Compounding Probabilistic Evidence for Hyperbolic Rogue 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—**Hyperbolic position bounding of malicious devices aims to estimate the location of a wireless network rogue insider that transmits an attack message containing falsified information to mislead honest nodes. A probabilistic path loss model is used to construct an area in Euclidian space bounded by minimum and maximum distance difference hyperbolas between each pair of trusted receivers. This hyperbolic area is said to contain the rogue insider with a degree of confidence. We explore the combination of evidence provided by a set of multiple receiver pairs supporting the intersection of their hyperbolic space. We propose a novel heuristic scheme to aggregate area probability so that the combined degree of confidence ascribed to the intersecting space is computed according to a paradigm of supportive rather than competitive evidence.**

Index Terms—**Combination of Evidence, Location Estimation, Vehicular Communications, Wireless Access Networks, Wireless Networks, Wireless Security**

I. INTRODUCTION

As attacks upon the integrity of wireless networks migrate from theoretical pursuits in academic laboratories to front-page news, the imperative for security mechanisms ensuring attack detection and attribution becomes increasingly compelling. The recent manipulation of tram system control signals by a young hacker in Poland nearly resulted in disastrous consequences for the passengers of several trains [1]. Similar incidents in technologies safeguarding public safety, such as collision avoidance applications in vehicular networks, have an even greater potential for dire outcomes. High profile exploits underscore the vulnerability of wireless networks to attacks, given the open nature of the radio signal propagation medium. Insider attacks are perpetrated by malicious nodes capitalizing on their access to valid credentials such as digital certificates. Since these rogues are authenticated members of the wireless network, they pose a particularly daunting challenge. Not only can they evade detection due to the inherent trust vested in them by network authorities, but if their credentials are fraudulently obtained, for example through theft, they can also escape retribution and eviction from the network. Since rogues cannot be trusted to provide credible clues to their identity, the attribution of an attack to its perpetrator must rely on distinguishing characteristics which cannot be falsified. One method for attributing an attack message to its originator is to pinpoint the physical location of the signal source using information divulged inadvertently, such as the signal strength of the transmission.

In [2], we describe a hyperbolic position bounding scheme to surmise the location of a transmitter using the relative received signal strength (RSS) measured at a number of trusted receivers. The threat model assumes the transmission of an attack message originating from a rogue insider capable of generating verifiable, authenticated messages. Infrastructure units with known coordinates, for example base stations (BSs) in wireless access networks such as WiMAX/802.16 [3] or road-side units (RSUs) in vehicular networks [4], constitute the receivers tasked with locating an attacker. A probabilistic model is used to estimate the minimum and maximum distance differences between a transmitter and each pair of receivers, assuming an unknown effective isotropic radiated power (EIRP) and signal fluctuations commensurate with a large scale propagation path loss model. Hyperbolas feature an interesting geometric property: every point on a hyperbola between two foci is located at the same distance difference of the foci. We exploit this property and compute hyperbolas between each receiver pair at the minimum and maximum bound of the distance difference range with both receivers at the foci. The maximum and minimum hyperbolas thus define a hyperbolic area in Euclidian space where the transmitter is located with a degree of confidence. The confidence provided by multiple receiver pairs must be combined for a higher degree of confidence associated with a smaller area as more receiver pairs are considered. When combining evidence supporting a given candidate area for a transmitter, the intuitive expectation is that an area endorsed by a large number of receivers should be assigned a greater confidence than the areas advocated by few. However in existing mechanisms, the opposite is true. For example, in multiplicative probabilities based on a binomial distribution, if two receiver pairs agree with confidence 0.95 that a transmitter is located in a particular area, that area is assigned confidence 0.95^2. If four receiver pairs agree, the confidence drops to 0.95^4. This counter-intuitive reduction in confidence has led us to develop a new probability distribution mechanism. We propose a novel heuristic scheme based on the Bayesian conditioning model to compound the degree of confidence endorsed by multiple receiver pairs in such a way that additional evidence supports the probability assignment in the common hyperbolic area intersection rather than redistributing it outside the intersection.

Section II outlines the existing literature on the combination of evidence. Section III reviews the hyperbolic position bound-

ing mechanism. Section IV describes our heuristic method for compounding probabilistic localization evidence. Section V analyzes the performance of our compounding probability algorithm. Section VI concludes the paper.

II. RELATED WORK

RSS values are used in location estimation mechanisms based on established signalprint maps [5], [6] and geometric methods [7], [8]. However, in assuming the cooperation of the device being localized, these mechanisms are unsuitable for insider attack attribution. In [2], we expand upon the probabilistic rogue detection scheme outlined by Barbeau and Robert [9]. Our mechanism bounds the possible location of a transmitter within hyperbolic areas, each associated with a degree of confidence. These confidence levels must be aggregated so that additional evidence supports rather than weakens the common hyperbolic area intersections.

The seminal work of Dempster and Shafer in establishing the Dempster-Shafer theory of evidence [10], [11] formulates the foundations for belief functions and rules for the combination of evidence provided by a set of independent observers. Previously, a multiplicative probability approach reconciled varying degrees of confidence in a given event by multiplying together the probabilities assigned to the event by the observers. In contrast, the Dempster-Shafer rule of combination introduces a normalization mechanism to compensate for the lack of knowledge of an observer vis-à-vis an event and to resolve the degree of conflict between observers. Our threat model requires the combination of probabilities in a hyperbolic area intersection common to a large number of receiver pairs, each assigning the intersection a high degree of confidence. By definition, the common intersections are the subject of little conflict in the evidence supplied by the receiver pairs. As demonstrated in Section IV-B, in circumstances of little conflict, the Dempster-Shafer rule of combination reduces to simple multiplicative probability.

Variants on the Dempster-Shafer theory aim to address situations with even greater sources of conflict, for example in Yager [12] and Inagaki [13]. As with the Dempster-Shafer approach, these reduce to multiplicative probability in the absence of significant conflict. Proportional assignment of probability according to the percentage of observations supporting an event is presented in Zhang [14] and Cholvy [15]. In the case of our threat model, where we are interested in a small intersection of relatively large hyperbolic areas, proportional assignment distributes the probability over the vast extent of the hyperbolic areas, rather than concentrating it in the intersection. The consensus operator introduced by Jøsang [16] yields similar results by combining both positive and negative observations for an event, but attributing weight to each observer according to a proportional assignment basis.

