Detecting and Localizing Transmitters in a Wireless Evil-Twin Attack *

Payal Bhatia, *Carleton University, Ottawa, ON, Canada*
Christine Laurendeau, *Carleton University, Ottawa, ON, Canada*
Michel Barbeau, *Carleton University, Ottawa, ON, Canada*

Abstract

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 describe an algorithm to detect such a wireless evil-twin attack, and locate the truth-teller and the evil-twin transmitter. Four-square antennas are used by the receivers to detect an attack. RSS values measured at the receivers are used by Hyperbolic Position Bounding (HPB) to locate the transmitters in the wireless network with a degree of confidence. The performance of the algorithm is tested using a simulation of a wireless network.

Keywords: Wireless Networks, Wireless Security, Location Estimation, Evil-Twin Transmitter Attack

1. Introduction

With the wireless technology on the boom, the types of attacks in the wireless networks are ever growing. This report is concerned with the wireless evil-twin transmitter attack, in which an attacker places an evil-twin transmitter in a wireless network. In order for a transmitter to be an evil-twin of an honest transmitter, the evil-twin needs to be sending messages using the same identity as the honest transmitter and at the same time as the honest transmitter. The attacker can have multiple reasons for launching this type of an attack. The evil-twin transmitter may be sending malicious packets with false information to the unsuspecting receivers in the wireless network. In a vehicular networks setting, the attacker can use the evil-twin transmitter to send incorrect traffic information to the vehicles in the network, thereby disrupting services. It may also be that both the transmitters in the network are malicious. The evil-twin transmitter may confuse the receivers about the actual location of the transmitters, only making it harder for the receivers to localize the transmitters correctly.

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. Sending messages synchronously with the other transmitter is another challenge in identifying that the network is under an evil-twin transmitter attack.

Our aim is to devise a way to find out whether a wireless network is under an evil-twin transmitter attack and if it is, to localize the honest as well as the evil-twin transmitter. As part of the solution, each receiver is equipped with a four-square antenna, which is a directional antenna and is capable of distinguishing signals received from different angles. If the whole area of the wireless network is assumed to be a square grid and is divided into n zones, then $(\sqrt{n}-1)^2$ receivers are placed in the grid as shown in Figure 4. Using the different directions in which each receiver gets the signals, the potential zones containing the transmitters are decided upon. If the receivers in the network are getting two signals from two different directions, or equivalently, two potential zones are detected, it is concluded that the system is under the evil-twin transmitter attack. Once an attack is detected, the next step is to localize the two transmitters. The Hyperbolic Position Bounding (HPB) algorithm [5] is used to probabilistically estimate the areas containing the two transmitters. In cases where the HPB algorithm fails to localize either of the transmitters, a fall back mechanism is used to estimate the areas in which the transmitters lie. The fall back mechanism returns the zone as the estimated location of the

*The authors gratefully acknowledge the financial support received for this research from the Natural Sciences and Engineering Research Council of Canada (NSERC).

transmitter.

The Section 2 of the report gives an overview of the related work in detection of evil-twin attacks and reviews some information on four-square antennas and HPB. Section 3 describes in detail our approach to detect an evil-twin transmitter attack and to localize the transmitters in case of an attack. Section 4 describes the metrics used to evaluate the performance of the algorithm and evaluates the algorithm against those metrics in a simulated environment. Section 5 concludes the report and provides some directions for future work.

2. Related Work

Work related to locating multiple adversaries in a wireless network has been done previously. Yang et. al. outline an algorithm for detecting spoofing attacks in a wireless network with multiple adversaries in [12] by using the K-means cluster algorithm as described in [1]. The work in [12] uses a similar scheme as [2], i.e. RSS fingerprints, to detect the spoofing attack. Sheng et. al. modeled RSS values gathered as a result of antenna diversity using a Gaussian mixture model for detecting spoofing attacks in [11]. The information received by various receivers is passed on to a central server to calculate a global metric to determine the spoofing attack. The paper uses the fact that different RSS values are produced if transmitters are present at different locations and uses this to determine if the system is under attack. Authors in [4] give a method for detecting a rogue access point from a legitimate access point. The work in [10] also provides a mechanism for defending against evil-twin access points, but it requires the access point to have a light capable of displaying two colours. The authors in [5] describe an algorithm to localize transmitters using HPB, which is also used by our algorithm to localize both transmitters.

