SECURITY AND COMMUNICATION NETWORKS
Security Comm. Networks 2012; **5**:384–403
Published online 12 May 2011 in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/sec.323

RESEARCH ARTICLE

Toward attack-resistant localization under infrastructure attacks

Jie Yang* and Yingying Chen

Department of Electrical and Computer Engineering, Stevens Institute of Technology, Castle Point on Hudson, Hoboken, NJ 07030, U.S.A.

ABSTRACT

Trustworthy location information is important because it is a critical input to a wide variety of location-based applications. However, the localization infrastructure is vulnerable to physical attacks, and consequently, the localization results are affected. In this paper, we aim to achieve robust localization under infrastructure attacks. We first investigated the impact of infrastructure attacks on localization and showed that the performance of location estimations degraded significantly under the attack. We then derived an attack-resistant scheme that is not algorithm specific and can be integrated with existing localization algorithms. Our attack-resistant scheme exploited the characteristics of the geometric patterns returned by location estimates under the attack; that is, the localization results of a wireless device under the normal situation were clearly clustered together, whereas the localization results were scattered when an attack was present. Thus, our attack-resistant scheme is grounded on *K*-means clustering analysis of intra-distance of localization results from all possible combinations of any three access points. To evaluate the effectiveness and scalability of our proposed scheme, we used received signal strength for validation and applied our approach to three broad classes of localization algorithms: lateration based, fingerprint matching, and Bayesian networks. We validated our scheme in the ORBIT test bed (North Brunswick, NJ, USA) using an 802.11 (Wi-Fi) network and in a real office building environment using an 802.15.4 (ZigBee) network. The extensive experimental results demonstrated that the application of our scheme could help the broad range of localization algorithms to achieve comparable or even better localization performance when under infrastructure attacks as compared with normal situations without attack, thus, effectively eliminating the effects of infrastructure attacks.

KEYWORDS
wireless localization; secure localization; infrastructure attacks; received signal strength

***Correspondence**
Jie Yang, Department of Electrical and Computer Engineering, Stevens Institute of Technology, Castle Point on Hudson, Hoboken, NJ 07030, U.S.A.
E-mail: jyang@stevens.edu

1. INTRODUCTION

The rapid advancement of wireless technologies has enabled a variety of emerging applications ranging from location-based tracking and monitoring in healthcare environments, to location-aware traffic monitoring in VANETs, and to location-centric emergency rescue and military surveillance. However, without the trustworthy location information, many of these applications will not function properly. For instance, an enemy may attack the anchor points used by the localization infrastructure and fool the location-oriented military surveillance, or an adversary may modify its radio signal readings at an access point and thus attract more traffic during geographic routing [1]. Therefore, the trustworthiness of the location information of wireless devices plays a critical role in the successful deployment of high-level pervasive applications.

Wireless localization techniques usually involve the measurement of various physical properties such as time of arrival (ToA) [2], time difference of arrival (TDoA) [3], angle of arrival (AoA) [4], and received signal strength (RSS) [5–7]. Among these, characterization of the relationship between physical locations and a given radio measurement of physical property allows a localization system to localize a wireless device through observation of radio signals between the wireless device to some anchor points, for example, Wi-Fi access points with known locations.

However, unlike traditional systems, the localization infrastructure is vulnerable to physical attacks, especially in hostile environments; for example, the anchor points are

unattended after deployment. Our prior study [8] showed that the performance of localization degrades significantly under physical attacks, for example, when signals are attenuated, amplified, or reflected by an adversary. Physical attacks can be launched either at the device side or at the anchor points. Moreover, attacking anchor points is more harmful because it will affect the localization results for a group of devices. Thus, in this paper, we focused on attacks on anchor points, which we call *infrastructure attacks*.

In previous works, Li *et al*. [9] used data redundancy and robust statistical methods to achieve reliable localization in the presence of malicious attacks, whereas Liu *et al*. [10] proposed to detect attacks based on data inconsistency from the received beacons and used a greedy search or voting algorithm to eliminate the malicious beacon information. However, most of these methods are algorithm specific and are thus not scalable. In this paper, we propose a mechanism that can be integrated into existing localization algorithms to provide an attack-resistant location estimation. In particular, our mechanism exploited the characteristics of the geometric patterns returned by the location estimates. By leveraging the geometric relationship between the localization results from the benign anchor points and those from the attacked anchor points, our scheme performed the cluster analysis to the localization estimates obtained from subsets of anchor points to separate correct localization results from corrupted ones. Our approach is not algorithm specific and can be easily scalable to any localization algorithms.

To validate the effectiveness of our approach, we conducted experiments in the ORBIT test bed using an 802.11 (Wi-Fi) network and in a real office building environment using an 802.15.4 (ZigBee) network. We used the measured RSS from wireless devices to multiple anchor points to perform localization. To test the scalability, we validated our method by integrating with three broad classes of localization algorithms: lateration-based algorithms, whereby a set of least squares (LS) equations based on the signal propagation model was solved under the objective of minimizing the location estimation errors; fingerprint matching algorithms, whereby a database of collected radio-frequency (RF) fingerprints measured at several anchor points for an initial set of locations served as training data, and the location estimation came from the matching between the measured RF fingerprint and the fingerprint database and Bayesian networks (BNs), whereby the distribution of the estimated location was obtained through a Bayesian graphical model. Although the RSS-based localization algorithms are used to evaluate our scheme, we note that our proposed method can be applied to other localization strategies based on different physical modalities, such as ToA-based and AoA-based localization. The experimental results show that our approach is highly effective in providing an accurate location estimation under the presence of infrastructure attacks, thus achieving attack-resistant localization.

The rest of the paper is organized as follows: Section 2 puts our research in the broader background of wireless localization and secure localization. We present our network model and adversary model in Section 3. In Section 4, we analyze the effectiveness of the infrastructure attacks and then describe our attack-resistant approach. To evaluate the effectiveness of our approach, we present the test bed infrastructure and develop the evaluation metrics in Section 6. Section 5 presents the evaluation of our approach. Finally, we conclude in Section 8.

2. RELATED WORK

There has been active work in exploring wireless localization. Examining the localization infrastructure, which is the foundation of localization, Want *et al*. [11] used infrared methods and Priyantha *et al*. [3] used ultrasound to perform localization. Both of them need to deploy specialized infrastructure for localization. On the other hand, in spite of its several meter-level accuracy, using RSS [5,6,12] is an attractive approach because it can reuse the existing wireless infrastructure, providing tremendous cost savings.

Furthermore, based on ranging methodology, there are range-based and range-free algorithms. Range-based algorithms involve distance estimations to anchor points using the measurement of various physical properties [13] such as RSS [5,14], ToA [2], and TDoA [3], whereas range-free algorithms [15–18] use coarser metrics (e.g., hop count) to place bounds on candidate positions. Another method of classification describes the strategy used to map a node to a location. Lateration approaches [2,9,17,19–21] use distances to anchor points, whereas angulation uses the angles from anchor points. Fingerprint matching strategies [5,22,23] use a function that maps observed radio properties to locations on a pre-constructed fingerprint radio map or database.

On the other hand, there has been considerably less work on the problem of securing localization, which is used to ensure the trustworthiness of wireless localization. Sastry *et al*. [24] proposed distance bounding protocols for verification of node positions. Capkun and Hubaux [25] proposed the verifiable multilateration mechanism, which is based on the distance bounding protocols for secure position computation and verification. Capkun and Hubaux [26] used hidden and mobile base stations to localize and verify location estimates.

The works that are closely related to ours are those of Li *et al*. [9] and Liu *et al*. [10]. Both tried to eliminate attack effects and still provide accurate localization. Li *et al*. used data redundancy and statistical methods to achieve reliable localization in the presence of attacks. Liu *et al*. proposed to detect attacks based on data inconsistency from the received beacons and then used a greedy search or voting algorithm to eliminate the malicious beacon information. However, these methods are mostly localization algorithm specific and cannot be easily scaled to work other localization algorithms. Our approach is different in that it is algorithm independent and can be integrated into the existing localization algorithms and thus is highly scalable. Furthermore, we validated our approach using a large-scale wireless network test bed and a real office environment.

3. OVERVIEW OF NETWORK MODEL AND ADVERSARY MODEL

In this section, we outline the basic wireless network and the adversary model that we used throughout the paper.

3.1. Network model

Our attack-resistant approach aims to be developed generic enough to be applied across a wide range of wireless networks such as wireless sensor networks, Wi-Fi networks, and cellular networks, where wireless technologies are prevalent. For instance, Wi-Fi (802.11) technology is heavily used and Wi-Fi hotspots are deployed everywhere [27] to support applications in residential, commercial, and healthcare areas. In our network model, wireless networks consist of both static and mobile nodes, where each node represents a user equipped with a wireless device (e.g., laptop, cell phone, or sensor).

Furthermore, we assume that a certain number of anchor points (such as Wi-Fi access points and cell towers) or traffic sniffers are deployed with known locations, from which the RSS of the wireless devices can be measured. This is a reasonable assumption because the War Drive by Skyhook Wireless in 2006 collected more than 5 million Wi-Fi access points, which is approximately only 10% of the deployed access points in USA [27]. This is especially true when focusing on high-density population areas; for example, Manhattan has a density of more than 1800 access points per square kilometer.

We note that RSS is made widely available across a variety of wireless devices and governed by the distance from a wireless device to an anchor point. The RSS measurements will be used by various localization algorithms when performing position estimations. For instance, the lateration-based algorithms will use the measured RSS extracted from the wireless devices to derive the propagation parameters in the signal propagation model, whereas the fingerprint matching algorithms will use the RSS as the RF fingerprint to construct the radio database through training.

3.2. Adversary model

We considered localization infrastructure attacks. In particular, we focused on the physical attacks present on anchor points (e.g., Wi-Fi access points). Compromising anchor points can affect the localization accuracy of a group of wireless devices, because the measured RSS from these wireless devices at anchor points is used to perform position estimations. An adversary can compromise an anchor point and modify the measured RSS at the anchor point, or an adversary can directly attenuate or amplify the signals between an anchor point and the wireless device.

Furthermore, multiple adversaries can collaborate and compromise more than one anchor points. However, they cannot afford to deploy their own wireless devices throughout the network, nor do they have the ability to monitor the entire network communications. Thus, we can assume that not all of the anchor points are compromised in the network. Specifically, we assume that there exist more than half of the access points remaining non-attacked in the localization infrastructure.

4. ACHIEVING ATTACK-RESISTANT LOCALIZATION

In this section, we first analyze the effects of infrastructure attacks on localization by using lateration-based algorithms as an example. We then present our attack-resistant scheme.

4.1. Effects of infrastructure attacks

Before introducing our attack-resistant approach, let us first understand the effects of infrastructure attacks to localization accuracy. When exploiting RSS to perform localization, the measured RSS is determined by the distance between the wireless device and the anchor points. However, the RSS measurements are also affected by the random noise, environmental bias, and multipath effects. We call these factors as environmental effects. These environmental effects will consequently affect the accuracy of the location estimation. We use lateration-based algorithms to study the impact introduced by infrastructure attacks versus the localization errors caused by environmental effects.

4.1.1. Lateration-based methods—an algorithm example.

Lateration-based approaches are widely used in wireless localization [9,17,19]. They estimate the position of the wireless device by estimating the distance to multiple anchor points and then derive the location estimation by solving a LS problem.