Voorbraak [17], [18] and Wakker [19] advocate the Dempster-Shafer theory for scenarios dealing with ignorance and Bayesian conditioning for those involving uncertainty. The open world principle assumed by the Dempster-Shafer theory of evidence is best suited to knowledge acquisition systems seeking to expand a corpus of beliefs and thus to alleviate ignorance. Our threat model assumes a closed world, where a transmitter must necessarily be positioned within the radio range of receivers. Although the transmitter's precise location within Euclidian space is uncertain, each receiver pair assigns this entire space a fully defined probability distribution. Because our attack scenario models uncertainty rather than ignorance, the Bayesian conditioning model emerges as more suitable for our purposes.

III. HYPERBOLIC POSITION BOUNDING

Fluctuations in large scale radio signal path loss are known to follow a log-normal model, as outlined by Rappaport [20]. Other empirical propagation models can be used for predicting path loss as a function of a transmitter-receiver distance, such as the Okumura [21], Okumura-Hata [22] and Nakagami [23] models, but they are unsuitable for forecasting the distance given the path loss computed from RSS values, as observed in [2]. The Rappaport model relies on a path loss exponent n dependent upon the propagation environment, a reference distance d_0 close to the transmitter and the standard deviation in path loss signal shadowing σ. These parameter values are obtained for a given frequency through practical experiments, as demonstrated by Durgin *et al.* [24] and Liechty *et al.* [25], among others. The average loss $\overline{L}(d_0)$ at the reference distance d_0 is calculated using free space propagation equations [26].

For a given confidence level $\mathcal{C}$, its associated normal distribution constant $z = \Phi^{-1}(\frac{1+\mathcal{C}}{2})$ available from a normal distribution table, and an estimated EIRP range $[\mathcal{P}^-, \mathcal{P}^+]$, we establish in [2] the minimum and maximum bounds of the distance difference range between a transmitter T and a pair of receivers R_i and 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 $\mathcal{C}$.*

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

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 $\mathcal{C}$.*

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

Proof: The proof can be found in [2]. ∎

From the distance difference range computed in Theorem 1, we construct the associated minimum and maximum hyperbolas between a receiver pair with both receivers lying at the foci. The minimum and maximum hyperbolas delineate the possible location of the transmitter, with the given degree of confidence.

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 [2]. ∎

For example, Figure 1 illustrates the hyperbolic areas between receiver pairs R_1, R_2 and R_3, R_4, as bounded by the minimum hyperbolas computed for both receiver pairs. The maximum hyperbolas are too large to be plotted to scale.
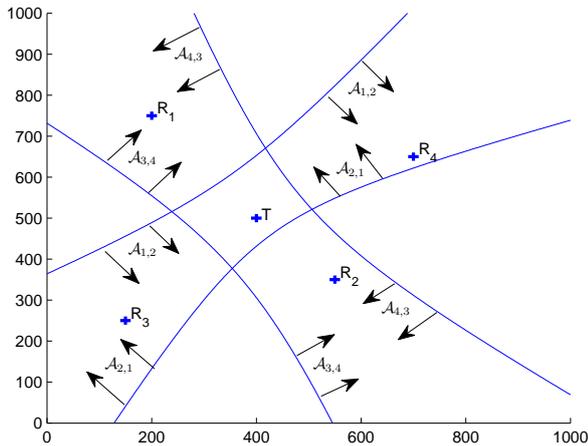

Fig. 1. Hyperbolic Areas for R_1, R_2 and R_3, R_4

IV. COMPOUNDING POSITION BOUNDING CONFIDENCE

Theorem 2 provides the means to delineate a hyperbolic area to bound the possible location of a transmitter, with a desired confidence level. However, given a number of receivers, hyperbolic areas can be constructed between multiple receiver pairs, and the confidence levels aggregated together. We define a set of partitions over the hyperbolic areas and their intersections. We revisit the application of existing mechanisms to combine the confidence levels in the partitions. We introduce a heuristic scheme to compound the evidence contributed by multiple receiver pairs and thus the probability in each hyperbolic area partition.

A. Partitioning the Hyperbolic Areas

We first define the partitioning of the Euclidian space encompassing the transmitter range, based on the number of intersecting hyperbolic areas in which each sub-area lies.

Definition 1. *Let $\mathcal{W}$ be the set of all defined hyperbolic areas computed using Theorem 2:*

$$\mathcal{W} = \{\mathcal{A}_{i,j} : \exists\, \mathcal{H}_{i,j}^-, \mathcal{H}_{i,j}^+ \text{ and } \\ \mathcal{A}_{i,j} \text{ is the area situated} \\ \text{between } \mathcal{H}_{i,j}^- \text{ and } \mathcal{H}_{i,j}^+\}$$

where $n = |\mathcal{W}|$. Let ξ be the union of all hyperbolic areas in $\mathcal{W}$ and the Euclidian space comprising their complements.

We define disjunctive partitions S^k of ξ such that for all $0 \leq k \leq n$, the partition S^k contains the sub-areas s_m of ξ situated at once within the intersection of k hyperbolic areas and within the intersection of the complements of the remaining $n - k$ hyperbolic areas in $\mathcal{W}$. More formally:

$$S^k = \left\{ s_m : s_m = (\cap^k \mathcal{A}_{i,j}) \cap (\cap^{n-k} \overline{\mathcal{A}}_{i,j}) \right\}$$

where $\cap^k \mathcal{A}_{i,j}$ is the intersection of any k hyperbolic areas and $\cap^{n-k} \overline{\mathcal{A}}_{i,j}$ is the intersection of the complements of the remaining $n - k$ hyperbolic areas.

