This paper was presented as part of the Mini-Conference at IEEE INFOCOM 2011

Designing Localization Algorithms Robust to Signal Strength Attacks

Xiaoyan Li
Department of Computer Science
Lafayette College, Easton, PA 18042
Email:lix@lafayette.edu

Yingying Chen, Jie Yang, Xiuyuan Zheng
Department of Electrical and Computer Engineering
Stevens Institute of Technology, Hoboken, NJ 07030
Email:{yingying.chen,jyang,xzheng1}@stevens.edu

Abstract—**Received Signal Strength (RSS) based localization algorithms are sensitive to a set of non-cryptographic attacks. For example, the attacker can perform signal strength attacks by placing an absorbing or reflecting material around a wireless device to modify its RSS readings. In this work, we first formulate the all-around signal strength attacks, where similar attacks are launched towards all landmarks, and experimentally show the feasibility of launching such attacks. We then propose a general principle for designing RSS-based algorithms so that they are robust to all-around signal strength attacks. To evaluate our approach, we adapt two RSS-based localization algorithms according to our principle and experiment with real attack scenarios. All the experiments show that our design principle can be applied to achieve comparable performance with much better robustness.**

I. Introduction

With the proliferation of wireless communication and wireless networks, ubiquitous wireless applications are becoming commonplace. Contextual information such as location of the wireless devices is critical for many of the high level applications as it is inherent to their logic. The problem of accurately localizing wireless node's location thus has drawn intense research interests recently. Among all the proposed approaches, Received Signal Strength (RSS) based algorithms [1], [2] are particularly attractive since they allow the reuse of existing communication infrastructure and are applicable to many commodity radio technologies.

A typical setup for an RSS-based localization system is as follows: within the environment, there are a few pre-deployed landmarks with known location information, $L_i(x_i, y_i)$, $i = 1, 2..., n$; when a mobile device enters the area, its signal can be sensed by all landmarks, which together form a *fingerprint* of its current position $\overrightarrow{SS}(< SS_1, SS_2..., SS_n >)$ and can be used for localization. In order to account for the chaotic signal propagation in indoor environment, many previously proposed RSS based indoor localization systems have an offline phase and an online phase. In the offline phase, signal fingerprints are empirically measured at m locations. All m fingerprints along with their locations $[(x_i, y_i), \overrightarrow{SS_i}]$ constitute the fingerprints for the sampled environment. In the online localization phase, RSS fingerprint collected for the mobile device is then used to compare with the pre-collected fingerprints during offline to estimate the location.

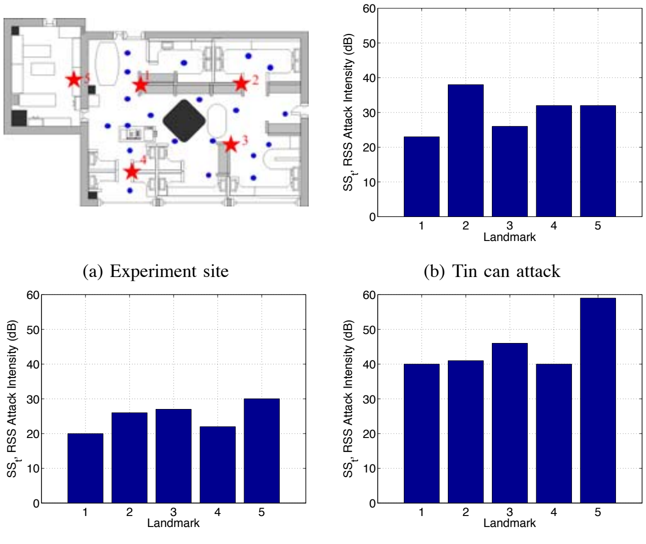
RSS-based localization algorithms, however, are sensitive to a set of non-cryptographic attacks, where the physical measurement process itself can be corrupted by adversaries [2]. For example, the attacker can perform signal strength attacks by placing an absorbing or reflecting material around a wireless device to modify its RSS. [2] evaluated a whole spectrum of algorithms in terms of robustness to such attacks through simulation and observed performance degradation for all algorithms. Such vulnerability to signal strength attacks threatens the localization algorithms' viability for a wide domain of applications using wireless systems.

