Insider Attack Attribution Using Signal Strength Based Hyperbolic Location Estimation

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

A rogue insider, in a wireless network, is an authenticated member that exploits possession of a valid identity in order to launch an attack. A typical example is the transmission of a verifiable message containing false or incomplete information. An important step, in enabling the network authorities to attribute an attack message to its originator, involves locating the physical source of the transmission. We propose a probabilistic scheme to determine the location of a transmitting rogue, with a degree of confidence, using the relative signal strength received by neighboring devices, even if the effective isotropic radiated power (EIRP) employed by the rogue is unknown. The relative received signal strength between pairs of trusted receivers are combined with a range of possible EIRP values to construct an area in Euclidian space bounded by minimum and maximum distance hyperbolas. The area contained within the intersection of multiple hyperbola pairs pinpoints the location of the rogue transmitter with a specific level of confidence.

Index Terms

Insider Attack, Location Estimation, Wireless Networks, Wireless Security, Wireless Access Networks, Vehicular Communications

I. Introduction

Some of the most insidious security attacks are conducted by rogue insiders, and wireless networks are in no way immune. In a recent survey of IT security professionals [25], nearly half of the respondents reported that security breaches committed by malicious insiders engaging in corporate sabotage was a frequent occurrence. As the owner of a valid logical identity such as a MAC address or digital certificate in an open medium, the rogue insider in a wireless network can broadcast with impunity verifiable messages containing falsified information. It may also evade retribution once an attack is detected, especially if its identity is fraudulently obtained, for example through theft.

Before a rogue can be stopped, an attack must be detected. In some networks, unauthorized activity can be flagged through access control mechanisms or unusual usage patterns. However in many domains, for example vehicle safety applications where transmitted broadcast messages are digitally signed for authentication and non-repudiation, an attack may only be detected if an invalid digital certificate is used to sign the message. Attack broadcasts by a rogue insider can thus go unchallenged. In such technologies, additional mechanisms to expose attack messages are required.

Once an attack is detected, current means of attributing the attack to an insider node are based on its logical identity. This approach can be fraught with problems if the identity is forgeable. Dynamic MAC addresses are supported in some domains, for example in vehicular networks [12], to promote privacy. A rogue may easily abuse this feature to assume a new identity at will. Password-based access control and digital certificates associated with public/private key pairs constitute additional means of identification. However, in vehicular applications where messages may be signed but not encrypted, digital signatures

This is a preprint of an article published in *Security and Communication Networks* 2008, 1(4): 337-349 (www.interscience.wiley.com)

have been deemed a critical threat to privacy for facilitating location tracking [15]. The current trend in securing this type of message in vehicular networks circumvents the use of individualized digital certificates for each node [16], [27], [29]. In a revocation scheme based solely on the originator's logical identity or other falsifiable credential, the network cannot attribute the source of an attack message directly to the rogue, nor can it prevent the attacker from using a new identity in subsequent attacks. Determining the physical location of the attack message's originator can be an important first step in apprehending the perpetrator, possibly linking its location to additional logical identities, and alerting neighboring devices to its presence in order to preemptively contain the impact of further attacks.

An additional advantage to the use of a node's physical location as a unique unforgeable identity allows the network to detect and circumvent Sybil attacks, first described by Douceur [6], where one attacker may assume multiple colluding identities in order to mislead honest nodes. Linking a node to a geographical position ensures that it is a unique physical device in the network and not a virtual entity under an attacker's control.

We put forth a hyperbolic localization scheme for estimating the position of a transmitter using the relative received signal strength (RSS) obtained by a number of trusted receivers. Since the effective isotropic radiated power (EIRP) of the transmitter is unknown and RSS values may fluctuate, a probabilistic model is used to estimate the range of distance differences between receiver pairs and the transmitter. These differences are used to construct minimum and maximum hyperbolas between two receivers where the transmitter may be located, with a certain degree of confidence. Multiple pairs of such hyperbolas may be constructed by considering different pairs of receivers. As a result, the intersecting hyperbolic area can be said to contain the transmitter with the combined degree of confidence.

Section II outlines the existing literature in location determination. Section III describes our relative RSS based location estimation scheme. Section IV evaluates the performance of our localization algorithm. Section V concludes the paper.

II. Related Work

The lion's share of existing research into wireless device location determination presumes the collaboration of the node being localized. Whether geometric localization is used, such as *time of arrival* (TOA), or the heuristic schemes commonly utilized in sensor networks [11], these techniques rely on the trusted cooperation of the node seeking to learn its position. However, in the case where the node is a rogue, any voluntarily supplied information may be falsified to enable the rogue to evade detection and retribution. As a result, we focus our efforts on the use of information inadvertently leaked by the rogue, such as the RSS associated with its transmitted message.

RSS-based localization algorithms come in two flavours: signature dependent or geometric. Signature dependent techniques rely on an existing training set of RSS signalprints established during an offline training phase. This map of known RSS measurements is subsequently consulted during the localization phase to estimate a node's location based on the similarity of the signals received at trusted base stations or access points to the signalprints found in the training set, as outlined in Bahl and Padmanabhan [2], Roos *et al.* [28] and Ladd *et al.* [13]. Such experiments have been conducted in indoor environments. Use in outdoor scenarios, for example in WiMAX/802.16 wireless access networks or vehicular networks, remains an open question. Geometric RSS-based localization techniques aim to estimate a node's location in Euclidian space based on the signal strength of messages received from trusted nodes within range, as proposed by Chong Liu *et al.* [21] and Bo-Chieh Liu *et al.* [20]. These schemes assume the complicity of the target node in reliably measuring the RSS of received beacon messages. As such, they cannot be used to localize a rogue node. Existing hyperbolic localization schemes are based on *Time Difference of Arrival* (TDOA) techniques. They take an algebraic approach to estimate a device's coordinates by solving a set of non-linear hyperbolic equations, for example in Chan and Ho [5]. Signal strength fluctuations taken into account are restricted to small scale fading. As well, some of these techniques such as the ones outlined by Bo-Chieh Liu *et al.* [20] [19] assume a known distance from the transmitter to the closest receiver reference point.