Example. Figure 2 depicts the partitioning of the Euclidian space covered by the $n = 4$ hyperbolic areas $\{\mathcal{A}_{1,2}, \mathcal{A}_{2,1}, \mathcal{A}_{3,4}, \mathcal{A}_{4,3}\}$ shown in Figure 1. To define sub-area G, for example, we compute the intersection of $k = 3$ hyperbolic areas $(\mathcal{A}_{1,2}, \mathcal{A}_{2,1}, \mathcal{A}_{4,3})$, which yields $D \cup G$. The complement of the remaining $n - k = 1$ hyperbolic area $\mathcal{A}_{3,4}$ consists of $J \cup G \cup M$. The intersection of both defines sub-area G, since $(D \cup G) \cap (J \cup G \cup M) = G$. So we see that $G = \mathcal{A}_{1,2} \cap \mathcal{A}_{2,1} \cap \mathcal{A}_{4,3} \cap \overline{\mathcal{A}}_{3,4}$. In Figure 2, partition $S^4 = \{D\}$, $S^3 = \{E, F, G, H\}$, $S^2 = \{J, K, M, N\}$ and $S^1 = S^0 = \{\}$. If the Euclidean space could be displayed in its entirety, additional sub-areas for S^2, S^1 and S^0 would be visible. However, we restrict the scope of this example to a 1000×1000 meter grid.
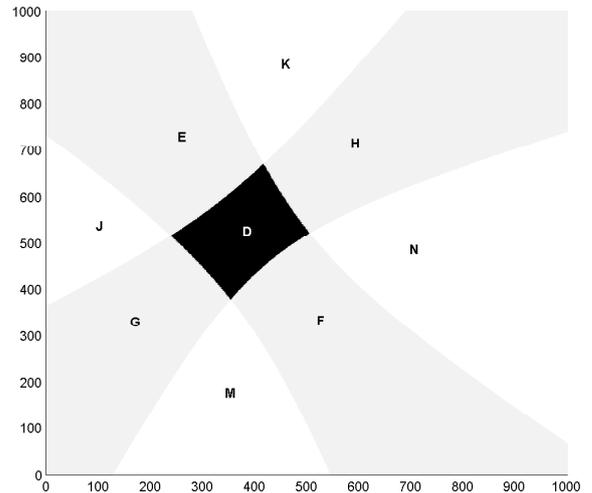

Fig. 2. Hyperbolic Area Partitions

B. Existing Evidence Combination Schemes

Every partition S^k is comprised of sub-areas situated in the intersection of the same number k of hyperbolic areas, and are thus equally likely sub-areas for the location of the

transmitter. As a result, we assign a single probability to each partition S^k based on the value of k. The intuitive idea is that the more hyperbolic areas a partition belongs to, the more likely it is that the transmitter is located in that partition, i.e. $Pr(T \in S^j) < Pr(T \in S^k)$ for all $0 \leq j < k \leq n$.

One method to compute the probability in a given partition involves multiplying together the probabilities assigned to its sub-areas by each receiver pair.

Lemma 1. *The multiplicative probability Pr^* of a transmitter located in sub-area s_m of partition S^k is the probability that it is situated in the intersection of k hyperbolic areas and the intersection of the complements of the remaining $(n-k)$ hyperbolic areas:*

$$Pr^*(T \in s_m \in S^k) = \mathcal{C}^k \times (1-\mathcal{C})^{n-k}$$

Proof:

$$
\begin{aligned}
Pr^*(T \in s_m \in S^k) &= Pr((T \in \cap^k \mathcal{A}_{i,j}) \\
&\quad \cap (T \in \cap^{n-k} \overline{\mathcal{A}}_{i,j})) \\
&\text{by Definition 1} \\
&= [Pr(T \in \mathcal{A}_{i,j})]^k \\
&\quad \times [Pr(T \in \overline{\mathcal{A}}_{i,j})]^{n-k} \\
&= \mathcal{C}^k \times (1-\mathcal{C})^{n-k} \\
&\text{by Theorem 2}
\end{aligned}
$$

∎

Of even greater interest is the probability assigned to the set of all sub-areas situated within a given partition S^k. Each hyperbolic area computed by a receiver pair can be thought of as an independent Bernoulli trial with probability of success $\mathcal{C}$ and probability of failure $(1-\mathcal{C})$. The findings of each receiver pair are independent of each other even if they share a common receiver, because the distance difference is unique to each pair. The probability distribution of a total of n hyperbolic areas is akin to n Bernoulli trials, and the resulting distribution is binomial.

Lemma 2. *The multiplicative probability Pr^* of a transmitter located in partition S^k is the probability that it lies in any of the sub-areas of S^k:*

$$Pr^*(T \in S^k) = \binom{n}{k} \times \mathcal{C}^k \times (1-\mathcal{C})^{n-k}$$

Proof: Since there are $\binom{n}{k}$ possible ways in which the transmitter can be located in k hyperbolic areas and in the complements of the remaining $n-k$ hyperbolic areas, there

are $\binom{n}{k}$ possible sub-areas in partition S^k. Therefore:

$$
\begin{aligned}
Pr^*(T \in S^k) &= \bigcup_{m=1}^{\binom{n}{k}} Pr^*(T \in s_m \in S^k) \\
&= \sum_{m=1}^{\binom{n}{k}} Pr^*(T \in s_m \in S^k) \\
&= \sum_{m=1}^{\binom{n}{k}} [\mathcal{C}^k \times (1-\mathcal{C})^{n-k}] \\
&\quad \text{by Lemma 1} \\
&= \binom{n}{k} \times \mathcal{C}^k \times (1-\mathcal{C})^{n-k}
\end{aligned}
$$

∎

However, the multiplicative probability method fails to effectively compound the confidence levels. Combined evidence from an increasing number of receiver pairs supporting the confidence in a given intersection actually *decreases* the overall probability in that area, since the multiplicative probability scheme re-distributes the associated probability outside the intersection. In the example depicted in Figure 1, with $\mathcal{C} = 0.95$, two hyperbolic areas inform us that the probability of the transmitter located in the intersection is $0.95^2 = 0.90$. But the evidence provided by four hyperbolic areas locates the transmitter in a smaller area with probability $0.95^4 = 0.81$. In effect, additional evidence supporting the original finding reduces the probability of the transmitter's location in the intersection, leading to the counter-intuitive conclusion that the transmitter is more likely to be found in the intersection of two hyperbolic areas than in the intersection of four areas.

The Dempster-Shafer method computes the plausibility Pl in a sub-area as its multiplicative probability, normalized to exclude the sub-areas of conflict. For our scenario, the Dempster-Shafer plausibility applies as follows:

$$Pl(T \in S^k) = \binom{n}{k} \times \frac{\mathcal{C}^k \times (1-\mathcal{C})^{n-k}}{1-K} \tag{1}$$

where K equals $(1-\mathcal{C})^k \times \mathcal{C}^{(n-k)}$ and represents the degree of conflict.

For our threat model, we are interested in localizing the rogue insider with a high degree of confidence, so $\mathcal{C}$ will generally be close to one, and so $(1-\mathcal{C})$ will be close to zero. The more useful probabilities are vested in the partitions with k close to n, since that is where the transmitter is most likely to be located. With a relatively large k compared to $(n-k)$ and a low value of $(1-\mathcal{C})$, the value of K is nearly equal to zero, so the denominator of Equation 1 is close to one. The Dempster-Shafer plausibility Pl thus reduces to the multiplicative probability Pr^* defined in Lemma 2.