Several previous works [3]–[5] have proposed secure localization algorithms to address the non-cryptographic signal strength attacks. They, however, assume that only a small percentage (less than half) of the landmark readings are under attack. In this work, instead, we focus on addressing *all-around signal strength attacks*, where similar attacks are launched towards all landmarks. Such attacks are easy to launch in practice and may affect many applications. For example, in an environment where valuable commodities are monitored via RSS-based localization. A thief can easily put what he stole in a metal box or suitcase, which essentially causes all-around attacks, to throw off the localization system.

To address the all-around attacks, we propose a principle that advises the usage of a new ratio-based signal strength metric instead of RSS in designing localization algorithms. Such a metric maps to information about distance ratio to a set of landmarks (thus ratio-based metric), which aims to achieve robust localization under attacks. The attack resilience of algorithms following our principle guidance comes from the inherent robustness of this new metric to all-around attacks.

Several previous works have proposed ratio-based localization algorithms [6], [7]. Our principle, however, does not correspond to any particular algorithms. It, instead, is a general design rule that can be applied to many different algorithms. To demonstrate such general applicability, we adapt two representative localization algorithms according to our principle. We then evaluate the adapted algorithms with realistic attacks. Our experiments show that the adapted algorithms offer comparable performance with the original RSS-based algorithms under normal conditions. When all-around attacks are launched, however, the adapted algorithms demonstrate much less performance degradation, thus achieve better robustness.

978-1-4244-9921-2/11/$26.00 ©2011 IEEE



(a) Experiment site

(b) Tin can attack

(c) Power variation attack: 20 dB

(d) Power variation attack: 40 dB

Fig. 1. All-around signal strength attacks: attack feasibility study.

In the rest of the paper, we first discuss the all-around signal strength attacks in Section II. Section III presents the design principle we propose. Section IV explains the algorithms adaptation according to our principle. Finally, we validate our principle by evaluating the adapted algorithms in Section V.

II. All-Around Signal Strength Attacks

In this section, we first present our attack model. We then conduct two real signal strength attacks to demonstrate the feasibility of such attacks.

A. Attack Model

We define the all-around signal strength attacks as that when similar attacks are launched towards all landmarks. Specifically, if the normal signal strength fingerprint for a mobile device is as follows with n landmarks:

$$\overrightarrow{SS} = < SS_1, SS_2, ..., SS_n >,$$

then the fingerprint measurement under the all-around signal strength attack would be

$$\begin{aligned} \overrightarrow{SS}' &= < SS_1^{'}, SS_2^{'}, ..., SS_n^{'} > \\ &= < SS_1 - SS_t, SS_2 - SS_t, ..., SS_n - SS_t >, \end{aligned}$$

which indicates that it suffers a signal attenuation of SS_t under the attack.

B. Attack Feasibility Study

Practically, all-around signal strength attacks are easy to launch. We next experimentally demonstrate its feasibility by launching such attacks with two simple methods.

Our experimental data were collected on the second floor of Buchard building at Stevens Institute of Technology, which is a $80ft \times 70ft$ area as shown in Figure 1 (a). This is a large lab area containing office wall dividers and furniture, such as desks, shelves and chairs. We deployed 5 landmarks and collected RSS fingerprints for 20 sample locations. Landmarks and sample locations are shown as stars and dots respectively in the figure. RSS measurements were collected with active RFID tags and readers from InPoint [8]. We connected the RFID readers to a Linux machine to serve as our landmarks, which then continuously monitor the channels' traffic at the packet-level. In our experiments, each averaged RSS reading was obtained over 100 packets.

