Robust Wireless Localization to Attacks on Access Points

Jie Yang*, Yingying Chen*, Victor B. Lawrence* and Venkataraman Swaminathan†
*Dept. of ECE, Stevens Institute of Technology
Castle Point on Hudson, Hoboken, NJ 07030
{jyang, yingying.chen, victor.lawrence}@stevens.edu
† Acoustics and Networked Sensors Division, US Army
RDECOM-ARDEC, Picatinny, NJ 07806
v.swaminathan@us.army.mil

***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 focus on achieving robust wireless localization when attacks are present on access points. We first investigate the effects of attacks on localization. We then derive an attack-resistant scheme that can be integrated with existing localization algorithms and are not algorithm-specific. Our attack-resistant scheme are based on K-means clustering analysis. We examined our approach using received signal strength (RSS) in widely used lateration-based algorithms. We validated our method in the ORBIT testbed with an IEEE 802.11 (Wi-Fi) network. Our experimental results demonstrate that our proposed approach can achieve comparable localization performance when under access-point attacks as compared to normal situations without attack.**

I. Introduction

The advancement of wireless technologies is resulting in a variety of emerging applications ranging from location-based services, to location-aware security techniques, and to location-centric military surveillance. Without accurate location information, many of these applications will not function properly, e.g., geographic routing [1]. Thus, the trustworthiness of location information of wireless nodes plays a critical role in the successful development of these applications.

Wireless localization techniques usually involve the measurement of various physical properties such as time of arrival (ToA), time difference of arrival (TDoA), angle of arrival (AoA), and received signal strength (RSS). 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 access points. However, the localization infrastructure is vulnerable to physical attacks, especially in hostile environments. For instance, RSS can be attenuated and amplified [2] and consequently the resulting location estimation is corrupted. In this paper, we focus on the physical attacks present on access points, i.e., a malicious attacker can compromise the access points and modify the measured RSS at access points or an attacker can directly attenuate or amplify the signals between the access points and the wireless device.

In previous work, [3] makes use of the data redundancy and robust statistical methods to achieve reliable localization in the presence of malicious attacks, whereas [4] proposes to detect attacks based on data inconsistency from received beacons and use 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 to other localization algorithms. In this paper, we propose an attack-resistent localization method, which can be integrated into existing localization algorithms. Our approach is not algorithm-specific and can be easily scalable to other localization algorithms. In particular, our method is based on the geometric relationship between the localization results from the benign access points and those from attacked access points. To achieve robust localization under attacks, we use cluster analysis to the localization results obtained from subsets of access points to separate correct localization results from corrupted localization results.

To evaluate the effectiveness of our approach, we conducted experiments using the ORBIT testbed, which simulated a large scale wireless network using IEEE 802.11 radios. We used the measured RSS from wireless devices to multiple access points to perform localization. We examined our method using widely used lateration-based algorithms including both nonlinear least squares and linear least squares methods. The experimental results show that our approach is attack-resistent and can provide accurate location estimation under the presence of attacks on access points.

The rest of the paper is organized as follows. Section II discusses exiting research in localization techniques and secure localization. We then propose our attack-resistant approach in Section III. Section IV presents the experimental methodology and evaluation of our approach. Finally, we conclude in Section V.

II. Related Work

There has been active work in exploring wireless localization. Based on localization infrastructure, [5] used infrared methods and [6] employed 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 [7]–[9] is an attractive approach because it can reuse the existing wireless infrastructure. Based on ranging methodology, range-based algorithms involve distance estimation to access points using the measurement of various physical properties [10], whereas range-free algorithms [11], [12] use coarser metrics to place bounds on candidate positions. Another method of classification describes the strategy used to map a node to a location. Lateration approaches [3], [13] use distances to access points, while angulation uses the angles from access points. Scene matching (or fingerprint matching) strategies [7] use a function that maps observed

radio properties to locations on a pre-constructed radio map or database.

There has been considerably less work on the problem of securing localization, which is used to ensure the trustworthiness of wireless localization. [14] proposed distance bounding protocols for verification of node positions. [15] proposed the Verifiable Multilateration mechanism which is based on the distance bounding protocols for secure position computation and verification. [16] uses hidden and mobile base stations to localize and verify location estimates.