There are two main steps when performing lateration-based localization: *ranging* and *lateration*. The ranging step is used to estimate the distance (e.g., d_i) between the wireless device and the ith anchor point. In this work, we used the measured RSS of the wireless device at anchor points to derive the propagation parameters in the signal propagation model and then obtain the distance estimation from the signal-to-distance relationship:

$$P(d)[dBm] = P(d_0)[dBm] - 10\gamma \log_{10}\left(\frac{d}{d_0}\right) \qquad (1)$$

where $P(d_0)$ represents the transmitting power of a wireless device at the reference distance d_0, d is the distance between the transmitting device and the anchor point, and γ is the path loss exponent.

In the lateration step, we study both *non-linear least square* (NLS) and *linear least square* (LLS) methods.

4.1.1.1. Non-linear least squares. Given the estimated distances d_i and known positions (x_i, y_i) of the anchor points, the position (x, y) of the wireless node can be estimated by finding $(\hat{x}, \hat{y})$ satisfying:

$$(\hat{x}, \hat{y}) = \arg \min_{x,y} \sum_{i=1}^{N} \left[\sqrt{(x_i - x)^2 + (y_i - y)^2} - d_i \right]^2 \quad (2)$$

where N is the number of access points that is used to estimate the location of the wireless node. NLS can be viewed as an optimization problem where the objective is to minimize the sum of the error square. The NLS problem usually involves iterative searching techniques, such as gradient descent or Newton method, to obtain the solution and thus requires significant computational complexity.

4.1.1.2. Linear least squares. The LLS is an approximation of NLS. It linearizes the NLS problem by introducing a constraint in the formulation and obtaining a closed form solution of the location estimation. Compared with NLS, LLS has less computational complexity. The location of the wireless device can be obtained by solving the form $\mathbf{A}x = \mathbf{b}$ with the following:

$$\mathbf{A} = \begin{pmatrix} x_1 - \frac{1}{N}\sum_{i=1}^{N} x_i & y_1 - \frac{1}{N}\sum_{i=1}^{N} y_i \\ \vdots & \vdots \\ x_N - \frac{1}{N}\sum_{i=1}^{N} x_i & y_N - \frac{1}{N}\sum_{i=1}^{N} y_i \end{pmatrix} \quad (3)$$

$$\mathbf{b} = \frac{1}{2} \begin{pmatrix} \left(x_1^2 - \frac{1}{N}\sum_{i=1}^{N} x_i^2\right) + \left(y_1^2 - \frac{1}{N}\sum_{i=1}^{N} y_i^2\right) \\ \quad - \left(d_1^2 - \frac{1}{N}\sum_{i=1}^{N} d_i^2\right) \\ \vdots \\ \left(x_N^2 - \frac{1}{N}\sum_{i=1}^{N} x_i^2\right) + \left(y_N^2 - \frac{1}{N}\sum_{i=1}^{N} y_i^2\right) \\ \quad - \left(d_N^2 - \frac{1}{N}\sum_{i=1}^{N} d_i^2\right) \end{pmatrix} \quad (4)$$

where $\mathbf{A}$ is only described by the coordinates of anchor points, $\mathbf{b}$ is represented by the distances to the anchor points together with the coordinates of anchor points, and x is the estimated location of the wireless device. Thus, the location estimation can be obtained as $x = (\mathbf{A}^T\mathbf{A})^{-1}\mathbf{A}^T\mathbf{b}$.

4.1.2. Error analysis.

To examine the impact introduced by infrastructure attacks versus the localization errors caused by environmental effects, we assume the RSS variations caused by environmental factors follow the normal distribution with zero mean and δ standard deviation [28,29], and the signal propagation model becomes [28] as follows:

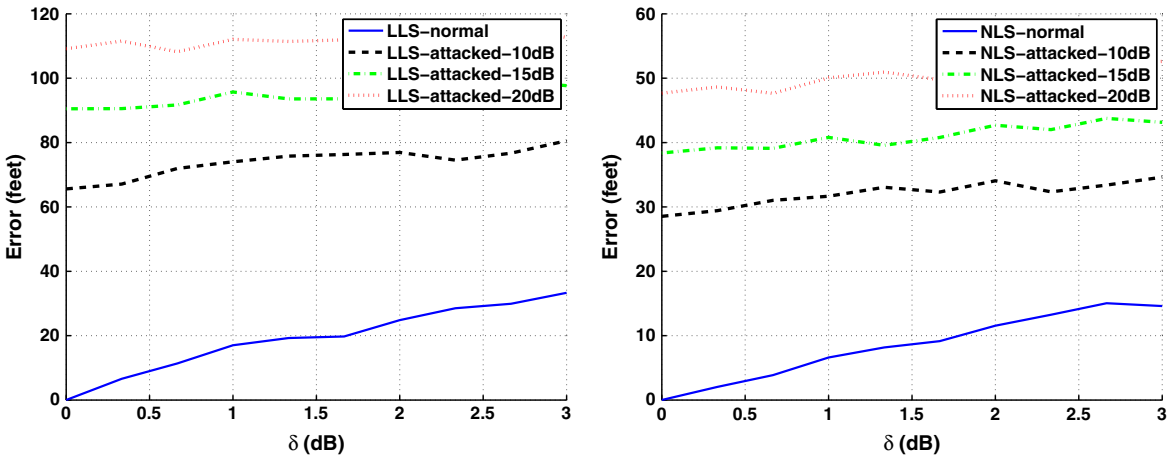
$$P(d)[dBm] = P(d_0)[dBm] - 10\gamma \log_{10}\left(\frac{d_i}{d_0}\right) + S_\delta \quad (5)$$

where S_δ is the RSS variations caused by environmental factors. On the other hand, when an anchor point is compromised, the adversary will attack the anchor point by attenuating or amplifying the measured RSS. To maximize its attacking impact, we assume the adversary will vary the RSS measurements by 10 to 20 dB at the attacked anchor point.

We conducted a simulation study by deploying three anchor points in a 200 × 200 ft square area. We varied the standard deviation δ of the measurement errors caused by environmental effects from 0 to 3 dB. When an anchor point is compromised, the measured RSS readings at the attacked anchor point are altered by 10, 15, and 20 dB. We ran the simulation tests for 1000 times to obtain an average behavior of the localization accuracy under attack.

Figure 1 presents the average location estimation errors for lateration-based methods when one anchor point is attacked in our simulation. The solid line in Figure 1 presents the localization error under a normal situation without attacks, whereas the dotted lines represent the localization errors when the RSS measurements are attacked by 10, 15, and 20 dB. By examining the performance of lateration-based algorithms, we found that the location estimation errors caused by infrastructure attacks are much larger than the localization errors caused by environmental effects. In particular, under an infrastructure attack, the location estimation errors using NLS are three times larger than those under a normal situation without attacks and six times larger when using LLS. This indicates that the localization results are close to the true location of the wireless device under normal situations. However, under infrastructure attacks, even when only one anchor point (out of three) is attacked in this case, the location estimations are far away from the true location of the wireless node. Figure 2 presents the statistical results of the location estimations by using NLS algorithm under normal situations and those when the access points are attacked. We ran the simulation tests for 1000 times for each case. We put the wireless device at the center of the experiential floor and set the attack strength uniformly distributed from 10 to 20 dB. From Figure 2, we observed that the location estimations under normal situations are clustered together around the true location of the wireless device, whereas the location estimation under attacked situations are scattered all over the place.

Furthermore, we conducted experiments by performing localization in multiple runs when putting the wireless device at location (124 ft, 82 ft) in an office floor with a dimension of 220 by 120 ft. Figure 3 presents the experimental results of the location estimations under normal situations and those when one individual anchor point is attacked. We observed that the localization results of a wireless device under the normal situation with no attacks are clearly *clustered* together and close to the true location of the device. On the other hand, when an attack is present on anchor points, the localization results are *scattered* and far from the true location of the device. Thus, the geometric relationship of the localization results from multiple runs presents a *clustering–scattering* effect. The clustering–scattering effect enables us to distinguish



(a) LLS algorithms (b) NLS algorithms

Figure 1. Error analysis when using LLS and NLS algorithms. LLS, linear least square; NLS, non-linear least square.

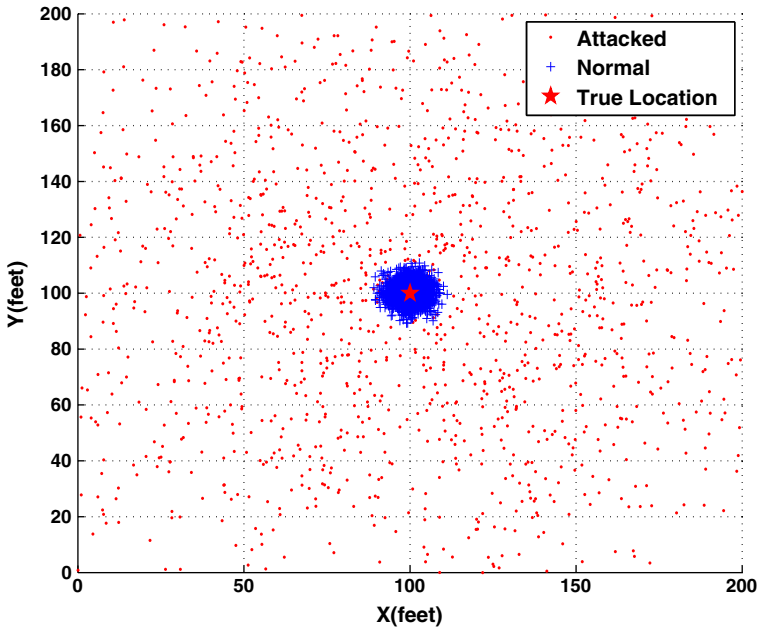


Figure 2. Illustration of statistical localization results under normal situations and with attacks on anchor points.

the correct location estimations from the corrupted ones caused by infrastructure attacks.

4.2. Attack-resistant scheme

The objective of attack-resistant localization is to keep the benign location estimations and filter out the corrupted location estimations by exploiting the clustering–scattering effect. However, the true location of the wireless device is unknown and thus cannot be used for a direct comparison to remove the corrupted localization results. To address this issue, we seek to design the attack-resistant scheme that uses the location estimations to verify with each other based on the clustering–scattering effect. We propose our scheme as follows.

4.2.1. Obtaining the intra-distance.

As stated in our adversary model, not all of the anchor points are being attacked. This means that there exists a portion of the anchor points on which the measured RSS readings are not altered by adversaries. Suppose there are N anchor points in the area of interest. To localize a wireless device, we choose any three of the N access points to perform the location estimation by using a localization

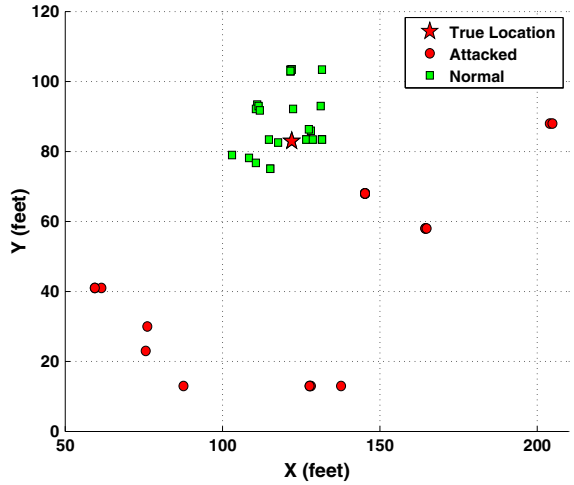


Figure 3. Illustration of localization results of a wireless device under normal situations and with attacks on anchor points.

algorithm. We can then obtain multiple localization results from $\binom{N}{3}$ possible combinations. We denote these location estimations as $(x_i, y_i), i \in 1, 2 \ldots \binom{N}{3}$. The traditional approach is to average the multiple location estimations to obtain an accurate localization result of the wireless device. However, when an infrastructure attack is present, the corrupted location estimations will significantly affect the final localization result as shown in Section 4.1.2. Thus, the corrupted location estimations need to be identified and filtered out so that they cannot contribute to the final localization result.

