Wireless Netw (2012) 18:45–58
DOI 10.1007/s11276-011-0386-z

Achieving robust wireless localization resilient to signal strength attacks

Xiaoyan Li · Yingying Chen · Jie Yang · Xiuyuan Zheng

Published online: 18 September 2011

Abstract Received signal strength (RSS) based algorithms have been very attractive for localization since they allow the reuse of existing communication infrastructure and are applicable to many commodity radio technologies. Such algorithms, however, are sensitive to a set of non-cryptographic attacks, where the physical measurement process itself can be corrupted by adversaries. 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 a set of representative RSS-based localization algorithms according to our principle. We experiment with both simulated attacks and two sets of real attack scenarios. All the experiments show that our design principle can be applied to a wide spectrum of algorithms to achieve comparable performance with much better robustness.

Keywords Wireless localization · Signal strength attacks · Robust algorithms · Design principle

1 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 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 $\overrightarrow{SS}(\langle SS_1, SS_2..., SS_n\rangle)$ 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

X. Li (✉)
Department of Computer Science, Lafayette College, Easton,
PA 18042, USA
e-mail: lix@lafayette.edu

Y. Chen · J. Yang · X. Zheng
Department of Electrical and Computer Engineering,
Stevens Institute of Technology, Hoboken,
NJ 07030, USA
e-mail: yingying.chen@stevens.edu

J. Yang
e-mail: jyang@stevens.edu

X. Zheng
e-mail: xzheng1@stevens.edu

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.

However, RSS-based localization algorithms are sensitive to a set of non-cryptographic attacks, where the physical measurement process itself can be corrupted by adversaries [6]. For example, the attacker can perform signal strength attacks by placing an absorbing or reflecting material around a wireless device to modify its RSS. Chen et al. [6] 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 [20, 21, 29] have proposed secure localization algorithms to address the signal strength attacks that are non-cryptographic. 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 to throw off the localization system; Malicious devices (for example, performing jamming) in wireless systems can also continuously change their transmission power level to avoid being caught by 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 (RSM) 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.

Our principle 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 a set of representative localization algorithms according to our principle. We then evaluate the set of adapted algorithms with data collected across multiple experiment sites, and with both simulated attack scenarios and two sets of 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.

In the rest of the paper, we first discuss the all-around signal strength attacks in Sect. 2. Section 3 presents the principle we propose to design localization algorithms robust to signal strength attacks. Section 4 demonstrates the general applicability of our principle by adapting a set of existing algorithms according to our principle. We further validate our principle by evaluating the adapted algorithms in Sect. 5. Section 6 discusses related research work and finally we conclude in Sect. 7.

2 All-around signal strength attacks

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

2.1 Attack model

In this work, we consider all-around signal strength attacks. We define the all-around signal strength attacks as that when similar attacks are launched towards all landmarks. When such an attack is launched against a wireless device, the collected RSS measurements of the wireless device will be corrupted. Specifically, if the normal signal strength fingerprint for a mobile device is as follows with n landmarks:

$$\overrightarrow{SS} = \langle SS_1, SS_2, \ldots, SS_n \rangle,$$

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

$$\begin{aligned}\overrightarrow{SS}' &= \langle SS_1', SS_2', \ldots, SS_n' \rangle \\ &= \langle SS_1 - SS_t, SS_2 - SS_t, \ldots, SS_n - SS_t \rangle,\end{aligned}$$

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

We consider addressing this type of attack because it is easy to launch and very harmful to many localization algorithms [6]. Several previous works [20, 21, 29] have proposed solutions to another attack where only a small percentage (less than half) of the landmark readings are under attack.

2.2 Attack feasibility study

Practically, all-around signal strength attacks are easy to launch. We next 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 80 ft × 70 ft area as shown in Fig. 1 (We

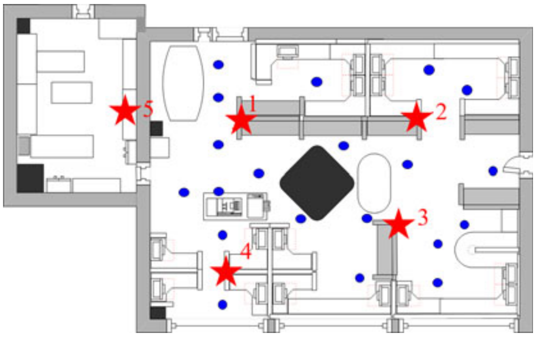


Fig. 1 Experiment site I

refer to this experimental area as Site I in the rest of the paper). 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 Fig. 1.

Received signal strength measurements were conducted using a localization testbed [5] with active RFID tags and readers from InPoint [32]. Each RFID tag has a unique identifier and periodically beacons its identifier, which is received by the landmarks. The tags transmit without collision avoidance or detection; the readers identify overlapping signals. We connect the RFID reader to a Linux machine with 2 GHz CPU, 1 GB RAM and 20 GB disk to serve as our landmark. In our localization testbed, landmarks continuously monitor the channels' traffic at the packet-level and forward their observed RSS readings to a central server. The server is responsible for averaging the RSS readings over multiple packets to produce fingerprints. In our experiments, each averaged RSS reading is 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 and −30 dBm, thus launching attacks of 20 and 40 dB respectively.

Figure 2 plots 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 20–30 dB attenuation, and the power variation attack achieves an average of around 20 and 40 dB signal attenuation corresponding to its attack severity of 20 and 40 dB respectively. The attacks on all landmarks are not exactly the same, however they are indeed very similar. We show in Sect. 3 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 is sufficient to achieve robustness.

