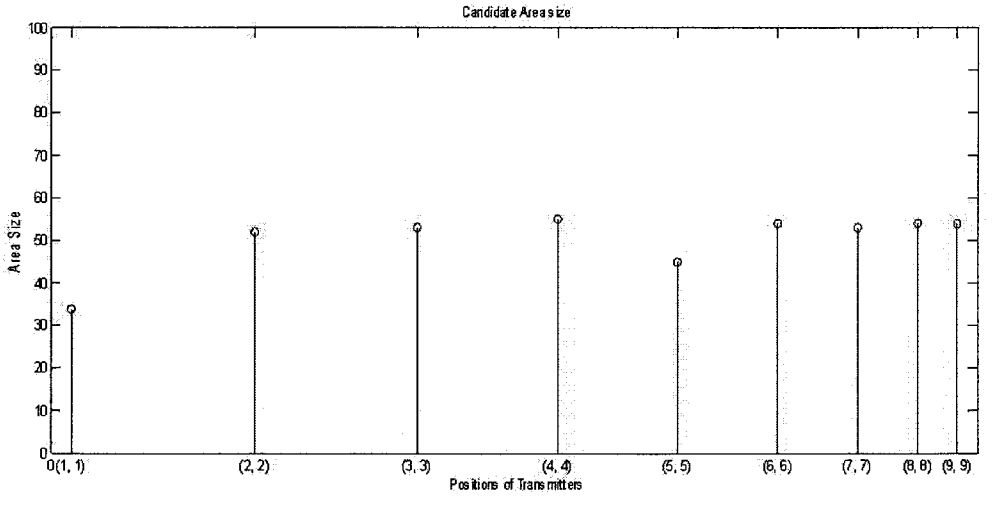

Figure 6.3: Candidate area sizes when transmitters are in same zone.

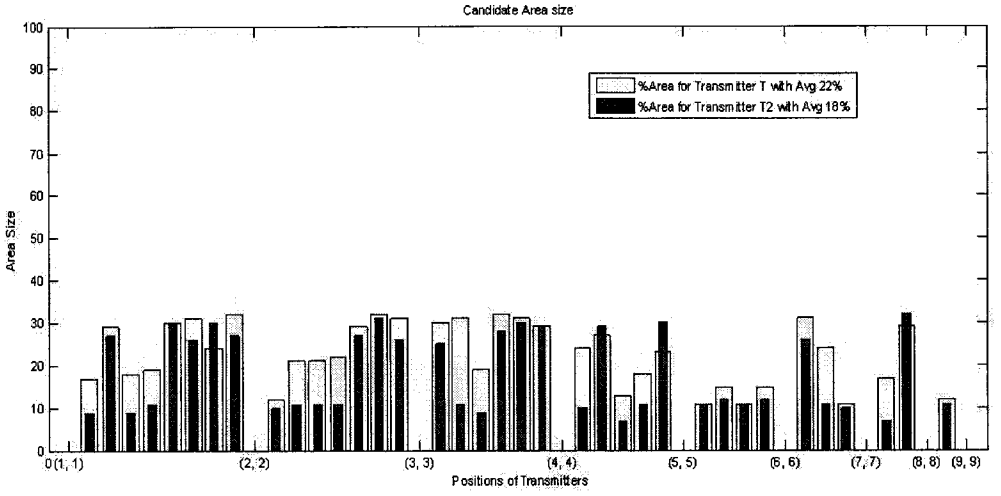

Figure 6.4: Candidate area sizes when transmitters are in different zones.

in this case is 50% of the entire simulation grid, and is not very informative of the location of the transmitters. For cases where the two transmitters are in different zones, the candidate area size comes to an average of about 18% with a standard deviation of 9%, and 22%, with a standard deviation of 7%, of the whole grid for the two transmitters. This is shown in Figure 6.4. In cases where the fallback mechanism is used to localize the transmitter, the area returned is the area of a zone, which is about 11% or $1/9^{th}$ of the area of the whole grid. In cases where the HPB is used, the candidate area goes upto about an average of 30% of the whole grid. The average areas are calculated only over the cases in which an attack is detected by the algorithm.

6.2.2 Results With HPB and Fallback

In this scenario, a combination of the localization mechanisms, HPB and fallback, are used to localize the transmitters. Using this approach, we see an improvement in the candidate area size that is given for localization of the transmitters. We also notice an improvement in the number of times both transmitters are correctly localized. The results of a simulation of 1000 runs are presented in this section.