C. Compounding Hyperbolic Area Confidence

We propose an alternate, heuristic method for aggregating evidence in such a manner that supporting evidence increases the likelihood of a transmitter located in a given area. The intuitive idea behind our mechanism is based on the Bayesian

conditional probability model and reflects the democratic principle. Given n hyperbolic areas, if all n agree that the transmitter is located in their common intersection with probability $\mathcal{C}$, then the partition corresponding to this intersection is assigned probability $\mathcal{C}$. Of the remaining probability $(1-\mathcal{C})$, the proportion assigned to the intersection of $n-1$ hyperbolic areas is $\mathcal{C}$, for $\mathcal{C} \times (1-\mathcal{C})$. Of the remaining $(1-\mathcal{C}) \times (1-\mathcal{C})$, $\mathcal{C}$ is assigned to the intersection of $n-2$ hyperbolic areas, and so on until the intersection of zero hyperbolic areas is assigned the remainder $(1-\mathcal{C})^n$.

Theorem 3. *Let ξ be the Euclidian space covered by n hyperbolic areas and their complements. Let the* compound *probability $Pr^\diamond$ that a transmitter is located in a partition S^k of ξ lying within k hyperbolic areas, for $k > 0$, be the probability that it is situated within k hyperbolic areas, given the supporting evidence that it is within $k-1$ of these areas, combined with the probability that it is outside the remaining $n - k$ hyperbolic areas. In the case where the partition is outside of all hyperbolic areas, i.e. for $k = 0$, the compound probability reduces to the simple multiplicative probability. Thus:*

$$Pr^\diamond(T \in S^k) = \begin{cases} \mathcal{C} \times (1-\mathcal{C})^{n-k}, & \text{for } k > 0 \\ (1-\mathcal{C})^n, & \text{for } k = 0 \end{cases}$$

Proof:

1. (i) For $k > 0$:

$$Pr^\diamond(T \in S^k) = Pr(T \in \cap^k \mathcal{A}_{i,j} \mid T \in \cap^{k-1} \mathcal{A}_{i,j})$$
$$\times Pr(T \in \cap^{n-k} \overline{\mathcal{A}}_{i,j})$$
$$= \frac{Pr(T \in [\cap^k \mathcal{A}_{i,j}] \cap [\cap^{k-1} \mathcal{A}_{i,j}])}{Pr(T \in \cap^{k-1} \mathcal{A}_{i,j})}$$
$$\times Pr(T \in \cap^{n-k} \overline{\mathcal{A}}_{i,j})$$
$$\text{by the definition of}$$
$$\text{conditional probabilities}$$
$$= \frac{Pr(T \in \cap^k \mathcal{A}_{i,j})}{Pr(T \in \cap^{k-1} \mathcal{A}_{i,j})}$$
$$\times Pr(T \in \cap^{n-k} \overline{\mathcal{A}}_{i,j})$$
$$\text{since } \cap^k \mathcal{A}_{i,j} \subseteq \cap^{k-1} \mathcal{A}_{i,j}$$
$$= \frac{[Pr(T \in \mathcal{A}_{i,j})]^k}{[Pr(T \in \mathcal{A}_{i,j})]^{k-1}}$$
$$\times [Pr(T \in \overline{\mathcal{A}}_{i,j})]^{n-k}$$
$$= \frac{\mathcal{C}^k}{\mathcal{C}^{k-1}} \times (1-\mathcal{C})^{n-k}$$
$$\text{by Theorem 2}$$
$$= \mathcal{C} \times (1-\mathcal{C})^{n-k}$$

(ii) For $k = 0$:

$$Pr^\diamond(T \in S^0) = Pr(T \in \cap^0 \mathcal{A}_{i,j})$$
$$\times Pr(T \in \cap^n \overline{\mathcal{A}}_{i,j})$$
$$= Pr(T \in \xi) \times [Pr(T \in \overline{\mathcal{A}}_{i,j})]^n$$
$$= 1 \times (1-\mathcal{C})^n = (1-\mathcal{C})^n$$
$$\text{by Theorem 2}$$

2. $Pr^\diamond(T \in S^k)$ is a probability distribution, since $\sum_{k=0}^{n} Pr^\diamond(T \in S^k) = 1$.

$$\sum_{k=0}^{n} Pr^\diamond(T \in S^k) = (1-\mathcal{C})^n$$
$$+ \sum_{k=1}^{n}[\mathcal{C} \times (1-\mathcal{C})^{n-k}]$$
$$= (1-\mathcal{C})^n + \mathcal{C} \times \sum_{k=0}^{n-1}(1-\mathcal{C})^k$$
$$= (1-\mathcal{C})^n$$
$$+ \mathcal{C} \times \left(\frac{1 - (1-\mathcal{C})^n}{1 - (1-\mathcal{C})}\right)$$
$$= (1-\mathcal{C})^n + 1 - (1-\mathcal{C})^n$$
$$= 1$$

∎

In contrast to the multiplicative probability Pr^* which follows a binomial distribution, the compound probability $Pr^\diamond$ reflects a geometric distribution. Every hyperbolic area within which the transmitter is located counts for a successful Bernoulli trial for Pr^*, but these are compounded as one combined success with probability $\mathcal{C}$ for $Pr^\diamond$, due to the democratic agreement. Consequently, only the number of failures $(n - k)$ with probability $(1 - \mathcal{C})$ are counted.

Example. The compound probability for the example illustrated in Figures 1 and 2 is shown in Figure 3. The probability associated with partition $S^4 = \{D\}$ is $\mathcal{C} = 0.95$, with partition $S^3 = \{E, F, G, H\}$ is $0.05 \times 0.95 = 0.0475$ and with partition $S^2 = \{J, K, M, N\}$ is $0.05^2 \times 0.95 = 0.002375$. If any sub-areas were associated with partition S^1, their probability would be $0.05^3 \times 0.95$, and the remainder would be assigned to S^0 with 0.05^4.
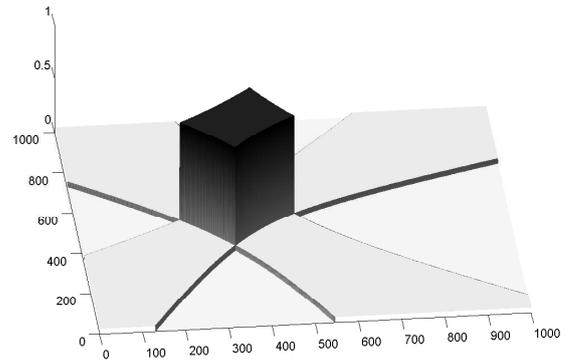

Fig. 3. Compound Probability for Hyperbolic Area Partitions

An optimization of Theorem 3 can be achieved by considering the probability of a transmitter's location within paired hyperbolic areas. The reason for this is one of symmetry. If a transmitter is centrally located between a pair of receivers R_i and R_j, it must necessarily lie within the symmetric hyperbolic area pair $\mathcal{A}_{i,j}$ and $\mathcal{A}_{j,i}$. If the transmitter is not

centrally situated, little granularity is lost by twinning the asymmetric pairs of hyperbolic areas within which it lies. We thus require a mechanism for combining the probabilities of paired hyperbolic areas, whether they correspond to symmetric receiver pairs or not.