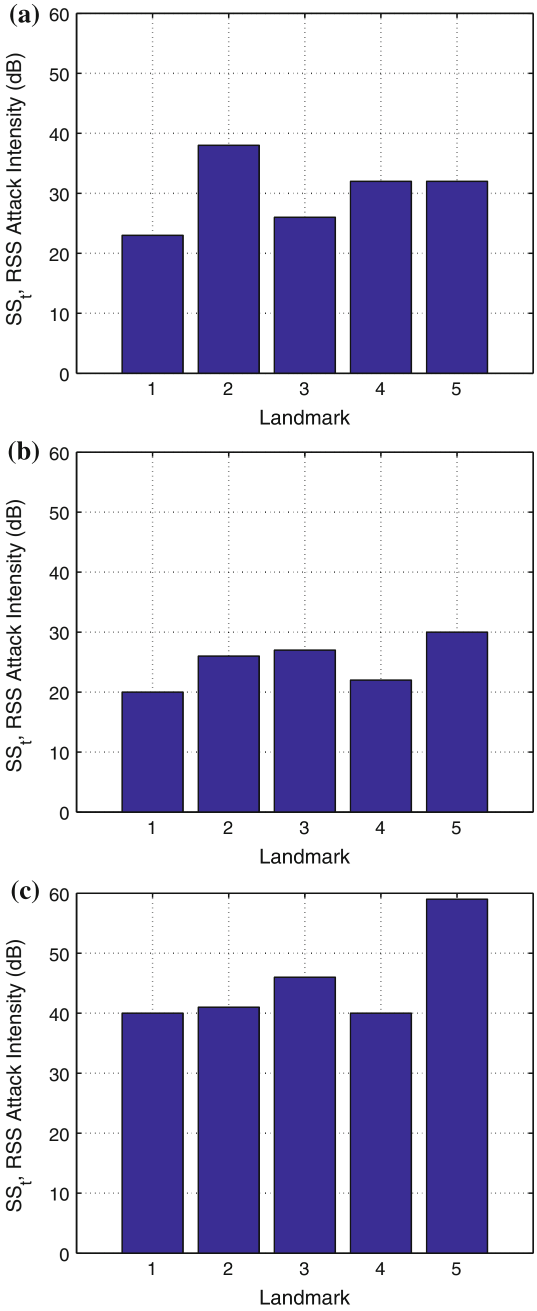


Fig. 2 All-around signal strength attacks: attack feasibility study. **a** Tin can attack. **b** Power variation attack: 20 dB. **c** Power variation attack: 40 dB

3 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 in Sect. 3.1 and then explain how it allows for localization in Sect. 3.2.

3.1 A robust signal strength metric

Received signal strength-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, $d_i, i = 1, 2\ldots, n$). 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 $\left(\frac{d_i}{d_j}\right)$, which can still be used for localization. We thus propose to use RSM to achieve robustness. More details about how this metric relates to distance ratio and how it allows for localization is discussed in Sect. 3.2.

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:

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

According to our attack model, RSM is robust to all-around 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 Sect. 2 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 3 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 Sect. 5 that such robustness in RSM metric does translate to better robustness in localization.

3.2 RSM allows for localization

We explain the feasibility of using RSM for localization in two steps. First, we map RSM metric to distance ratio in Sect. 3.2.1. We then explain why distance ratio information can be used for localization in Sect. 3.2.2.

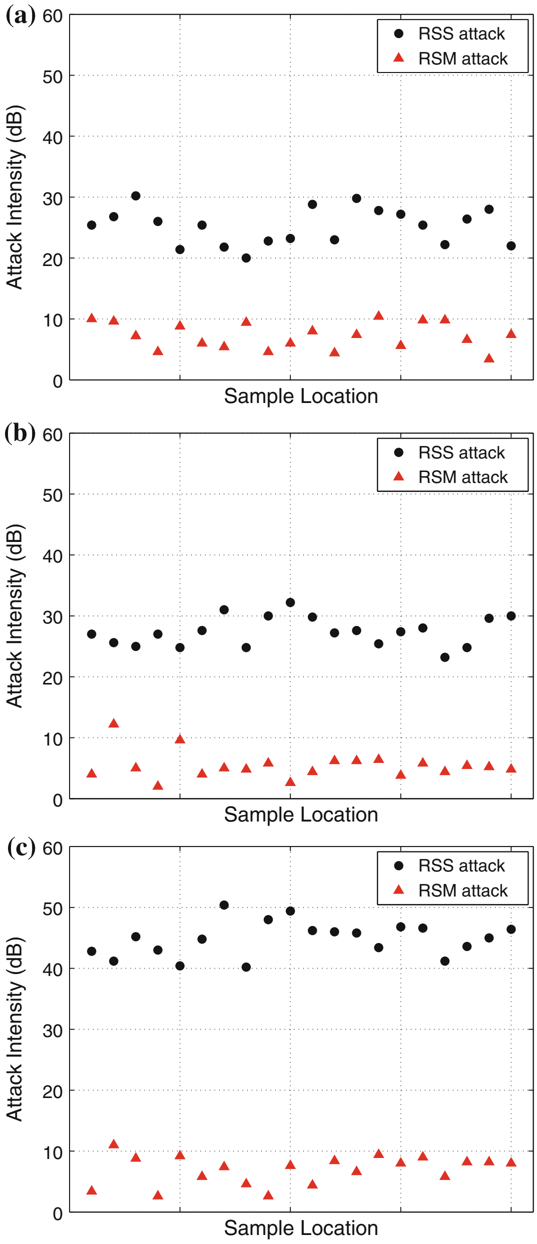


Fig. 3 Metric robustness analysis: RSS versus RSM. **a** Tin can attack. **b** Power variation attack: 20 dB. **c** Power variation attack: 40 dB

3.2.1 RSM maps to distance ratio

Normally, signal propagation is modeled as the distance dependent path loss model [1, 27]. For example, with consideration of possible attacks, the signal strength (dBm) measured at landmark L_i from a mobile device can be modeled as:

$$SS_i(d_i) = SS_i(d_0) - n_i log_{10}\left(\frac{d_i}{d_0}\right) + \delta SS_i - SS_t \qquad (4)$$
$$\delta SS_i \sim N(0, \sigma_i)$$

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 should be 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

$$RSM_{ij} = n_j log_{10}\left(\frac{d_j}{d_0}\right) - n_i log_{10}\left(\frac{d_i}{d_0}\right) + \delta SS_{ij} \qquad (5)$$
$$\delta SS_{ij} \sim N(0, \sigma_{ij})$$

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 Eq. 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, Eq. 5 can be further simplified as

$$RSM_{ij} = n log_{10}\left(\frac{d_j}{d_i}\right) + \delta SS_{ij} \qquad (6)$$
$$\delta SS_{ij} \sim N(0, \sigma_{ij})$$

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.

3.2.2 Ratio-based localization

Apollonius circles [11] 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 $m = n$, this set of points become a line, which is the perpendicular bisector of the line segment connecting the two fixed points. For example, in Fig. 4 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 Fig. 4). If we know the distance ratio from a mobile device to the set of landmarks $\left(\frac{d_A}{d_B}, \frac{d_B}{d_C}, \frac{d_A}{d_C}\right)$, 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 Fig. 4 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, $\frac{d_B}{d_C} = \frac{d_A}{d_C}\Big/\frac{d_A}{d_B}$. 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 Fig. 4, 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. Our RSM-based localization algorithms thus require one additional landmark than the set of RSS-based algorithms [2, 12, 13, 22, 25, 31].