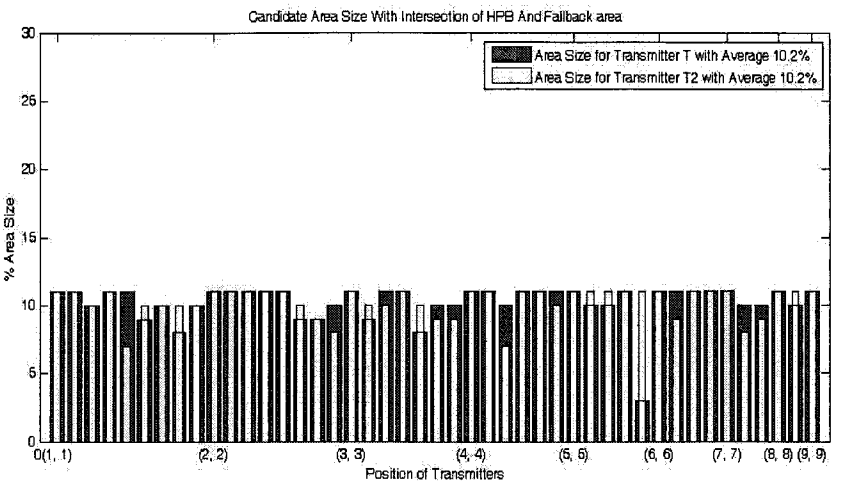

Figure 6.5: Candidate area of transmitters with HPB and fallback.

The success rate of localization of transmitters calculates the percentage of times both transmitters are correctly localized by the algorithm, at least one of the transmitters is correctly localized, and neither is correctly localized. On an average, both transmitters are correctly localized 74% of the time. In cases where the transmitters were located in different zones, the transmitters are correctly localized is 94% of the time on an average and at least one transmitter is correctly localized 81% of the time on an average. This result is consistent with the results obtained in the version of the algorithm used in the previous section.

In terms of the candidate area size, Figure 6.5 gives the average percentage area for both transmitters. The average candidate area is 10.2%, and is definitely an improvement over the average areas given in Section 6.2.1 by using either HPB or fallback. The maximum area returned as candidate area for a transmitter is the area of the zone, which is about 11% or $1/9^{th}$ of the area of the whole grid. But in some cases, due to the intersection of the areas given by HPB and the fallback mechanism, the candidate area size is further reduced. The standard deviation is approximately zero in cases where the transmitters are located in different zones. The average areas are calculated only over the cases in which an attack is detected by the algorithm.

We also calculated the number of times the intersection of HPB and fallback was effective in giving a candidate area. On an average, an intersection of candidate areas given by HPB and the fallback mechanism was used 25% of the time to compute the candidate area for localizing the transmitters. However, 75% of the time, only the fallback mechanism was used to calculate the candidate area. The fallback mechanism was used to calculate the candidate area in cases where either HPB did not yield any candidate area, or the candidate area yielded by HPB did not have any points common to the area given by the fallback mechanism. On an average, the zones that were calculated were correct 84% of the time. When the transmitters were in different zones, the zones were correctly calculated 93% of the time.

6.3 Summary

Our algorithm is able to detect an attack for 100% of the times when the transmitters are located in different zones, and on an average, detects 53% of the attacks in cases where the transmitters are present in the same zone. In terms of success rate of localizing the transmitters, the transmitters are correctly localized on an average of 74% of the time. The average candidate area size also differs in cases where transmitters are in the same zone, as opposed to cases where the transmitters are in different zones. In the former case an average candidate area of 50% is yielded, whereas in the latter case the average candidate area of 20% is given with a standard deviation of 8%. With the improved version of the algorithm combining HPB and fallback area, these results are further improved, and the average candidate area size is 10.2% of the simulation grid.

Chapter 7

Conclusion and Future Work

We described an algorithm for detecting the evil-twin transmitter attack in a wireless network using a four-square directional antenna on each receiver. No assumptions are made about the EIRPs of the transmitters. If an attack is detected in the network, the algorithm tries to localize the two transmitters' positions by tracing candidate areas with a degree of confidence using the HPB mechanism. In cases where HPB fails to localize the transmitter, a fallback mechanism is used to estimate the candidate area of the transmitter. The algorithm for detection of the attack is presented in Chapter 4 and the algorithm for localizing the two transmitters is detailed in Chapter 5; the performance of the algorithm is assessed with simulation, the setup of which is described in Chapter 6.