We conducted two sets of attacks: *tin can attack* and *power variation attack*. In *tin can attack*, the attacker places the RFID tag within a tin can to attenuate its signal strength. Whereas in *power variation attack*, the attacker programs the RFID tag to change its transmission power to affect signal strength measurements. We assume the normal transmission power to be 10 dBm while attackers can use both -10 dBm and -30 dBm, thus launching attacks of 20 dB and 40 dB respectively.

Figure 1 (b)-(d) plot the signal strength attack, $SS_t = SS_i^{'} - SS_i$, on all landmarks at a particular sample location. It shows the effects of both tin can attack and two levels of power variation attacks. We observed that the simple tin can attack is very effective, resulting in 20 to 30 dB attenuation, and the power variation attack achieves an average of around 20 dB and 40 dB signal attenuation corresponding to its attack severity of 20 dB and 40 dB respectively. The attacks on all landmarks are not exactly the same, however, they are indeed very similar. We show in Section III that our attack model allows for the derivation of a simple yet effective principle for robustness design, while the similarities of attacks among the landmarks are sufficient to achieve robustness.

III. Design Principle for Robust Localization

The key principle we propose is to use a more robust signal strength metric instead of RSS while designing localization algorithms. In the following, we first introduce the new metric and then explain how it allows for localization.

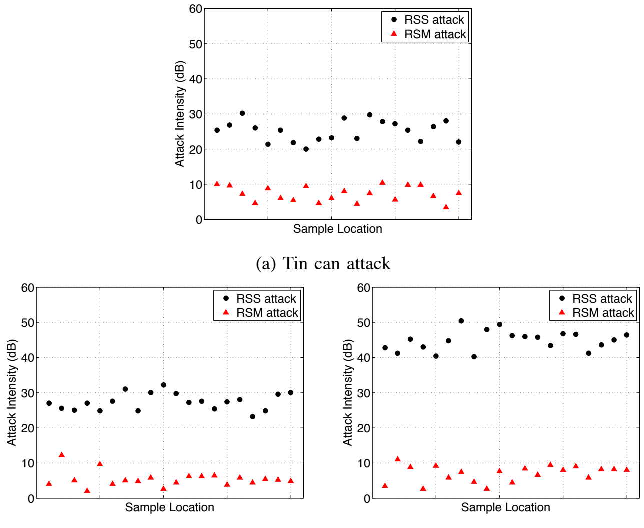
A. A Robust Signal Strength Metric

RSS-based localization is feasible mainly because it is a metric inherently characterizing the distance separation between the transmitter and the receiver (for example, between the mobile device and the landmarks, $d_i, i = 1, 2..., n$). When all-around signal strength attack is launched, such relationship is corrupted. However, since similar attacks are launched towards all the landmarks, any pair of signal strength value (SS_i, SS_j) still carries correct information about the relative length of the distance separations, i.e. distance ratio $(\frac{d_i}{d_j})$, which can still be used for localization. We thus propose to use Ratio-based Signal strength Metric (RSM) to achieve robustness.

Our RSM metric characterizes the relative signal strength values measured at two landmarks, L_i and L_j, for a particular mobile device. Its formal definition is as following:

$$RSM_{ij} = SS_i - SS_j. \qquad (1)$$

According to our attack model, RSM is robust to all-around



(a) Tin can attack

(b) Power variation attack: 20 dB

(c) Power variation attack: 40 dB

Fig. 2. Metric robustness analysis: RSS vs. RSM

signal strength attacks since

$$\begin{aligned} RSM'_{ij} &= SS'_i - SS'_j \\ &= (SS_i - SS_t) - (SS_j - SS_t) = RSM_{ij}. \end{aligned} \quad (2)$$

We noticed in Section II that exact uniform attacks to all landmarks may not be practical. However, the similarity among attacks towards all landmarks still offers RSM better robustness than RSS. To demonstrate such robustness, we quantify the attacks to both metrics as:

$$\begin{aligned} Attack_{RSS} &= \frac{\sum_{i=1}^{n} |SS'_i - SS_i|}{n} \\ Attack_{RSM} &= \frac{\sum_{i=1}^{n-1} \sum_{j=i+1}^{n} |RSM'_{ij} - RSM_{ij}|}{\frac{n \times (n-1)}{2}}. \end{aligned} \quad (3)$$

Figure 2 plots the attack intensity to both RSS and RSM in our three different all-around attacks. We see that RSM is subject to significantly less attacks than RSS under the same attack scenarios. We show in Section V that such robustness in RSM metric does translate to better robustness in localization.