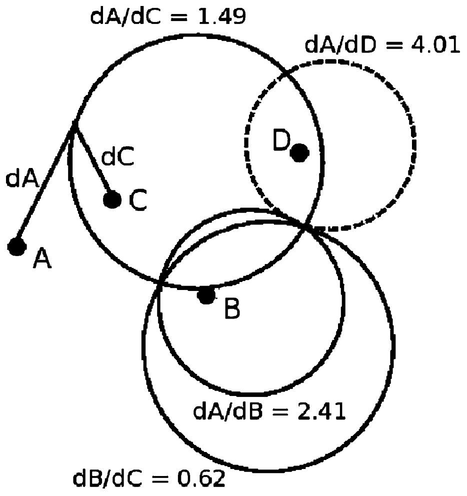


Fig. 4 Apollonius circles

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.

4 Adaptation of localization algorithms

Our proposed principle in Sect. 3 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 a set of previously proposed representative localization algorithms according to our design principle. We further use them to evaluate the effectiveness of our principle in Sect. 5.

4.1 Lateration based

Localization using the lateration based approach is popular [8, 14, 23] and involves 2 steps: *ranging* and *lateration*. In the ranging step, distances (d_i, $i = 1, 2\ldots, n$) 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. There are a variety of physical modalities can be used to perform the ranging and many methods have been proposed to perform lateration. 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:

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

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:

$$(\hat{x}, \hat{y}) = argmin_{x,y} RR \quad (8)$$

where ratio residual RR is defined as

$$RR = \sum_{i=1}^{n-1} \sum_{j=i+1}^{n} \left[\sqrt{\frac{(x_i - x)^2 + (y_i - y)^2}{(x_j - x)^2 + (y_j - y)^2}} - \hat{r}_{ij} \right]^2 \quad (9)$$

4.2 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) [7] 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.

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:

$$F_{RSS}(\overrightarrow{SS}^1, \overrightarrow{SS}^2) = \sqrt{\sum_{i=1}^{n} (SS_i^1 - SS_i^2)^2} \quad (10)$$

We now instead measures Euclidean distance in RSM:

$$F_{RSM}(\overrightarrow{SS}^1, \overrightarrow{SS}^2) = \sqrt{\sum_{i=1}^{n-1} \sum_{j=i+1}^{n} (RSM_{ij}^1 - RSM_{ij}^2)^2} \quad (11)$$

4.3 Probabilistic based

In this work, we choose to study area based probability (ABP) [7], which is a representative method based on the statistical Bayes' Rule to perform location estimation. ABP also uses the interpolated signal map as in GR and computes the likelihood of the observed fingerprint of a mobile device matching a fingerprint of each tile in the interpolated signal map. The top probability tile set whose sum matches the desired confidence level α (for example, $\alpha = 0.75$ in our experiments) represents the area where the mobile device is most likely to be in. For ease of comparison, we use a point-based version of ABP algorithm, where the center of the probable area is returned as the position estimate.

By using Bayes' rule, ABP computes the probability of being at each tile T_k (with expected fingerprints as $\overrightarrow{SS}^k$) on the floor given the fingerprint of the mobile device $\overrightarrow{SS}$ as:

$$P(T_k | \overrightarrow{SS}) = \frac{P(\overrightarrow{SS} | T_k) \times P(T_k)}{P(\overrightarrow{SS})} \quad (12)$$

where

$$P(\overrightarrow{SS} | T_k) = \prod_{i=1}^{n} P(SS_i | SS_i^k) \quad (13)$$

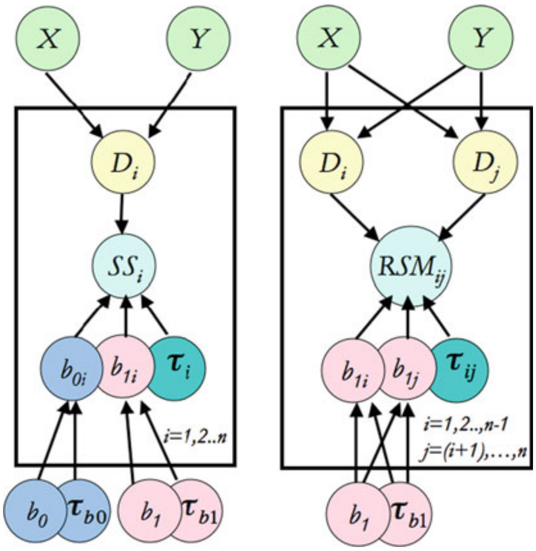
To adapt ABP algorithm, we simply change the calculation of $P(\overrightarrow{SS} | T_k)$ to use RSM:

$$P(\overrightarrow{SS}|T_k) = \prod_{i=1}^{n-1}\prod_{j=1+1}^{n} P(RSM_{ij}|RSM_{ij}^{k}) \qquad (14)$$

4.4 Bayesian networks

Bayesian Networks [7] utilizes the Bayesian Graphical Model to compute the distribution of the position (*x*, *y*) of a mobile device. In particular, Bayesian Networks encodes the relationship between the RSS readings and the location based on the signal-distance propagation model. The initial parameters of the model are unknown, and the training set collected from multiple known locations is used to adjust the parameters of the model according to the relationships encoded in the network.

Figure 5(a) depicts the basic Bayesian Graphical Model. The random variables $SS_i, i = 1\ldots n$ denotes the expected signal strength at landmark L_i. The values of these random variables depend on the Euclidean distance d_i between the landmark's location (x_i, y_i), and the location where the signal SS_i is measured (*x*, *y*). The baseline expected value of SS_i follows a signal propagation model $SS_i = b_{0i} + b_{1i}\log(d_i)$, where b_{0i}, b_{1i} are the parameters specific to each L_i. The distance $d_i = \sqrt{(x - x_i)^2 + (y - y_i)^2}$ in return depends on the location (*x*, *y*) of the measured signal. The network models noise and outliers by modeling the expected value, SS_i, as a Gaussian distribution around the propagation model, with variance τ_i, $SS_i \sim N(b_{0i} + b_{1i} logd_i, \tau_i)$. The usage of b_0, τ_{b0}, b_1, τ_{b1} is to exploit the similarities of signal propagation for all landmarks in the same environment. Using the training fingerprints, the network can learn the specific values for all the unknown parameters b_0, τ_{b0}, b_1, τ_{b1}, b_{0i}, b_{1i}, τ_i and the joint distribution of (*x*, *y*) location of the mobile device. In general, there is no closed form solution for the returned joint distribution of the (*x*, *y*) location. Therefore, we use a Markov Chain Monte Carlo (MCMC) simulation approach to draw samples from the joint density, and then return the center of the sample area as the estimated position.