An evil-twin attack is a further specialization of spoofing attacks in that an evil-twin not only masquerades the identity of an honest transmitter, but also transmits at the same time as the honest transmitter. Also, in spoofing attacks, at least one of the transmitters is considered to be a good node, and is thus cooperative. With the evil-twin transmitter attack, we are not making any assumptions about the $goodness$ of either of the transmitters. We assume that the Effective Isotropic Radiated Power (EIRPs) of the transmitters are unknown. The attack model in our work is not specific only to access points, it works for any wireless network with malicious transmitters. To the best of our knowledge, no work has been done previously to detect this type of an attack.

2..1 Background of HPB

The Hyperbolic Position Bounding (HPB) algorithm uses a large scale path loss model to estimate a range of distance differences. Hyperbolas computed at the maximum and minimum bounds of this range bound the transmitter with a degree of confidence [5]. The HPB algorithm shows the maximum and minimum hyperbolas computed between all transmitter-receiver pairs, and the transmitter lies in the area bounded by the intersection of all the hyperbola pairs. Figure 3 shows how HPB localizes a transmitter. The candidate area given by HPB in Figure 3 is about 11% of the grid. HPB assumes that the receivers do not know the Effective Isotropic Radiated Power (EIRP) of the transmitter. The signals received at the receivers' end have suffered some path loss or shadowing as demonstrated by Rappaport [9]. 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, a path loss $\overline{L}(d_0)$ at d_0 assuming free space propagation [3], 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 [7]. The following formula is used to calculate the path loss

$$L(d) = \overline{L}(d_0) + 10\eta log_{10}\frac{d}{d_0} + X_\sigma \tag{1}$$

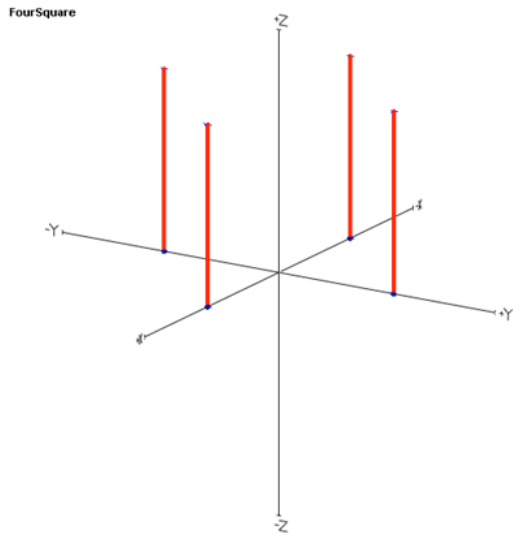

Figure 1: A four-square antenna.

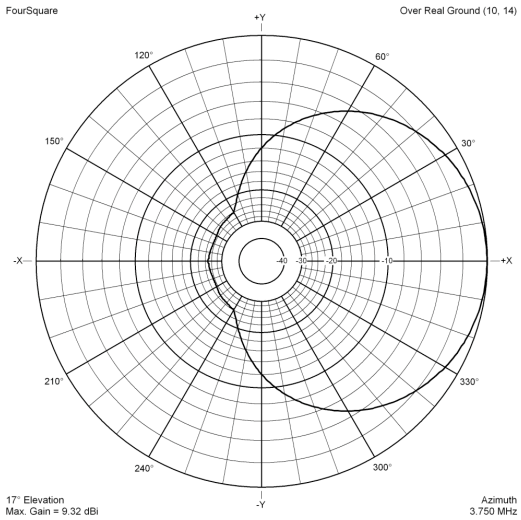

Figure 2: Radiation pattern of an element of the four-square antenna.

Since HPB was not designed to handle cases with two transmitters in the grid, we will do some computations before using HPB for our purpose.

2..2 Background of Directional Antennas

For this work, a directional antenna called the four-square antenna is used. Figure 1 shows the physical structure of the four-square antenna. The antenna has four different elements, each an antenna in itself. Figure 2 shows the radiation pattern for one element of the four-square antenna [6]. 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, and the direction of maximum gain is the direction of the incoming signal.