Localization mechanisms that function independently of the targeted node are used in location verification and rogue detection. Location verification algorithms are predicated upon a set of trusted verifiers substantiating the alleged position of a prover within a specified area. The majority of existing schemes rely on TOA information collected by the verifiers to bound the prover's position, as outlined in Brands and Chaum [4], Sastry *et al.* [30] and Waters and Felten [32]. Xiao *et al.* [33] describe a signal strength based location verification method with an exhaustive set of possible rogue positions to identify Sybil nodes in vehicular networks. In the realm of rogue detection, Faria and Cheriton [8] outline a signature dependent RSS-based scheme in an indoor environment to detect rogue mobile stations (MSs) in WiFi/802.11. Barbeau and Robert [3] employ RSS measurements in outdoor wireless access networks (such as WiMAX/802.16) to allow a MS to detect whether a base station (BS) advertising its availability for a handoff may be a rogue. A probabilistic RSS-based geometric model is presented where the RSS measurements obtained from neighboring BSs by a non-localized MS may be used to construct annuli whose non-empty intersection likely contains the MS. An empty intersection may indicate a RSS measurement originating from a rogue BS.

Our scheme extends the RSS-based geometric model proposed in [3] to localize a single transmitter from multiple receivers, taking into account the unknown EIRP employed by a rogue. In addition, since the compounding effect of a large EIRP range and probabilistic fluctuations in RSS measurements may result in a potentially extensive area for the rogue, we propose the use of hyperbola pairs rather than annuli for the localization. In this manner, relative rather than absolute RSS values are used to effectively reduce the area containing the rogue's probable location.

III. Localization Using Relative Signal Strength

We outline the assumptions inherent in our threat model and examine suitable propagation models for obtaining a signal source's location information from RSS values. We describe our scheme for estimating probabilistic minimum and maximum transmitter-receiver distances from RSS values and the subsequent computation of minimum and maximum bounds on the distance difference from a transmitter to a pair of receivers.

A. Threat Model

The goal of our localization scheme is to ascertain the source position of an attack message broadcast as a radio frequency (RF) signal to all receivers within its range. We assume that the transmitting rogue is a mobile device and that a number of trusted receiving stations are within range and can communicate with each other over a secure channel to collect and aggregate RSS measurements. The coordinates of the receiving stations are globally known. Such a scenario is feasible in a number of wireless technologies, for example with WiMAX/802.16 [14] MSs and BSs or the On-Board Units and Road-Side Units in vehicular network architectures [1].

In order to evade revocation from the network, the rogue may combine changes in its transmission power with the judicious use of directional antennas to modify the signal gain and obfuscate its true position. As a result, no assumptions can be made regarding the EIRP employed to transmit the attack message.

B. Radio Propagation Models

RF signals are subject to attenuation as they propagate through the air. Large scale fading occurs when a signal encounters large terrain-based obstacles such as buildings, trees and hills. Small scale signal fading is caused by the movement of a mobile device. The cumulative effect of fading over time and distance is termed the *path loss*. A number of theoretical models for estimating path loss have been put forth in the literature for the purpose of simulating propagation environments, and these models may be classified into two categories. Empirical propagation models use probabilistic methods to predict received signal characteristics such as path loss and strength. Deterministic models are specific to a particular area and take into account the various obstacles therein. The dynamic nature of outdoor environments inherent to wireless access networks such as WiMAX/802.16 and vehicular networks lends itself better to empirical models rather than deterministic ones. As a result, we focus on the former approach.

Several empirical propagation models have been proposed for forecasting large scale path loss as a function of the distance between a transmitter and a receiver. These are of particular interest, since they lend themselves to our purpose. If the distances between the transmitter and receivers can be approximated from the path loss, which is directly proportional to the RSS values, the transmitter's location can be estimated. The Okumura model [24] predicts path loss based on transmitter and receiver antenna height, as well as the mean attenuation and the environment-based gain which can be obtained from experimental results. Miyashita *et al.* [22] observe that the Okumura model is unsuitable over complex terrain due to the difficulty in ascertaining the required correction factors. The validity of the Hata model [10], also known as the Okumura-Hata model [22], has been demonstrated for frequencies between 150-1500 MHz, but not at the higher frequencies commonly used in newer technologies. For example, WiMAX/802.16 uses the 2-11 or 10-66 GHz bands, while DSRC vehicular networks operate in the 5.9 GHz band. The two-parameter Nakagami model [23] has been suggested as best suited for modeling channel characteristics in vehicular communications [31]. This model is dependent upon two parameters, the mean received power and a fading parameter, that are both obtained through experimental studies for a given discrete value of the distance d between a transmitter and a receiver. If d changes, so do the values of both parameters. As a result, the Nakagami model is unusable for predicting d from the measured path loss, since the parameters required to compute the path loss are dependent upon d. The log-normal shadowing model outlined by Rappaport [26] provides a simple model to measure large scale path loss from d. Since our aim is to approximate d based on a measured path loss, the log-normal shadowing model is best suited to our purpose.

C. Estimating Distance From Signal Strength

We outline Rappaport's large scale path loss model and describe how the minimum and maximum distance between a transmitter and a receiver can be computed from the RSS with a desired level of confidence.

1) The Log-Normal Shadowing Model: In [26], Rappaport outlines a *log-normal shadowing* model, which is a statistical path loss model for a signal received at distance d from a transmitter. This model is used to estimate the signal loss at various distances from the transmitter, based on a pre-defined reference distance d_0 close to the transmitter, a path loss exponent n dependent upon the propagation environment and the standard deviation σ for the path loss. Values for n and σ can be obtained from experimental measurements, for example in [18] and [7], where linear regression techniques are used to ascertain values of n and σ from actual path loss measurements.

In describing the log-normal shadowing model, Rappaport defines the path loss $L(d)$ of a signal at distance d as a Gaussian (Normal) distribution random variable with mean $\overline{L}(d)$ and standard deviation σ:

$$L(d) = \overline{L}(d) + X_\sigma$$

where X_σ is a Normal distribution zero-mean random variable with standard deviation σ. The mean path loss at distance d is in turn defined as:

$$\overline{L}(d) = \overline{L}(d_0) + 10n\log(\frac{d}{d_0})$$

where $\overline{L}(d_0)$ is the average path loss at the reference distance d_0, assuming free space propagation, and n is the path loss exponent. Rappaport concludes the following fact.

Fact 1. *The path loss $L(d)$ of a signal at distance d from the transmitter is stated as:*

$$L(d) = \overline{L}(d_0) + 10n\log(\frac{d}{d_0}) + X_\sigma$$

A further observation can be made about X_σ.

Fact 2. *For a selected confidence level $\mathcal{C}$, X_σ lies in the confidence interval $[-z\sigma dB, +z\sigma dB]$, where $z = \Phi^{-1}(\frac{1+\mathcal{C}}{2})$ and can be obtained from a Normal distribution table.*

From Facts 1 and 2, we can specify the probabilistic path loss more precisely.

Lemma 1. *The path loss $L(d)$ of a signal at distance d from the transmitter is defined with a confidence level $\mathcal{C}$ as:*

$$L(d) = \overline{L}(d_0) + 10n\log(\frac{d}{d_0}) \pm z\sigma$$

where $z = \Phi^{-1}(\frac{1+\mathcal{C}}{2})$.