The works that are closely related to ours are [3], [4], which tries to eliminate attack effects and still provide accurate localization. [3] makes use of the data redundancy and statistical methods to achieve reliable localization in the presence of attacks. [4] 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. However, these methods are mostly algorithm-specific and can not be easily scaled to other localization algorithms. Our approach is novel in that it is algorithm independent and can be integrated into the existing localization algorithms, and thus are highly scalable. Further, we validated our approach using a large-scale wireless network testbed.

III. Robust Localization

In this section, we introduce lateration based algorithms that are used to validate our approach. We then investigate the effects of the attacks on access points on localization. Next, we derive our attack-resistant scheme.

A. Localization Algorithm

Lateration approaches are widely used in wireless localization [3], [12], [13]. They estimate the position of the wireless device by estimating the distance to multiple access points and derive the location estimation based on least squares methods.

There are two main steps in least squares methods: ranging step and lateration step. The ranging step is used to estimate the distance d_i (i^{th} number of access points) between the wireless device and multiple access points. In this work, we use the measured RSS of the wireless device to fit the propagation parameters in the signal propagation model and derive the distance estimation from the signal-to-distance relationship:

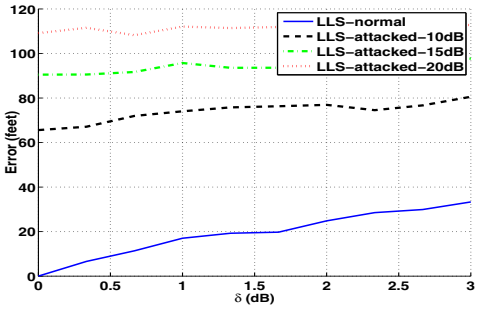
$$P(d)[dBm] = P(d_0)[dBm] - 10\gamma \log_{10}\left(\frac{d}{d_0}\right), \quad (1)$$

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 access point, and γ is the path loss exponent.

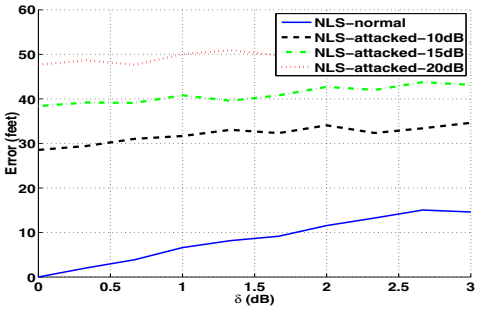
In the lateration step, we study both *Non-Linear Least Square (NLS)* and *Linear Least Square (LLS)* methods.

Non-Linear Least Square (NLS): Given the estimated distances d_i and known positions (x_i, y_i) of the access points, the position (x, y) of the wireless node can be estimated by finding $(\hat{x}, \hat{y})$ satisfying:

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



(a) LLS algorithms



(b) NLS algorithms

Fig. 1. Error analysis when using LLS and NLS algorithms.

where N is the number of access points that used to estimate the location of the wireless node. Non-linear least square 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 technique, such as gradient descent or Newton method, to get solution and thus requires significant computational complexity.

Linear Least Square (LLS): The LLS is an approximation of NLS solution. It linearize the NLS problem by introducing a constraint in the formulation and obtain a closed form solution of location estimation. Compared with NLS, LLS has less computational complexity. The location of the wireless node can be obtained by solving the form $\mathbf{Ax} = \mathbf{b}$ with:

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

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

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

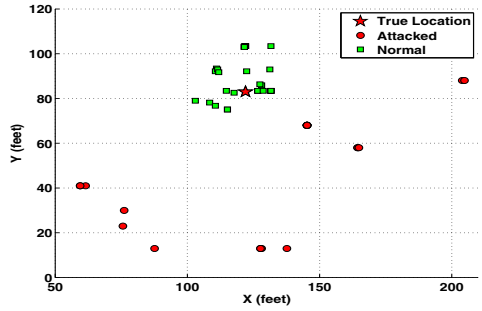


Fig. 2. Illustration of localization results of a wireless device under normal situations and with attacks on access points.

B. Error Analysis

Under normal situations, the measured RSS is determined by the distance between the access point and the wireless device. The RSS is affected by the random noise, environmental bias, and multipath effects. We assume the measurement error of RSS follow the normal distribution with zero mean and δ standard deviation. Whereas under attacks on access points, we assume the adversary will attack the access points by attenuating or amplifying the measured RSS. For example, the attacker can simply add 10dB or 20dB to the measured RSS at the access points.