3. The Algorithm

In this section, a description of the algorithm is given. The scenario that is taken into consideration is a wireless network having some receivers and an honest transmitter. An attacker trying to launch an attack in this wireless network gains access to the network and adds a malicious transmitter to the network. The malicious transmitter avoids detection by using the same MAC address as the honest transmitter and by sending signals at the same time as the honest transmitter. The malicious transmitter is called the *evil-twin* of the honest transmitter. Since HPB wasn't meant to handle the evil twin attack, we do some computation before using HPB for identifying the location of the transmitters.

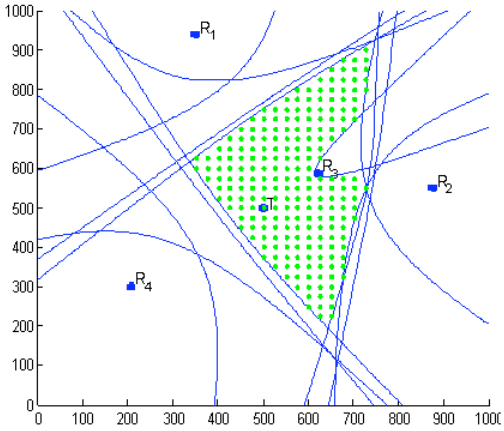

Figure 3: HPB with one transmitter.

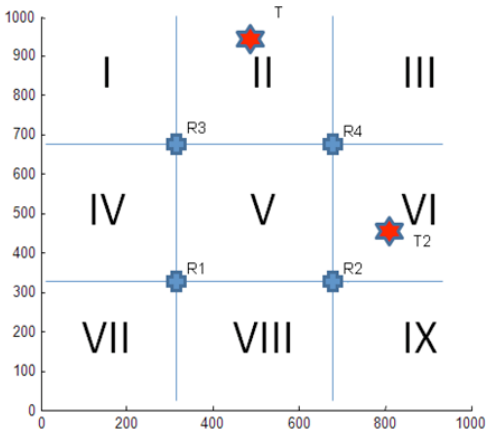

Figure 4: The area is divided into 9 zones and the 4 receivers are placed at the innermost corners.

3..1 Identifying the Attack

As part of the solution, each receiver in the network is equipped with a four-square directional antenna. As previously mentioned, the four-square antenna is capable of detecting what direction the signal is being received from. We assume that each of the transmitters (honest 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:

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

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. Each of the receivers is equipped with a four-square antenna. This means that the receiver is able to figure out 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 in 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 essentially 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, designated first, second, third, and fourth, counting counterclockwise from the area in which both coordinates are positive. For example, in Figure 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. Alternatively, if receiver R_3 receives a signal from sector 4, the transmitter can potentially lie in zones V, VI, VIII and IX. Therefore, 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. Also, if either of the RSS values is beyond the sensitivity level of the receiver, it is not registered.

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 belongs to one transmitter. With the information about sectors, the receivers calculate 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 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

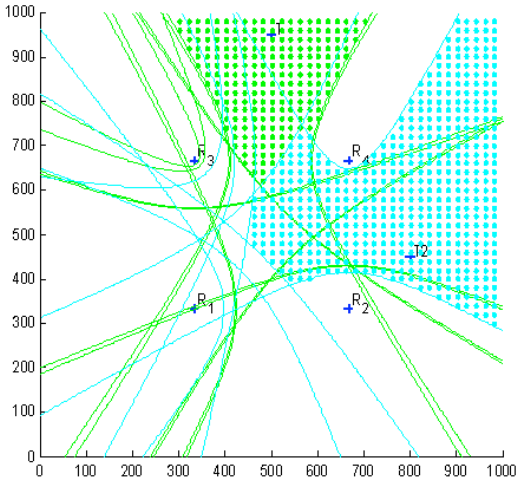

Figure 5: Candidate Areas with HPB.