Proof: This can be derived directly from Fact 1 and Fact 2. ■

Example. Figure 1 illustrates an example of the distribution of path loss at a distance of $d = 100$ m from the transmitter. In the 2.4 GHz frequency band, the average free space path loss measured at $d_0 = 1$ m equals 40 dB. For a path loss exponent of 2.76, we obtain the average loss at 100 m as $\overline{L}(100\text{ m}) = 95$ dB. With a standard deviation $\sigma = 5.62$, the shaded area in Figure 1 depicts 95% of the probability distribution around the average path loss. The path loss shadowing lies in the interval $[-1.96 \times 5.62\text{ dB}, +1.96 \times 5.62\text{ dB}] = [-11\text{ dB}, +11\text{ dB}]$ with probability 0.95, and so $L(100\text{ m})$ is contained in the interval $[84\,\text{dB}, 106\,\text{dB}]$ with probability 0.95.

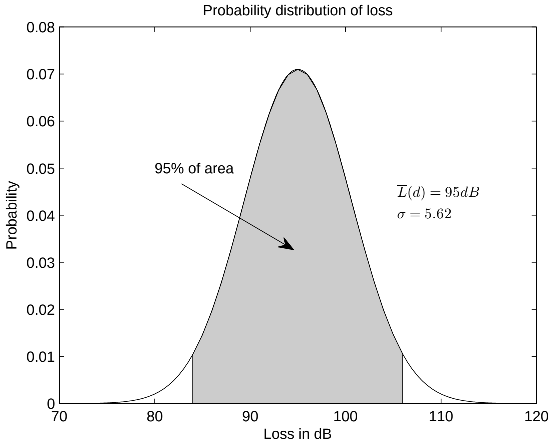

Fig. 1. Example of Log-Normal Shadowing Model

2) Distance Range with Log-Normal Shadowing: In [3], Barbeau and Robert demonstrate that the minimum and maximum distances from a transmitter to a receiver can be calculated from the path loss using Rappaport's log-normal shadowing model.

Lemma 2. *For a chosen confidence level $\mathcal{C}$, the minimum and maximum distances (d^- and d^+ respectively) from a transmitter to a receiver can be computed as a function of path loss with:*

$$d^- = d_0 \times 10^{\frac{L(d) - \overline{L}(d_0) - z\sigma}{10n}}$$

$$d^+ = d_0 \times 10^{\frac{L(d) - \overline{L}(d_0) + z\sigma}{10n}}$$

Proof: The proof is based on Lemma 1 and can be found in [3]. ■

In the threat model specified in Section III-A, each receiver R_k obtains a RSS measurement RSS_k, but the path loss $L(d)$ value required to compute the distance using the equations in Lemma 2 is not readily available. We can thus replace the path loss with its equivalent, based on the transmitted power EIRP and RSS.

Fact 3. *The path loss $L(d)$ at distance d can be stated in terms of the EIRP and RSS at receiver R_k:*

$$L(d) = EIRP - RSS_k$$

A rogue may transmit at various EIRP levels in order to mask its location. In our solution, we address this issue by assuming an unknown value for the EIRP. We thus update Barbeau and Robert's minimum and maximum distance equations for a range of EIRP values, bounded by a minimum and a maximum EIRP, denoted as $\mathcal{P}^-$ and $\mathcal{P}^+$ respectively.

Lemma 3. *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:*

$$d_k^- = d_0 \times 10^{\frac{\mathcal{P}^- - RSS_k - \overline{L}(d_0) - z\sigma}{10n}} \tag{1}$$

$$d_k^+ = d_0 \times 10^{\frac{\mathcal{P}^+ - RSS_k - \overline{L}(d_0) + z\sigma}{10n}} \tag{2}$$

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:

1. For a single EIRP value $\mathcal{P}$, Lemma 2 and Fact 3 can be combined to show that d_k^- and d_k^+ are the minimal and maximal distances respectively.
2. For a range of EIRP values $[\mathcal{P}^-, \mathcal{P}^+]$, let $\mathcal{D}_k(\mathcal{P}, \mathcal{V})$ represent the distance between a transmitter T and receiver R_k if the signal EIRP is $\mathcal{P}$ and the signal shadowing value within the shadowing interval $[-z\sigma, +z\sigma]$ is $\mathcal{V}$. Therefore, $\mathcal{D}_k(\mathcal{P}, \mathcal{V}) = d_0 \times 10^{\frac{\mathcal{P} - RSS_k - \overline{L}(d_0) + \mathcal{V}}{10n}}$.

   Four possible distance boundaries between T and R_k can be computed using combinations of EIRP and shadowing interval bounds:

   (i) $\mathcal{D}_k(\mathcal{P}^-, -z\sigma)$
   (ii) $\mathcal{D}_k(\mathcal{P}^-, +z\sigma)$
   (iii) $\mathcal{D}_k(\mathcal{P}^+, -z\sigma)$
   (iv) $\mathcal{D}_k(\mathcal{P}^+, +z\sigma)$

   These points form a lattice with an infimum, and so a minimum distance d_k^-, of $\mathcal{D}_k(\mathcal{P}^-, -z\sigma)$, since $\mathcal{P}^-$ is the minimum EIRP and $-z\sigma$ is the minimum shadowing bound. Its supremum, and thus the maximum distance d_k^+, is the value $\mathcal{D}_k(\mathcal{P}^+, +z\sigma)$, because $\mathcal{P}^+$ is the maximum EIRP and $+z\sigma$ is the maximum shadowing bound.

■

An additional observation may be gleaned from the results uncovered in Lemma 3.

Lemma 4. *For a given EIRP value $\mathcal{P}$, the minimum and maximum distances between a transmitter and a receiver are bounded solely by the signal shadowing range $[-z\sigma, +z\sigma]$ with confidence level $\mathcal{C}$.*

Proof: With a constant EIRP value $\mathcal{P} = \mathcal{P}^- = \mathcal{P}^+$, the proof can be directly inferred from Lemma 3, since $-z\sigma$ and $+z\sigma$ are the lower and upper bounds, respectively, of the signal shadowing range. ■

D. Estimating Location From Distance

Minimum and maximum distances between a transmitter and a receiver have been used, for example in [3], [21] and [20], to construct a pair of rings forming an annulus within which a transmitter may be located. Multiple annuli may be computed around several receivers, and the location of the transmitter can be estimated within the annuli intersection area. However, this approach is more successful when the difference between minimum and maximum distances is not significant. If it is, the annuli may be so wide that their intersection is too large to effectively locate the transmitter, even if multiple receivers are considered.