Based on the clustering–scattering effect, we found that the distance between location estimations may be used as a verification criterion for identifying corrupted location estimations. Toward this end, we measure the distance from each location estimation to the rest of them. We define the *intra-distance* D_i for the ith location estimation as follows:

$$D_i = \frac{1}{\binom{N}{3} - 1} \sum_{\substack{j=1,\ldots\binom{N}{3} \\ j \neq i}} \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2} \quad (6)$$

where $(x_i, y_i), i \in 1, 2 \ldots \binom{N}{3}$ are the location estimations from $\binom{N}{3}$ possible combinations of N anchor points. Thus, D_i represents the geographic relationship between the ith location estimation result and the rest of the localization estimations. According to the clustering–scattering effect, if the ith location estimation is derived from anchor points containing compromised ones, D_i will be large, whereas the intra-distance D_i should be small if the location estimation is obtained from benign anchor points. Under the assumption that there are more than half of the access points that are non-attacked, even if multiple adversaries collaboratively create mutually consistent ranges, the number of combinations in which the access points are all chosen from the attacked access points is smaller than that chosen from the benign access points. Consequently, the intra-distance of the localization results from the benign access points is smaller than that of the localization results of the combination in which all the access points are chosen from the attacked access points. Therefore, applying a threshold τ on D_i can filter out the corrupted location estimations when $D_i > \tau$.

4.2.2. Filtering via clustering analysis.

Using a single threshold τ may result in a high false positive when identifying corrupted location estimations because the measured RSS readings are affected by environmental changes. We propose to use K-means clustering analysis on D_i based on the clustering–scattering effect to separate the benign location estimations from those corrupted ones. The K-means algorithm is one of the most popular iterative descent clustering methods [30]. In the K-means algorithm, the squared Euclidean distance is chosen as the dissimilarity measure. If there is M-measured D_i from the location estimations, the K-means clustering algorithm partitions M-measured D_i into K disjoint subsets Q_j containing M_j-measured distances so as to minimize the sum-of-squares criterion:

$$\mathbf{I}_{\min} = \sum_{j=1}^{K} \sum_{D_m \in Q_j} \|D_m - O_j\|^2 \quad (7)$$

where D_m is a measured distance representing the intra-distance for the mth location estimation and O_j is the geometric centroid of the measured distance for Q_j.

In our K-means clustering analysis, we set $K = 2$ and group the intra-distances resulted from the location estimations into two clusters: one holds the benign location estimations and the other consists of the corrupted ones. Thus, as a result of the K-means analysis, the measured distances are partitioned into two clusters: the intra-distances $\{D_i\}, i = 1, 2, \ldots n$ inside one cluster should be small and represent the location estimations obtained from benign anchor points, whereas $\{D_i\}, i = n+1, n+2, \ldots M$ in

another cluster should be large and represent the location estimations involving compromised anchor points.

4.2.3. Achieving attack-resistant results.

After the location estimations are partitioned into two clusters, we then average over the coordinates of the location estimations in the cluster with smaller $\{D_i\}$, shown as green squares in Figure 3, to represent the final localization result of the wireless device. We call this result as the *cluster* result. In a similar way, the localization result whose D_i is the smallest is at the centroid of this cluster. We can also represent the final localization result by using the location estimation with the smallest D_i. We call this result as the *single* result.

5. ALGORITHMS

In this section, we describe the localization algorithms that are used to validate our approach. In particular, we study three categories of algorithms: *lateration based*, *fingerprint matching*, and *BNs*.

5.1. Lateration-based algorithms

Lateration is a widely used localization algorithm, as is evidenced by its application as in many recent localization research works [2,9,17,19,20]. Lateration-based algorithms construct a set of LS equations by estimating the distance to anchor points and solve for the position estimation. The detailed description of the algorithm is presented in Section 4.1.1.

5.2. Fingerprint matching algorithms

Rather than relying on modeling the signal strength and distance relationship, fingerprint matching-based methods match RSS observations against a pre-built signal map that is constructed by using the training data. Next, we briefly introduce two representative fingerprint matching-based algorithms, *RADAR* and *Gridded-RADAR*, which are used to validate our attack-resistant scheme.

5.2.1. RADAR.

In RADAR [5], during the off-line phase, a mobile transmitter with known position broadcasts beacons periodically, and the RSS readings are measured at a set of anchor points. Collecting together the averaged RSS readings from each of the anchor points for a set of known locations provides a radio map. At runtime, localization is performed by measuring a transmitter's RSS at each anchor point, and the vector of RSS values is compared with the radio map. The record in the radio map whose signal strength vector is the closest in the Euclidean sense to the observed RSS vector is declared to correspond to the location of the transmitter.

5.2.2. Gridded-RADAR.

The Gridded-RADAR algorithm is extended from RADAR [14]. Gridded-RADAR uses an interpolated map grid (IMG), which is built from a set of averaged RSS readings with known (x, y) locations. Because the quality of the signal map is sensitive to the number of known location [12], the purpose to use an IMG is to improve the resolution of the signal map so as to obtain better localization accuracy. Because directly measuring the RSS at a large number of known locations is expensive, the interpolation approach is used to improve the quality of the signal map based on the averaged RSS readings from a small number of known locations. We build an IMG for each anchor point independently on a grid of 10-in square tiles. Particularly, we used triangle-based linear interpolation, which divides the floor into triangular regions using a Delaunay triangulation. We then linearly interpolate the expected signal strength at the center of each tile. When performing localization, given observed RSS readings with an unknown location, Gridded-RADAR returns the (x, y) of the nearest neighbor in the IMG to the one to localize.

To apply our proposed attack-resistant scheme to fingerprint matching algorithms, we first obtain all the possible fingerprint subsets from the combination of any three access points. Suppose there are N access points, we can have $\binom{N}{3}$ subset fingerprints and get $\binom{N}{3}$ localization results after performing fingerprinting matching using each subset. The attack-resistant scheme can be applied to these $\binom{N}{3}$ localization results to obtain the location estimate of the targeting device.

5.3. Bayesian networks

Bayesian network localization is a machine learning-based algorithm that uses the Bayesian graphical model to encode the signal-to-distance relationship for the location estimation [31]. Figure 4 shows the basic BN used for our study. The vertices X and Y represent a location in a two-dimensional space; the vertex s_i is the RSS reading from the ith anchor point, and the vertex D_i represents the Euclidean distance between the location specified by X and Y and the ith anchor point. The value of s_i follows the log-distance propagation model $s_i = b_{0i} + b_{1i}\mathbf{log}D_i$, where b_{0i}, b_{1i} are the parameters specific to the ith anchor point. The distance $D_i = \sqrt{(X-x_i)^2 + (Y-y_i)^2}$ in turn depends on the location (X, Y) of the measured signal and the coordinates (x_i, y_i) of the ith anchor point. The network models noise and outliers by modeling the s_i as a Gaussian distribution around the mentioned propagation model, with variance $\tau_i : s_i ; N(b_{0i} + b_{1i}\mathbf{log}D_i, \tau_i)$. Through Markov chain Monte Carlo simulation, BN returns the sampling distribution of the possible location of X and Y as the localization result.

To apply our proposed attack-resistant scheme to BNs algorithm, we first obtain $\binom{N}{3}$ localization results from all the possible combinations of three access points chosen from N access points. Our attack-resistant scheme can then be applied to these $\binom{N}{3}$ localization results to obtain the final position estimate.

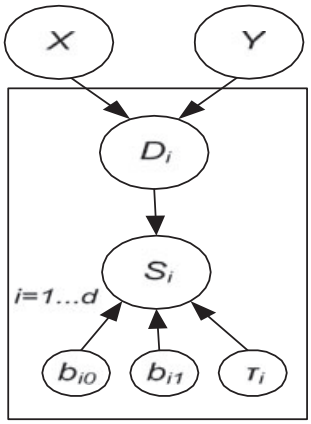


Figure 4. Bayesian graphical model in our study.

6. TEST BED INFRASTRUCTURE AND METHODOLOGY

In this section, we first describe our test bed infrastructure under an IEEE 802.11 (Wi-Fi) network as well as an IEEE 802.15.4 (ZigBee) network. We then present our experimental methodology and develop the evaluation metrics.

6.1. Test bed setup

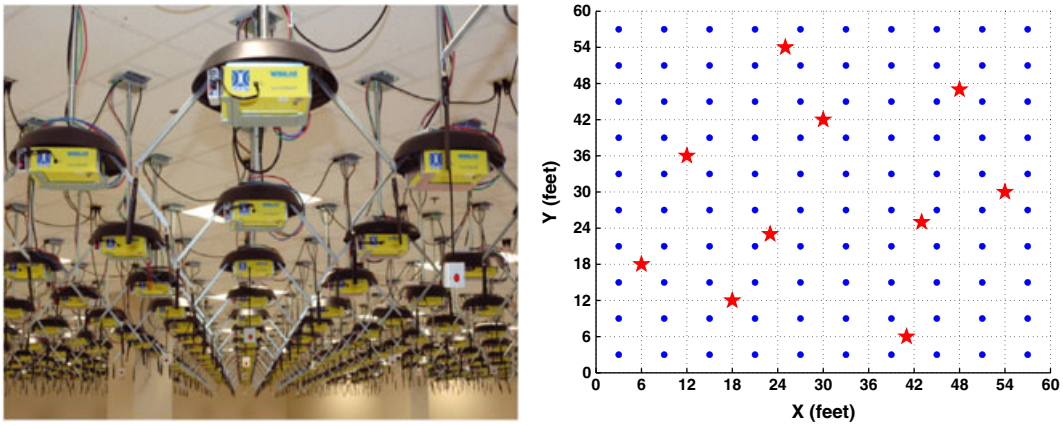
In order to evaluate the effectiveness and generality of our attack-resistant scheme, we conducted experiments in two test beds under two wireless networks: the ORBIT test bed in WINLAB (North Brunswick, NJ, USA) using an 802.11 (Wi-Fi) network and the open office floor where WINLAB is resided using an 802.15.4 (ZigBee) network. The sizes of these two testing areas are 60×60 and 219×169 ft, respectively.

6.1.1. Configuration of anchor points.

The ORBIT test bed simulates a large-scale wireless network consisting of 400 network nodes with IEEE 802.11a/b/g wireless interface. Figure 5(a) shows the layout of the ORBIT test bed. To run our experiments, we configured 10 orbit nodes as anchor points to monitor the packet traffic transmitted from a movable ORBIT node located at different locations. Figure 5(b) depicts the deployment of 10 anchor points, shown in red stars, in the Wi-Fi network using the ORBIT test bed. Furthermore, Figure 6 depicts the layout of the office floor in WINLAB. We configured 10 anchor points, shown in red stars, in the ZigBee network. Each anchor point in the ZigBee network is a Linux machine with a 1-GHz CPU, 512 MBs of RAM, and a 20-GB disk. We attached a Tmote Sky (San Francisco, CA, USA) mote on each anchor point, and each Tmote Sky mote is connected to an external 7-dBi omnidirectional antenna. We configured each attached mote as a receiver to monitor the packets transmitted from a mobile Tmote sky located at different locations.