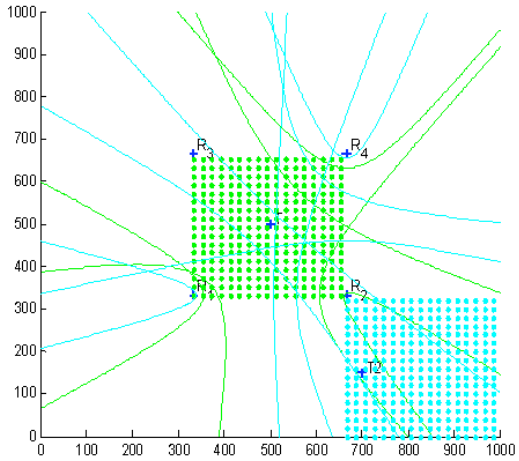

Figure 6: Candidate Areas with Fallback.

the zones common to all receivers.

$$\Omega = \bigcap_{i=1}^{m} Z_i \tag{3}$$

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.

The Algorithm 1 describes the steps for identifying an attack. The RSS and $sector$ values are recorded by each receiver. Then, each receiver calculates its $PotentialZone$, which is a set of Zones where the transmitter(s) may lie for the receiver to receive in the manner it does. The $PotentialZone$ set is calculated using the $sector$ or reception of signal and the coordinates of the zones. An intersection of all $PotentialZone$ 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.

3..2 Localizing the Transmitters

After an attack in the network is detected, we also need to locate the two transmitters. The set Ω calculated from Equation (3) 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 [5].

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. Our algorithm provides a fallback mechanism to calculate the area in case HPB fails. Since we have a zone already calculated for the presence of the transmitter, we use that zone as the estimated candidate area as the location of the grid. The area size is $1/n^{th}$ the size of

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 Zone 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

the whole grid, where n is the number of zones in the grid. For our purposes $n = 9$, therefore, the fallback mechanism gives us a candidate area of size 11% for each transmitter. Figure 5 shows a case where HPB is able to localize both transmitters after an attack has been detected. Figure 6 shows a case where the fallback mechanism is used to localize the transmitters after HPB has failed.

The Algorithm 2 describes the steps for localizing the transmitters. 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 [5]. If the HPB fails to give a candidate area, then the fallback mechanism $coordinates$ is used, and that returns the coordinates of the zone the transmitter lies in, as the candidate area.

Algorithm 2 $Localize\_Transmitters$

Calculate $RSSPool1$, $RSSPool2$
//$RSSPool(1)$ and $RSSPool(2)$ are calculated based on the two zones in Ω
for $i = 1$ to $\mid \Omega \mid$ **do**
  $candidateAreaCoordinates(i) = HPB(RSSPool(i))$
  //HPB(RSS) method calculates the coordinates of the candidate area based on the RSS pool
  if $candidateAreaCoordinates(i) == \phi$ **then**
    $candidateAreaCoordinates(i) = coordinates(\Omega(j))$
    //coordinates(zone) gives the coordinates of the zone where one transmitter lies
  end if
end for
return $(candidateAreaCoordinates)$

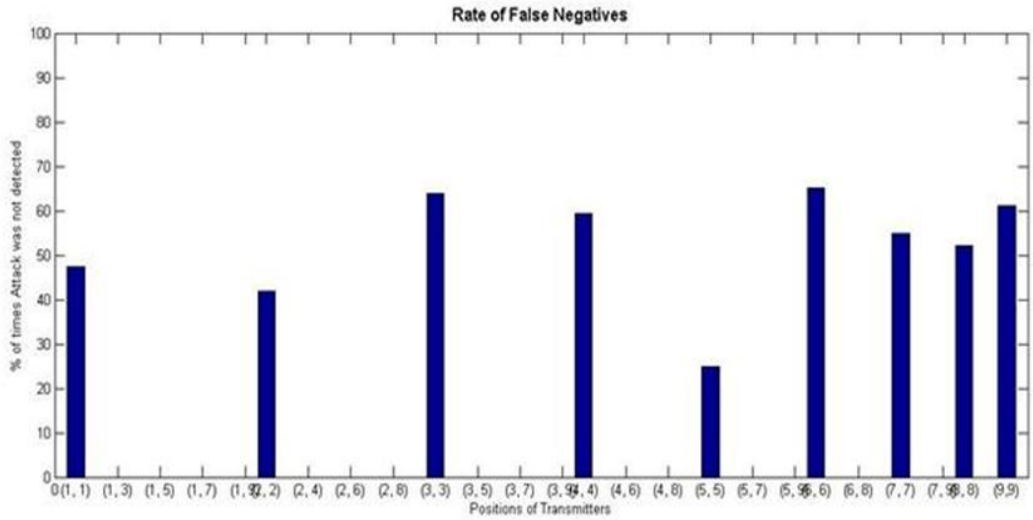

Figure 7: Rate of False Negatives.