(a) **(b)**

Fig. 5 Bayesian graphical model in our study. **a** RSS-based. **b** RSM-based

Figure 5(b) explains our adaptation of BN algorithm. The random variables RSM_{ij} denotes the expected RSM metric for landmark L_i and L_j. The baseline expected value of RSM_{ij} follows the model $RSM_{ij} = b_{1i}log(d_i) - b_{1j}log(d_j)$, where b_{1i}, b_{1j} are the parameters specific to L_i and L_j respectively. Measured RSM_{ij} is also modeled as a Gaussian distribution around the above propagation model, with variance τ_{ij} to accommodate for noise.

5 Evaluation

In this section, we evaluate the algorithms adapted according to our design principle. We first explain the experimental setup in Sect. 5.1. The algorithms' performance and robustness to attacks are then evaluated in detail in Sects. 5.2 and 5.3 respectively.

5.1 Experimental setup

We focus our evaluation of the algorithms on both performance and robustness. Our experimental data collected at Site I (as described in Sect. 2) allow us to evaluate realistic scenarios on RFID networks from both perspectives.

To extend our coverage, we experimented with many other data traces using simulated attacks. Due to the simulation nature, such experiments are more relevant in evaluating the algorithms' performance, we thus use them only in Sect. 5.2. Our evaluation results are compatible from all the trace data collected in three other sites, including both WiFi and Zigbee (using mote sensors) data. Due to the space constraint, we present experiments from only one other site in this paper.

Figure 6 represents the floor plan of our second experiment site—a floor in a computer science department building at an academic institution, which we refer to as Site II. In the figures, grey spaces are corridors; white spaces are offices or laboratories. Site II contains just over 50 rooms in a 200 ft × 80 ft area. We collected 286 fingerprints with the pre-deployed WiFi network [Fig. 6(a)] using a Dell laptop running Linux equipped with an Orinoco silver card. The Zigbee network [Fig. 6(b)] was setup with 4 Telos Sky motes as landmarks and 94 fingerprints were collected. For both networks, each RSS value is

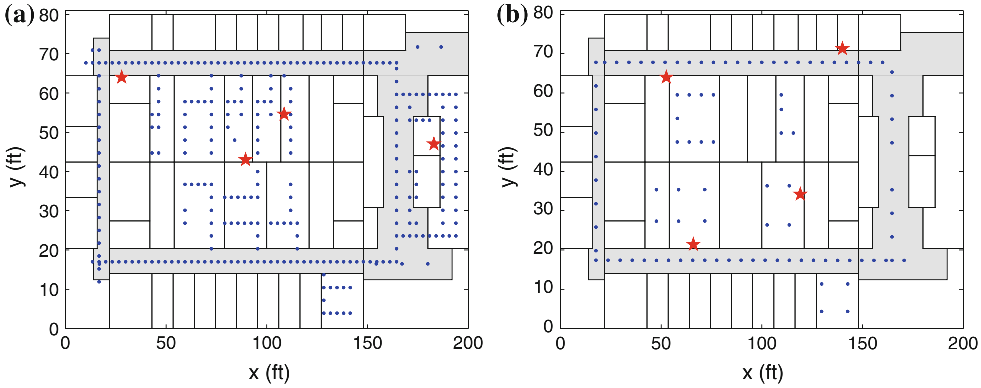


Fig. 6 Experiment site II. **a** WiFi. **b** Zigbee

obtained as average over 60 sampled readings. Landmarks and sample locations for both networks are shown as stars and dots respectively.

We used the leave-one-out method for evaluating the localization performance, 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 algorithms' accuracy.

5.2 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 well as with attacks so that tradeoff can be evaluated within the robustness context. We evaluate the performance comparison with simulated attacks at Site II and real attacks at Site I.

5.2.1 Site II, simulated attacks

Attacks in the experiments at Site II were simulated by attenuating the testing point's signal strength fingerprint for the same amount (5, 10, and 20 dB) along all the landmarks. Figures 7 and 8 plot the distance accuracy CDF (Cumulative Distribution Function) for both the original and the adapted algorithms using WiFi and Zigbee data respectively. Both sets of algorithms were evaluated for without attack and under different intensity of signal strength attenuation attacks, annotated via legends. The adapted algorithms have only one plot for each setup since they offer complete robustness under strict all-around signal strength attacks, which is the case with the simulation.

Firstly, we see that all the algorithms degrade significantly as the attack becomes more intense. This illustrates the importance of designing algorithms robust to signal strength attacks. Notice that in Fig. 8(d), algorithm degradation appears to be less significant, mainly because its *X*-axis scale is much larger than the other plots in the same figure.

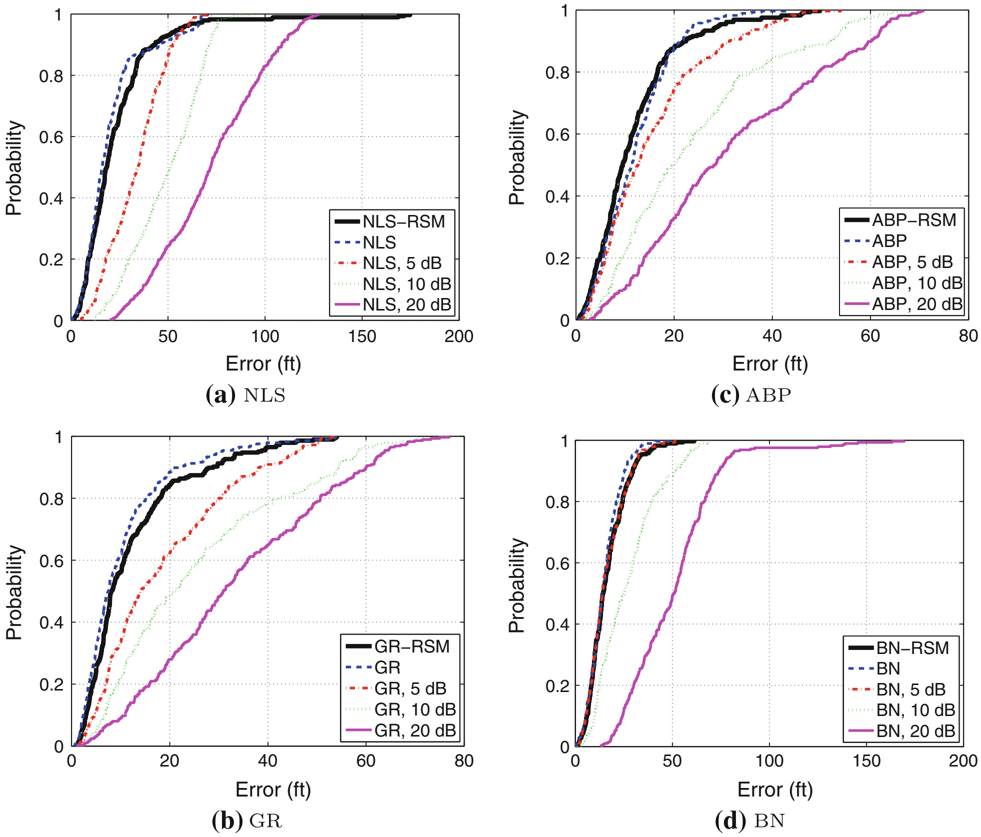
Secondly, when there are no attacks, the adapted algorithms have achieved comparable performance to the original algorithms. For WiFi data, the performance is almost identical. For Zigbee data, the adapted algorithms suffer a little more accuracy loss. We suspect this is due to the inherent weakness and less-differentiating nature of this data set. Notice, however, that all the adapted algorithms still offer better performance than the original algorithms under 10 dB attenuation attacks. Considering the attack intensity we achieved with the simple tin can attack (20–30 dB, as shown in Sect. 2), we believe our adapted algorithms still offer better tradeoff.