Definition 2. *Let $r = \frac{n}{2}$ be the number of paired hyperbolic areas associated with the total n hyperbolic areas. We define disjunctive partitions V^γ of ξ such that for all $0 \leq \gamma \leq r$, the partition V^γ contains the sub-areas of ξ situated in the intersection of at least γ paired hyperbolic areas. More formally:*

$$V^\gamma = \begin{cases} S^{2\gamma}, & \text{for } \gamma = r \\ S^{2\gamma} \cup S^{2\gamma+1}, & \text{for } 0 \leq \gamma \leq r-1 \end{cases}$$

Example. In the example shown in Figure 2, partition $V^2 = \{D\}$ is comprised of the sub-area situated within four hyperbolic areas and thus two paired areas, for example $\mathcal{A}_{1,2}, \mathcal{A}_{2,1}$ or $\mathcal{A}_{3,4}, \mathcal{A}_{4,3}$. Partition $V^1 = \{E, F, G, H, J, K, M, N\}$ includes the sub-areas located in the intersection of two or three hyperbolic areas and thus in at least one paired area. Some of these paired areas are symmetric, as for sub-areas $\{E, F, G, H\}$ appearing in $\mathcal{A}_{1,2}, \mathcal{A}_{2,1}$ or in $\mathcal{A}_{3,4}, \mathcal{A}_{4,3}$. Other sub-areas are situated in asymmetric paired areas, for example $\{J\}$ is located in the intersection of $\mathcal{A}_{2,1}$ and $\mathcal{A}_{4,3}$. Partition V^0 equals $\{\}$ since every sub-area in Figure 2 appears in at least one paired hyperbolic area.

We extend the compound probability method proposed in Theorem 3 to consider paired hyperbolic areas.

Corollary 1. *Let the compound probability $Pr^\diamond$ that a transmitter is located in a partition V^γ of ξ lying within γ paired hyperbolic areas, for $\gamma < r = \frac{n}{2}$, be the probability that it is situated within partition $S^{2\gamma}$ or $S^{2\gamma+1}$. In the case where the transmitter is located in the intersection of all hyperbolic areas, i.e. for $\gamma = r$, the compound probability is equal to that of S^n. Thus:*

$$Pr^\diamond(T \in V^\gamma) =$$

$$\begin{cases} \mathcal{C}, & \text{for } \gamma = r \\ \mathcal{C} \times (2 - \mathcal{C}) \\ \quad \times (1 - \mathcal{C})^{(n-2\gamma-1)}, & \text{for } 1 \leq \gamma \leq r-1 \\ (1 - \mathcal{C})^{n-1}, & \text{for } \gamma = 0 \end{cases}$$

Proof:

1. For $\gamma = r$:

$$\begin{aligned} Pr^\diamond(T \in V^r) = Pr^\diamond(T \in S^n) & \quad \text{by Definition 2} \\ = \mathcal{C} \times (1 - \mathcal{C})^0 = \mathcal{C} & \quad \text{by Theorem 3} \end{aligned}$$

2. For $1 \leq \gamma \leq r - 1$:

$$\begin{aligned} Pr^\diamond(T \in V^\gamma) &= Pr^\diamond(T \in S^{2\gamma} \cup S^{2\gamma+1}) \\ & \quad \text{by Definition 2} \\ &= Pr^\diamond(T \in S^{2\gamma}) + Pr^\diamond(T \in S^{2\gamma+1}) \\ &= \mathcal{C} \times (1 - \mathcal{C})^{n-2\gamma} \\ & \quad + \mathcal{C} \times (1 - \mathcal{C})^{(n-(2\gamma+1))} \\ & \quad \text{by Theorem 3} \\ &= \mathcal{C} \times (1 - \mathcal{C})^{(n-2\gamma-1)} \times (2 - \mathcal{C}) \end{aligned}$$

3. For $\gamma = 0$:

$$\begin{aligned} Pr^\diamond(T \in V^0) &= Pr^\diamond(T \in S^0 \cup S^1) \\ & \quad \text{by Definition 2} \\ &= Pr^\diamond(T \in S^0) + Pr^\diamond(T \in S^1) \\ &= (1 - \mathcal{C})^n + \mathcal{C} \times (1 - \mathcal{C})^{n-1} \\ & \quad \text{by Theorem 3} \\ &= (1 - \mathcal{C})^{n-1} \end{aligned}$$

$\blacksquare$

V. PERFORMANCE EVALUATION

We describe the scenario configuration employed to acquire our simulation results. We compare the performance of both the compound and multiplicative probability schemes against our experimental results.

A. Scenario Configuration

The attack scenario is modeled on a 1000×1000 meter grid. The possible location of a transmitter is simulated along each grid point located at 100 meter intervals. Four receivers are simulated, and the RSS values computed at each receiver follow the Rappaport model [20] with a random amount of shadowing along a normal distribution curve with mean zero. We assume the radio signal frequency to be 2.4 GHz. The reference distance, path loss exponent and shadowing standard deviation measured experimentally for this frequency by Liechty *et al.* [25], [27] are used. One thousand executions of the position bounding algorithm are computed for each of four confidence levels $\mathcal{C} = \{0.95, 0.90, 0.85, 0.80\}$, for each possible transmitter location on the grid. The number of hyperbolic areas in which the transmitter is located is accumulated over the executions. The success rate of our results is deemed accurate within a confidence interval of $\pm 3\%$ to $\pm 4\%$ of the grid point mean, depending on distance between the transmitter location and center of the grid, with confidence 90%.