4. Evaluation and Results

The algorithm is evaluated by simulating random locations of the malicious transmitter and honest transmitter in a 1000 x 1000 m^2 grid such that all zones are tested. Therefore, there are 45 possible combinations in which the two transmitters can be placed in the zones. The whole area is divided into 9 equal sized zones. The scenario assumes 4 receivers in a wireless network, 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 [7], [8] at 2.4 GHz and also used in [5]. 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 generates a random amount of signal shadowing along a 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 as shown in Equation (1). The dynamic range of the receivers is chosen to be 20 dB and the sensitivity of the receivers is chosen to be -83 dBm. In the Attack Detection and Localization Phase, the algorithm detects an evil-twin transmitter attack and then tries to localize the transmitters using the RSS values generated at each receiver, without knowledge of the EIRP or gain.

The performance of the algorithm 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.

Figure 7 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. Clearly, 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 about 47% and the rate of true positives is about 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 none of the transmitters are correctly localized. Both the transmitters are correctly localized 62% of the time and at least one of the transmitters is correctly localized 83% of the time. The algorithm calculates the correct zones for both

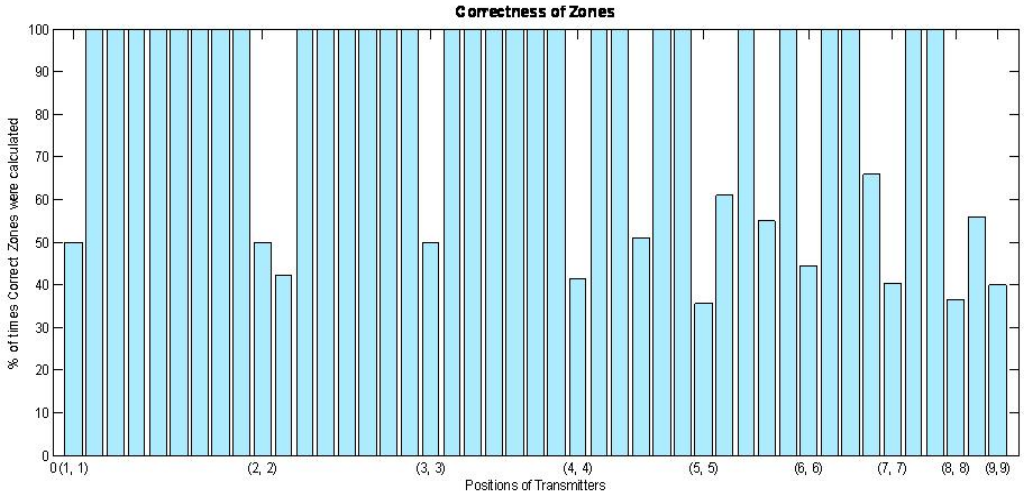

Figure 8: Correctness of Zones.

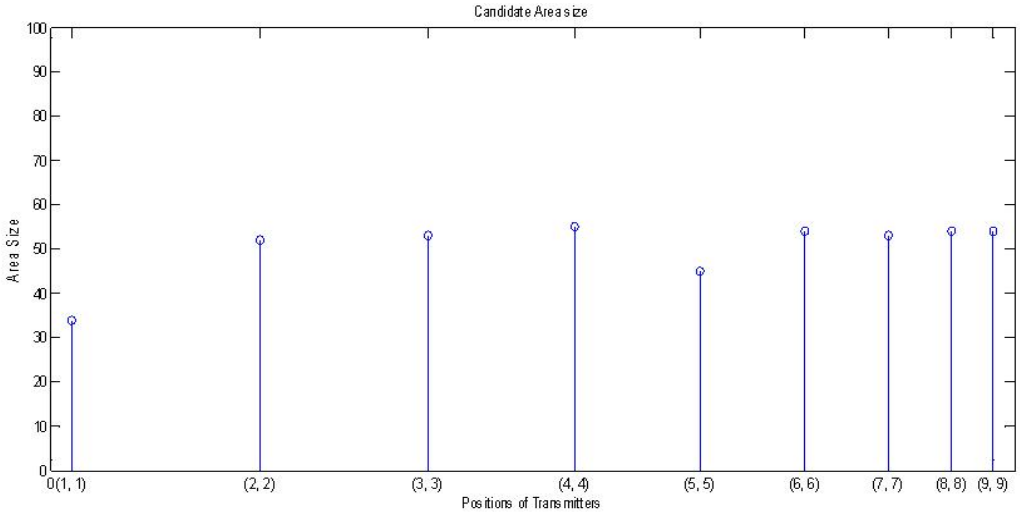

Figure 9: Candidate Areas When Transmitters are in Same Zone.

