Malicious Node Position Bounding in Mobile WiFi/802.11 Networks

Christine Laurendeau and Michel Barbeau
School of Computer Science, Carleton University
1125 Colonel By Drive, Ottawa, ON Canada K1S 5B6
Tel: 613-520-2600; Fax: 613-520-4334
E-mail: {claurend,barbeau}@scs.carleton.ca

***Abstract*—Hyperbolic position bounding (HPB) provides a mechanism to probabilistically delimit the location of a wireless network malicious insider to a candidate area. A large scale path loss model is used to construct a probable distance difference range between a rogue transmitter and a pair of trusted receivers. Hyperbolas are constructed at the minimum and maximum bounds of this range to delineate the position of a rogue with a given confidence level. We describe an outdoor experiment with a WiFi/802.11 network. Measured received signal strength (RSS) values, as well as path loss parameters obtained from signal propagation losses, are used by HPB to bound the location of a mobile transmitter within the WiFi/802.11 network with a degree of confidence. Experimental results are compared against prior simulation results and found to be consistent.**

***Index Terms*—Insider Attacks, Location Estimation, Mobile Networks, WiFi/802.11 Networks, Wireless Networks, Wireless Security**

I. Introduction

Wireless mobile networks are on the cusp of actualizing revolutionary advances in many areas, including public safety and health care. Vehicular communications, for example, can convey real-time, life-preserving notifications of impending collisions and other hazards, and thus reduce the daily carnage on our roads. Implantable medical devices can regulate heart rhythm and automatically inject drugs into cardiac patients based on dynamic sensor readings. Consequently, attacks upon such networks can have dire consequences, possibly resulting in loss of life. The remote manipulation of tram system control signals by a young hacker in Poland nearly resulted in disastrous consequences for the passengers of several trains [1]. Researchers have demonstrated that implantable cardioverter defibrillator devices are vulnerable to reprogramming and denial of service attacks [2]. To bolster public faith in mobile networks and ensure that these don't fall prey to unscrupulous attackers from within and without, security mechanisms must be put in place for attack prevention. Yet the majority of them focus on protecting wireless networks solely from outsider attacks, even though network insiders, as authorized nodes entrusted with valid credentials, can thwart most security measures. A survey conducted by CSO Magazine, the U.S. Secret Service and CERT reports that over 40% of the attributable security breaches uncovered were committed by malicious insiders [3]. Because of these attackers' privileged position in the network, the mitigation of their exploits poses a far more formidable challenge.

In [4], we propose a hyperbolic position bounding (HPB) mechanism to pinpoint the probable location of a malicious node to a candidate area, with a degree of confidence. Our threat model assumes that a rogue insider, in possession of valid credentials such as an authorized MAC address or digital certificate, broadcasts an attack message providing falsified information, for example an erroneous position report in vehicular networks or a tampered sensor reading input to an implantable medical device. Credentials which are forged or stolen may be untraceable to an attacker's real identity. An important first step in apprehending a malicious insider and containing the impact of subsequent attacks lies in determining the physical location of the signal source at the time of the exploit. A mobile attacker's whereabouts may thus be tracked as it continues broadcasting. Because little is known about the rogue insider and the radio equipment used in an attack, no assumptions can be made regarding cooperation with localization efforts or the effective isotropic radiated power (EIRP) of a broadcast transmission. An attack message is simultaneously received at a number of trusted nodes with globally known coordinates. These receivers can communicate with each other over a secure channel in order to aggregate relative received signal strength (RSS) values. Using a large scale radio signal path loss model to estimate transmitter-receiver (T-R) distances, each pair of receivers computes its probable distance difference range to a rogue transmitter. Hyperbolas are defined at the minimum and maximum bounds of the distance difference range. A rogue transmitter is located in the hyperbolic area between the minimum and maximum hyperbolas with a degree of confidence. With multiple receiver pairs, a hyperbolic area is computed for each possible pair, and the rogue is deemed to lie in the intersection of all hyperbolic areas with a confidence level aggregated according to the compound probability scheme put forth in [5]. The HPB mechanism is executed with simulated RSS values, and its performance is evaluated according to two metrics: the success rate in correctly bounding the position of a transmitter to a candidate area consisting of the intersection of all computed hyperbolic areas; and the size of the candidate area as a percentage of the total simulation grid size.

We follow up the work in [4] with an evaluation of the HPB mechanism using measured, rather than simulated, RSS values. We describe an outdoor experiment conducted to harvest RSS values from a WiFi/802.11 network. A mobile laptop is used as a rogue transmitter as it moves through five separate locations. Packets are broadcast from each transmitter location and received by four monitoring desktops. The packets' RSS values are recorded at each receiver, as is the T-R distance. The HPB algorithm is executed for each packet received by all four desktop monitors. The experimental results are evaluated along the same metrics as the simulation results, and the two are compared.

Section II outlines existing work in location estimation. Section III presents the HPB algorithm and its performance evaluation using simulated RSS values. Section IV describes the outdoor experiment with a WiFi/802.11 network, evaluates HPB with measured RSS values and compares the experimental and simulation results. Section V discusses the suitability of HPB for tracking a mobile attacker. Section VI concludes the paper.

II. Related Work

Existing localization schemes are largely predicated upon a number of restrictive assumptions regarding the target node being localized, as illustrated in Table I.