6.1.2. Distribution of testing points.

We measured RSS readings from 100 locations in the ORBIT test bed under the Wi-Fi network, which are depicted as small dots in Figure 5(b). The distance between two adjacent locations is 6 ft. On the other hand, in the floor area of WINLAB, we measured RSS readings from 101 locations under the ZigBee network. These locations are shown as small points in Figure 6. The distance between two adjacent locations is 5–10 ft. To collect the RSS measurements, the mobile transmitter moves from one location to another and transmits packets at different locations. Every anchor point then forwards the RSS readings from the observed packets to a centralized server to store. At each testing location, the sever waits for at least 350 packets from each anchor point and then uses the averaged RSS values as the RSS measurement.



(a) Wireless nodes lay out in ORBIT testbed

(b) Deployment of anchor points

Figure 5. ORBIT test bed setup in WINLAB.

Figure 6. The floor layout of the office space in WINLAB.

To validate our method, we evaluated the performance of the attack-resistant scheme under different types of localization algorithms including lateration-based methods, fingerprint matching, and BNs. The well-known leave-one-out method is applied, which means that we choose one location as the testing point to be localized whereas the rest of the locations as the training data. For the ZigBee network, the size of the training data is 99 locations. Similarly, it is 100 locations for the Wi-Fi network.

6.1.3. Injecting attacks.

To simulate the attacks on anchor points, we attenuate or amplify the RSS values measured by anchor points. Furthermore, various attack scenarios are created, including different percentage of compromised anchor points, for example, 10% or 30% of anchor points are attacked, and different magnitudes of the attacking severity, for example, the attacking severity is 20 dB.

6.2. Evaluation metrics

We next present the metrics that we developed to quantify the effectiveness of our attack-resistant scheme.

(1) *Accuracy*. Localization accuracy is the Euclidean distance between the estimated location and the true position of the wireless device in the physical space. We also refer to this distance as localization error. To capture the statistical characterization of the localization error, we study the cumulative distribution function (CDF) of the localization error for all the testing points.

(2) *Degradation rate*. We define the degradation rate (DR) as the ratio of the localization accuracy under the normal situation without attacks to the localization accuracy under an infrastructure attack. The DR measures how much impact an infrastructure attack can affect the localization accuracy with respect to the localization error under normal situations.

(3) *Resistance rate*. The resistance rate (RR) quantifies the effectiveness of the attack-resistant scheme. Suppose the localization accuracy under normal situations is E_n, whereas it is E_a with $E_a > E_n$ when an infrastructure attack is present. If the attack-resistant scheme is applied, the localization accuracy is represented by E_r. Then, the RR can be defined as

$$\mathrm{RR} = \frac{(E_a - E_r)}{(E_a - E_n)} \tag{8}$$

The value of the RR indicates the effectiveness of the attack-resistant scheme under infrastructure attacks:

- RR = 1 indicates that the attack-resistant scheme can eliminate the effect of the infrastructure attack and is thus highly effective. As a result, the localization accuracy when the attack-resistant scheme is applied under an infrastructure attack achieves the same performance as that under normal situations.
- RR > 1 indicates that the application of the attack-resistant scheme can not only eliminate the impact of the infrastructure attack but also achieve better localization accuracy than that under normal situations.
- 0 < RR < 1 indicates that the application of the attack-resistant scheme can mitigate the impact of the infrastructure attack, although it cannot fully eliminate the effects of the attack.
- RR < 0 indicates that the application of the attack-resistant scheme will lead to even larger localization errors than those under the infrastructure attack. The attack-resistant scheme is thus not effective.

7. EVALUATION RESULTS

In this section, we first present the performance evaluation of our approach by applying the attack-resistant scheme to lateration-based algorithms. We further conduct a robustness evaluation when applying our scheme to other algorithms including fingerprinting matching and BNs. Finally, we compare the performance of our approach with the existing method using least median squares (LMS) to achieve reliable localization results.

7.1. Performance evaluation when working with lateration-based algorithms

7.1.1. Ten per cent of anchor points are compromised.

Figure 7 presents the performance comparison in terms of the localization error CDFs of lateration-based methods under the Wi-Fi and ZigBee networks when 10% of anchor points are attacked. The four performance curves in each subfigure correspond to the following scenarios: (i) under normal situations without attacks; (ii) 10% anchor points are compromised; (iii) our attack-resistant scheme is applied and the *cluster* result is shown; and (iv) our attack-resistant scheme is applied and the *single* result is shown. The DR and RR for these four scenarios are presented in Table I. In general, we found from Figure 7 that the infrastructure attack significantly degrades the localization accuracy. The striking observation in Figure 7 is that the localization results obtained from the application of the attack-resistant scheme even outperforms those under normal situations in terms of accuracy. In addition, we found that the performance of the *single* result is comparable with that of the *cluster* result.

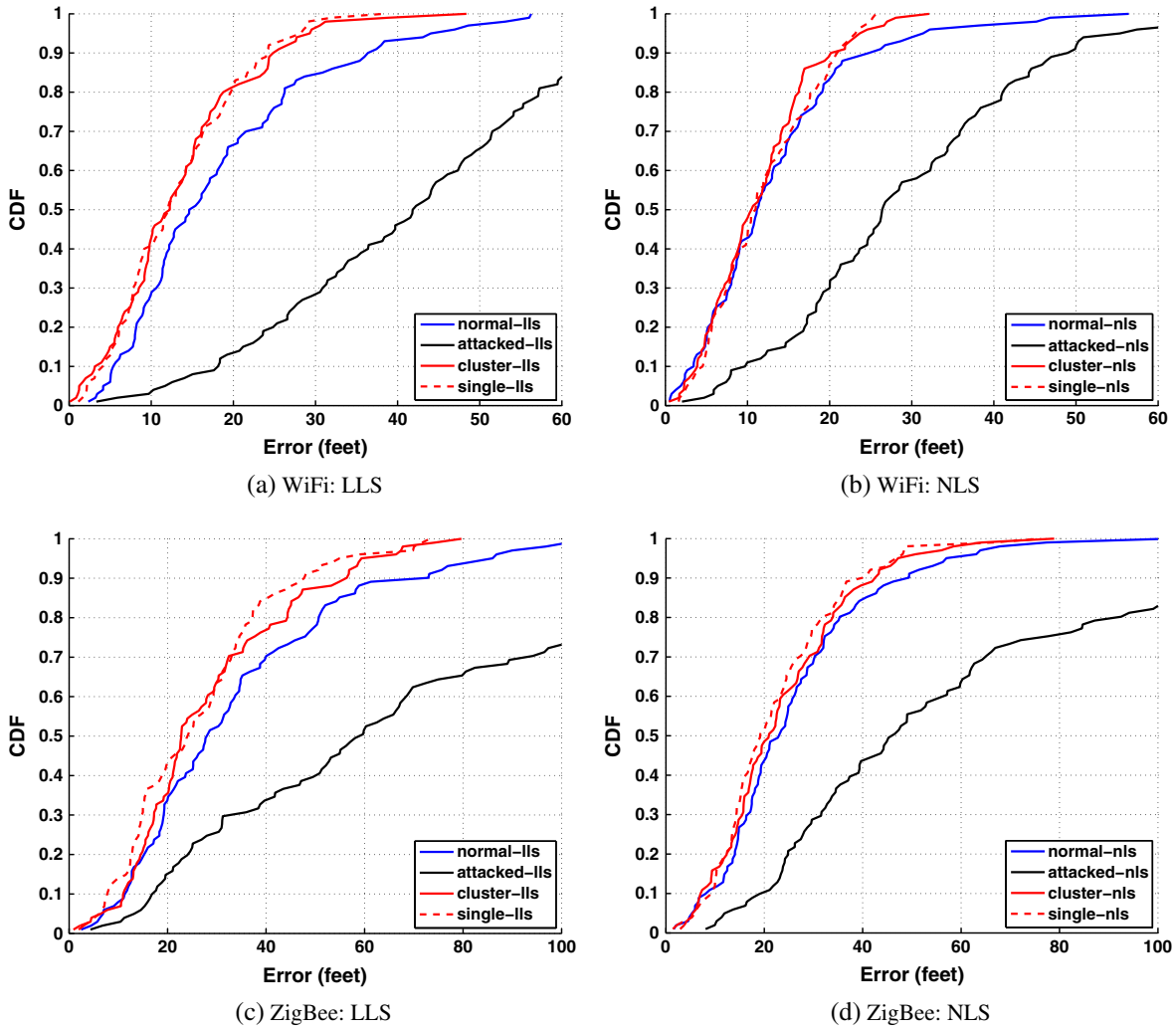
In particular, Figure 7(a) shows the localization error CDFs of the LLS method in the Wi-Fi network. We observed that applying the attack-resistant scheme results in a significant improvement of the localization accuracy when infrastructure attacks are present on anchor points. Specifically, the median error is improved from 42 to 12 ft under an infrastructure attack, compared with 15 ft for the normal situation. Similarly, the 90th percentile error is improved from 64 to 24 ft under an infrastructure attack, compared with 37 ft under the normal situation. Furthermore, as shown in Table I, the DR of median error is 1.86 under an attack, indicating that the infrastructure attack has a severe impact on localization accuracy. Examining the RR after the application of the attack-resistant scheme in Table I, we found that the RRs of median error for both *single* and *cluster* results are all 1.09. And the RR of 90% percentile error is 1.43 for *single* and 1.46 for *cluster*, respectively.

Furthermore, Figure 7(b) is the localization error CDFs of the NLS method in the Wi-Fi network. First, we found that the NLS method achieves better localization accuracy than that of LLS method under the normal situation. This is because LLS is an approximation of NLS. Furthermore, we observed comparable performance improvement when applying the attack-resistant scheme to that by using LLS under an infrastructure attack. In particular, the median error is improved from 25 to about 10 ft when using the attack-resistant scheme under an infrastructure attack, whereas it is 11 ft under the normal situation. Correspondingly, the 90th percentile error can be improved from 49 to 21 ft under an infrastructure attack, compared with 25 ft under the normal situation. By studying the RRs of the median error and the 90th percentile error when using NLS from Table I, we found that our attack-resistant scheme can completely eliminate the impact of the infrastructure attack and achieves the RRs' value higher than 1, indicating better localization accuracy than that under the normal situation.

Finally, comparing the results from the ZigBee network with those of the Wi-Fi network in Figure 7(c, d), the error CDF curves when applying the attack-resistant scheme in the ZigBee network have similar performance improvement. The RRs, as shown in Table I, are all higher than 1 for both the median error and the 90th percentile error. This shows that the results from the ZigBee network are consistent with those from the Wi-Fi network.

7.1.2. Discussion.

The given results are encouraging because it indicates that the application of the attack-resistant scheme can not only eliminate the impact of the infrastructure attack but also achieve better localization accuracy than that under normal situations. When under normal situations, the RSS measurements are affected by environmental factors and may contain outliers. Basically, the effects of RSS outliers on localization accuracy are similar to those caused by corrupted RSS readings under an infrastructure attack. However, the RSS outliers are introduced unintentionally. Therefore, the localization accuracy can be affected by RSS outliers even under normal situations. Our observation indicates that the



(a) WiFi: LLS (b) WiFi: NLS

(c) ZigBee: LLS (d) ZigBee: NLS

Figure 7. Lateration-based methods: localization error CDFs for NLS and LLS under networks Wi-Fi and ZigBee when 10% access points are compromised. CDF, cumulative distribution function; NLS, non-linear least square; LLS, linear least square.