Finally, we notice that the adapted algorithms may sometimes result in a few outliers with really bad performance, shown as the long tails in Figs. 7(a) and 8(d). We suspect this is due to the underlying ratio-based localization approach in our adapted algorithms being less constraining, and further investigation is part of our future work. Such outlier cases, however, should not outweigh the overall comparable performance and robustness benefits offered by the adapted algorithms.

5.2.2 Site I, real attacks

Figure 9 plots the distance accuracy CDF for both the original and the adapted algorithms with or without tin can attack. Figure 10 plots the performance for both versions of algorithms with or without power variation attacks.

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, Fig. 9(a)]. Secondly, from the performance degradation in reaction to attacks, we see that adapted algorithms offer



(a) NLS

(c) ABP

(b) GR

(d) BN

Fig. 7 Performance comparison, site II, WiFi

much better robustness to attacks. Finally, we see that power variation attacks of 20 and 40 dB have similar effects on the set of original algorithms (Fig. 10). This is different from what we observe in Sect. 5.2.1, where the algorithms continuously degrade as the attack intensity increases (Figs. 7, 8). This will be part of our further investigation, while currently we suspect it may be related to the limited amount of sample locations at Site I.

In summary, evaluations across two sites under different wireless technologies (RFID, WiFi, and Mote sensor), with both simulated and real attacks, demonstrate that algorithms adapted according to our design 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.

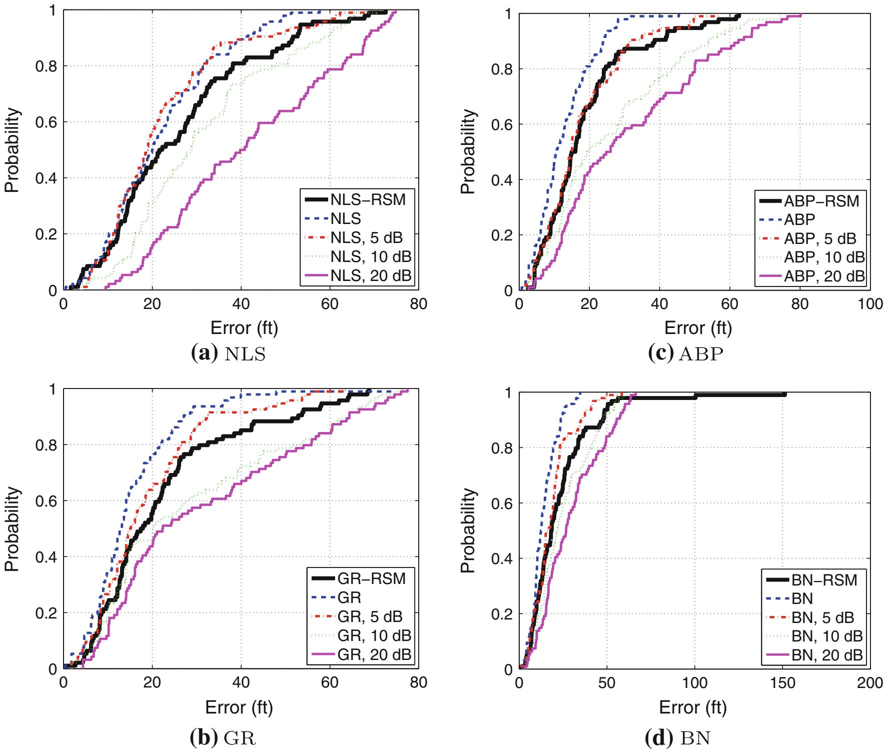
5.3 Robustness comparison

As mentioned in Sect. 3, real attacks do not strictly follow all-around signal strength attack model. We expect our design principle to achieve better robustness because the RSM metric tends to go under less severe attack than RSS. In this section, we evaluate if the adapted algorithms are more robust, i.e. experience less performance degradation than the original ones when under attacks.

Part of our evaluations in Sect. 5.2.2 on real attacks scenarios demonstrated the overall robustness of our adapted algorithms via the comparison of distance accuracy CDF. When attacks happen, however, 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.

Figures 11 and 12 draw the boxplot for the distribution of accuracy degradation from all algorithms under tin can attack and power variation attack respectively. 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.

Firstly, notice that some of the degradation distributions extend into negative values, which means that for certain sample locations attacks have in fact improved localization accuracy. This is possible because signal propagation is very noisy in indoor environment, and the attacks may to some extent correct the bias introduced by the noise.