TABLE I
Localization Scheme Assumptions

Scheme	Special Hardware	Local Knowledge	Cooperation	EIRP Knowledge
Triangulation	directional rec. antenna	none	none	none
Time-based [6]–[8]	acc. CPU, synch. clocks	none	round-trip response	none
Sig.-based [9]–[12]	none	signal profiles	none	training phase EIRP
Relative RSS [13], [14]	none	none	none	same as other nodes
RSS ring-based [15], [16]	none	distance to ref. point	none	must be known
HPB [4]	none	none	none	none

Triangulation, for example, requires a directional antenna at the receiver to detect the source direction of an inbound signal. Such specialized hardware poses an additional burden on network deployment costs.

Time-based mechanisms, where T-R distances are estimated from Time-of-Arrival (TOA) round-trip beacons, include the location verification methods put forth by Brands and Chaum [6], Sastry *et al.* [7] and Waters and Felten [8]. These schemes make a number of assumptions that are unsuitable for our threat model. They require the availability of accelerated processors at both the transmitter and receiver to factor out the relatively large processing delays compared with the beacon's time of flight. They assume that the clocks at each node feature nanosecond precision and are synchronized with each other. They also require the cooperation of the target node, since the round-trip beacon must be returned.

Signature-based localization schemes using RSS values necessitate the compilation of a training set of signalprints in advance of the position estimation efforts, as described by Bahl and Padmanabhan [9], Faria and Cheriton [10], Ladd *et al.* [11] and Roos *et al.* [12]. These methods have been used solely in indoor scenarios where typically few environmental variations occur.

With relative RSS localization mechanisms, such as the ones described by He *et al.* [13] and Chong Liu *et al.* [14], a node seeking to learn its position compares the RSS values it receives from trusted anchors. While this scheme may possibly be reversed to have an anchor localize a node without its cooperation by comparing the target node's RSS with that of other anchors, this method assumes that all transmitter EIRPs are equal.

RSS variations are taken into account by Barbeau and Robert [15] and Bo-Chieh Liu *et al.* [16] to construct a minimum and maximum distance annulus between a transmitter and a receiver. The latter scheme requires a known distance to at least one other node. Both mechanisms assume a known EIRP, which is inconsistent with our threat model.

III. Hyperbolic Position Bounding

We describe how the HPB algorithm uses a large scale path loss propagation model to estimate a probable range of distance differences between a transmitter and a pair of receivers. Hyperbolas computed at the minimum and maximum bounds of this range bound the transmitter position with a degree of confidence. We outline the simulation scenario employed in [4] and present the results in terms of success rate and candidate area size.

A. Location Estimation Algorithm

Radio signals attenuate as they travel through the air between a transmitter and a receiver, so that for a fixed distance and EIRP, the signal loss between the EIRP and RSS values fluctuate around a mean loss in a predictable fashion. Rappaport [17] demonstrates that the path loss variations, or *shadowing*, follow a Normal probability distribution. Rappaport's *log-normal shadowing model* predicts the amount of path loss at a given T-R 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 [18], a path loss exponent n dependent upon the propagation environment, and a random amount of signal shadowing with mean zero and standard deviation σ. The path loss parameters in the log-normal shadowing model, n and σ, are measurable through experimental results, for example in [19] and [20]. Linear regression techniques are used to ascertain values of n and σ from actual path loss measurements.

Barbeau and Robert [15] broaden the applicability of the log-normal shadowing model to compute probable minimum and maximum T-R distances, based on the minimum and maximum bounds of the signal shadowing interval associated with a given level of confidence. These minimum and maximum distances are used to construct an annulus around a receiver,

in order to estimate the location of a transmitter within the annulus with a degree of confidence.

In [4], we extend Barbeau and Robert's algorithm to consider a range of possible EIRP values, as required by our threat model. We define the minimum and maximum bounds of the distance range between a transmitter and a receiver R_k as d_k^- and d_k^+ respectively, using an estimated EIRP interval [$\mathcal{P}^-$, $\mathcal{P}^+$], a RSS value RSS_k, and the minimum and maximum bounds of the signal shadowing range $[-z\sigma, +z\sigma]$ associated with a desired level of confidence. The value of z is the Normal distribution constant corresponding to confidence $\mathcal{C}$, where z equals $\Phi^{-1}(\frac{1+\mathcal{C}}{2})$ and can be obtained from a Normal distribution table. The value of σ is the standard deviation of the signal shadowing.

Lemma 1. *The minimum and maximum distances, d_k^- and d_k^+ respectively, between transmitter T and receiver R_k, sent within an estimated EIRP interval [$\mathcal{P}^-$, $\mathcal{P}^+$], can be computed with confidence level $\mathcal{C}$ as:*

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

Alternately, we say that the probability that transmitter T is located in the area bounded by $[d_k^-, d_k^+]$ is $\mathcal{C}$:

$$Pr(d_k^- \leq T \leq d_k^+) = \mathcal{C}$$

Proof: The proof can be found in [4]. ∎

Multiple annuli may be computed around several receivers, and the location of the transmitter can be estimated within the annuli intersection. This approach is more successful when the difference between minimum and maximum distances is not significant. With the introduction of an EIRP range, the annuli may be so wide that their intersection is too large to effectively locate the transmitter, even if multiple receivers are considered.

The HPB mechanism therefore exploits the geometric properties of hyperbolas, where every point on a curve is at an equal distance difference of two foci. In our approach, a pair of receivers computes their probable distance difference range to a transmitter. Hyperbolas associated with the minimum and maximum bounds of this range are constructed with the receiver pair as the foci.