B. RSM Allows for Localization

We explain the feasibility of using RSM for localization in two steps. First, we map RSM metric to distance ratio. We then explain why distance ratio information can be used for localization.

1) RSM Maps to Distance Ratio: Normally, signal propagation is modeled as the distance dependent path loss model [1]. For example, with consideration of possible attacks, the signal strength (dBm) measured at landmark L_i from a mobile device can be modeled as:

$$\begin{aligned} SS_i(d_i) = SS_i(d_0) - n_i log_{10}(\frac{d_i}{d_0}) + \delta SS_i - SS_t \\ \delta SS_i \sim N(0, \sigma_i) \end{aligned} \quad (4)$$

where $SS_i(d_0)$ is the RSS measured at some reference distance d_0 which is normally small, n_i indicates the signal degradation rate, d_i is the distance from the mobile device to L_i, δSS_i represents the signal strength bias caused by local environmental noise around the measurement location, and SS_t is the effect from signal strength attacks.

$SS_i(d_0)$ is mostly decided by the transmitter's model and its transmission power. For localizing a particular device, since all landmarks measure signal strength from the same device, $SS_i(d_0)$ should be the same for all landmarks. According to our attack model, the same amount of attack is applied to all landmarks, thus SS_t are the same for all landmarks as well.

With the above clarification, RSM metric for any two landmarks, L_i and L_j, for a particular mobile device can be represented as

$$\begin{aligned} RSM_{ij} &= n_j log_{10}(\frac{d_j}{d_0}) - n_i log_{10}(\frac{d_i}{d_0}) + \delta SS_{ij} \\ & \quad \delta SS_{ij} \sim N(0, \sigma_{ij}) \end{aligned} \quad (5)$$

where d_i and d_j are the distance from the mobile device to L_i and L_j, respectively. RSM_{ij} also has a normal distributed noise, since the subtraction of normal distributions still follows normal distribution.

The signal degradation rate n_i (as shown in Equation 4) is generally decided by the travel path of the signal, thus even though measured for the same transmitter, the rates for signals arriving at different landmarks may be different. However, all the signal propagation is subject to the same environmental effect at a coarse level. If we approximate the rates to be the same (n) in an environment, Equation 5 can be further simplified as

$$\begin{aligned} RSM_{ij} = nlog_{10}(\frac{d_j}{d_i}) + \delta SS_{ij} \\ \delta SS_{ij} \sim N(0, \sigma_{ij}) \end{aligned} \quad (6)$$

Equation 6 shows that there is direct mapping between RSM metric, RSM_{ij}, and distance ratio $\frac{d_j}{d_i}$. RSM-based localization is feasible mainly because knowing distance ratio to a set of landmarks allows for localization.

2) Ratio-based Localization: Apollonius circles [9] can be used to demonstrate how distance ratio information helps with localization. Apollonius circles represent the set of all points whose distances from two fixed points are in a constant ratio $m : n$. (In case $m = n$, these set of points become a line, which is the perpendicular bisector of the line segment connecting the two fixed points.) For example, in Figure 3 the top most circle drawn in solid line represents all the points whose distance to point A, d_A, and point C, d_C, satisfy the constraint that $\frac{d_A}{d_C} = 1.49$. Similarly, the other two circles drawn in solid line represents all the points where $\frac{d_A}{d_B} = 2.41$ and $\frac{d_B}{d_C} = 0.62$ respectively.