B. Experimental Results

We partition the simulation grid into three ranges of grid points within which the hyperbolic position bounding algorithm exhibits different behaviors. As with the bounding scheme, the compound probability mechanism performs optimally when the transmitter is located between pairs of receivers. Figure 4 illustrates the grid points at which the

transmitter locations are simulated, as well as the positions of the four receivers, each depicted by a small cross. The *central range* comprises the centrally located grid points, the *aggregate range* includes the grid points located between pairs of receivers so that the confidence levels can be combined, and the *outer range* includes the points outside the scope of any pair of receivers. The aggregate range points are deemed to encompass the central range points as well.
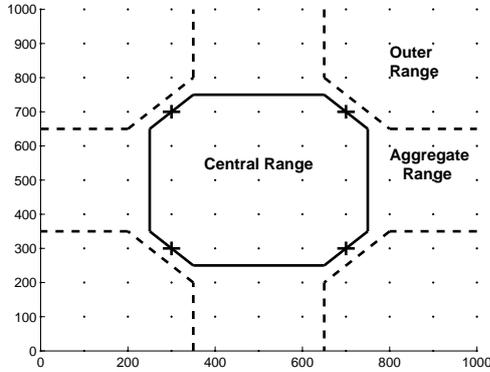

Fig. 4.   Simulation Grid Ranges

With four receivers in the simulation scenario, six possible receiver pairs compute a total of 12 hyperbolic areas. Figures 5 and 6 compare the probability distributions within these hyperbolic areas for $\mathcal{C} = 0.95$ and $\mathcal{C} = 0.90$. The compound probability (CP) and multiplicative probability (MP) distributions are computed according to Theorem 3 and Lemma 2 respectively. The experimental results depicted correspond to the simulated transmitter locations within the central (CR) and aggregate (AR) ranges. While both computed probability distributions decrease noticeably below the maximum 12 hyperbolic areas, the CP distribution remains more proportional to the simulation results obtained within both the central and aggregate ranges. For example, the relative probability decrease exhibited in the simulation results from 12 to 11 hyperbolic areas for $\mathcal{C} = 0.95$ averages around 93%, and the same decrease in compound probability is 95%. By contrast, the multiplicative probability decreases by only 37%.

The goodness-of-fit of the CP and MP distributions to the experimental results is measured using the statistic D_N associated with the Kolmogorov-Smirnov test [28], [29]. The Kolmogorov-Smirnov statistic expresses the difference between an empirical probability distribution $F_0(x)$ and a hypothesized one $F_N(x)$ as the least upper bound of the absolute difference between all the corresponding points of both distributions: $D_N = sup_x[\|F_N(x) - F_0(x)\|]$. Figure 7 depicts the Kolmogorov-Smirnov statistics with the computed distributions, CP and MP, as the empirical distribution, and the experimental results in the central and aggregate ranges as the hypothesized distribution. For all confidence levels, the maximum point-wise differences between the CP distribution and simulation results in both ranges are minimal, compared to their differences with the MP distribution. For $\mathcal{C} = \{0.95, 0.90\}$, the Kolmogorov-Smirnov statistics for CP and the simulation data remain below 15%, while they reach
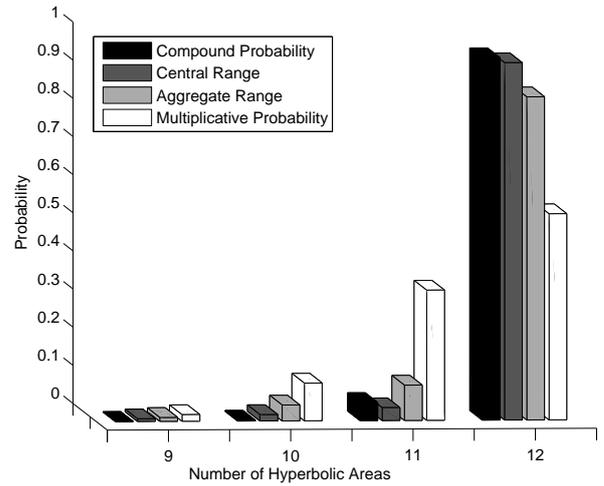

Fig. 5.   Hyperbolic Area Probability Distributions for $\mathcal{C} = 0.95$
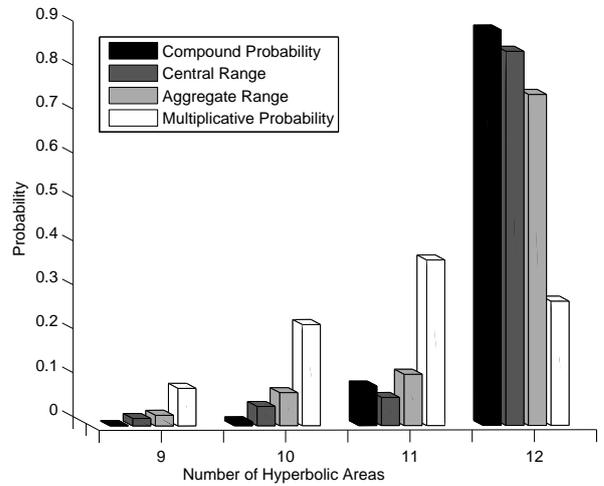

Fig. 6.   Hyperbolic Area Probability Distributions for $\mathcal{C} = 0.90$

60% when MP is considered. The performance of the CP algorithm in the central range alone is even better, with the maximum difference not exceeding 5% for $\mathcal{C} = \{0.95, 0.90\}$. The compound probability distribution is clearly the better model for the experimental results than multiplicative probability, although compound probability performs even better for the central range points.