Theorem 1. *Let d_i and d_j be the unknown distances between a transmitter T and receivers R_i and R_j respectively.*

1. *The minimum bound $\Delta d_{i,j}^-$ of the distance difference range between d_i and d_j, with confidence level $\mathcal{C}$, is the distance difference at the minimal EIRP ($\mathcal{P}^-$) over the full signal shadowing range $[-z\sigma, +z\sigma]$.*

$$\Delta d_{i,j}^- = \left(d_0 \times 10^{\frac{\mathcal{P}^- - RSS_i - \overline{L}(d_0) - z\sigma}{10n}}\right) - \left(d_0 \times 10^{\frac{\mathcal{P}^- - RSS_j - \overline{L}(d_0) + z\sigma}{10n}}\right)$$

2. *The maximum bound $\Delta d_{i,j}^+$ of the distance difference range between d_i and d_j, with confidence level $\mathcal{C}$, is the distance difference at the maximal EIRP ($\mathcal{P}^+$) over the full signal shadowing range $[+z\sigma, -z\sigma]$.*

$$\Delta d_{i,j}^+ = \left(d_0 \times 10^{\frac{\mathcal{P}^+ - RSS_i - \overline{L}(d_0) + z\sigma}{10n}}\right) - \left(d_0 \times 10^{\frac{\mathcal{P}^+ - RSS_j - \overline{L}(d_0) - z\sigma}{10n}}\right)$$

Proof: The proof can be found in [4]. ∎

The minimum and maximum hyperbolas between a pair of receivers can be constructed from the bounds of the distance difference range defined in Theorem 1. The transmitter is located in the resulting hyperbolic area with confidence $\mathcal{C}$.

Theorem 2. *Let a transmitter T be located at unknown coordinates (x, y) and a pair of receivers R_i, R_j at known coordinates (x_i, y_i) and (x_j, y_j) respectively. Let $\Delta d_{i,j}^-$ and $\Delta d_{i,j}^+$ be defined as the minimum and maximum bounds, respectively, of the distance difference range between R_i and R_j with confidence level $\mathcal{C}$. Let $\mathcal{H}_{i,j}^-$ be the hyperbola representing the minimum bound of the distance difference range between R_i and R_j, as defined by equation $\sqrt{(x-x_i)^2+(y-y_i)^2} - \sqrt{(x-x_j)^2+(y-y_j)^2} = \Delta d_{i,j}^-$. Let $\mathcal{H}_{i,j}^+$ be the hyperbola representing the maximum bound of the distance difference range between R_i and R_j, as defined by equation $\sqrt{(x-x_i)^2+(y-y_i)^2} - \sqrt{(x-x_j)^2+(y-y_j)^2} = \Delta d_{i,j}^+$.*

A transmitter T is located in the area $\mathcal{A}_{i,j}$ between the hyperbolas $\mathcal{H}_{i,j}^-$ and $\mathcal{H}_{i,j}^+$ with confidence level $\mathcal{C}$. Alternately, we say that $Pr(T \in \mathcal{A}_{i,j}) = \mathcal{C}$ and $Pr(T \in \overline{\mathcal{A}}_{i,j}) = (1-\mathcal{C})$, where $\overline{\mathcal{A}}_{i,j}$ is the complement of $\mathcal{A}_{i,j}$.

Proof: The proof can be found in [4]. ∎

B. Simulation Results

The HPB mechanism is evaluated by simulating the location of a rogue transmitter at 100-meter intervals along the X and Y axes of a 1000 × 1000 m^2 grid, as depicted in Figure 1. Our simulation scenario features four receivers, and thus six possible receiver pairs, executing the HPB algorithm 1000 times for each transmitter location, for each of four confidence levels $\mathcal{C} = \{0.95, 0.90, 0.85, 0.80\}$. The simulation assumes a frequency of 2.4 GHz, consistent with WiFi/802.11 networks. The path loss parameters n and σ are taken from experiments conducted by Liechty *et al.* [19], [21] for this frequency. RSS values are simulated at each receiver, using the log-normal shadowing model. For each HPB execution, every receiver generates a random amount of signal shadowing along a Normal distribution curve with mean zero and standard deviation σ. The shadowing is added to the receiver simulated RSS value. The EIRP range is determined dynamically by taking the receiver with the highest RSS as a reference point and assuming it is the closest receiver to the transmitter location. The EIRP range is set to the intersection of the EIRP ranges required for each remaining receiver to reach the reference point.

The candidate area determined by HPB as the probable location of the transmitter consists of the intersection of the hyperbolic areas computed by every possible receiver pair

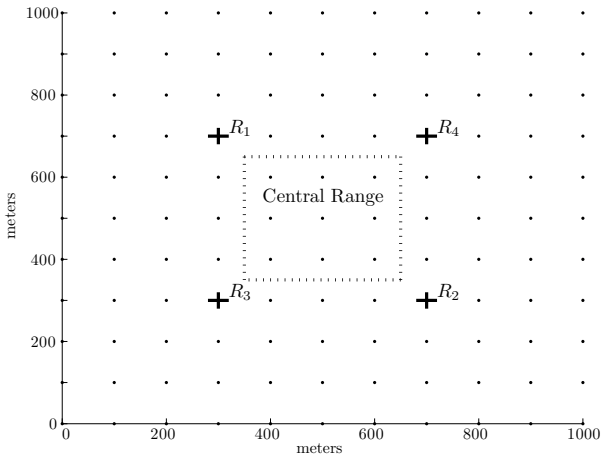

Fig. 1. Simulation Grid

using Theorem 2. An example illustrating a likely candidate area can be found in [4]. The performance of HPB is evaluated along two metrics: the success rate and candidate area size.