For localization, landmarks can be treated as a set of fixed points (for example, point A, B, C, D in Figure 3). If we know the distance ratio from a mobile device to the set of landmarks $(\frac{d_A}{d_B}, \frac{d_B}{d_C}, \frac{d_A}{d_C})$, its location can then be calculated as the intersection point of a set of Apollonius Circles. Although our RSM-based algorithms do not use distance ratio information explicitly, the direct mapping relationship between RSM and distance ratio determines the feasibility of localization using our RSM metric.

Normally we need at least three circles to find a unique intersection point. We, however, see in Figure 3 that the three Apollonius circles drawn in solid line do not render a unique intersection point. This is because the third Apollonius circle from the three fixed points, A, B, C, is redundant in terms of locating the intersection point. Given the first two circles, $\frac{d_A}{d_C} = 1.49$ and $\frac{d_A}{d_B} = 2.41$, the third one could easily be calculated without requiring any new information, $\frac{d_B}{d_C} = \frac{d_A}{d_C} / \frac{d_A}{d_B}$. It does not contribute any new constraint either. This determines that we need at least four fixed points to uniquely identify the intersection point. In Figure 3, the circle drawn in dashed line represents $\frac{d_A}{d_D} = 4.01$. The addition of this circle uniquely identifies an intersection point.

For localization, this constraint translates to the need of at least four landmarks in order to uniquely locate mobile devices using RSM information. However, due to the unpredictable nature of indoor signal propagation, normally at least four landmarks are deployed even for the RSS-based algorithms. We thus consider this requirement as easily satisfiable.

IV. Adaptation of Localization Algorithms

Our proposed principle is a general rule that can be used while designing new algorithms or be applied to adapt many existing algorithms. In this section, we demonstrate its usage by adapting two previously proposed localization algorithms.

A. Lateration Based

Localization using the lateration based approach is popular [10] and involves 2 steps: *ranging* and *lateration*. In the ranging step, distances ($d_i, i = 1, 2.., n$) from the mobile device $M = (x, y)$ to all the landmarks ($L_i = (x_i, y_i), i = 1, 2.., n$) are estimated, where $d_i = \sqrt{(x_i - x)^2 + (y_i - y)^2}$. In the lateration step, the position of the mobile device is estimated based on the estimated distances $\hat{d_i}$ and the known positions $L_i = (x_i, y_i)$ of the landmarks. In this work, we use RSS to perform ranging and Nonlinear Least Squares (NLS) method to localize. In NLS, the position (x, y) of the mobile device is estimated by finding $(\hat{x}, \hat{y})$ satisfying:

$$(\hat{x}, \hat{y}) = argmin_{x,y} \sum_{i=1}^{n} [\sqrt{(x_i - x)^2 + (y_i - y)^2} - \hat{d_i}]^2 \quad (7)$$

To adapt NLS to use RSM, we estimate distance ratios ($r_{ij} = \frac{d_i}{d_j}$) in the ranging step, and in the lateration step, the position (x, y) of the mobile device is estimated by finding $(\hat{x}, \hat{y})$ satisfying:

$$(\hat{x}, \hat{y}) = argmin_{x,y} \sum_{i=1}^{n-1} \sum_{j=i+1}^{n} [\sqrt{\frac{(x_i - x)^2 + (y_i - y)^2}{(x_j - x)^2 + (y_j - y)^2}} - \hat{r_{ij}}]^2 \quad (8)$$

B. Fingerprint Matching

The Radar algorithm [1] is a classic machine learning method based on fingerprint matching, which requires building a signal map consisting of RSS fingerprints with known (x, y) locations. Gridded Radar (GR) [2] is an extension to the Radar algorithm. It builds a regular grid of tiles over the localization area and uses the measured training fingerprints to interpolate RSS fingerprints for each tile in the grid. Given a RSS fingerprint of a mobile device, GR returns the position (x, y) of the tile in the IMG (Interpolated Map Grid) that has a fingerprint closest to the one of the mobile device as the location estimation, where closeness is measured in Euclidean distance in the signal space.