Table I. Degradation rate and resistance rate of lateration-based algorithm when 10% of anchor points are compromised.

Median error	Wi-Fi, LLS	Wi-Fi, NLS	ZigBee, LLS	ZigBee, NLS
DR	1.8630	1.3784	1.0567	0.9825
RR, cluster	1.0956	1.0392	1.1846	1.0893
RR, single	1.0956	1.0719	1.1477	1.1607
90th percentile	Wi-Fi, LLS	Wi-Fi, NLS	ZigBee, LLS	ZigBee, NLS
DR	0.7473	0.9758	0.8356	1.2470
RR, cluster	1.4265	1.1612	1.2721	1.1120
RR, single	1.4596	1.1612	1.4148	1.1510

LLS, linear least square; NLS, non-linear least square; DR, degradation rate; RR, resistance rate.

application of the attack-resistant method has removed the effects of these outliers when appropriately clustering the multiple localization estimations based on their geometric relationship with each other. Therefore, after the application of the attack-resistant scheme, better localization accuracy may be achieved.

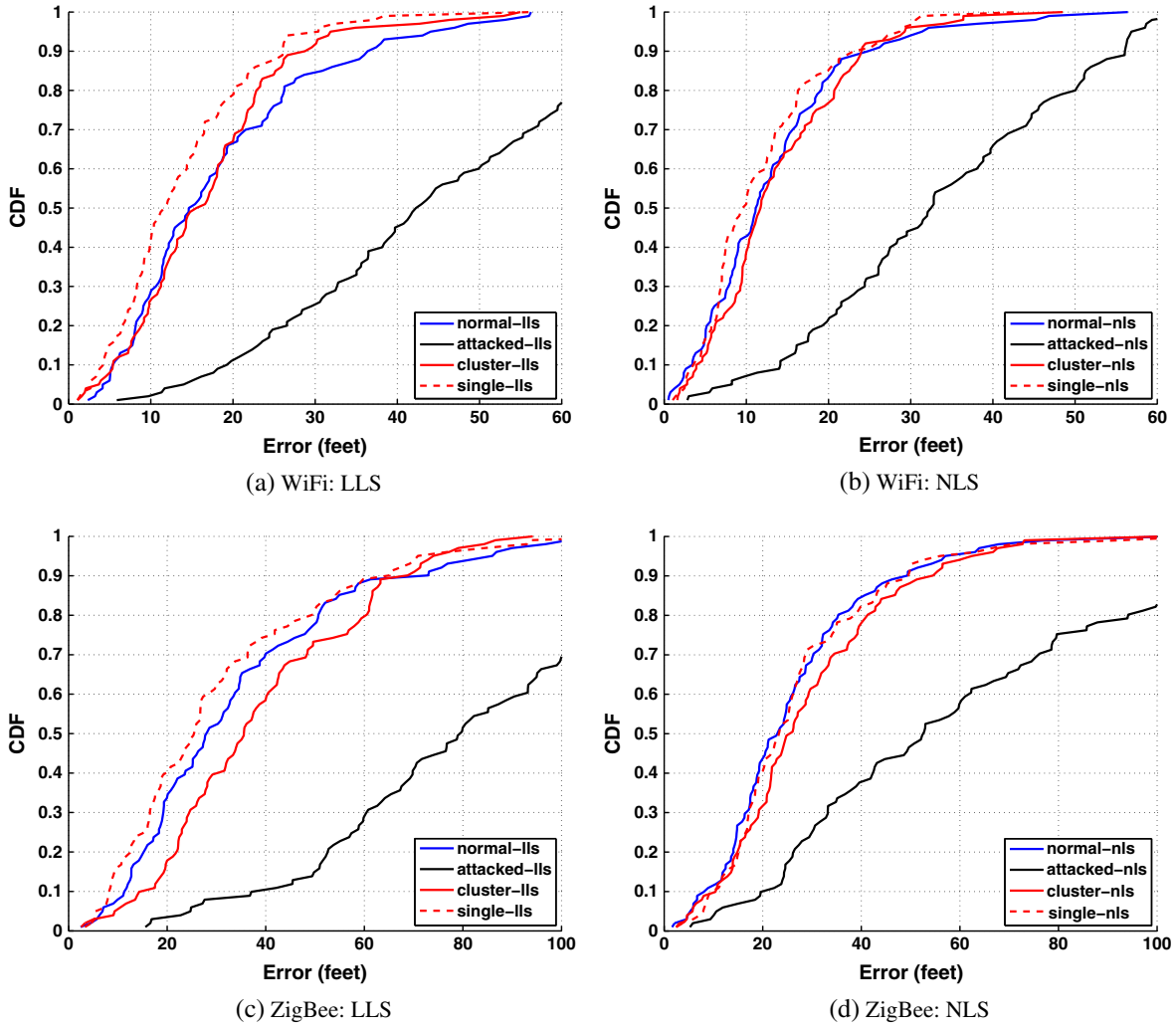
7.1.3. Thirty per cent of anchor points are compromised.

We further studied the localization performance of applying our attack-resistant scheme when 30% of anchor points are attacked. Figure 8 presents the localization error CDF curves for both the Wi-Fi and ZigBee networks. The DR and RR are presented in Table II. First, comparing the results when 30% access points are attacked with those when 10% access points are attacked, we observed that the more the attacked access points, the more the localization accuracy got impacted by infrastructure attacks. Second, under the application of the attack-resistant scheme, the location estimations can achieve similar performance as those under the normal situation.

Particularly, Figure 8(a) shows the localization error of the LLS method in the Wi-Fi network. From Figure 8(a), we see that the median error can be improved from 43 to around 13 ft under an infrastructure attack, and the 90th percentile error can be improved from 68 to around 27 ft. As shown in Table II, the DR on the median error is 1.89, whereas it is 0.86 on the 90th percentile error. The RRs on both the median error and the 90th percentile error are around 1.

Figure 8(b) is the corresponding error CDFs for the NLS method in the Wi-Fi network. We observed comparable performance improvement by using our attack-resistant method with that when using LLS method under an infrastructure attack. Specifically, the attack RR on the median error is around 1 (from 33 to around 10 ft), whereas it is around 1.03 on the 90th percentile error (from 56 to around 23 ft).

In addition, as shown in Figure 8(c, d) for the ZigBee networks, the localization accuracy after applying the attack-resistant scheme exhibits similar improvement. These results consistently show that our attack-resistant scheme can effectively eliminate the impact of the infrastructure attack when using lateration-based localization methods. More importantly, the improved results can achieve comparable or better localization accuracy as those under normal situations.



(a) WiFi: LLS (b) WiFi: NLS

(c) ZigBee: LLS (d) ZigBee: NLS

Figure 8. Lateration-based method: localization error CDFs for networks Wi-Fi and ZigBee when 30% access points are attacked. CDF, cumulative distribution function; NLS, non-linear least square; LLS, linear least square.

Table II. Degradation rate and resistance rate of lateration-based algorithm when 30% access points are attacked.

Median error	Wi-Fi, LLS	Wi-Fi, NLS	ZigBee, LLS	ZigBee, NLS
DR	1.8973	1.9279	1.7979	1.2939
RR, cluster	0.9675	0.9720	0.8560	0.9322
RR, single	1.1083	1.0748	1.0513	0.9864
90th percentile	Wi-Fi, LLS	Wi-Fi, NLS	ZigBee, LLS	ZigBee, NLS
DR	0.8571	1.2581	0.8493	1.2874
RR, cluster	1.2468	1.0577	1.0694	0.9198
RR, single	1.3333	1.0256	1.1290	0.9984

LLS, linear least square; NLS, non-linear least square; DR, degradation rate; RR, resistance rate.

7.2. Robustness evaluation when applied to other algorithms

7.2.1. Fingerprinting matching algorithms.

7.2.1.1. Ten per cent of anchor points are compromised. Figure 9 presents the localization error CDFs of fingerprint matching-based methods for both the Wi-Fi and ZigBee networks, when 10% of anchor points are attacked. The corresponding DR and RR are presented in Table III. From Figure 9, the overall observations are that the infrastructure attack degrades the localization performance, and applying the attack-resistant scheme brings back the localization performance to be comparable with that under the normal situation. The performance of using *cluster* is slightly better than that using *single*.

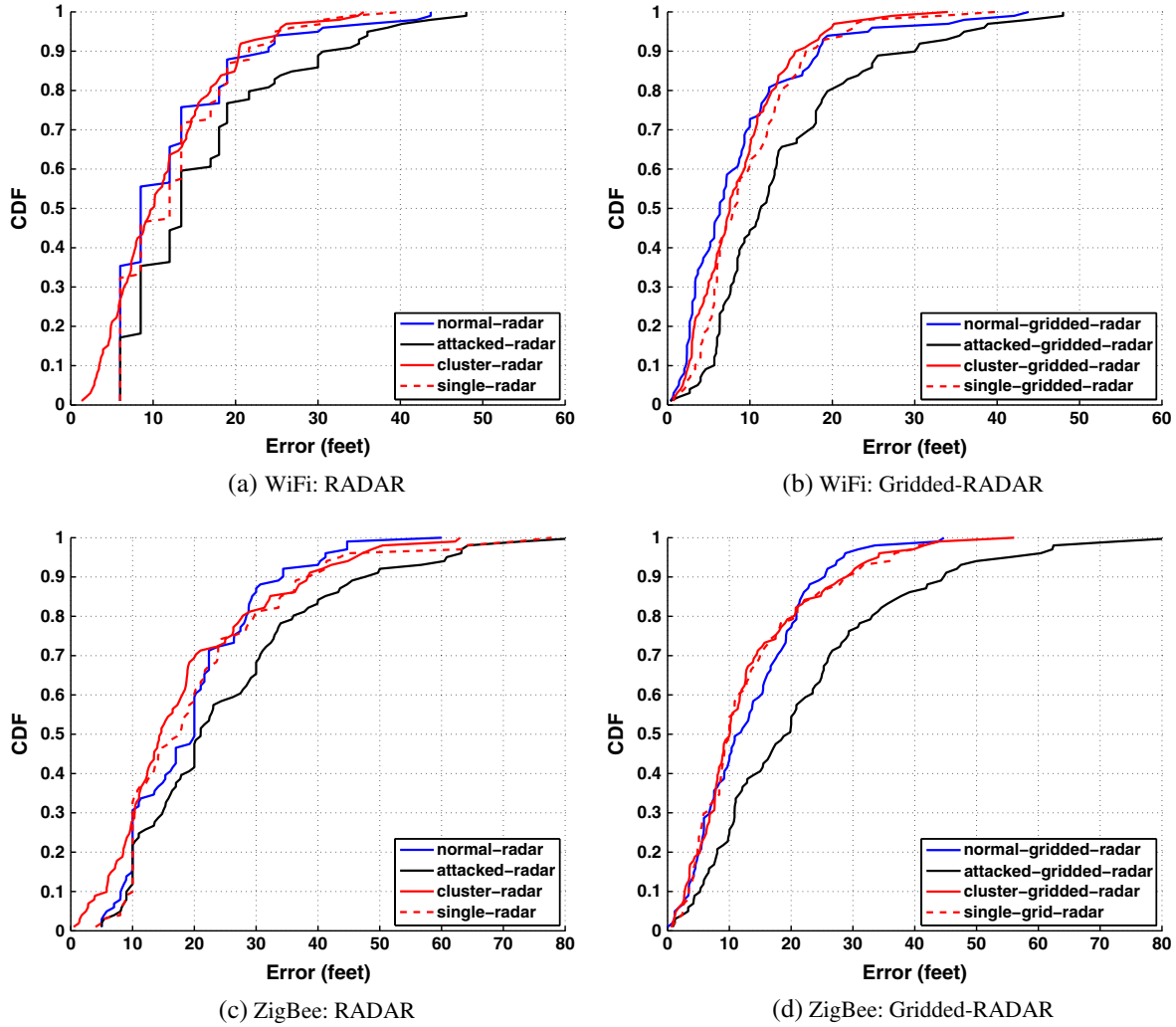
Particularly, in Figure 9(a), which shows the performance of RADAR in the Wi-Fi network, we observed that applying the attack-resistant method improves the localization accuracy under the infrastructure attack. Compared with the results without applying the attack-resistant scheme, we found that the median error is improved from 13.5 to around 10 ft under an infrastructure attack, whereas it is 9 ft for the normal situation. And the 90th percentile error is improved from 34 to around 21 ft under an infrastructure attack, compared with 24 ft under a normal situation. Thus, the RR on the median error is 0.78, whereas it is higher than 1.24 on the 90th percentile error.