The success rate reflects the percentage of HPB executions for which the transmitter is located in the candidate area. We define the *central range* points, shown in Figure 1, as the points located in the area between all four receivers. In our simulation results, we find that the success rate in the central range is commensurate with the confidence level. So for $\mathcal{C} = 0.95$, the success rate in the central range is 94%; for $\mathcal{C} = 0.90$, it is 86%; for $\mathcal{C} = 0.85$, it is 76%; and for $\mathcal{C} = 0.80$, it is 67%. The decrease in success rate with the confidence level reflects the narrowing of the shadowing interval due to the reduced value of the Normal distribution constant z. As less signal shadowing is taken into account, larger intervals of shadowing are ignored which may be associated with the actual transmitter location.

The candidate area size within the central range comprises 27% of the total simulation grid for $\mathcal{C} = 0.95$, 21% of the grid for $\mathcal{C} = 0.90$, 16% for $\mathcal{C} = 0.85$, and 12% for $\mathcal{C} = 0.80$. Again, the reduced area size for a decreasing confidence level is due to a smaller shadowing interval, resulting in smaller hyperbolic areas whose intersection is correspondingly smaller.

IV. Outdoor Experiment

In order to validate our simulation results and further evaluate the HPB algorithm's suitability for localizing a rogue transmitter, we describe an outdoor experiment involving five WiFi/802.11 devices, as outlined in [22]. We report on the path loss parameters computed from measured signal losses and assess them against Liechty's results for WiFi/802.11 networks [21]. We evaluate the performance of HPB using experimental RSS values. We assess the usability of the annuli method by comparing its localization performance with that of HPB. We compare the performance of HPB on the experimental RSS values with the prior simulation results.

A. Configuration

In order to facilitate a direct comparison between the experimental results and the simulation described in Section III-B, the experiment is configured to closely model the simulation scenario. It thus comprises one transmitter and four receivers.

We set up four fixed desktop receivers, labeled R_1 through R_4 in Figure 2, each equipped with a Trendnet network interface card, enabling access to the RSS values of received packets. A laptop is configured as a mobile transmitter, broadcasting packets with a transmitting power of 17 dBm using an antenna with a 7 dBi gain. Given that each receiver is also equipped with a 7 dBi gain antenna, the total EIRP is 31 dBm. The transmitter broadcasts from five separate locations, labeled T_1 through T_5 in Figure 2. The distances from the transmitter locations to each receiver are recorded in order to plot the path loss parameters. The transmitter antenna is situated at 1.5 m above the ground and the receiver antennas at 2.5 m.

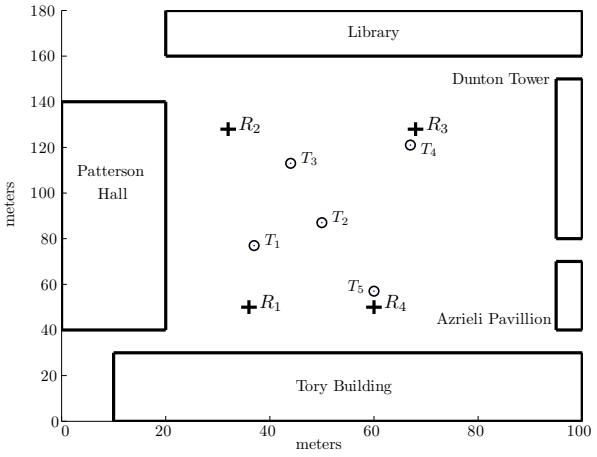

Fig. 2. Experimental Grid

To analyze the experimental results against the simulation results, we require both grids to be comparable in size with respect to the area of the central range. In the simulation scenario, the central range constitutes 16% of the simulation grid area. We therefore set the experimental grid to be 100 $\times$ 180 m^2, so that its central range between the four receivers also comprises 16% of the total area.

All the packets simultaneously received by the four desktop monitors are separated into two equal-sized groups. The first group is used to compute the path loss parameters for our experiment in Section IV-B. The second group is input to HPB for localization of each packet's originating position in Section IV-C.

B. Path Loss Parameters

Our experiment varies slightly from Liechty's previous work at the 2.4 GHz frequency because of the shorter T-R distances used. While our scenario involves a 100 $\times$ 180 m^2 grid, Liechty employed a larger 500 $\times$ 600 m^2 test area.

We compute the path loss exponent n and signal shadowing standard deviation σ for our experiment and compare our values with those in [21].

The path loss for each packet, as the difference between the EIRP and RSS, is plotted in Figure 3 as a function of the logarithm of the T-R distance. We find that the best-fit path loss exponent n equals 1.67 (depicted as a dashed line). The standard deviation associated with this value of n is $\sigma = 3.49$. Liechty's results yielded $n = 2.76$ and $\sigma = 5.62$. Although a path loss exponent of $n = 2$ is typically associated with free space propagation, lower values for n have been obtained in experiments at short distances close to 100 meters [23]. Given that all the T-R distances in our experiment are below 80 meters, our findings are consistent with previous research. A smaller shadowing standard deviation is also consistent with shorter T-R distances.