Our approach relies on the use of the relative distance difference from a transmitter between pairs of receivers, similar to the *Time Difference of Arrival* (TDOA) technique. In TDOA, a hyperbola is constructed with two points of known coordinates at the foci. The properties of hyperbolas are such that every point on the hyperbola is at the same distance difference of the two foci. For example, if the difference in distances from a transmitter T to two receivers A and B is known, the corresponding hyperbola $\mathcal{H}_{A,B}$ can be constructed, as shown in Figure 2. The transmitter must necessarily lie on the hyperbola between A and B. If a second distance difference is known, for example between receivers B and C, a second hyperbola can be plotted, and the location of the transmitter T is discovered at the intersection of the two hyperbolas.

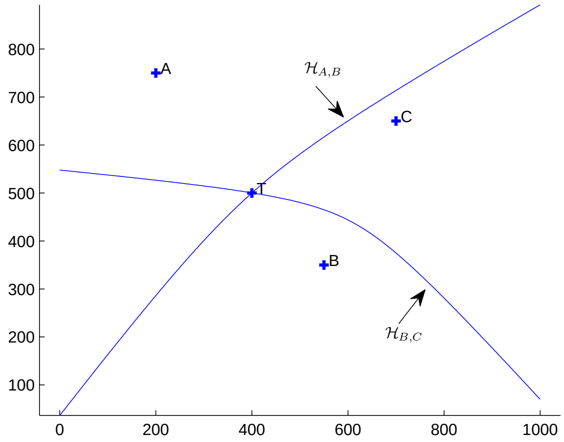

Fig. 2. TDOA Example

However in our threat model, because neither the transmitter EIRP nor its signal shadowing value are known, we cannot determine the precise distance difference between a pair of receivers. Instead, we use a TDOA-based technique combined with the estimated minimum and maximum distances between the transmitter and receivers. We can thus define a candidate area $\mathcal{A}_{i,j}$ bounded by two hyperbolas between a pair of receivers R_i and R_j: one hyperbola at the minimum bound of the distance difference range and another at the maximum bound.

1) Computing the Distance Difference Range: We use the minimum and maximum distance equations, defined in Lemma 3, to compute the minimum and maximum bounds in the range of distance differences between a pair of receivers R_i and R_j. Intuitively, the minimum bound of this range from R_i's perspective is the difference between the distances closest to R_i yet farthest from R_j, at the minimum transmission power. This bound is typically located between the two receivers. In turn, the maximum bound of the range from R_i's perspective is the difference between the distances farthest from R_i yet closest to R_j, at the maximum EIRP, resulting in a bound that may be located beyond R_j.

Theorem 1. *Let d_i be the unknown distance between a transmitter T and receiver R_i.*

1. *The minimum bound $\Delta d^-_{i,j}$ of the distance difference range between d_i and d_j is the distance difference*

at the minimal EIRP ($\mathcal{P}^-$) over the full signal shadowing range $[-z\sigma, +z\sigma]$ with confidence level $\mathcal{C}$.

$$\Delta d^-_{i,j} = \left(d_0 \times 10^{\frac{\mathcal{P}^- - RSS_i - \overline{L}(d_0) - z\sigma}{10n}}\right) - \left(d_0 \times 10^{\frac{\mathcal{P}^- - RSS_j - \overline{L}(d_0) + z\sigma}{10n}}\right) \tag{3}$$

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

$$\Delta d^+_{i,j} = \left(d_0 \times 10^{\frac{\mathcal{P}^+ - RSS_i - \overline{L}(d_0) + z\sigma}{10n}}\right) - \left(d_0 \times 10^{\frac{\mathcal{P}^+ - RSS_j - \overline{L}(d_0) - z\sigma}{10n}}\right) \tag{4}$$

Proof: Because both R_i and R_j receive the same attack message sent with a single (albeit unknown) transmitted power, the EIRP value used to calculate the distance difference between R_i and R_j must be the same. Thus the minimum bound of the distance difference range uses $\mathcal{P}^-$, and the maximum bound uses $\mathcal{P}^+$. From Lemma 4, we know that for each EIRP value, the range of minimum and maximum distances must encompass the full signal shadowing range between $-z\sigma$ and $+z\sigma$ with confidence level $\mathcal{C}$.

Let $\mathcal{D}_k(\mathcal{P}, \mathcal{V})$ represent the distance between T and R_k if the signal EIRP is $\mathcal{P}$ and the shadowing is $\mathcal{V}$. Thus according to Lemma 3, $\mathcal{D}_k(\mathcal{P}, \mathcal{V}) = d_0 \times 10^{\frac{\mathcal{P} - RSS_k - \overline{L}(d_0) + \mathcal{V}}{10n}}$.

1. At the minimal EIRP, the possible distance difference boundaries between R_i and R_j can be computed, with confidence level $\mathcal{C}$, using combinations of shadowing bounds:
   (i) $\mathcal{D}_i(\mathcal{P}^-, -z\sigma) - \mathcal{D}_j(\mathcal{P}^-, -z\sigma)$
   (ii) $\mathcal{D}_i(\mathcal{P}^-, -z\sigma) - \mathcal{D}_j(\mathcal{P}^-, +z\sigma)$
   (iii) $\mathcal{D}_i(\mathcal{P}^-, +z\sigma) - \mathcal{D}_j(\mathcal{P}^-, -z\sigma)$
   (iv) $\mathcal{D}_i(\mathcal{P}^-, +z\sigma) - \mathcal{D}_j(\mathcal{P}^-, +z\sigma)$

   These points form a lattice with infimum $\Delta d^-_{i,j} = \mathcal{D}_i(\mathcal{P}^-, -z\sigma) - \mathcal{D}_j(\mathcal{P}^-, +z\sigma)$, since $-z\sigma$ and $-(+z\sigma)$ represent the minimum shadowing bound. The supremum of this lattice consists of $\mathcal{D}_i(\mathcal{P}^-, +z\sigma) - \mathcal{D}_j(\mathcal{P}^-, -z\sigma)$, given that $+z\sigma$ and $-(-z\sigma)$ represent the maximum shadowing bound. It should be noted that this supremum equals $-\Delta d^-_{j,i}$, which is the minimum bound of the distance difference between d_j and d_i.
2. At the maximal EIRP, the possible distance difference boundaries between R_i and R_j can be computed, with confidence level $\mathcal{C}$, as follows:
   (i) $\mathcal{D}_i(\mathcal{P}^+, -z\sigma) - \mathcal{D}_j(\mathcal{P}^+, -z\sigma)$
   (ii) $\mathcal{D}_i(\mathcal{P}^+, -z\sigma) - \mathcal{D}_j(\mathcal{P}^+, +z\sigma)$
   (iii) $\mathcal{D}_i(\mathcal{P}^+, +z\sigma) - \mathcal{D}_j(\mathcal{P}^+, -z\sigma)$
   (iv) $\mathcal{D}_i(\mathcal{P}^+, +z\sigma) - \mathcal{D}_j(\mathcal{P}^+, +z\sigma)$