Figures 8 and 9 illustrate the cumulative probability distribution results for $\mathcal{C} = 0.95$ and $\mathcal{C} = 0.90$. Again, it can be seen that the CP distribution more closely models both the central and aggregate range simulation results than does the MP distribution. Figure 10 plots the cumulative probability distribution for both CP and MP, given each of four confidence levels $\mathcal{C} = \{0.95, 0.90, 0.85, 0.80\}$. It should be noted that as a binomial distribution, the multiplicative cumulative probability follows a Gaussian curve, while the compound cumulative probability reveals an exponential curve. Because the probabilities exhibited by the simulation data also follow an exponential curve, as shown in the central range results of Figure 11, the compound probability mechanism inherently provides the better model independently of the value of $\mathcal{C}$.
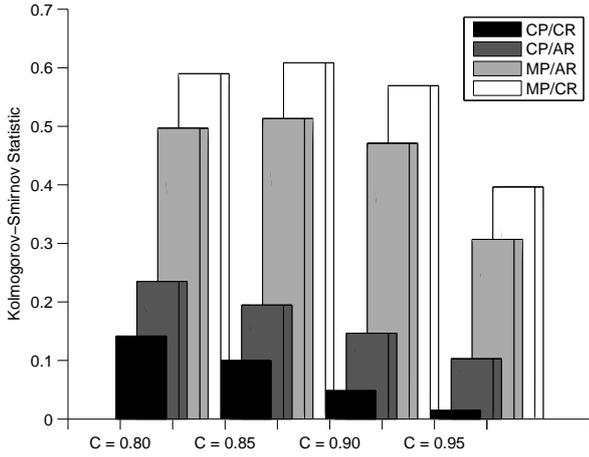
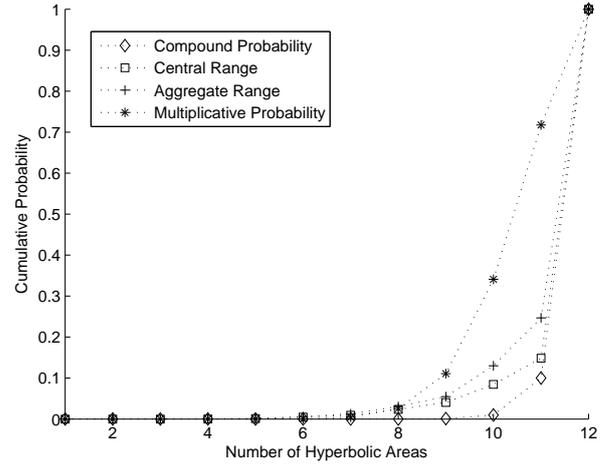Fig. 7.   Kolmogorov-Smirnov Statistic for Distribution Differences
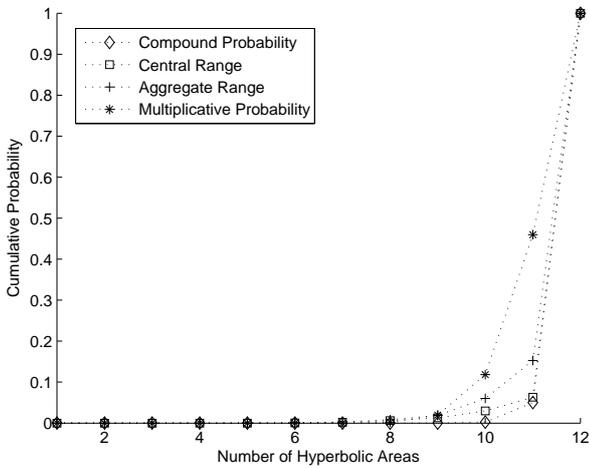

Fig. 9.   Cumulative Probability Distributions for $\mathcal{C} = 0.90$

Fig. 8.   Cumulative Probability Distributions for $\mathcal{C} = 0.95$
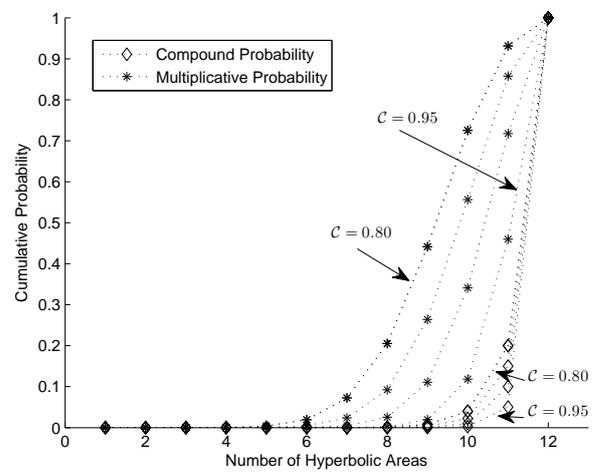

Fig. 10.   Compound and Multiplicative Cumulative Probability

The performance of the CP mechanism when hyperbolic areas are paired, as defined in Corollary 1 of Theorem 3, can be assessed by comparing the results of Figures 5 and 6 with those of Figures 12 and 13. Because the pairing algorithm exploits the natural symmetry between some of the hyperbolic area pairs, the correspondence between the CP distribution and simulation results is closer. For example, Figures 5 and 6 indicate a dip in the central range probability for 11 hyperbolic areas. Given that the grid points are centrally located, a significant portion of them are located in symmetric hyperbolic area pairs. As a result, their appearance in an odd number of hyperbolic areas is likely an anomaly. When hyperbolic areas are paired, as with Figures 12 and 13, this aberration disappears, and the corresponding probabilities are at once more commonsensical and better fitted to the experimental results.

VI. Conclusion

We presented a compound probability mechanism to combine together the confidence levels that the trusted receivers of an attack message assign to the hyperbolic areas delineating

a malicious insider node's probable position. These areas are computed using a position bounding algorithm that employs the relative RSS values of the attack message to estimate the location of the transmitting device within minimum and maximum hyperbolas, with a degree of confidence. The confidence of the hyperbolic areas computed by multiple pairs of receivers are aggregated to determine the confidence ascribed to the common intersections.

Given that our threat model is based on a closed world assumption necessitating the reduction of uncertainty rather than ignorance, the compound probability mechanism is based on the Bayesian conditioning model. This approach enables the supportive aggregation of concurring evidence rather than its weakening through competitive probability redistribution.

Performance evaluation through simulation reveals that the compounding probability paradigm constitutes a better probabilistic model of the hyperbolic position bounding experimental results than the simple multiplicative probability model. While the latter results in a maximum point-wise difference of up to 60% for the higher confidence levels when compared to the simulation data, our compound probability method
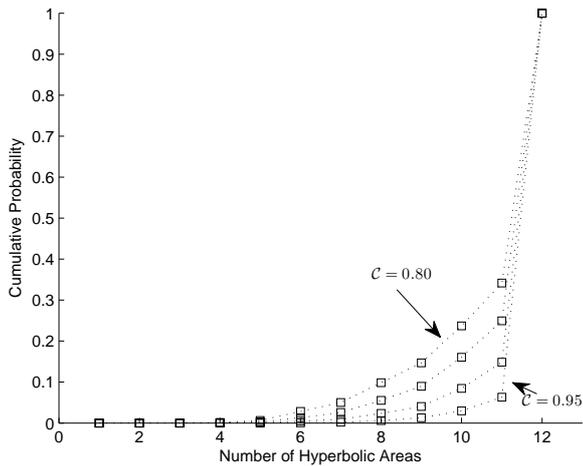
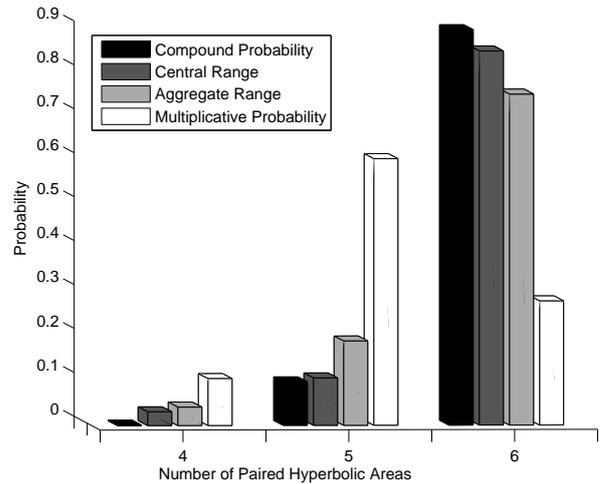Fig. 11.   Central Range Cumulative Probability