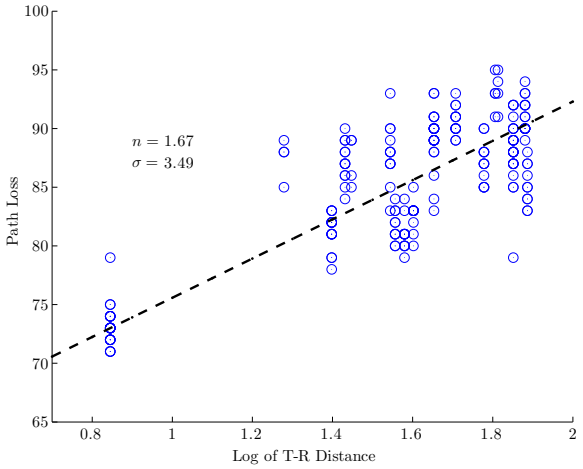

Fig. 3. Path Loss Parameters

C. HPB Experimental Results

The HPB success rate for every transmitter location in our experiment is computed for each of four confidence levels $\mathcal{C} = \{0.95, 0.90, 0.85, 0.80\}$. For $\mathcal{C} = 0.95$, 96% of HPB executions are successful; for $\mathcal{C} = 0.90$, the success rate is 89%; for $\mathcal{C} = 0.85$, it is 76%; and for $\mathcal{C} = 0.80$, it is 72%. Overall, the HPB success rate maps very closely to the corresponding confidence level.

The success rates at individual transmitter locations, for confidence level $\mathcal{C} = 0.95$, are illustrated in Figure 4. While success rates are quite high on the outer edges of the experimental grid, the successful localization of the middle transmitter position T_2 may suffer slightly from a large number of reflected packets, as it was within range of surrounding campus buildings on all four sides. For example, with transmitter location T_5, packets reflected off the Tory Building, positioned as shown in Figure 2, may be out of range for receivers R_2 and R_3 and not be measured. Since packets not received by all four monitors are unusable for our threat scenario, they are omitted from our evaluation. In contrast, packets originating from T_2 may be reflected from all surrounding buildings and received by all four monitors, but at RSS values that are not commensurate with T_2's relative distance to each receiver. Consequently, the success rate for transmitter location T_2 may have been affected.

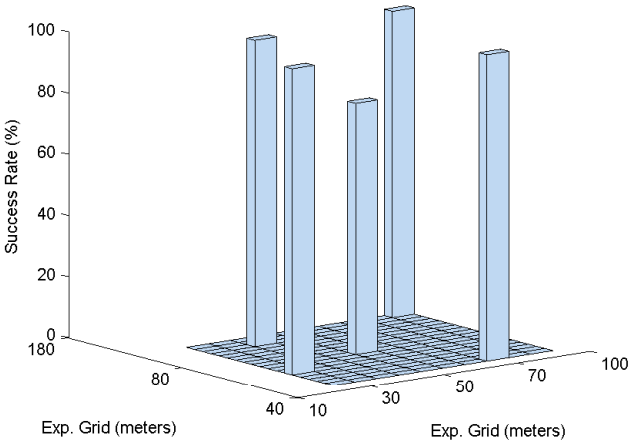

Fig. 4. HPB Experimental Results Success Rate for $\mathcal{C} = 0.95$

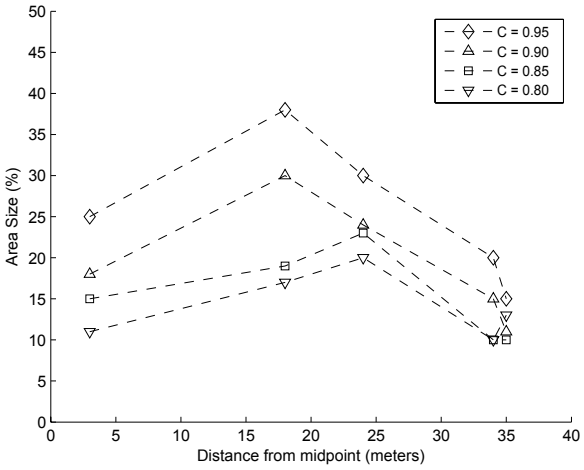

Fig. 5. HPB Experimental Results Candidate Area Size

Experimental results for candidate area sizes, given the four confidence levels, are found in Figure 5 and are deemed accurate with $\pm$ 4% within a 90% confidence interval. As with the simulation results outlined in Section III-B, the intersection of hyperbolic areas decreases in size as the confidence level drops, due to lower values of z, and thus smaller hyperbolic areas. Candidate area sizes also tend to decrease with the distance from the middle of the experimental grid, because a higher percentage of a centrally located area necessarily lies within the grid. Peripheral candidate areas are truncated at the edges of the grid and thus reflect a smaller percentage of the overall grid area.