   These form a lattice with supremum $\Delta d^+_{i,j} = \mathcal{D}_i(\mathcal{P}^+, +z\sigma) - \mathcal{D}_j(\mathcal{P}^+, -z\sigma)$, since $+z\sigma$ and $-(-z\sigma)$ represent the maximum shadowing bound. The infimum of this lattice consists of $\mathcal{D}_i(\mathcal{P}^+, -z\sigma) - \mathcal{D}_j(\mathcal{P}^+, +z\sigma)$, given that $-z\sigma$ and $-(+z\sigma)$ represent the minimum shadowing bound. This infimum equals $-\Delta d^+_{j,i}$, which is the maximum bound of the distance difference between d_j and d_i.

$\blacksquare$

2) Plotting the Minimum and Maximum Bound Hyperbolas: Given the definitions for the range of distance differences between a pair of receivers, we may construct the corresponding hyperbolas bounding the location of the transmitter.

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 $\sqrt{(x-x_i)^2+(y-y_i)^2} - \sqrt{(x-x_j)^2+(y-y_j)^2} = \Delta d_{i,j}^+$.

Then 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 $Pr(T \notin \mathcal{A}_{i,j}) = (1-\mathcal{C})$.

Proof: We define the distance between T and R_i as $d_i = \sqrt{(x-x_i)^2+(y-y_i)^2}$ and the distance between T and R_j as $d_j = \sqrt{(x-x_j)^2+(y-y_j)^2}$. If $\Delta d_{i,j} = d_i - d_j$ is defined as the distance difference between R_i and R_j, we obtain the equation for the hyperbola between R_i and R_j:

$$\sqrt{(x-x_i)^2+(y-y_i)^2} - \sqrt{(x-x_j)^2+(y-y_j)^2} = \Delta d_{i,j}$$

We know from Theorem 1 that $\Delta d_{i,j}^-$ is the minimum bound of the distance difference between d_i and d_j and that $\Delta d_{i,j}^+$ is the maximum bound of this difference with probability $\mathcal{C}$. We can therefore deduce that the probability of T being located in the area between $\mathcal{H}_{i,j}^-$ and $\mathcal{H}_{i,j}^+$ is $\mathcal{C}$ and the probability of T being located outside this area is $(1-\mathcal{C})$. ■

An additional pair of minimum and maximum bound hyperbolas can be constructed between receivers R_i and R_j, namely the hyperbolas based on the inverted order of the receivers, R_j and R_i. Thus any pair of receivers can yield four hyperbolas to help determine the location of the transmitter. We have also noted in simulations that the maximum bound of the distance difference range between receivers is often too large for the corresponding hyperbola to be plotted to scale. However, it is still required to bound candidate hyperbolic areas for the transmitter.

3) An Example: Let us compute the candidate hyperbolic areas $\mathcal{A}_{i,j}$ and $\mathcal{A}_{j,i}$ for the location of a transmitter T with confidence level $\mathcal{C} = 0.95$, which yields the normal distribution constant $z = 1.96$. We assume a transmitter frequency of 2.4 GHz. For a reference distance $d_0 = 1$ m, we use the parameter values obtained by Liechty *et al.* [18] [17] for Line of Sight (LOS) propagation and a seven meter high antenna, where the path loss exponent is $n = 2.76$ and the standard deviation is $\sigma = 5.62$. The average path loss at d_0 is calculated with Friis' transmission equation for free space propagation [9], assuming isotropic transmitting and receiving antennas:

$$\overline{L}(d_0) = (\frac{4\pi f d_0}{c})^2 = 40\,\text{dB}$$

We assume an example layout as depicted Figure 3, where receivers R_1 and R_2 receive an attack message from a transmitter T with signal strength $RSS_1 = -79.20$ dBm and $RSS_2 = -74.27$ dBm respectively, corresponding to an actual transmitted EIRP of 30 dBm. Further, we model the EIRP range with $\mathcal{P}^- = 15$ dBm and $\mathcal{P}^+ = 40$ dBm. Equations (1) and (2) reveal that the transmitter T is located between 37 m and 1848 m from R_1 and between 24 m and 1225 m from R_2 with probability $\mathcal{C} = 0.95$. Using equations (3) and (4), we compute the minimum bound of the distance difference between d_1 and d_2 as $\Delta d_{1,2}^- = -115$ m and the maximum bound as $\Delta d_{1,2}^+ = 1653$ m. Conversely, the minimum bound between d_2 and d_1 is calculated as $\Delta d_{2,1}^- = -205$ m and the maximum bound is $\Delta d_{2,1}^+ = 930$ m. The minimum bound hyperbolas $\mathcal{H}_{1,2}^-$ and $\mathcal{H}_{2,1}^-$ associated with $\Delta d_{1,2}^-$ and $\Delta d_{2,1}^-$, respectively, are depicted in Figure 3. The candidate areas for transmitter T include the area between $\mathcal{H}_{1,2}^-$ and $\mathcal{H}_{1,2}^+$, known as $\mathcal{A}_{1,2}$ and shown with dotted arrows, and the area between $\mathcal{H}_{2,1}^-$ and $\mathcal{H}_{2,1}^+$, named $\mathcal{A}_{2,1}$ and featured with dash-dotted arrows. T is located within $\mathcal{A}_{1,2}$ with probability 0.95 and within $\mathcal{A}_{2,1}$ with the same probability.

Minimum and maximum bound hyperbolas can be constructed between multiple pairs of receivers, forming a number of intersecting areas within which the transmitter location can be further bounded. For example, Figure 4 illustrates the minimum bound hyperbolas between receiver pairs R_1, R_2 and R_3, R_4.

IV. Performance Evaluation

In this section, we outline the results obtained by simulating our localization algorithm using various transmitter locations with two scenarios involving fixed receivers. We analyze the success rate of the algorithm in locating the transmitter and the corresponding candidate area size.