Fig. 13.   Paired Hyperbolic Area Probability Distributions for $\mathcal{C} = 0.90$
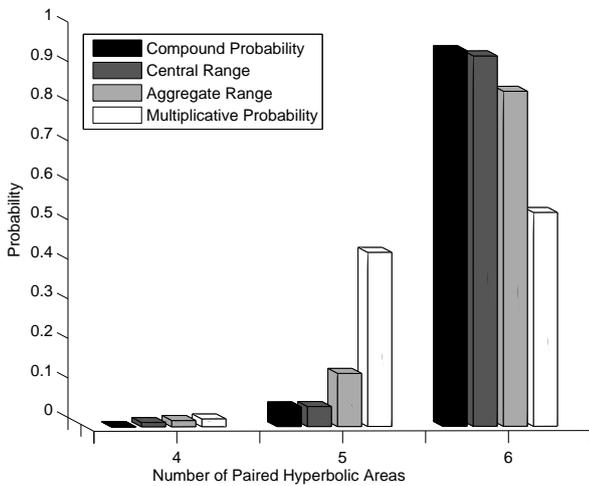

Fig. 12.   Paired Hyperbolic Area Probability Distributions for $\mathcal{C} = 0.95$

never exceeds a 15% difference. Our model clearly yields the better probability distribution for the experimental location estimation results.

The hyperbolic rogue position bounding algorithm is sufficiently generic to be applicable to various types of wireless technologies, such as WiMAX/802.16 access networks or vehicular networks. Consequently, any type of wireless technology adopting the position bounding mechanism will benefit from the probability compounding algorithm presented herein. What additional classes of problems in alternative domains can benefit from our confidence aggregation mechanism remains an open question.

REFERENCES

[1] G. Baker, "Schoolboy Hacks Into City's Tram System," The Telegraph, 11 January 2008, accessed 15 January 2008, [Online] http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2008/01/11/wschool111.xml.

[2] C. Laurendeau and M. Barbeau, "Rogue Attribution Using Relative Signal Strength Based Location Estimation," School of Computer Science, Carleton University, Technical Report TR-08-01, January 2008.

[3] 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, 2005.

[4] National ITS Architecture, "DSRC 5GHz: Dedicated Short Range Communication at 5.9 GHz Standards Group," [Online] http://www.iteris.com/itsarch/html/standard/dsrc5ghz.htm.

[5] 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.

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

[7] 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*, 2004, pp. 516–518.

[8] 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," in *IEEE Transactions on Vehicular Technology*, vol. 55, no. 2, March 2006, pp. 499–509.

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

[10] A. P. Dempster, "Upper and Lower Probabilities Induced by a Multivalued Mapping," in *The Annals of Mathematical Statistics*, vol. 38, no. 2, April 1967, pp. 325–339.

[11] G. Shafer, *A Mathematical Theory of Evidence*. Princeton University Press, 1976.

[12] R. R. Yager, "On the Dempster-Shafer Framework and New Combination Rules," in *Information Sciences*, vol. 41, no. 2, March 1987, pp. 93–137.

[13] T. Inagaki, "Interdependence Between Safety-Control Policy and Multiple-Sensor Schemes Via Dempster-Shafer Theory," in *IEEE Transactions on Reliability*, vol. 40, no. 2, June 1991, pp. 182–188.

[14] L. Zhang, "Representation, Independence and Combination of Evidence in the Dempster-Shafer Theory," in *Advances in the Dempster-Shafer*

Theory of Evidence, R. R. Yager, J. Kacprzyk, and M. Fedrizzi, Eds. New York: John Wiley & Sons, Inc., 1994, pp. 51–69.

[15] L. Cholvy, "Towards Another Logical Interpretation of Theory of Evidence and a New Combination Rule," in *Proceedings of the 9th International Conference on Information Processing and Management of Uncertainty in Knowledge-Based Systems*, 2002.

[16] A. Jøsang, "A Logic for Uncertain Probabilities," *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, vol. 9, no. 3, pp. 279–311, June 2001.

[17] F. Voorbraak, "Probabilistic Belief Expansion and Conditioning," ILLC, University of Amsterdam, Research Report LP-96-07, 1996.

[18] ——, "Deciding Under Partial Ignorance," in *Proceedings of the 2nd EUROMICRO Workshop on Advanced Mobile Robots*, 1997.

[19] P. P. Wakker, "Dempster Belief Functions Are Based on the Principle of Complete Ignorance," *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, vol. 8, no. 3, pp. 271–284, 2000.

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

[21] Y. Okumura, E. Ohmori, T. Kawano, and K. Fukuda, "Field Strength and its Variability in VHF and UHF Land-mobile Radio Service," in *Review of the Electrical Communication Laboratory*, vol. 16, no. 9–10, 1968, pp. 825–873.

[22] M. Hata, "Empirical Formula for Propagation Loss in Land Mobile Radio Services," in *IEEE Transactions on Vehicular Technology*, vol. 29, no. 3, August 1980, pp. 317–325.

[23] M. Nakagami, "The m-Distribution – A General Formula of Intensity Distribution of Rapid Fading," in *Statistical Methods in Radio Wave Propagation*, W. Hoffman, Ed. Oxford, England: Pergamon, 1960, pp. 3–36.

[24] 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," in *IEEE Transactions on Communications*, vol. 46, no. 11, November 1998, pp. 1484–1496.

[25] L. 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.

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

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

[28] A. N. Kolmogorov, "Sulla determinazione empirica di una legge di distribuzione," in *Giornale dell'Istituto Italiano degli Attuari*, vol. 4, 1933, pp. 83–91.

[29] N. Smirnov, "Estimate of Deviation Between Empirical Distribution Functions in Two Independent Samples," in *Moscow University Mathematics Bulletin*, vol. 2, 1933, pp. 3–16.

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.