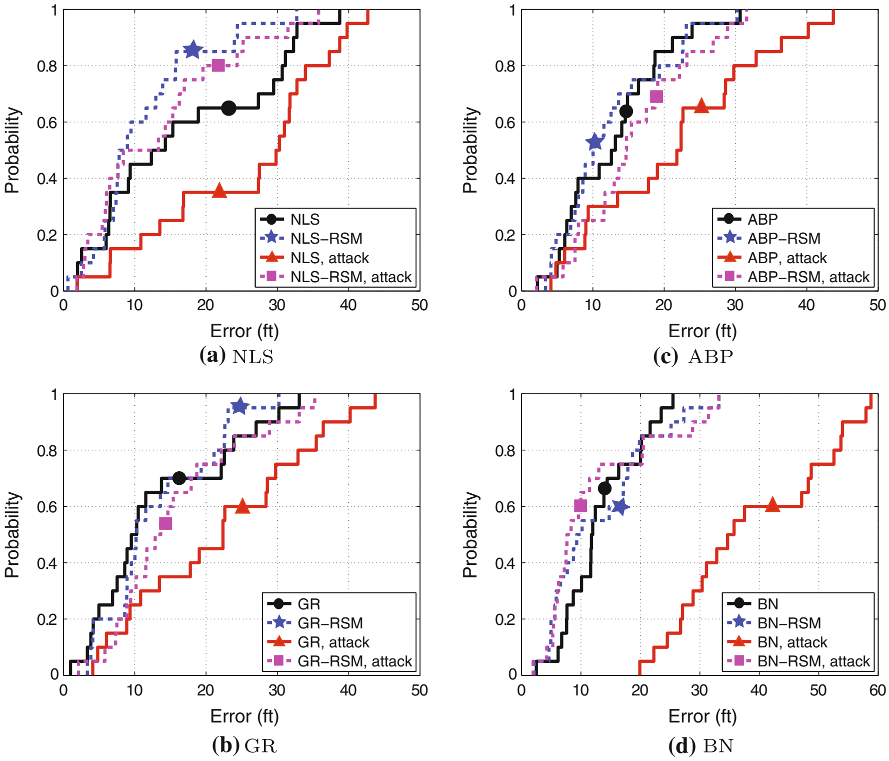
(a) NLS

(c) ABP

(b) GR

(d) BN

Fig. 8 Performance comparison, site II, Zigbee



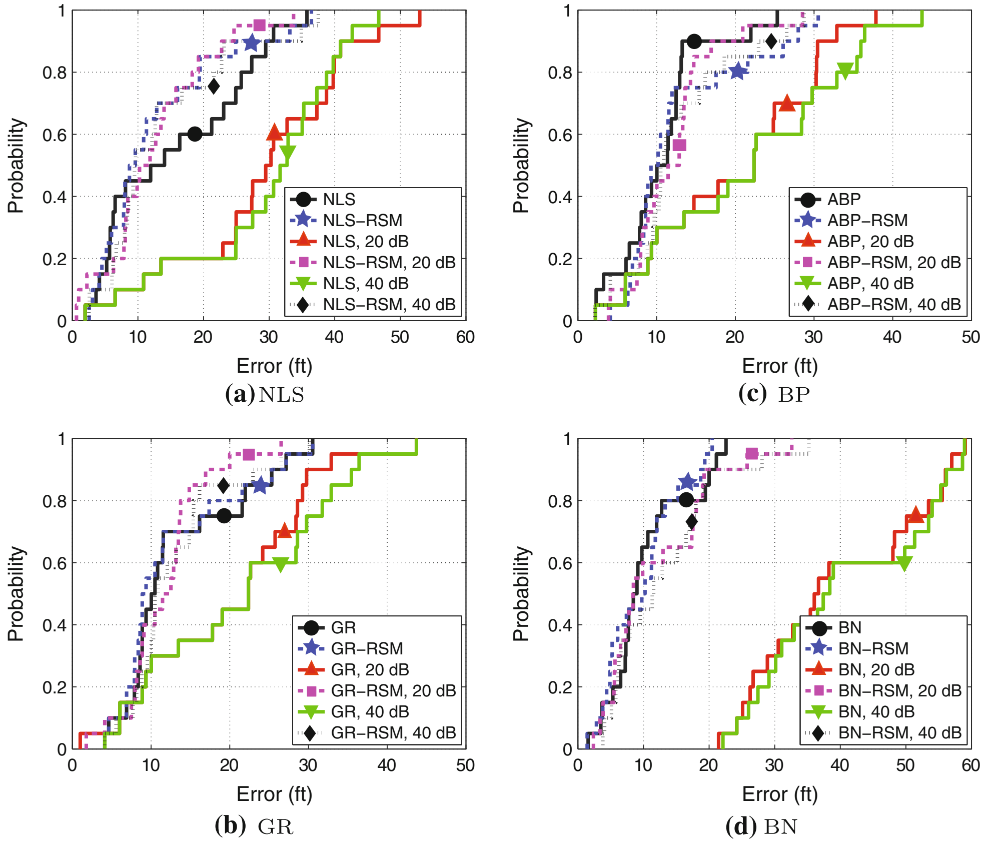
(a) NLS

(c) ABP

(b) GR

(d) BN

Fig. 9 Performance comparison, site I, tin can attack



(a) NLS

(c) BP

(b) GR

(d) BN

Fig. 10 Performance comparison, site I, power variation attack

Secondly, we see that the accuracy degradation plot reveals more details about the effect of attacks. For example, according to Fig. 9(c), we may expect the accuracy for using the adapted ABP algorithm, ABP-RSM, to degrade no more than 10 ft [comparing *ABP-RSM* vs. *ABP-RSM, attack* in Fig. 9(c)]. Figure 11, however, shows that in certain extreme cases the degradation goes up to more than 20 ft.

Finally, 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, for example, in Fig.12(b)], 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.

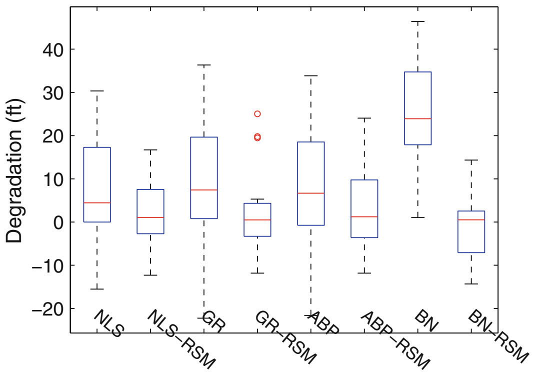
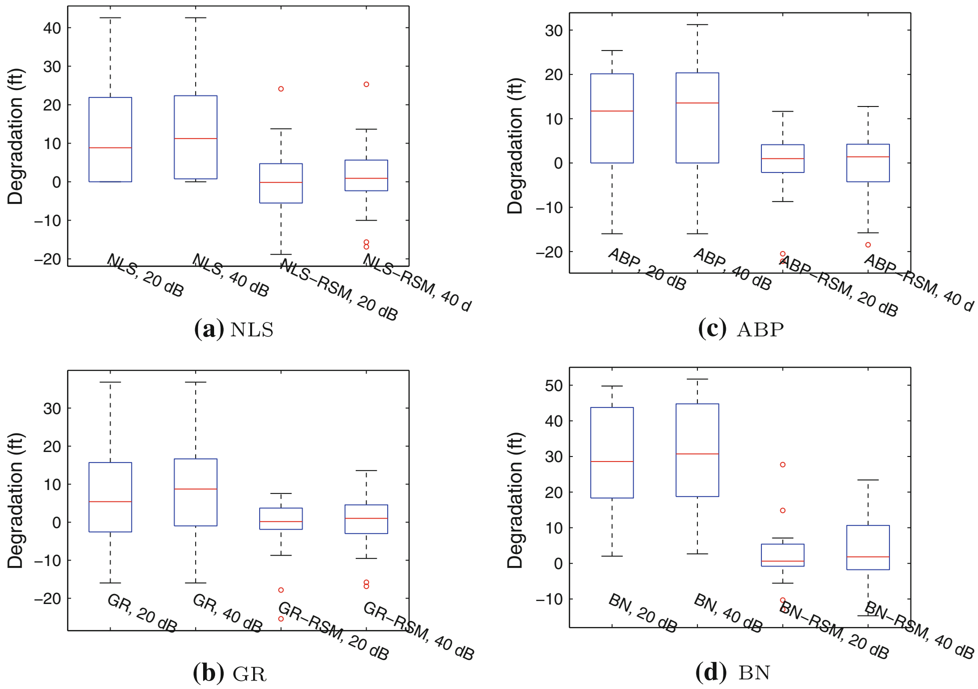