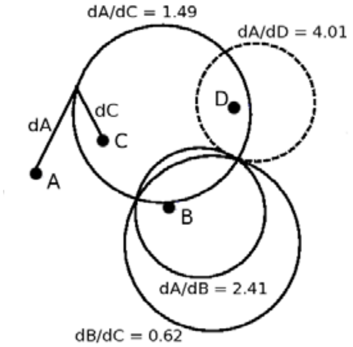


Fig. 3. Apollonius circles

To modify GR algorithm according to our principle, we simply change the matching function that measures the closeness of two fingerprints, $F(\overrightarrow{SS}^1, \overrightarrow{SS}^2)$, to use RSM instead of RSS. Specifically, the original function measures Euclidean distance in RSS:

$$F_{RSS}(\overrightarrow{SS}^1, \overrightarrow{SS}^2) = \sqrt{\sum_{i=1}^{n} (SS_i^1 - SS_i^2)^2} \quad (9)$$

We now instead measures Euclidean distance in RSM:

$$F_{RSM}(\overrightarrow{SS}^1, \overrightarrow{SS}^2) = \sqrt{\sum_{i=1}^{n-1} \sum_{j=i+1}^{n} (RSM_{ij}^1 - RSM_{ij}^2)^2} \quad (10)$$

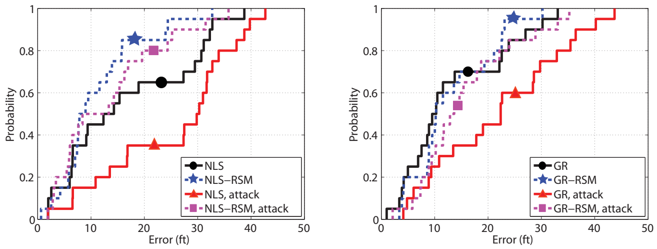
V. Evaluation

In this section, we evaluate the algorithms adapted according to our design principle. We used the leave-one-out method for evaluating localization, which means that we chose one location as the testing point, whereas the rest of the locations as the offline training data. As evaluation metric, we use *distance accuracy*, the distance between the true location and the estimated location, to characterize localization accuracy.

We conducted experiments with the same data set as described in Section II. Our evaluation results are compatible for both types of attack scenarios. Due to the space constraint, we only present results for tin can attack in this paper.

A. Performance Comparison

Our design principle allows us to adapt algorithms to achieve robustness to all-around signal strength attacks. We expect such adaptation to offer robustness with comparable performance when there is no attack, i.e. without considerable accuracy loss. To demonstrate this, we compare the performance of both versions of the algorithms without attacks as



(a) NLS

(b) GR

Fig. 4. Performance comparison, Tin can attack

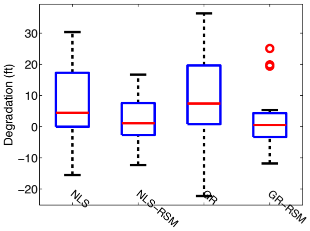


Fig. 5. Robustness comparison, Tin can attack

well as with attacks so that tradeoff can be evaluated within the robustness context.

Figure 4 plots the distance accuracy CDF for both the original and the adapted algorithms with or without tin can attack. Firstly, without attacks, the adapted algorithms offer very similar performance to the original algorithms. In fact, they even perform better in certain cases (for example, Figure 4 (a)). Secondly, from the performance degradation in reaction to attacks, we see that adapted algorithms offer much better robustness to attacks. Our evaluations thus demonstrate that algorithms adapted according to our principle offer comparable performance to the original ones when there is no attack, thus robustness is achieved (which will be further demonstrated in the next section) without sacrificing much accuracy.

B. Robustness Comparison

When attacks happen we are more concerned with the effect at each individual location. Thus here we conduct more detailed analysis on robustness by examining the accuracy degradation for each sample location. Specifically, we characterize the accuracy degradation as $accuracy_{attack} - accuracy_{normal}$. The robustness is then represented by the distribution of degradations across all the locations.