The Section 7.1 summarizes this work and provides a brief synopsis of the contributions of this work. Section 7.2 recommends a few directions for future work.

7.1 Contributions

We have devised an algorithm to detect if a wireless network is under an evil-twin transmitter attack. The attack can be an insider attack, i.e. the evil-twin transmitter possesses the wireless network credentials, or it can be a coordinated attack, i.e., both the transmitters are knowingly involved in launching the attack. The evil-twin transmitter can also be an outside device, which somehow got access to the wireless network. We equip the receivers with four-square antennas, which are directional in nature, and can determine the direction of an incoming signal. This was done to be able to detect that the wireless network is under the evil-twin transmitter attack. No assumptions are made about either of the transmitters' cooperation, including the EIRPs at which they are transmitting. This makes the algorithm more reliable in terms of dealing with transmitters that may or may not be lying about their EIRPs. The random amount of signal shadowing that each receiver is subjected to for the

incoming signal makes the simulated scenario a more realistic model of the real world.

Once it is determined that the wireless network is under attack, we have attempted to localize the transmitters as well. Based on the direction of the incoming signals, we calculate the two potential zones in which the transmitters will most likely lie, and also divide the RSS values received into two separate pools. We then use the Hyperbolic Position Bounding (HPB) mechanism [20] to locate the transmitters one by one. The candidate area that is given by HPB may be large in size, therefore to minimize the candidate area for finding a transmitter, we intersect the area given by HPB with the area given by the potential zone of the transmitter. Additionally, we have proposed to use the potential zone's area as the candidate area of the transmitter if the HPB fails to give a candidate area. We refer to this approach as the fallback mechanism.

Our algorithm detects an attack for all positions of transmitters, except when they are in the same zone, in which case, there is a 50% chance of detection of an attack. Our localization results are also consistent for all the positions of the two transmitters in a 1000 x 1000 m^2 grid, except for the cases in which the transmitters are present in the same zone.

Another benefit of this approach is that our attack detection algorithm can be used independently for detecting an evil-twin attack in any wireless network setting. Also, any localization scheme previously devised can be used in conjunction with our attack detection algorithm and fallback mechanism to localize the transmitters.

Our contributions with this work are listed below:

1. We have proposed an algorithm that uses directional antennas for determining the presence of an evil-twin transmitter attack.

2. After a successful determination of an attack, we have used an existing localization technique, the Hyperbolic Position Bounding (HPB) to localize the two transmitters in the wireless network. To better improve the results of the localization, we combined the results of the HPB with our fallback mechanism to further reduce the candidate area size, and also used the area given by the fallback mechanism as the candidate area in cases where HPB failed to give a candidate area.

7.2 Future Work

In this work, we try to detect an evil-twin transmitter attack, and in case of an attack, we also localize the two transmitters. However, this work assumes that both the transmitters are using omni-directional antennas. If either or both transmitters use directional antennas to transmit signals, the RSS values determined to be in the same pool at the receivers can no longer be trusted to be from the same transmitter. Furthermore, the relationship between the RSS values received by a pair of receivers and their distance difference from the transmitter would also be distorted if directional antennas are used. The attackers will have a benefit of using directional antennas, as chances are that the candidate area determined for their presence is the incorrect one. We have seen from the Chapter 2, that directional antennas do not have a uniform radiation pattern, and they are capable of transmitting more power in a certain direction. Thus, trying to solve the evil-twin transmitter attack for transmitters using directional antennas would be an interesting extension of this work.

From the results demonstrated in the Chapter 6, it can be seen that there is only a 50% chance that the algorithm detects an attack when the transmitters are in the same zone. If the two transmitters are coordinating the attack, it is unlikely for them to be close to each other, as that also means some receivers may not get the signal due to interference. In either case, this algorithm should be extended to be able to report an attack even in cases where both transmitters are in the same zone.

The focus of this work was to detect that the system is under an evil-twin transmitter attack and if so, to localize the transmitters in the network. Determining which of the two transmitters is the evil-twin is another problem that needs to be analyzed.