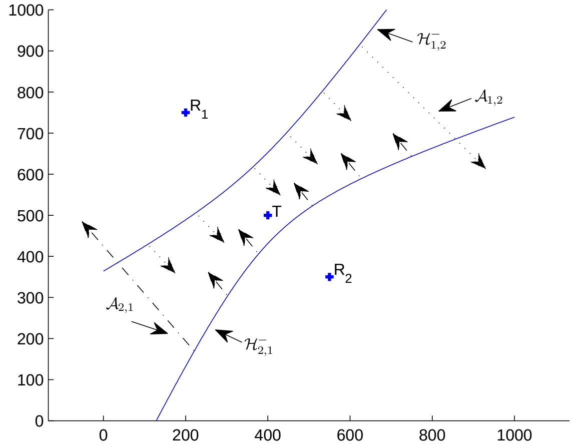

Fig. 3. Minimum Hyperbolas for R_1, R_2

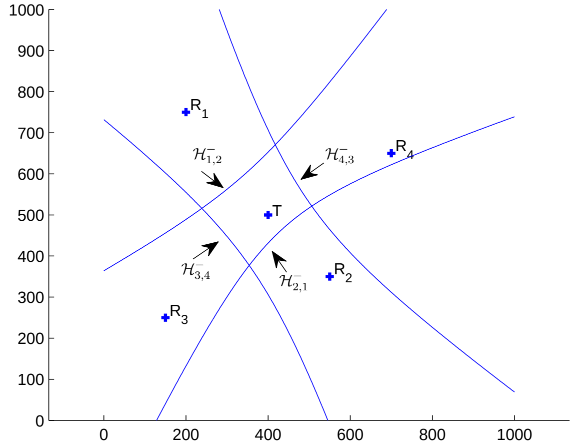

Fig. 4. Minimum Hyperbolas for R_1, R_2 and R_3, R_4

A. Configuration

Results are presented for two separate scenarios, one with two receivers and the other with four receivers, located on a 1000×1000 meter grid. The transmitter location is simulated at each 100 meter interval in the grid from zero meters to 1000 meters on both the X-axis and Y-axis, as shown in Figure 5. The transmitter localization algorithm yields results for each of the possible 121 transmitter locations, given four individual confidence levels: $\mathcal{C} = 0.95$, 0.90, 0.85 and 0.80. Minimum and maximum bound hyperbolas are constructed between each pair of receivers. The simulation assumes a frequency of 2.4 GHz, as well as the values for the reference distance, path loss exponent and shadowing standard deviation determined for this frequency in an outdoor environment by Liechty *et al.* [18] [17], where d_0 equals one meter, n equals 2.76 and σ equals 5.62. A transmitter EIRP of 30 dBm is assumed for computing simulated RSS values at each receiver. For each execution, a random amount of signal shadowing is added to the RSS values along a Normal distribution, with mean zero and Liechty's shadowing standard deviation. The EIRP range is determined dynamically by taking the closest receiver to the transmitter location, i.e. the receiver with the highest RSS, as a reference point. The EIRP range is set to the intersection of the EIRP ranges required for each remaining receiver to reach the reference point.

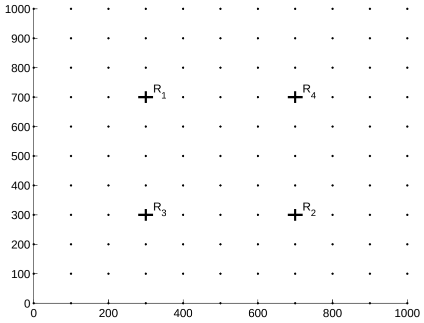

Fig. 5. Four-Receiver Scenario Simulation Grid

B. Results

The performance of the transmitter localization algorithm is evaluated along two metrics: the success rate in correctly localizing the transmitter within a bounded area, and the minimization of the size of this area. Consequently, both metrics were gathered for each execution of the localization algorithm. The success rate reflects the percentage of executions for which the intersection of all hyperbolic areas, i.e. the maximal probability candidate area, contains the actual transmitter location. The area size represents the percentage of the 1000×1000 meter grid covered by the candidate area. Optimal results are obtained when the success rate is maximized and the area size is minimized.

Figure 6 illustrates the success rate for the four-receiver scenario, given $\mathcal{C} = 0.95$. Since metrics were gathered solely for the grid points shown in Figure 5, values for the intermediate points were intrapolated linearly between the values for the computed grid points. The success rate is highest in the cross shape between the receivers, which we term the *aggregate range*. This range constitutes the zone in which the transmitter is located between at least one pair of receivers, enabling the receivers to aggregate and support each other's findings. The lowest success rates are achieved in the corners of the grid, outside the aggregate range, since these zones are not situated between any pair of receivers. Low success rates are also obtained when the transmitter is located precisely at the receiver locations. These special cases are eliminated from our subsequent analysis, because a zero meter distance is less than the reference distance of d_0 (one meter) used in the path loss model. Figure 6 displays the success rates averaged over the 1000 executions of the localization algorithm for each transmitter location. With a confidence of 90%, the success rate associated with each grid point within the aggregate range lies in a confidence interval of $\pm 3\%$ of the mean for that point. The non-aggregate range points are situated in an interval of $\pm 4\%$ from the grid point mean, with confidence 90%. Consequently, not only is the success rate of the localization algorithm lower in the non-aggregate range, the results are also less reliable due to their greater variance. This bears out the intuition that a greater receiver coverage poses a significant advantage to the localization of a rogue device.

Figure 7 depicts the success rate as a function of the distance from the grid's midpoint, located at coordinates (500, 500), for the four-receiver scenario. This success rate is shown for each of the four confidence levels tested, with a 90% confidence interval depicted with each point for $\mathcal{C} = 0.95$. Intuitively, the farther the transmitter from the midpoint, the lower the expected success rate, and Figure 7 confirms this hypothesis for all confidence levels. At the midpoint, where the distance is zero, the highest success rate is achieved. However, because the higher success rates occur between the receivers in a cross shape rather than concentric circles, Figure 7 does not show a completely linear decrease in success rate. For example, noticeable dips in the graph occur at distances 361 m, 424 m, 500 m and 566 m. These correspond to the instances where the transmitter is located in the non-aggregate range at the corners of the grid, and thus within the range of only one receiver. Figure 8 captures the same data as Figure 7, but with the non-aggregate range points excluded. A more linear success rate is achieved as the transmitter location moves away from the midpoint.