Fig. 11 Robustness comparison, site I, tin can attack

6 Related work

Localization has been researched in several settings (indoor, outdoor, and with the use of wireless sensor networks) and a wide range of technologies has been explored (ultrasound [24], infrared [28], WiFi, and custom radios). Within this wide variance, the works using WiFi and signal strength [1, 13, 22] are most closely related to ours. Our work is not a specific localization approach. It instead proposes a general design guideline that can be applied to many RSS-based algorithms to achieve the desired robustness to signal strength attacks.

The usage of new metric RSM in our design principle essentially relies on the fact that distance ratio information allows for localization. Several previous works have proposed ratio-based localization algorithms. Yang et al. [30] proposed a ratio-based localization algorithm within



(a) NLS

(c) ABP

(b) GR

(d) BN

Fig. 12 Robustness comparison, site I, power variation attack

wireless sensor networks for better energy efficiency, where distance information is straightforwardly approximated by hop-count from the sensor node to the landmark nodes. Li et al. [17] proposed to localize by solving the non-linear least square problem formed by the ratio relationship. Lee et al. [16] proposed a less computationally intensive algorithm to iteratively localize. Lee et al. [16], Li et al. [17] both assume signal degradation rate is known to translate RSS directly into distance ratio, which requires inference from the offline profiling data. Li [18] demonstrated that the fundamental ratio relationship in the RSS data (even without knowing the exact distance ratio) can be explored to completely avoid the offline profiling phase. Our work is not another ratio-based algorithm. It is instead a general design principle, which recognizes that the benefits of robustness from using RSM metric can be integrated into many existing RSS-based algorithms. Hossain et al. [9, 10] are related to our work as they also made use of the RSM metric. Their work, however, focused on robustness across different mobile devices. Comparatively, we have also extended the applicability of our principle to a broader spectrum of algorithms.

Recently, it has been recognized that there are many non-cryptographic attacks that can affect localization performance [6] and secure localization algorithms have been proposed to address these attacks. Capkun and Hubaux [4] uses a distance bounding protocol [3, 26] to upperbound the distance between two nodes. Location estimation (via multilateration) with distances from the bounding protocol can be verified against these bounds and any inconsistency will then indicate attack. Lazos et al. [15] uses both directional antenna and distance bounding to achieve security. Liu et al. [21] proposes to detect attacks based on data inconsistency from received beacons and to use a greedy search or voting algorithm to eliminate the malicious beacon information. Li et al. [20] makes use of the data redundancy and robust statistical methods to achieve reliable localization in the presence of attacks. Li et al. [20] is most related to our work as they proposed a possible solution to the fingerprinting-based localization that we focus on. Their solution works when less than half of the landmark readings are under attack while we focus on all-around attacks, where all the landmark readings are affected.

7 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 so-called 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 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 demonstrated its usage by adapting a broad set of localization algorithms, including lateration based, fingerprint matching, probabilistic based, and Bayesian Networks, according to our proposed design principle.

We evaluated both performance and robustness of the adapted localization algorithms. Through the real attacks conducted in experiment site I by using RFID tags and the simulated attacks applied to the data sets collected from experiment site II by using both WiFi cards and mote sensors (Zigbee), we compared the performance of our adapted algorithms to those original ones. Our results obtained from the set of adapted algorithms are promising, showing comparable performance to the original ones under normal condition (no attacks). Moreover, we conducted two real sets of attacks by using tin can and varying transmitter's power level respectively. 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 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.

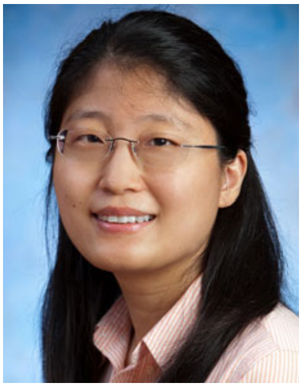
Acknowledgments Preliminary results of this paper have been presented in part in IEEE INFOCOM mini-Conference 2011 [19]. The work was supported in part by National Science Foundation Grants CNS-0954020 and CCF-1018270.