Figure 5 draws the boxplot for the distribution of accuracy degradation from all algorithms under tin can attack. On each box, the central mark is the median, the edges of the box are the 25th and 75th percentiles, the whiskers extend to the most extreme data points not considered outliers, and outliers are plotted individually.

Our key obsesrvation is that, compared to the corresponding original algorithms, although the adapted algorithms are not always better in terms of the best case in the degradation distribution (minimum degradation), they are always better and in many cases significantly better in terms of 25th percentile, median, 75th percentile, and the worst case of the degradation distribution. We thus conclude that our adapted algorithms experience considerable less degradation than the original algorithms, indicating much better robustness. In addition, we notice that some of the degradation distributions extend into negative values. This is because signal propagation is very noisy in indoor environment, and the attacks may to some extent correct the bias introduced by the noise.

VI. Conclusion

We focused this work on providing a principle to design localization algorithms so that they are robust to signal strength attacks. We formulated the all-around signal strength attack, where similar attacks are launched towards all landmarks. Our experiments in a real office-building environment confirmed the feasibility of launching such attacks. To make the location estimates resilient to attack, we proposed the Ratio-based Signal Strength Metric (RSM) to achieve robustness. We showed theoretically the correctness of using RSM to perform robust wireless localization under the all-around signal strength attack. We further adapted lateration based and fingerprint matching localization algorithms to validate our approach. We found that the adaptive algorithms experienced significantly less performance degradation under attacks than original algorithms, indicating much better robustness when using our RSM design principle. Our work thus provides design guidance for achieving resilient location estimation under all-around signal strength attacks, which does not require additional computational cost yet easy to adapt.

Acknowledgements: The work was supported in part by National Science Foundation Grants CNS-0954020 and CCF-1018270.

References

[1] P. Bahl and V. N. Padmanabhan, "RADAR: An In-Building RF-Based User Location and Tracking System," in *Proceedings of the Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM)*, Mar. 2000.

[2] Y. Chen, K. Kleisouris, X. Li, W. Trappe, and R. P. Martin, "A security and robustness performance analysis of localization algorithms to signal strength attacks," *ACM Trans. Sen. Netw.*, vol. 5, no. 1, pp. 1–37, 2009.

[3] Z. Li, W. Trappe, Y. Zhang, and B. Nath, "Robust statistical methods for securing wireless localization in sensor networks," in *Proceedings of the Fourth International Symposium on Information Processing in Sensor Networks (IPSN 2005)*, 2005.

[4] D. Liu, P. Ning, and W. Du, "Attack-resistant location estimation in sensor networks," in *Proceedings of the Fourth International Symposium on Information Processing in Sensor Networks (IPSN 2005)*, 2005.

[5] J. Yang, Y. Chen, V. Lawrence, and V. Swaminathan, "Robust wireless localization to attacks on access points," in *Sarnoff Symposium, 2009. SARNOFF '09. IEEE*, 30 2009-April 1 2009, pp. 1–5.

[6] J. Lee, K. Cho, S. Lee, T. Kwon, and Y. Choi, "Distributed and energy-efficient target localization and tracking in wireless sensor networks," *Elsevier Computer Communications*, vol. 29, Aug. 2006.

[7] X. Li, "Ratio-based Zero-profiling Indoor Localization," in *Proceedings of the 6th IEEE International Conference on Mobile Ad-hoc and Sensor Systems(MASS)*, Oct. 2009.

[8] Y. Zhang, G. Bhanage, W. Trappe, Y. Zhang, and R. Howard, "Facilitating an active transmit-only rfid system through receiver-based processing," in *Proceedings of the Fourth Annual IEEE Communications Society Conference on Sensor, Mesh, and Ad Hoc Communications and Networks (SECON)*, 2007.

[9] http://mathworld.wolfram.com/ApolloniusCircle.html, "Apollonius Circle."

[10] P. Enge and P. Misra, *Global Positioning System: Signals, Measurements and Performance*. Ganga-Jamuna Pr, 2001.