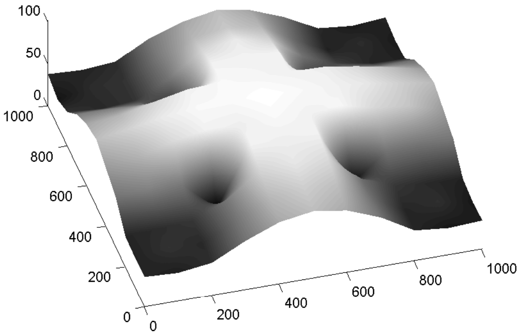

Fig. 6. Success Rate for $\mathcal{C} = 0.95$

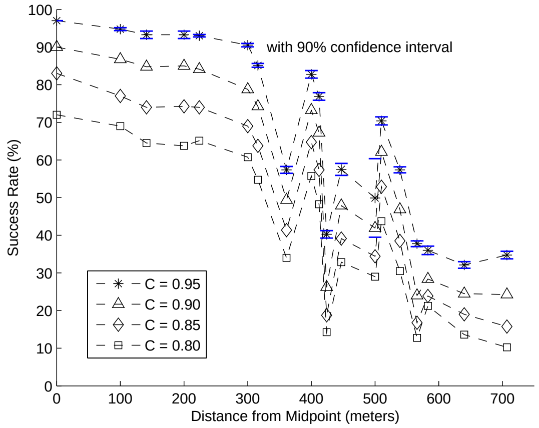

Fig. 7. Success Rate for Distances from Midpoint

While the highest success rates are associated with higher confidence levels, so are the area sizes. Figure 9 shows the area size as a percentage of the total area depicted in the 1000×1000 meter grid for the simulations using the two-receiver and four-receiver scenarios. In each scenario, the area size decreases with the confidence level. This reflects the reduced value of the normalization constant z for lower confidence levels. The shadowing interval is therefore smaller, resulting in reduced hyperbolic areas whose intersections are correspondingly smaller. However, the candidate areas for the two-receiver scenario are significantly larger than those for the four-receiver scenario, reaching 62% of the total area in some instances. Clearly, this type of result is of very little use in locating an attacker. The four-receiver scenario yields more promising results, where even the 0.95 confidence level produces a candidate area on average below 25% of the total size of the grid. This finding is consistent with the expectation that a higher number of receivers yields finer grained results and thus bounds the transmitter location to a smaller candidate area.

Figure 10 illustrates the average area size for the success rates achieved with each confidence level in the four-receiver scenario. In general, the size of the candidate area is larger for given success rate as the confidence level increases. For example, a success rate of 80% yields a candidate area of 23% for $\mathcal{C} = 0.95$, an area size of 18% for $\mathcal{C} = 0.90$ and an area of 17% for $\mathcal{C} = 0.85$. Thus the average area size clearly decreases with the confidence level, due to the reduced shadowing interval.

C. Discussion

The localization algorithm can be applied to multiple types of wireless networks for the purpose of bounding the position of an uncooperative transmitting device. Applications for wireless network security

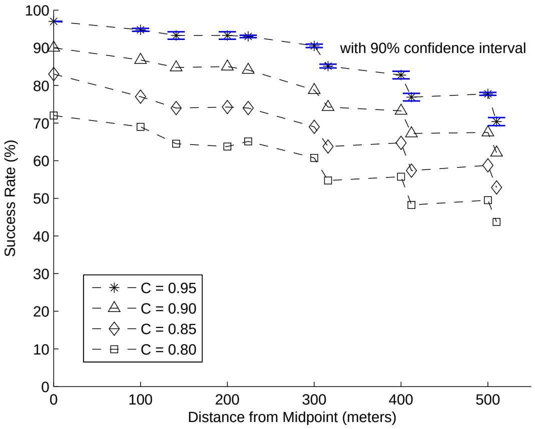

Fig. 8. Success Rate for Aggregate Range Points

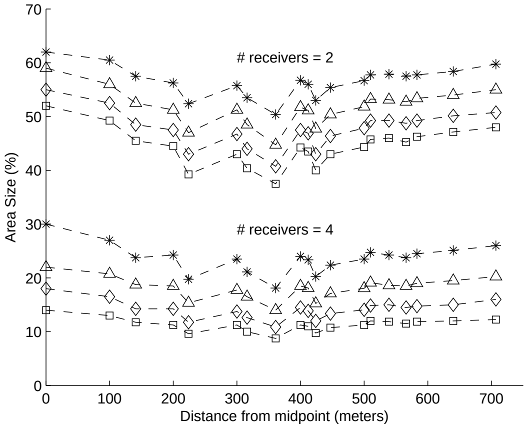

Fig. 9. Area Size for Distances from Midpoint

include the localization of nodes that cannot be trusted. For example, the attribution of attack messages as originating from a particular candidate area may implicate devices known to the trusted members of the network and thus suspect. It is also possible that our mechanism can play a role in localizing nodes that are simply unable to assist with efforts to determine their position, for example in sensor networks.

We expect that future experiments involving the application of our localization mechanism to specific types of wireless technologies, for example in vehicular networks, will confirm our findings that a greater number of receivers reduces the candidate area size. While our simulations focus on two and four-receiver scenarios, evidence of a vehicular communications attack may be gathered from receivers such as private and commercial vehicles in order to supplement the information obtained from the trusted infrastructure devices. Additional reductions in candidate area size can also be achieved using available navigation information, such as street and road layouts and building positions. If a rogue device's location is restricted to a known navigable space, the size and shape of hyperbolic areas can be tailored to this layout. Further research is required to investigate the degree to which the size of a candidate area can be minimized while maximizing the rogue localization success rate.

While our scheme accounts for a range of possible EIRP values employed by a rogue in order to obfuscate its position, the use of directional antennas may influence the relative RSS values received by trusted devices and foil our attempts at localization. An important area for future research involves assessing the potential impact of directional signals and augmenting our mechanism accordingly.

Another area for future investigation is the combination of the confidence levels ascribed to the intersection of hyperbolic areas by multiple receiver pairs. Intuitively, an area endorsed by a greater number

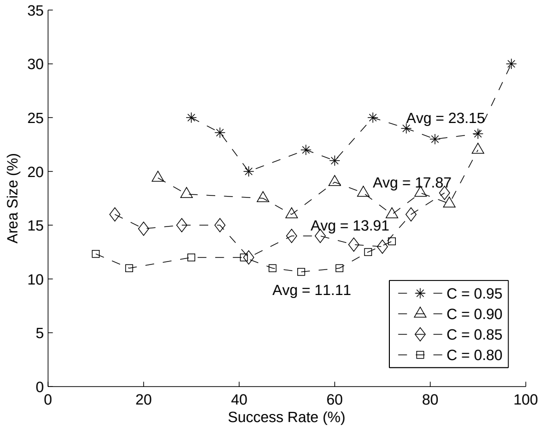

Fig. 10. Area Size per Success Rate

of receivers should be given a higher probability than areas advocated by fewer receivers. However in multiplicative probabilities, if two receiver pairs agree with confidence 0.95 that a transmitter is located in a particular area, then that area is assigned confidence 0.95^2. If four receiver pairs agree, then the confidence drops to 0.95^4. We require a scheme to assign a probability distribution to the possible transmitter location where agreement from multiple receivers compounds the probability inside the intersecting hyperbolic areas without redistributing it outside the intersections.