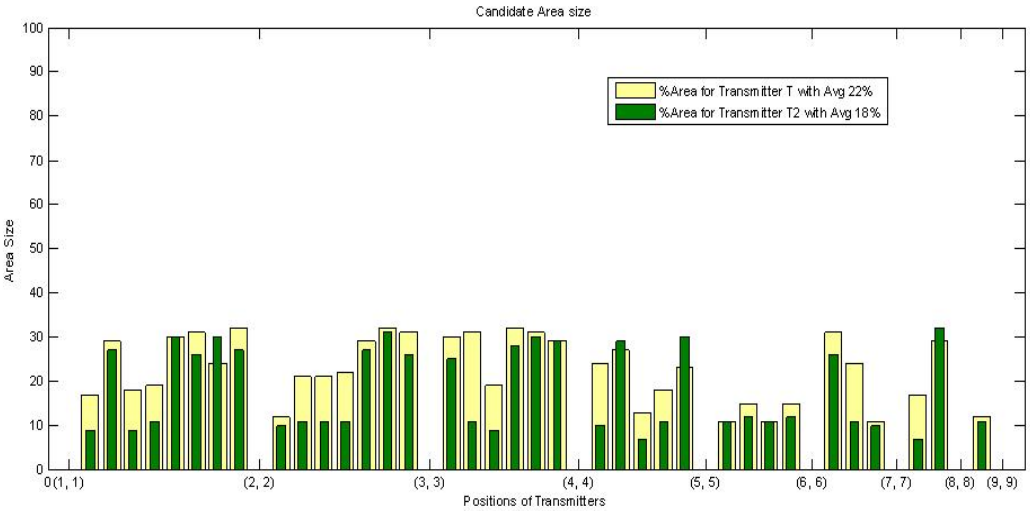

Figure 10: Candidate Areas When Transmitters are in Different Zones.

the transmitters 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 8 shows the correctness of zones as a function of the positions of the two transmitters.

In terms of the candidate area size, Figure 9 gives the Average Percentage Area for both transmitters when both transmitters are located in the same zone. The average area in this case is 50%, and is not very informative of the location of the transmitters. For all the other cases, 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 10. In cases where the fallback mechanism is used to localize the transmitter, the area returned is the area of the zone, which is about 11% or $1/9^{th}$ of the area of the whole grid. The average areas are calculated only over the cases in which an attack is detected by the algorithm.

5. Conclusion

We described an algorithm for detecting the evil-twin transmitter attack in a wireless network using a four-square antenna on each receiver. The EIRP of the transmitters are unknown. The RSS values received at each of the receivers are calculated. 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 performance of the algorithm is assessed with the simulation.

The algorithm is able to detect an attack for 100% of the times when the transmitters are present in different zones, but detects only 53% of the attacks in cases where the transmitters are present in the same zone. In terms of success rate of localizing the transmitters, about 77% of the times the transmitters are correctly localized. The average candidate area size also differs in cases where transmitters are in the same zone, as opposedz 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%.

This algorithm successfully detects an evil-twin transmitter attack, and estimates the locations of the two transmitters transmitting at unknown EIRPs, with a high success rate and about $1/5^{th}$ size of the grid as the candidate area. The average candidate area returned by this method is also an improvement in the candidate area given by HPB with a confidence level of 95%.

References

[1] 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.

[2] 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.

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

[4] 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.

[5] C. Laurendeau and M. Barbeau. Insider Attack Attribution Using Signal Strength-based Hyperbolic Location Estimation. *Security and Communication Networks*, July-August 2008.

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

[7] 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.

[8] 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.

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

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

[11] 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.

[12] 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.