Figure 9(b) shows the localization error CDFs of Gridded-RADAR in the Wi-Fi network. We observed that the localization accuracy of Gridded-RADAR is better than RADAR. This is because the Gridded-RADAR uses the interpolation technique to build a fine-gained signal map. Furthermore, we also observed that the attack-resistant method mitigates the impact of the infrastructure attack. Specifically, the median error can be improved from 11 to about 7.5 ft under an infrastructure attack, whereas it is 7 ft for the normal situation. And the 90th percentile error can be improved from 30 to around 16 ft under an infrastructure attack, compared with 18.5 ft for the normal situation. These improvements yield the RRs of 0.77 on the median error and higher than 1.15 on the 90th percentile error.

Turning to examining the localization performance in the ZigBee network, shown in Figure 9(c, d), applying the attack-resistant scheme achieves the similar improvement compared with the results in the Wi-Fi network. Specifically, the attack RR on the median error is higher than 3.8 (improved from 21 to around 15 ft, whereas it w 20 ft under the normal situation) for RADAR. And it is 1.1 for Gridded-RADAR (improved from 20 to 10 ft, whereas it is 11 ft under the normal situation). Checking the attack RR on the 90th percentile, it is 0.7 for RADAR (improved from 48 to 38 ft, whereas it is 34.4 ft under the normal situation), whereas it is 0.82 for Gridded-RADAR (improved from 45 to 30 ft, compared with 25.4 ft under the normal situation).

7.2.1.2. Thirty per cent of anchor points are compromised. Furthermore, we studied the localization performance when applying our attack-resistant approach when 30% of anchor points are attacked. Figure 10 presents the localization error CDFs for both the Wi-Fi and ZigBee networks. The DR and RR are shown in Table IV. Obviously, the localization accuracy under the scenario that 30% anchor points are attacked is worse than that when 10% anchor points are attacked. For both RADAR and Gridded-RADAR, the DRs increase when the number of compromised anchor points increases. Encouragingly, the localization performance when applying the attack-resistant scheme is still comparable with that under the normal situation. This indicates that the application of our attack-resistant method can effectively help the localization algorithms to resist the impact of the infrastructure attack under different number of attacked anchor points.

Particularly, Figure 10(a) shows the localization error of the RADAR in the Wi-Fi network. From Figure 10(a), we observed that the median error is improved from 22 to around 11 ft under the infrastructure attack, which yields RRs between 0.62 and 0.82. And the 90th percentile error is improved from 44 to around 22 ft under the infrastructure attack. This results in an RR higher than 1. Figure 10(b) presents the localization error CDFs of Gridded-RADAR in the Wi-Fi network. We observed comparable performance improvement when applying our attack-resistant method with that when using RADAR under the infrastructure attack. In particular, the attack RR on the median error is around 0.8 (from 21.5 to around 10 ft), whereas it is higher than 0.9 on the 90th percentile error (from 42 to around 19 ft).



(a) WiFi: RADAR (b) WiFi: Gridded-RADAR

(c) ZigBee: RADAR (d) ZigBee: Gridded-RADAR

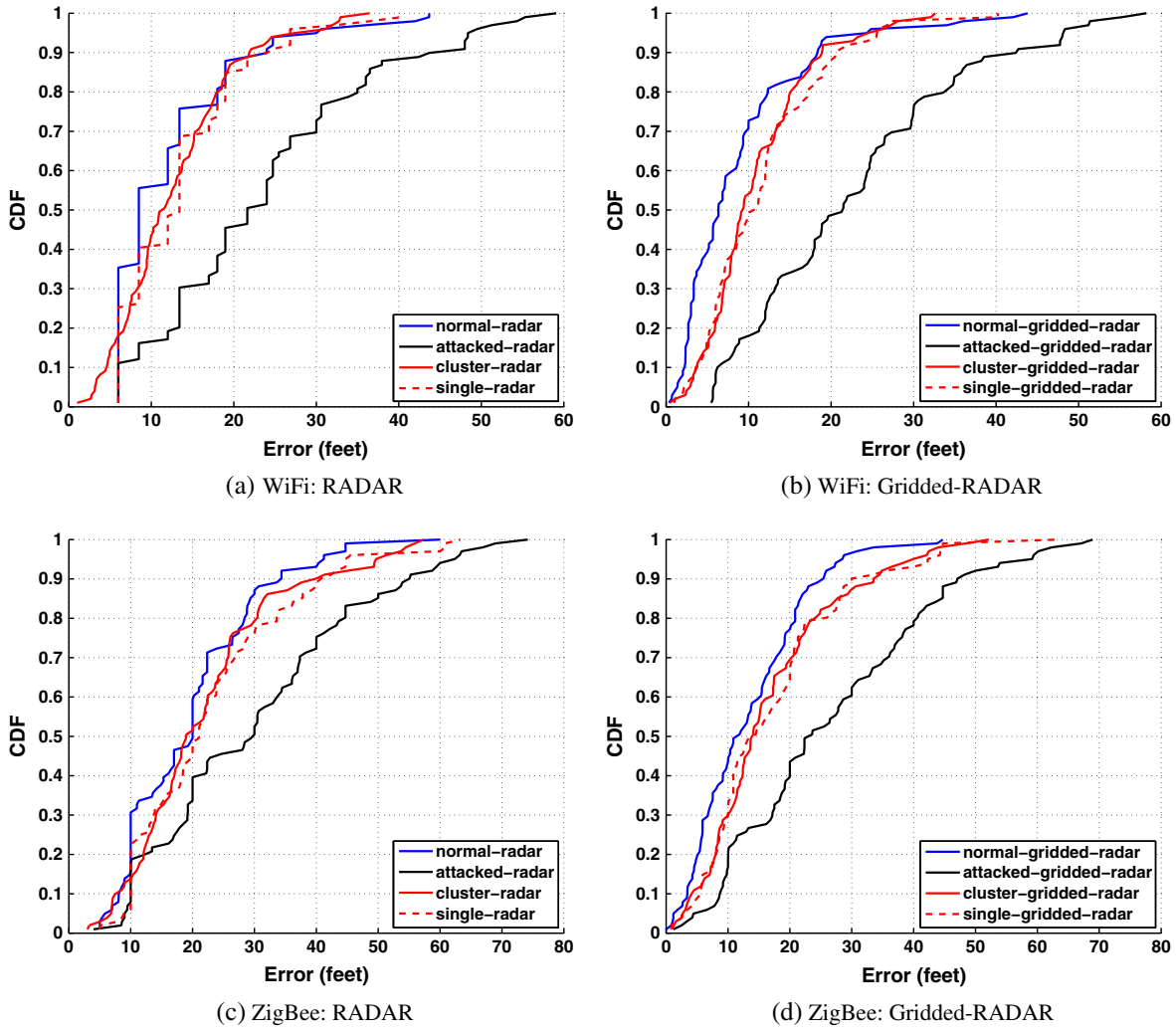
Figure 9. Fingerprint matching-based method: localization error CDFs for networks Wi-Fi and ZigBee when 10% access points are attacked. CDF, cumulative distribution function.

Table III. Degradation rate and resistance rate of fingerprint matching-based algorithm when 10% access points are attacked.

Median error	Wi-Fi, RADAR	Wi-Fi, GR	ZigBee, RADAR	ZigBee, GR
DR	0.5882	0.7500	0.0500	0.8257
RR, cluster	0.7800	0.7708	6.7000	1.1000
RR, single	0.3000	0.6667	3.8000	1.1000
90th percentile	Wi-Fi, RADAR	Wi-Fi, GR	ZigBee, RADAR	ZigBee, GR
DR	0.4167	0.6304	0.3895	0.7598
RR, cluster	1.3600	1.2500	0.7015	0.8238
RR, single	1.2400	1.1466	0.7015	0.8238

GR, Gridded-RADAR; DR, degradation rate; RR, resistance rate.

In addition, as shown in Figure 10(c, d) for the ZigBee network, the localization performance when applying the attack-resistant method shows the similar improvement. For fingerprint matching-based algorithms, the RRs of *cluster* is larger than those of *single*, suggesting that using the results obtained from *K*-means clustering analysis is more effective in performing attack-resistant localization. Finally, these results consistently confirm that our attack-resistant scheme can mitigate the impact of the infrastructure attack under different number of compromised anchor points when applied to fingerprint matching-based localization algorithms.



(a) WiFi: RADAR (b) WiFi: Gridded-RADAR

(c) ZigBee: RADAR (d) ZigBee: Gridded-RADAR

Figure 10. Fingerprint matching-based method: localization error CDFs for networks Wi-Fi and ZigBee when 30% access points are attacked. CDF, cumulative distribution function.

Table IV. Degradation rate and resistance rate of fingerprint matching-based algorithm when 30% access points are attacked.

Median error	Wi-Fi, RADAR	Wi-Fi, GR	ZigBee, RADAR	ZigBee, GR
DR	1.5412	2.3594	0.4700	1.0550
RR, cluster	0.8168	0.8278	1.1170	0.7913
RR, single	0.6260	0.7616	0.8936	0.7913
90th percentile	Wi-Fi, RADAR	Wi-Fi, GR	ZigBee, RADAR	ZigBee, GR
DR	0.8333	1.3043	0.6017	0.8543
RR, cluster	1.1100	0.9833	0.7295	0.6267
RR, single	1.0000	0.9167	0.6957	0.7880

GR, Gridded-RADAR; DR, degradation rate; RR, resistance rate.

7.2.2. Bayesian networks.

7.2.2.1. Ten per cent of anchor points are compromised. Figure 11 presents the localization error CDF curves of the BN method for both the Wi-Fi and the ZigBee networks, when 10% of anchor points are attacked. The DR and RR are presented in Table V. From Figure 11, we found that the infrastructure attack reduces the localization accuracy significantly. Applying our attack-resistant

scheme can achieve qualitatively similar performance under the normal situation; the CDF curves when applying the attack-resistant method are mixed together with those under the normal situation. Furthermore, the results of *single* are comparable with those obtained from *cluster*.