V. Conclusion

In this paper, we presented a hyperbolic location estimation mechanism for attributing an attack message to an originating rogue device by estimating its position in a wireless network without the rogue's cooperation. The localization algorithm utilizes the relative RSS values of the attack message received at a set of trusted receivers to estimate the position of the transmitting device based on the aggregated RSS values, even though the transmitting EIRP power is unknown.

The scheme presented employs a large scale path loss statistical model to estimate the distances from the transmitter to a set of trusted receivers, with a selected confidence level. These distances are computed from the RSS values and yield a distance difference range between the transmitter and each pair of receivers. Hyperbolas are then constructed between each receiver pair at the minimum and maximum bounds of the distance difference range. The intersecting hyperbolic area between multiple pairs of receivers constitutes a candidate area for the location of the transmitting device with the given degree of confidence. Performance evaluation through simulations reveals a success rate commensurate with the selected confidence level, although the size of the candidate area also increases with the success rate. Correspondingly, a confidence level of 95% yields an average candidate area size slightly below 25% of the simulated grid area.

The localization algorithm presented herein is sufficiently generic to be applicable to various types of wireless networks. It may also play a role outside the realm of network security where an attack is attributed to a rogue insider. For example in sensor networks, a malfunctioning device may be localized with our mechanism even if it is unable to assist in efforts to pinpoint its position. We foresee that each specific type of technology, for example WiMAX/802.16 access networks or vehicular networks, can exploit its particular characteristics to enhance the localization algorithm. It is expected that future research into the application of the localization algorithm to specific wireless technologies will result in the reduction of candidate area size for more precise rogue localization with higher success rates.

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] ASTM International. Standard Specification for Telecommunications and Information Exchange Between Roadside and Vehicle Systems – 5 GHz Band Dedicated Short Range Communications (DSRC) Medium Access Control (MAC) and Physical Layer (PHY) Specifications. ASTM E2213-03, September 2003.

[2] 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.

[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] 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.

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

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

[7] 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*, 46(11):1484–1496, November 1998.

[8] 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)*, pages 43–52, September 2006.

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

[10] M. Hata. Empirical Formula for Propagation Loss in Land Mobile Radio Services. *IEEE Transactions on Vehicular Technology*, 29(3):317–325, August 1980.

[11] 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.

[12] IEEE 802 Committee of the IEEE Computer Society. Draft Amendment to Standard for Information Technology - Telecommunications and Information Exchange Between Systems - LAN/MAN Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Wireless Access in Vehicular Environments (WAVE). Draft IEEE Standard, IEEE P802.11p/D1.1, January 2005.

[13] 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.

[14] LAN MAN Standards Committee of the IEEE Computer Society and the IEEE Microwave Theory and Techniques Society. IEEE Standard for Local and Metropolitan Area Networks - Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems - Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands and Corrigendum 1. IEEE Std 802.16e-2005, December 2005.

[15] C. Laurendeau and M. Barbeau. Threats to Security in DSRC/WAVE. In *Ad-Hoc, Mobile, and Wireless Networks: Proceedings of the 5th International Conference (ADHOC-NOW)*, volume 4104 of *Lecture Notes in Computer Science*, pages 266–279. Springer Berlin / Heidelberg, 2006.

[16] C. Laurendeau and M. Barbeau. Secure Anonymous Broadcasting in Vehicular Networks. In *Proceedings of the 32nd IEEE Conference on Local Computer Networks (LCN)*, pages 661–668, October 2007.

[17] 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.

[18] 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.

[19] B.-C. Liu and K.-H. Lin. Distance Difference Error Correction by Least Square for Stationary Signal-Strength-Difference-based Hyperbolic Location in Cellular Communications. *IEEE Transactions on Vehicular Technology*, 57(1):227–238, January 2008.

[20] 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.

[21] 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.

[22] 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.

[23] 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.

[24] 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.

[25] L. Ponemon. National Survey on Managing the Insider Threat. Technical report, Ponemon Institute, LLC, September 2006.

[26] T. S. Rappaport. *Wireless Communications: Principles and Practice*. Prentice-Hall, New Jersey, second edition, 2002.

[27] M. Raya, A. Aziz, and J.-P. Hubaux. Efficient Secure Aggregation in VANETs. In *Proceedings of the 3rd International Workshop on Vehicular Ad Hoc Networks (VANET)*, pages 67–75, September 2006.

[28] 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*, 9(3):155–164, July 2002.

[29] K. Sampigethaya, L. Huang, M. Li, R. Poovendran, K. Matsuura, and K. Sezaki. CARAVAN: Providing Location Privacy for VANET. In *Proceedings of the Conference on Embedded Security in Cars (ESCAR)*, November 2005.

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

[31] V. Taliwal, D. Jiang, H. Mangold, C. Chen, and R. Sengupta. Empirical Determination of Channel Characteristics for DSRC Vehicle-to-Vehicle Communication. In *Proceedings of the 1st ACM International Workshop on Vehicular Ad Hoc Networks (VANET)*, page 88, October 2004.

[32] B. R. Waters and E. W. Felten. Secure, Private Proofs of Location. Technical Report TR-667-03, Department of Computer Science, Princeton University, January 2003.

[33] B. Xiao, B. Yu, and C. Gao. Detection and Localization of Sybil Nodes in VANETs. In *Proceedings of the 2006 Workshop on Dependability Issues in Wireless Ad Hoc Networks and Sensor Networks (DIWANS)*, pages 1–8, September 2006.

Christine Laurendeau received her B.Sc. and M.Sc. in Computer Science from the University of Ottawa in 1989 and 1992. She is currently a Ph.D. candidate at Carleton University's School of Computer Science in Ottawa, Canada. She focuses her research efforts on wireless communications security, specifically the security of wireless access networks and vehicular communications.

Michel Barbeau is a professor of Computer Science. He got a Bachelor, a Master's and a Ph.D., in Computer Science, from Université de Sherbrooke, Canada ('85), for undergraduate studies, and Université de Montréal, Canada ('87 & '91), for graduate studies. From '91 to '99, he was a professor at Université de Sherbrooke. During the '98-'99 academic year, he was a visiting researcher at the University of Aizu, Japan. Since 2000, he works at Carleton University, Canada. The topic of wireless communications has been his main research interest. He puts his efforts more particularly on the topics of wireless security, vehicular communications and wireless access network management. He also conducts work on small satellite software and AI for computer games.