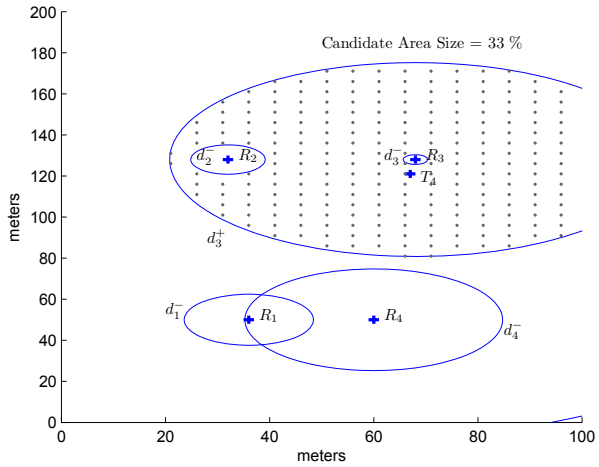

Fig. 6. Example of Intersecting Annuli for T_4

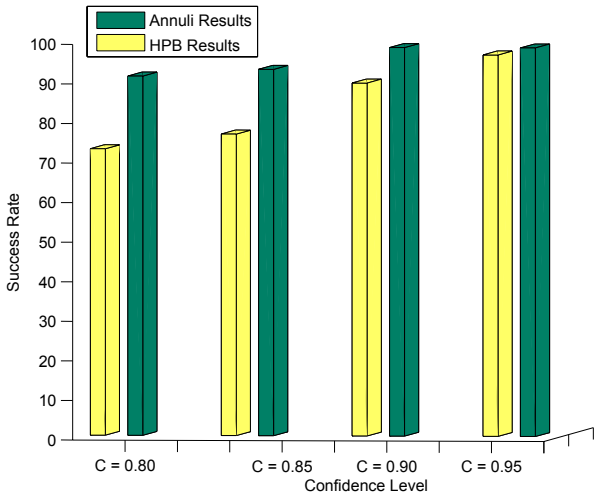

Fig. 8. HPB vs. Annuli Method Success Rate

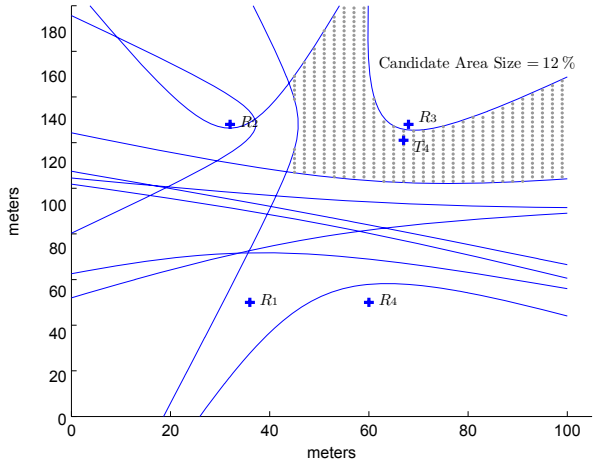

Fig. 7. Example of HPB Candidate Area for T_4

D. HPB vs. Annuli Method Experimental Results

With the annuli method described in Section III, the candidate area comprises the intersection of the minimum and maximum distance annuli around all the receivers, computed using Lemma 1. However, as previously observed, this candidate area may be too large to suitably pinpoint the location of a rogue transmitter. We use our experimental scenario and measured RSS values to examine the relative performance of the annuli method and HPB.

For example, Figure 6 illustrates the minimum and maximum distances, d_k^- and d_k^+ respectively, from each receiver R_k to the transmitter, computed using Lemma 1. The reference distance d_0 is set to seven meters, in keeping with the reference distance used for the experiment. The dynamic EIRP range is set to $\mathcal{P}^-$ equals 30 dBm and $\mathcal{P}^+$ equals 38 dBm. The RSS values measured at each receiver R_1 to R_4 are -54 dBm, -50 dBm, -42 dBm and -59 dBm, respectively. The loss at d_0 measured in the experiment equals 73 dB. The path loss parameters $n = 1.67$ and $\sigma = 3.49$ are determined in Section IV-B. The transmitter is located within each annulus with confidence level $\mathcal{C} = 0.95$, and so the associated normal distribution constant z equals 1.96. The signal shadowing is thus contained within the interval $[-1.96 \times 3.49\,\text{dB}, +1.96 \times 3.49\,\text{dB}] = [-7\,\text{dB}, +7\,\text{dB}]$ with probability 0.95.

For R_1, the minimum and maximum distances to the transmitter are 12 m and 247 m; for R_2, 7 m and 142 m; for R_3, 2 m and 47 m; and for R_4, 25 m and 292 m. The corresponding annuli are depicted in Figure 6. The dotted area represents the intersection of all annuli within the 100×180 m^2 grid and constitutes 33% of the grid area.

Figure 7 represents the candidate area computed by HPB for the same example scenario as in Figure 6. The intersection of all hyperbolic areas constructed with Theorem 2 yields a candidate area consisting of only 12% of the experimental grid. In this case, the HPB area size is approximately 36% of the annuli candidate area shown in Figure 6, illustrating a clear improvement over the annuli method when a range of EIRP is used.

Overall, for each of the four confidence levels, Figure 8 depicts a success rate for the annuli method higher than the corresponding confidence level, and thus greater than the HPB success rate as well. This phenomenon is due to the significantly greater candidate area size achieved with the annuli method.

Figure 9 illustrates the magnitude of this problem for confidence levels $\mathcal{C} = \{0.95, 0.90\}$. While the HPB candidate area size for $\mathcal{C} = 0.95$ averages 26% of the experimental grid, the corresponding annuli method average candidate area size is 59% of the grid, more than twice the size obtained with HPB. Our experimental results thus confirm the limited usability of the annuli method in localizing a rogue transmitter.

E. HPB Experimental vs. Simulation Results

Figure 10 compares the HPB experimental and simulation success rates for the four confidence levels. While the two sets of results are comparable, the experimental results yield a slightly higher success rate.