Taking a closer look, Figure 11(a) shows the error CDFs of BN in the Wi-Fi network. We found that applying the attack-resistant method results in a significant improvement by reducing the large localization errors under the presence of an infrastructure attack. Specifically, the median error is improved from 15 to 11 ft under the infrastructure attack, the same as the 11 ft under the normal situation. And the 90th percentile error is improved from 33 to 21 ft, compared with 23 ft under the normal situation. As shown in Table V, the DR on the median error is about 0.34 under an attack, whereas the RR on the median error is around 1. In addition, the RR on the 90% percentile error is higher than 1.

Comparing the results of the ZigBee network to those of the Wi-Fi network in Figure 11, the error CDFs of attack-resistant method in the ZigBee network, as shown in Figure 11(b), have similar improvement. The RRs, as shown in Table V, are all around 1 for both the median error and the 90th percentile error. This indicates that the infrastructure attack cannot affect the localization results when applying our attack-resistant scheme.

7.2.2.2. Thirty per cent of anchor points are compromised. We further studied the localization performance of applying our attack-resistant method when 30% of anchor points are attacked. Figure 12 presents the localization error CDFs for both the Wi-Fi and ZigBee networks. The corresponding DR and RR are presented in Table VI. First, comparing the results when 30% anchor points are attacked to those when 10% anchor points are attacked, the DR increases rapidly, from 34% to 134% for the median error and from 45% to 110% for the 90th percentile error, indicating that the more anchor points are compromised, the more localization performance is impacted. Second, we observed that the error CDFs of attack-resistant scheme are mixed together with those under normal situations, which shows that the localization accuracy when using the attack-resistant method under an attack is comparable with that under the normal situation.

More specifically, Figure 12(a) shows the error CDFs of BN in the Wi-Fi network. From Figure 12(a), we observed that the median error is improved from 26 to around 11 ft under the infrastructure attack, and the 90th percentile error is improved from 48 to around 23 ft under the infrastructure attack. As shown in Table VI, the RRs on both the median error and the 90th percentile error are all around 1.

In addition, Figure 12(b) is the error CDFs in the ZigBee network. We observed comparable performance improvement of our attack-resistant method with that in the Wi-Fi network. In particular, the attack RR on the median error is around 0.9 (from 38 to around 21 ft), whereas it is around 0.95 on the 90th percentile error (from 68 to around 46 ft). These results consistently show that applying the attack-resistant method can eliminate the impact of the infrastructure attack under different numbers of attacked anchor points

Table V. Degradation rate and resistance rate of Bayesian networks when 10% access points are attacked.

Median error	Wi-Fi, BN	ZigBee, BN
DR	0.3364	0.3158
RR, cluster	0.8919	1.0000
RR, single	1.2162	0.9167
90th percentile	Wi-Fi, BN	ZigBee, BN
DR	0.4537	0.0907
RR, cluster	1.2718	1.2857
RR, single	1.0097	1.2857

BN, Bayesian network; DR, degradation rate; RR, resistance rate.

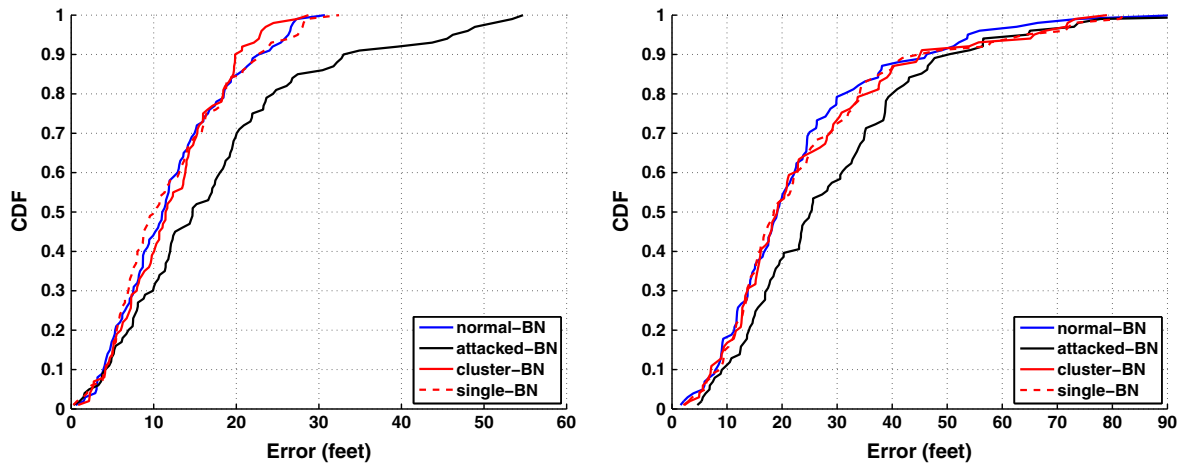


Figure 11. Bayesian networks: localization error CDFs for networks Wi-Fi and ZigBee when 10% access points are attacked. BN, Bayesian network; CDF, cumulative distribution function.

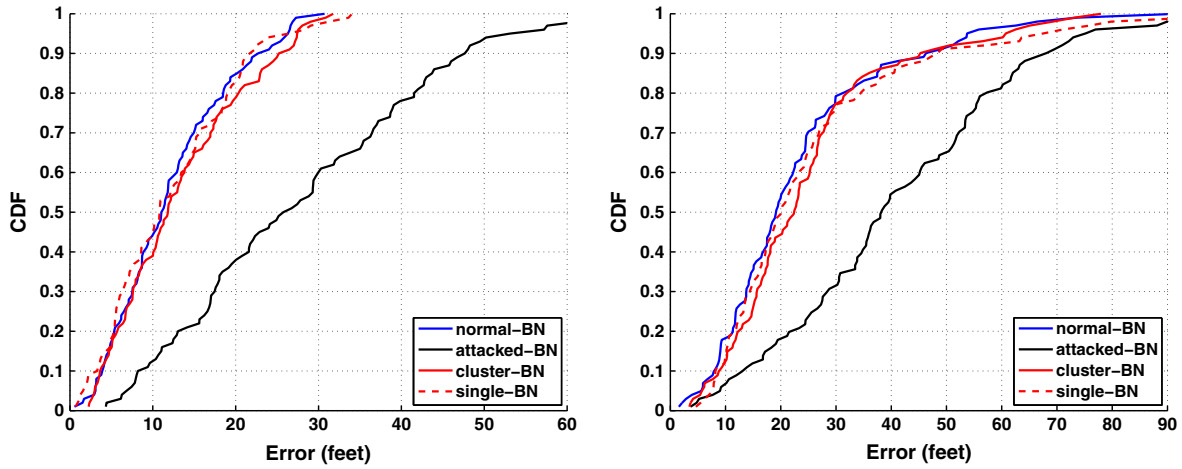


Figure 12. Bayesian networks: localization error CDFs for networks Wi-Fi and ZigBee when 30% access points are attacked. BN, Bayesian network; CDF, cumulative distribution function.

Table VI. Degradation rate and resistance rate of Bayesian networks when 30% access points are attacked.

Median error	Wi-Fi, BN	ZigBee, BN
DR	1.3455	1.0000
RR, cluster	0.9459	0.8211
RR, single	1.0135	0.9421
90th percentile	Wi-Fi, BN	ZigBee, BN
DR	1.1013	0.4708
RR, cluster	0.9000	1.0505
RR, single	1.0400	0.9220

BN, Bayesian network; DR, degradation rate; RR, resistance rate.

when using BNs algorithm to perform localization. And the improved localization accuracy is comparable with that under normal situations.

7.3. Comparing with existing study using LMS

7.3.1. Background

Researchers proposed robust statistical methods to achieve reliable localization results when less than half of the access points are compromised [9]. The basic idea is to use LMS as an improvement over LS for achieving robustness to physical attacks. The LMS approach has been applied to the lateration-based methods as well as the fingerprinting matching method.

In lateration-based methods, given the distance from a wireless device to the access points d_i together with the access points' location (x_i, y_i), the device location estimate $(\hat{x}, \hat{y})$ can be found by LS (i.e., using Equation (2)). In order to achieve an accurate localization estimation when there are physical attacks present, LMS can be applied instead of using LS. That is, $(\hat{x}, \hat{y})$ can be found such that

$$(\hat{x}, \hat{y}) = \arg \min_{(x_0, y_0)} \operatorname{med}_i \left[\sqrt{(x_i - x_0)^2 + (y_i - y_0)^2} - d_i \right]^2 \quad (9)$$

Turning to examine the fingerprinting matching method, we recall that the record in the radio map whose signal strength vector is the closest in the Euclidean sense to the observed RSS vector, that is, RSS fingerprint $(ss'_1, \ldots, ss'_N)$, is declared to correspond to the location of the targeting wireless device:

$$(\hat{x}, \hat{y}) = \arg \min_{(x_j, y_j)} \sqrt{\sum_{i=1}^{N} \left(ss'_i - ss_i(x_j, y_j) \right)^2} \quad (10)$$

By applying the LMS method, the estimated location of the wireless device can be represented by the following:

$$(\hat{x}, \hat{y}) = \arg \min_{(x_j, y_j)} \operatorname{med}_j \sqrt{\sum_{i=1}^{N} \left(ss'_i - ss_i(x_j, y_j) \right)^2} \quad (11)$$

In this section, we compare the performance of our attack-resistant scheme with LMS by applying it to both NLS and RADAR algorithms.

7.3.2. Performance comparison

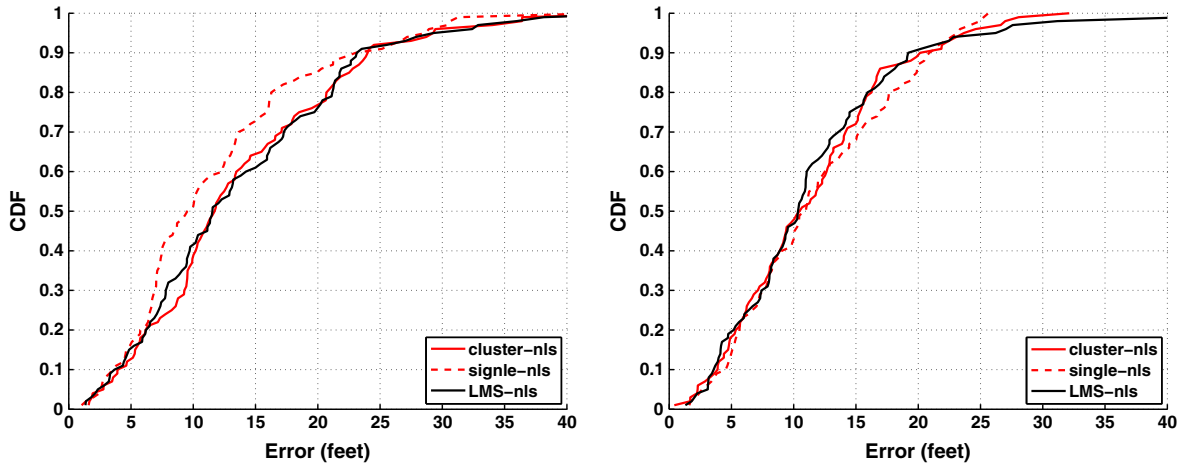
7.3.2.1. Non-linear least square algorithm. We plotted the localization error CDFs of our attack-resistant scheme and LMS for the NLS algorithm when 10% and 30% access points are attacked, respectively, in the Wi-Fi network. From Figure 13(a), we observed that the localization results of LMS is comparable with those of the cluster method, but they are slightly worse than those of the single method when 10% access points are attacked. From Figure 13(b), we found that these three CDF curves are very lose to each other, indicating that all these methods have comparable performance when there are 30% access

points. Thus, for the NLS algorithm, our approach achieves similar and slightly better performance than LMS.