7.3 Summary

Our algorithm successfully detects an evil-twin transmitter attack 90% of the time on an average, and estimates the locations of the two transmitters transmitting in the wireless network, with a high success rate of 74%. The algorithm also provides a maximum candidate area size of 11% of the simulation grid as the area where the transmitter can be found, with a confidence level of 95%. The evil-twin transmitter attack detection algorithm can be used independently without the localization algorithm, as well as in conjunction with any other

localization scheme besides HPB as well. The Section 7.1 detailed the major contributions of this work in the field of wireless network security and Section 7.2 provided an insight into the directions of future work that can be taken following our work.

Bibliography

[1] P. Bahl and V. N. Padmanabhan. RADAR: An In-building RF-based User Location and Tracking System. In *Proceedings of the Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM)*, volume 2, pages 775–784, March 2000.

[2] M. Barbeau, E. Kranakis, D. Krizanc, and P. Morin. Improving Distance Based Geographic Location Techniques in Sensor Networks. In *Ad-Hoc, Mobile, and Wireless Networks: Proceedings of the 3rd International Conference (ADHOC-NOW)*, volume 3158 of *Lecture Notes in Computer Science*, pages 197–210. Springer Berlin / Heidelberg, 2004.

[3] M. Barbeau and J. M. Robert. Rogue-Base Station Detection in WiMax/802.16 Wireless Access Networks. *Annals of Telecommunications*, 61(11-12):1300–1313, November-December 2006.

[4] K. Bauer, H. Gonzales, and D. McCoy. Mitigating Evil Twin Attacks in 802.11. In *IEEE International Performance, Computing and Communications Conference*, pages 513–516, December 2008.

[5] S. Brands and D. Chaum. Distance-Bounding Protocols. In *Advances in Cryptology: Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques*, volume 765 of *Lecture Notes in Computer Science*, pages 344–359. Springer Berlin / Heidelberg, 1994.

[6] E. D. Cardenas. MAC Spoofing - an Introduction, August 2003.

[7] Y. Chen, W. Trappe, and R. P. Martin. Detecting and Localizing Wireless Spoofing Attacks. In *Proceedings of the 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks*, pages 193–202, June 2007.

[8] M. Cooper. Antennas Get Smart. *Scientific American*, pages 49–55, July 2003.

[9] G. Durgin, T. Rappaport, and H. Xu. Measurements and Models for Radio Path Loss and Penetration Loss in and Around Homes and Trees at 5.85 GHz. *IEEE Transactions on Communications*, 46(11):1484–1496, November 1998.

[10] D. B. Faria and D. R. Cheriton. Detecting Identity-based Attacks in Wireless Networks Using Signalprints. In *Proceedings of the 5th ACM workshop on Wireless security (WiSec)*, pages 43–52, September 2006.

[11] H. T. Friis. A Note on a Simple Transmission Formula. *Proceedings of the I.R.E.*, 34(5):254–256, May 1946.

[12] H. Han, B. Sheng, C. C. Tan, Q. Li, and S. Lu. A Measurement Based Rogue AP Detection Scheme. In *Proceedings of the 19th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM)*, pages 1593–1601, April 2009.

[13] M. Hata. Empirical formula for propagation loss in land mobile radio services. *IEEE Transactions on Vehicular Technology*, 29(3):317–325, August 1980.

[14] T. He, C. Huang, B. M. Blum, J. A. Stankovic, and T. Abdelzaher. Range-free Localization Schemes for Large Scale Sensor Networks. In *Proceedings of the 9th Annual International Conference on Mobile Computing and Networking (MobiCom)*, pages 81–95, September 2003.

[15] K. C. Ho and Y. T. Chan. A Simple and Efficient Estimator for Hyperbolic Location. *IEEE Transactions on Signal Processing*, 42(8):1905–1915, August 1994.

[16] L. Hu and D. Evans. Localization for Mobile Sensor Networks. In *Proceedings of the 10th annual international conference on Mobile computing and networking (MOBICOM)*, pages 45–57, September-October 2004.

[17] Y.-C. Hu, A. Perrig, and D. B. Johnson. Wormhole Attacks in Wreless Networks. *IEEE Journal on Selected Areas in Communications*, 24(2):370–380, February 2006.

[18] A. M. Ladd, K. E. Bekris, A. Rudys, L. E. Kavraki, and D. S. Wallach. Robotics-Based Location Sensing Using Wireless Ethernet. *Wireless Networks*, 11(1–2):189–204, January 2005.

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

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

[21] A. R. R. League. *The ARRL Antenna Book*. American Radio Relay League, 21st edition, May 2007.