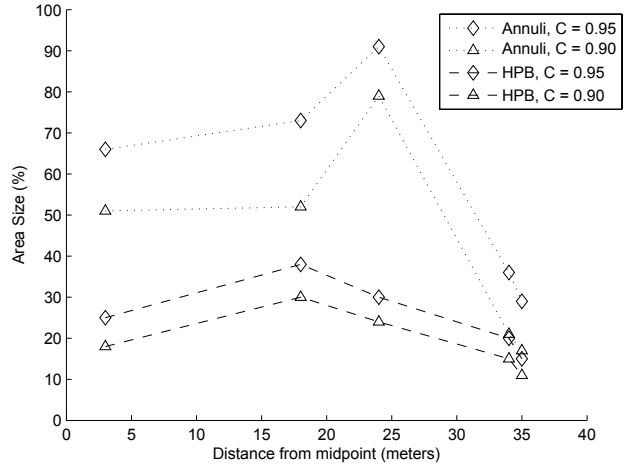

Fig. 9. HPB vs. Annuli Method Candidate Area Size

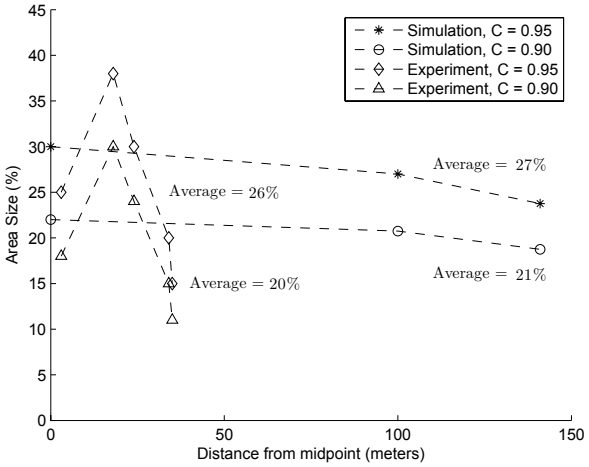

Fig. 11. HPB Experimental vs. Simulation Candidate Area Size

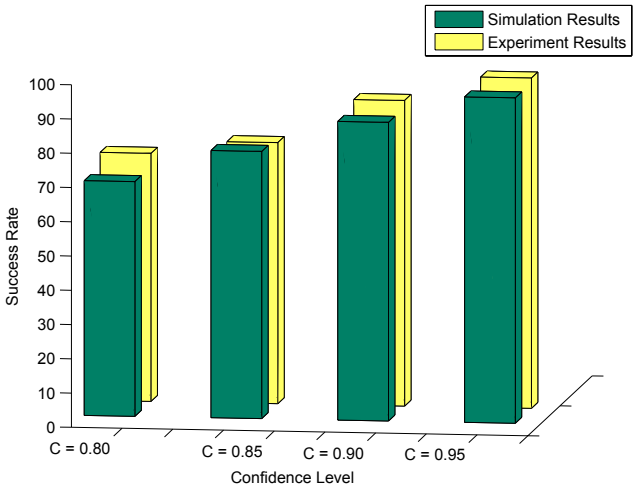

Fig. 10. HPB Experimental vs. Simulation Success Rate

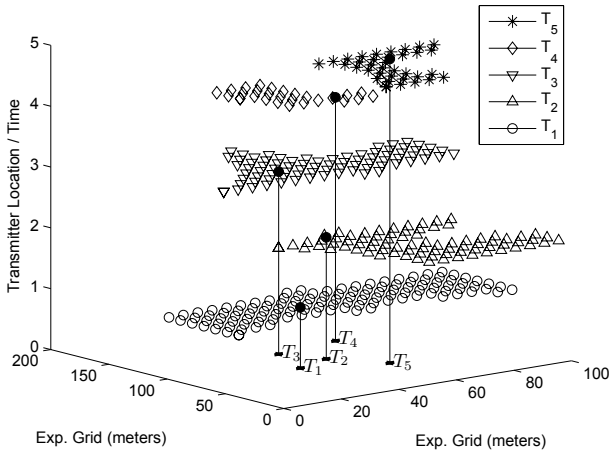

Fig. 12. Example of Candidate Areas for a Mobile Transmitter

Experimental and simulation candidate area sizes for $\mathcal{C} = \{0.95, 0.90\}$ are depicted in Figure 11. Inter-receiver distances for the experimental results are much shorter than for the simulation results, so fine-grained comparisons are difficult. However, within the central range, the average experimental candidate area size for $\mathcal{C} = 0.95$ is nearly identical to the simulation results, at 26% and 27% of the total grid, respectively. For $\mathcal{C} = 0.90$, the candidate area sizes are 20% and 21%; for $\mathcal{C} = 0.85$, they are 15% and 16%; and for $\mathcal{C} = 0.80$, they are 14% and 12%.

The performance of HPB along the success rate and candidate area size metrics yields consistent results in an experimental setting for T-R distances below 100 m, when compared with prior simulation results over longer distances.

V. Mobile Transmitter Tracking

Figure 12 illustrates an example set of HPB candidate areas computed from experimental RSS values, with each area associated with a rogue transmitter location T_1 to T_5, for $\mathcal{C} = 0.95$. The areas are staggered over time along the Z-axis to simulate mobility along a path from T_1 to T_5.

Given the size and central positioning of the T_1 to T_3 candidate areas, tracking a mobile transmitter from one of these areas to the next presents a significant challenge. However, as the transmitter moves away from the center of the experimental grid to positions T_4 and T_5, the corresponding candidate areas decrease in size. The shape and positioning of the T_4 and T_5 candidate areas, and the fact that they feature little overlap, unambiguously reveal the direction in which the rogue transmitter has traveled from one location to the next. In this manner, HPB can provide a rudimentary means for tracking a mobile device broadcasting attack messages, especially when the candidate areas are small. It is expected that the inclusion of additional receivers computing more hyperbolic areas can further reduce the candidate area size and enable HPB to provide even finer-grained tracking capability.