References

1. Bahl, P., & Padmanabhan, V. N. (2000). 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*).
2. Battiti, R., Brunato, M., & Villani, A. (2002). Statistical learning theory for location fingerprinting in wireless LANs. Technical Report DIT-02-086, University of Trento, Informatica e Telecomunicazioni.
3. Brands, S., & Chaum, D. (1994). Distance-bounding protocols. In *Proceedings of the workshop on the theory and application of cryptographic techniques on advances in cryptology* (pp. 344–359).
4. Capkun, S., & Hubaux, J. P. (2005). Secure positioning of wireless devices with application to sensor networks. In *Proceedings of the IEEE international conference on computer communications* (*INFOCOM*).
5. Chen, Y., Chandrasekaran, G., Elnahrawy, E., Francisco, J., Kleisouris, K., Li, X., et al. (2008). GRAIL: A general purpose localization system. Sensor review, special edition. *Localisation Systems, 28*(2), 115–124.
6. Chen, Y., Kleisouris, K., Li, X., Trappe, W., & Martin, R. P. (2009). A security and robustness performance analysis of localization algorithms to signal strength attacks. *ACM Transactions on Sensor Networks, 5*(1), 1–37.
7. Elnahrawy, E., Li, X., & Martin, R. P. (2004). The limits of localization using signal strength: A comparative study. In *Proceedings of IEEE international conference on sensor and ad hoc communications and networks* (*SECON'04*). Santa Clara, CA.
8. Enge, P., & Misra, P. (2001). *Global positioning system: Signals, measurements and performance*. Lincoln, MA: Ganga-Jamuna Press.
9. Hossain, A. K. M. M., & Soh, W. S. (2010). Cramer-rao bound analysis of localization using signal strength difference as location fingerprint. In *Proceedings of IEEE international conference on computer communications* (*INFOCOM*).
10. Hossain, A., Van, H., Jin, Y., & Soh, W. (2007). Indoor localization using multiple wireless technologies. In *Proceedings of the IEEE MASS* (pp. 1–8).
11. http://mathworld.wolfram.com/ApolloniusCircle.html: Apollonius Circle.
12. Krishnan, P., Krishnakumar, A. S., Ju, W. H., Mallows, C., & Ganu, S. (2004) A system for LEASE: Location estimation assisted by stationary emitters for indoor RF wireless networks. In *Proceedings of the annual joint conference of the IEEE computer and communications societies* (*INFOCOM*).
13. Ladd, A. M., Bekris, K. E., Rudys, A., Marceau, G., Kavraki, L. E., & Wallach, D. S. (2002). Robotics-based location sensing using wireless ethernet. In *Proceedings of the eighth ACM international conference on mobile computing and networking* (*MOBICOM*).
14. Langendoen, K., & Reijers, N. (2003). Distributed localization in wireless sensor networks: A quantitative comparison. *Computer Networks, 43*(4), 499–518.
15. Lazos, L., Poovendran, R., & Capkun, S. (2005). Rope: Robust position estimation in wireless sensor networks. In *Proceedings of the fourth international symposium on information processing in sensor networks* (*IPSN*) (pp. 324–331).
16. Lee, J., Cho, K., Lee, S., Kwon, T., & Choi, Y. (2006). Distributed and energy-efficient target localization and tracking in wireless sensor networks. *Elsevier Computer Communications, 29*, 2494–2505.
17. Li, D., Wong, K., Hu, Y. H., & Sayeed, A. M. (2002). Detection, classification, tracking of targets in micro-sensor networks. *IEEE Signal Processing Magazine, 19*, 1163–1171.
18. Li, X. (2009). Ratio-based zero-profiling indoor localization. In *Proceedings of the 6th IEEE international conference on mobile ad-hoc and sensor systems* (*MASS*).
19. Li, X., Chen, Y., Yang, J., & Zheng, X. (2011). Designing localization algorithms robust to signal strength attacks. In *Proceedings of IEEE international conference on computer communications* (*INFOCOM*), *mini-conference*.
20. Li, Z., Trappe, W., Zhang, Y., & Nath, B. (2005). Robust statistical methods for securing wireless localization in sensor networks. In *Proceedings of the fourth international symposium on information processing in sensor networks* (*IPSN*).
21. Liu, D., Ning, P., & Du, W. (2005). Attack-resistant location estimation in sensor networks. In *Proceedings of the fourth international symposium on information processing in sensor networks* (*IPSN*).
22. Madigan, D., Elnahrawy, E., Martin, R. P., Ju, W. H., Krishnan, P., & Krishnakumar, A. S. (2005). Bayesian indoor positioning systems. In *Proceedings of the annual joint conference of the IEEE computer and communications societies* (*INFOCOM*).
23. Niculescu, D., & Nath, B. (2001). Ad hoc positioning system (APS). In *Proceedings of IEEE GLOBECOM'01* (pp. 2926–2931).
24. Priyantha, N., Chakraborty, A., & Balakrishnan, H. (2000). The cricket location-support system. In *Proceedings of ACM international conference on mobile computing and networking* (*MobiCom*).
25. Roos, T., Myllymaki, P., & Tirri, H. (2002). A statistical modeling approach to location estimation. *IEEE Transactions on Mobile Computing, 1*(1), 59–69.

26. Sastry, N., Shankar, U., & Wagner, D. (2003). Secure verification of location claims. In *Proceedings of the ACM workshop on wireless security*.
27. Seidel, S. Y., & Rappaport, T. S. (1992). 914 MHz path loss prediction models for indoor wireless communications in multi-floored buildings. *IEEE Transactions on Antennas and Propagation, 40*(2), 207–217.
28. Want, R., Hopper, A., Falcao, V., & Gibbons, J. (1992). The active badge location system. *ACM Transactions on Information Systems, 10*(1), 91–102.
29. Yang, J., Chen, Y., Lawrence, V., & Swaminathan, V. (2009). Robust wireless localization to attacks on access points. In *Sarnoff Symposium, 2009. SARNOFF '09. IEEE* (pp. 1–5). doi: 10.1109/SARNOF.2009.4850372.
30. Yang, S., Yi, J., & Cha, H. (2007). HCRL: A hop-count-ratio based localization in wireless sensor networks. In *Proceedings of the fourth IEEE communications society conference on sensor, mesh, and ad hoc communications and networks* (*SECON*).
31. Youssef, M., Agrawal, A., & Shankar, A. U. (2003). WLAN location determination via clustering and probability distributions. In *Proceedings of the first IEEE international conference on pervasive computing and communications* (*PerCom*).
32. Zhang, Y., Bhanage, G., Trappe, W., Zhang, Y., & Howard, R. (2007). 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*).

Author Biographies



Xiaoyan Li received her Ph.D. degree in Computer Science from Rutgers, the State University of New Jersey, in 2006. She is currently an assistant professor in the Department of Computer Science at Lafayette College. Her current research interests include wireless networking, sensor networks, and distributed systems.

Yingying Chen received her Ph.D. degree in Computer Science from Rutgers University. She is currently an assistant professor in the Department of Electrical and Computer Engineering at Stevens Institute of Technology. Her research interests include wireless and systems security and privacy, wireless networking, mobile social networks and pervasive computing. She has coauthored the book Securing Emerging Wireless Systems and published extensively in journal and conference papers. Prior to joining Stevens Institute of Technology, she was with Bell Laboratories and Optical Networking Group at Lucent Technologies. She received the IEEE Outstanding Contribution Award from IEEE New Jersey Coast Section each year 2005–2009. She is the recipient of the NSF CAREER award. She is also the recipient of the Best Technological Innovation Award from the International TinyOS Technology Exchange in 2006, as well as the Best Paper Award from the International Conference on Wireless On-demand Network Systems and Services (WONS) in 2009.

Jie Yang received the B.E. degree in automatic control from Beijing Institute of Technology, China, in 2004. He was in the Ph.D. program in the Department of Automatic Control of Beijing Institute of Technology from 2005 to 2007. He is currently working toward the Ph.D. degree in the Electrical and Computer Engineering Department at Stevens Institute of Technology. His research interests include the areas of information security and privacy, wireless localization, and location-based services (LBS).

Xiuyuan Zheng is currently a Ph.D. student of the Electrical and Computer Engineering Department at Stevens Institute of Technology. His research interests include information security & privacy, wireless localization and location based services (LBS), wireless and sensor networks. He is currently working in the Data Analysis and Information SecuritY (DAISY) Lab with Prof. Yingying Chen. He was in the Master program in the Electrical and Computer Engineering Department at Stevens Institute of Technology from 2007 to 2009. He received his Bachelor's degree from Department of Telecommunication Engineering at Nanjing University of Posts and Communications, China, in 2007.