7.3.2.2. RADAR algorithm. Figure 14 shows localization error CDFs comparison between our approach and LMS when applied to RADAR in the Wi-Fi network. From Figure 14(a), we found that the localization results of our proposed method outperform those of LMS clearly when 10% access points are attacked. Specifically, the median error of LMS-based method is 13.5 ft, whereas it is 12 ft for single radar and only 9.6 ft for cluster radar. In addition, LMS suffers a larger tail in CDF (e.g., 90% accuracy) than that of our proposed method, indicating larger maximum localization errors under LMS. Turning to examine the case when 30% access points are attacked, we found that our proposed approach consistently performs better than LMS. Therefore, we conclude that our approach has better performance than LMS when applied to RADAR algorithm. This shows that our proposed method is generic and can obtain more reliable localization results when applied to different localization algorithms.

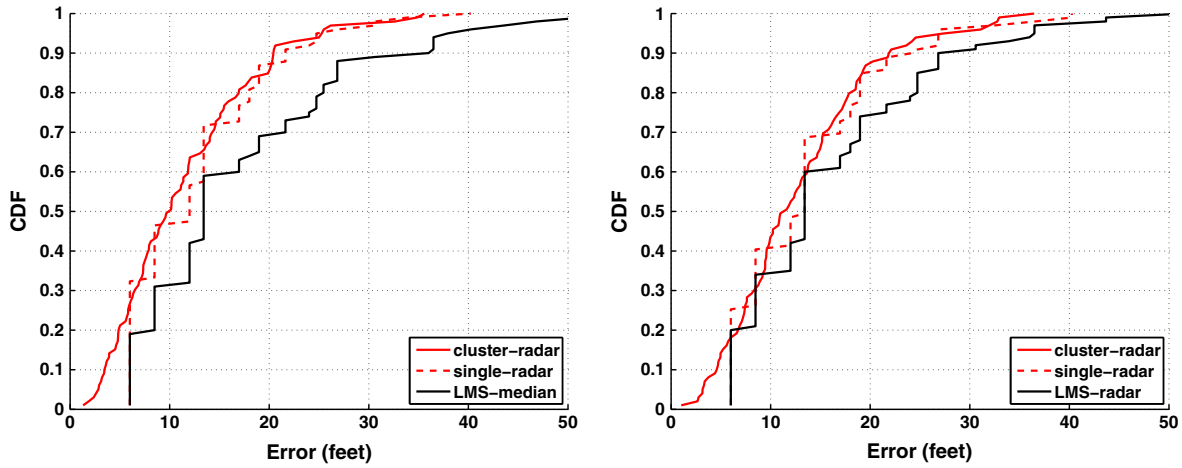
8. CONCLUSION

In this work, we showed that the localization infrastructure is vulnerable to physical attacks, and an infrastructure attack can significantly affect the localization performance. By



(a) 10% access points are attacked (b) 30% access points are attacked

Figure 13. Non-linear least square: localization error CDFs comparison between our approach and LMS in the Wi-Fi network when 10% and 30% access points are attacked, respectively. CDF, cumulative distribution function; NLS, non-linear least square; LMS, least median squares.



(a) 10% access points are attacked (b) 30% access points are attacked

Figure 14. RADAR: localization error CDFs comparison between our approach and LMS in the Wi-Fi network when 10% and 30% access points are attacked, respectively. CDF, cumulative distribution function; LMS, least median squares.

exploiting the characteristics of the geometric patterns returned by the location estimates, we developed an attack-resistant scheme that aims to integrate with localization algorithms and provide attack-resistant localization. Our attack-resistant scheme is built upon the geometric relationship of the localization results: the clustering effect of the localization estimates from the non-attacked anchor points versus the scattering effect of the localization estimates from the compromised anchor points. Our approach is not localization algorithm specific and is scalable to any localization methods.

To evaluate the effectiveness and scalability of our approach, we conducted experiments in the ORBIT test bed using an IEEE 802.11 (Wi-Fi) network as well as a real office building environment using an IEEE 802.15.4 (ZigBee) network. Our attack-resistant scheme is validated by applying it to three broad classes of localization algorithms, lateration-based, fingerprint matching algorithms, and BNs. In addition, we compared the performance of our approach to the existing study. Our experimental results showed that our approach can achieve similar or even better location accuracy when an infrastructure attack is present to that under normal situations, and thus provide strong evidence of achieving attack-resistant localization by using our proposed scheme.

ACKNOWLEDGMENTS

This work is supported in part by NSF grants CNS-0847211 and CNS-0954020.

REFERENCES

1. Akkaya K, Younis M. A survey on routing protocols for wireless sensor networks, *Ad Hoc Networks* 2005; **3**: 325–349.
2. Enge P, Misra P. *Global Positioning System: Signals, Measurements and Performance*. Ganga-Jamuna Press: Lincoln, MA, USA, 2001.
3. Priyantha N, Chakraborty A, Balakrishnan H. The cricket location-support system. In *Proceedings of the ACM International Conference on Mobile Computing and Networking (MobiCom)*, ACM: New York, NY, USA, August 2000; 32–43.
4. Rong P, Sichitiu M. Angle of arrival localization for wireless sensor networks. *Sensor and Ad Hoc Communications and Networks, 2006. SECON '06. 2006 3rd Annual IEEE Communications Society on*, Vol. 1, IEEE Computer Society: NY, New York, USA, September 2006; 374–382.
5. Bahl P, Padmanabhan VN. RADAR: an in-building RF-based user location and tracking system. In *Proceedings of the IEEE International Conference on Computer Communications (INFOCOM)*, IEEE Communication Society: New York, NY, USA, March 2000; 775–784.
6. Chen Y, Francisco J, Trappe W, Martin RP. A practical approach to landmark deployment for indoor localization. In *Proceedings of the Third Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON)*, IEEE Communication Society: New York, NY, USA, September 2006.
7. Kleisouris K, Chen Y, Yang J, Martin RP. The impact of using multiple antennas on wireless localization. In *Proceedings of the Fifth Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON)*, IEEE Communication Society: New York, NY, USA, June 2008.
8. Chen Y, Kleisouris K, Li X, Trappe W, Martin RP. A security and robustness performance analysis of localization algorithms to signal strength attacks. *ACM Transactions on Sensor Networks (ACM TOSN)* February 2009; **5**(1): 1–37.
9. Li Z, Trappe W, Zhang Y, Nath B. 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)*, IEEE Signal Processing Society: Piscataway, NY, USA, 2005; 91–98.
10. Liu D, Ning P, Du W. Attack-resistant location estimation in sensor networks. In *Proceedings of the Fourth International Symposium on Information Processing in Sensor Networks (IPSN 2005)*, IEEE Signal Processing Society: Piscataway, NY, USA, 2005; 99–106.
11. Want R, Hopper A, Falcao V, Gibbons J. The active badge location system, *ACM Transactions on Information Systems* 1992, January; **10**(1): 91–102.
12. Yang J, Chen Y. A theoretical analysis of wireless localization using RF-based fingerprint matching. In Proceedings of the Fourth International Workshop on System Management Techniques, Processes, and Services (SMTPS), April 2008.
13. Patwari N, Ash JN, Kyperountas S, Hero AO, Moses RL, Correal NS. Locating the nodes. IEEE Signal Processing Magazine, July 2005.
14. Elnahrawy E, Li X, Martin RP. The limits of localization using signal strength: A comparative study. In *Proceedings of the First IEEE International Conference on Sensor and Ad hoc Communications and Networks (SECON 2004)*, IEEE Communication Society: New York, NY, USA, October 2004; 406–414.
15. Shang Y, Ruml W, Zhang Y, Fromherz MPJ. Localization from mere connectivity, In *Proceedings of the Fourth ACM International Symposium on Mobile Ad-Hoc Networking and Computing (MobiHoc)*, ACM: New York, NY, USA, June 2003; 201–212.

16. He T, Huang C, Blum B, Stankovic JA, Abdelzaher T. Range-free localization schemes in large scale sensor networks. In *Proceedings of the Ninth Annual ACM International Conference on Mobile Computing and Networking (MobiCom'03)*, ACM: New York, NY, USA, 2003.
17. Niculescu D, Nath B. Ad hoc positioning system (APS). In *Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM)*, IEEE Communication Society: New York, NY, USA, 2001; 2926–2931.
18. Doherty L, Pister KSJ, ElGhaoui L. Convex position estimation in wireless sensor networks. In *Proceedings of the IEEE International Conference on Computer Communications (INFOCOM)*, IEEE Communication Society: New York, NY, USA, April 2001; 1655–1663.
19. Langendoen K, Reijers N. Distributed localization in wireless sensor networks: a quantitative comparison. *Computer Networks* 2003; **43**(4): 499–518.
20. Chintalapudi K, Dhariwal A, Govindan R, Sukhatme G. Ad hoc localization using ranging and sectoring. In *Proceedings of the IEEE International Conference on Computer Communications (INFOCOM)*, IEEE Communication Society: New York, NY, USA, March 2004.
21. Yang J, Chen Y. Indoor localization using improved RSS-Based lateration methods. In *IEEE Globecom 2009 Wireless Networking Symposium*, Honolulu, Hawaii, IEEE Communication Society: New York, NY, USA, November 2009.
22. Youssef M, Agrawal A, Shankar AU. WLAN location determination via clustering and probability distributions. In *Proceedings of the First IEEE International Conference on Pervasive Computing and Communications (PerCom)*, IEEE Communication Society: New York, NY, USA, March 2003; 143–150.
23. Roos T, Myllymaki P, Tirri H. A statistical modeling approach to location estimation, *IEEE Transactions on Mobile Computing* 2002, January–March; **1**(1): 59–69.
24. Sastry N, Shankar U, Wagner D. Secure verification of location claims. In *Proceedings of the ACM workshop on wireless security*, ACM: New York, NY, USA, 2003; 1–10.
25. Capkun S, Hubaux JP. Secure positioning of wireless devices with application to sensor networks. In *Proceedings of the IEEE International Conference on Computer Communications (INFOCOM)*, IEEE Communication Society: New York, NY, USA, 2005; 1917–1928.
26. Capkun S, Hubaux J. Securing localization with hidden and mobile base stations. In *Proceedings of the IEEE International Conference on Computer Communications (INFOCOM)*, IEEE Communication Society: New York, NY, USA, March 2006.
27. Jones K, Liu L. What where Wi: An analysis of millions of Wi-Fi access points. In *Portable Information Devices, 2007. PORTABLE07*. IEEE International Conference on May 2007.
28. Sarkar T, Ji Z, Kim K, Medouri A, Salazar-Palma M. A survey of various propagation models for mobile communication. *Antennas and Propagation Magazine, IEEE* 2003, June; **45**(3): 51–82.
29. Goldsmith A. *Wireless communications*. Cambridge University Press: New York, NY, 2005.
30. Hastie T, Tibshirani R, Friedman J. *The elements of statistical learning, data mining inference, and prediction*. Springer: New York, NY, 2001.
31. Madigan D, Elnahrawy E, Martin R, Ju W, Krishnan P, Krishnakumar AS. Bayesian indoor positioning systems. In *Proceedings of the IEEE International Conference on Computer Communications (INFOCOM)*, IEEE Communication Society: New York, NY, USA, March 2005; 324–331.