VI. Conclusion

We described an outdoor experiment for evaluating the hyperbolic position bounding of a mobile transmitting laptop emulating a malicious insider node in a WiFi/802.11 network, using RSS values harvested at four desktop receivers. This experiment provides a proof of concept scenario for the HPB algorithm in a practical setting, where a transmitter position is localized to a candidate area with a degree of confidence. The performance of HPB using experimental RSS values is assessed against simulation results obtained in previous research.

We found that the experimental results closely match the simulations along two tested metrics: the success rate in bounding a transmitter position to a candidate area, and the candidate area size. The success rate for the experimental results is found to be commensurate with the confidence level and slightly superior to that of the simulation results, especially in the experimental grid areas where the least signal reflection occurs. In terms of candidate area size, the experimental and simulation results average a candidate area of 26-27% of the total grid for confidence level $\mathcal{C} = 0.95$, and 20-21% for confidence level $\mathcal{C} = 0.90$. We also found that HPB can provide a coarse-grained tracking mechanism for a mobile transmitter as the computed candidate areas shift over time and space. The achievable level of tracking granularity is dependent upon the computation of sufficiently small candidate areas.

The experiment confirms the findings of prior simulation results. The HPB mechanism succeeds in pinpointing the location of a rogue transmitter using an unknown EIRP, with a high success rate and a candidate area size of nearly a quarter of the experimental grid with the highest confidence level. Further experiments are required to test the HPB mechanism for T-R distances greater than 100 m. Higher numbers of transmitter locations in a setting with fewer large buildings affecting reception is also planned for future work. Experiments with additional receivers are also envisioned, as these can assist in reducing the HPB candidate area size and thus provide for finer-grained tracking capability in mitigating mobile attackers.

Acknowledgment

The authors gratefully acknowledge the financial support received for this research from the Natural Sciences and Engineering Research Council of Canada (NSERC) and the Automobile of the 21st Century (AUTO21) Network of Centers of Excellence (NCE).

References

[1] G. Baker, "Schoolboy Hacks Into City's Tram System," The Telegraph, 11 January 2008, [Online] http://www.telegraph.co.uk.

[2] D. Halperin, T. S. Heydt-Benjamin, B. Ransford, S. S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno, and W. H. Maisel, "Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses," in *Proceedings of the IEEE Symposium on Security and Privacy*, May 2008.

[3] CSO Magazine, "2004 E-Crime Watch Survey," CSO Magazine, U.S. Secret Service and CERT Coordination Center, Survey, 2004.

[4] C. Laurendeau and M. Barbeau, "Insider Attack Attribution Using Signal Strength Based Hyperbolic Location Estimation," *To appear in: Security and Communication Networks*, 2008.

[5] ——, "Compounding Probabilistic Evidence for Hyperbolic Rogue Location Estimation," School of Computer Science, Carleton University, Tech. Rep. TR-08-04, February 2008.

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

[7] N. Sastry, U. Shankar, and D. Wagner, "Secure Verification of Location Claims," in *Proceedings of the 2nd ACM Workshop on Wireless Security (WiSe)*, September 2003, pp. 1–10.

[8] B. R. Waters and E. W. Felten, "Secure, Private Proofs of Location," Department of Computer Science, Princeton University, Tech. Rep. TR-667-03, January 2003.

[9] 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)*, vol. 2, March 2000, pp. 775–784.

[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 (WiSe)*, September 2006, pp. 43–52.

[11] A. M. Ladd, K. E. Bekris, A. Rudys, L. E. Kavraki, and D. S. Wallach, "Robotics-Based Location Sensing Using Wireless Ethernet," *Wireless Networks*, vol. 11, no. 1–2, pp. 189–204, January 2005.

[12] T. Roos, P. Myllymäki, H. Tirri, P. Misikangas, and J. Sievänen, "A Probabilistic Approach to WLAN User Location Estimation," *International Journal of Wireless Information Networks*, vol. 9, no. 3, pp. 155–164, July 2002.

[13] 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)*, September 2003, pp. 81–95.

[14] 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*, October 2004, pp. 516–518.

[15] M. Barbeau and J.-M. Robert, "Rogue-Base Station Detection in WiMax/802.16 Wireless Access Networks," *Annals of Telecommunications*, vol. 61, no. 11–12, pp. 1300–1313, November–December 2006.

[16] 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*, vol. 55, no. 2, pp. 499–509, March 2006.

[17] T. S. Rappaport, *Wireless Communications: Principles and Practice*, 2nd ed. New Jersey: Prentice-Hall, 2002.

[18] H. T. Friis, "A Note on a Simple Transmission Formula," *Proceedings of the I.R.E.*, vol. 34, no. 5, pp. 254–256, May 1946.

[19] 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*, September 2007, pp. 894–896.

[20] G. Durgin, T. S. Rappaport, and X. Hao, "Measurements and Models for Radio Path Loss and Penetration Loss In and Around Homes and Trees at 5.85 GHz," *IEEE Transactions on Communications*, vol. 46, no. 11, pp. 1484–1496, November 1998.

[21] 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.

[22] M. Rahman, "Path Loss Parameters in Wi-Fi Networks," School of Computer Science, Carleton University, Honours Project, December 2007.

[23] T. S. Rappaport and C. D. McGillem, "UHF fading in factories," *IEEE Journal on Selected Areas of Communications*, vol. 7, no. 1, pp. 40–48, January 1989.