[22] 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, August 2007.

[23] L. C. Liechty, E. Reifsnider, and G. Durgin. Developing the Best 2.4 GHz Propagation Model from Active Network Measurements. In *Proceedings of the 66th IEEE Vehicular Technology Conference*, pages 894–896, September 2007.

[24] B. C. Liu, K. H. Lin, and J. C. Wu. Analysis of Hyperbolic and Circular Positioning Algorithms Using Stationary Signal-Strength Difference Measurements in Wireless Communications. *IEEE Transactions on Vehicular Technology*, 55(2):499–509, March 2006.

[25] C. Liu, K. Wu, and T. He. Sensor Localization with Ring Overlapping Based on Comparison of Received Signal Strength Indicator. In *Proceedings of the IEEE International Conference on Mobile Ad-hoc and Sensor Systems*, pages 516–518, October 2004.

[26] M. Miyashita, Y. Serizawa, and T. Terada. Model Selection Method for Improving Path Loss Prediction of 400 MHz Band Land Mobile Radio. In *Proceedings of the 62nd IEEE Vehicular Technology Conference*, volume 2, pages 1337–1341, September 2005.

[27] R. L. Moses, D. Krishnamurthy, and R. M. Patterson. A Self-Localization Method for Wireless Sensor Networks. *EURASIP Journal on Applied Signal Processing*, 2003(4):348–358, January 2003.

[28] M. Nakagami. The m-Distribution – A General Formula of Intensity Distribution of Rapid Fading. In W. C. Hoffman, editor, *Statistical Methods in Radio Wave Propagation*, pages 3–36. Pergamon Press, New York, 1960.

[29] Y. Okumura, E. Ohmori, T. Kawano, and K. Fukuda. Field Strength and its Variability in VHF and UHF Land-Mobile Radio Service. *Review of the Electrical Communication Laboratory*, 16(9-10):825–873, September-October 1968.

[30] A. Orebaugh, G. Ramirez, and J. Beale. *Wireshark & Ethereal Network Protocol Analyzer Toolkit*. Syngress Publishing, February 2007.

[31] S. Y. Park, H.-S. Ahn, and W. Yu. Round-trip time-based wireless positioning without time synchronization. In *International Conference on Control, Automation and Systems*, pages 2323–2326, October 2007.

[32] J. N. Randall. Foursquare Antenna Radiating Element, July 1999.

[33] T. S. Rappaport. *Wireless Communications: Principles and Practice*. Prentice-Hall, 2nd edition, January 2002.

[34] V. Roth, W. Polak, E. Rieffel, and T. Turner. Simple and Effective Defense Against Evil Twin Access Points. In *Proceedings of the 1st ACM conference on Wireless Network Security (WiSec)*, pages 220–235, April 2008.

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

[36] Y. Sheng, K. Tan, G. Chen, D. Kotz, and A. Campbell. Detecting 802.11 MAC Layer Spoofing Using Received Signal Strength. In *Proceedings of the 27th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM)*, pages 1768–1776, April 2008.

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

[38] A. Thaeler, X. Cheng, G. Xue, and D. Chen. TPS: A Time-Based Positioning Scheme for Outdoor Wireless Sensor Networks. In *Proceedings of the 23rd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM)*, volume 4, pages 2685–2696, March 2004.

[39] W. Wang and B. Bhargava. Visualization of Wormholes in Sensor Networks. In *Proceedings of the 3rd ACM workshop on Wireless Security(WiSec)*, pages 51–60, October 2004.

[40] W. Wei, K. Suh, B. Wang, Y. Gu, J. Kurose, and D. Towsley. Passive Online Rogue Access Point Detection Using Sequential Hypothesis Testing with TCP ACK-Pairs. In *Proceedings of the 7th ACM SIGCOMM Conference on Internet Measurement*, pages 365–378, October 2007.

[41] J. Wright. Detecting Wireless LAN MAC Address Spoofing, January 2003.

[42] J. Yang, Y. Chen, W. Trappe, and J. Cheng. Determining the Number of Attackers and Localizing Multiple Adversaries in Wireless Spoofing Attacks. In *Proceedings of the 28th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM)*, pages 666–674, April 2009.

[43] S. Zhong, L. Li, Y. G. Liu, and R. Yang. Privacy-Preserving Location-based Services for Mobile Users in Wireless Networks. Technical Report TR1297, Department of Computer Science, Yale University, July 2004.