To study the effects of attacks on localization versus the localization errors caused by RSS measurement errors, We conducted a simulation study by deploying three access points and one localizing node in a 200ft X 200ft square area. Under a normal situation, the standard deviation of the measurement error δ varies from 0dB to 3dB, whereas under an access point attack, we altered the measured RSS of one access point by 10dB, 15dB and 20dB respectively. Figure 1 presents the average localization errors for both NLS and LLS methods when one access point is attacked out of three access points. The simulation was run for 1000 times.

The solid line in Figure 1 presents the localization error under a normal situation, whereas the dotted lines represent the localization errors when the RSS is attacked by 10dB, 15dB and 20dB respectively. We found that the localization errors caused by access-point attacks are much larger than the localization errors caused by RSS measurement errors for both NLS and LLS algorithms. Particularly, in NLS the localization errors under attack are more than three times larger than under a normal situation, and in LLS, it is more than six times larger. This indicates that the localization results are close to the true location of the wireless node under normal situations. However, under access-point attacks, even if there is only one access point (out of three) is attacked, the localized positions are far from the true location of the wireless node.

We further studied the geometric relationship of multiple runs of localization results of a wireless node under normal situations and with access-point attacks. From Figure 2, we can clearly see that the localization results of a wireless node under the normal situation are clustered together and close to the true location of the device, whereas the localization results are scattered and far from the true location of the device when an attack is present on access points. Thus, based on the geometric relationship, the clustering versus the scattering effects, observed from the localization results, it is possible to distinguish the correct localization results under normal situations from the corrupted localization results caused by attacks on access points.

C. Attack-Resistant Scheme

We propose an attack-resistant scheme based on the observation that the localization results from non-attacked access points are clustered around the true location of the wireless node, while the localization results are scattered farther away from the true location of the wireless node when attacks are present on access points. The challenge is that the true location of the wireless node is unknown, and thus can not be used for comparison to remove the corrupted localization results.

We assume that not all of the access points are attacked by adversaries, that is, there exists a portion of the access points on which the measured RSS values are not corrupted. Suppose there are N access points in the area of interest and a portion of the access points are attacked by adversaries. To localize a wireless device, we choose any three of the N access points to perform location estimation. We can thus obtain multiple localization results from $\binom{N}{3}$ possible combinations. We denote these localization results as $(x_i, y_i), i \in 1, 2...\binom{N}{3}$. To obtain an accurate location estimation of the wireless device, instead of simply averaging over the multiple localization results, we measure the distance from each localization result to the rest of them. The distance for the i^{th} localization result is defined as:

$$D_i = \frac{1}{\binom{N}{3} - 1} \sum_{\substack{j=1,...\binom{N}{3} \\ j \neq i}} \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2}, \quad (5)$$

where $(x_i, y_i), i \in 1, 2...\binom{N}{3}$ are the localization results from $\binom{N}{3}$ possible combinations of N access points. D_i represents the geographic relationship between the i^{th} location estimation result to the rest of the localization results. If the i^{th} localization result is derived from attacked access points, D_i will be large, while D_i should be small if the localization result is estimated by using the non-attacked access points.

Further, rather than using a single threshold, which may be sensitive to the environment changes, we use K-means cluster analysis of D_i to separate the localization results obtained by using non-attacked access points from those calculated by attacked access points. The K-means algorithm is one of the most popular iterative descent clustering methods [17]. The squared Euclidean distance is chosen as the dissimilarity measure. If there are M measured D_i from localization results, 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:

$$\mathcal{I}_{min} = \sum_{j=1}^{K} \sum_{\mathbf{D_m} \in Q_j} \|\mathbf{D_m} - \mathbf{O_j}\|^2 \quad (6)$$

where $\mathbf{D_m}$ is a measured distance representing the m^{th} localization result and $\mathbf{O_j}$ is the geometric centroid of the

measured distance for Q_j. In our K-means cluster analysis, we set $K = 2$, one for the normal localization results and the other for the corrupted localization results. Thus, as a result of K-means analysis, the measured distances are partitioned into two clusters: $\{D_i\}, i = 1, 2, ...n$ in one cluster should be small and represent the localization results coming from non-attacked access points, whereas $\{D_i\}, i = n+1, n+2, ...M$ in another cluster should be large and represent the localization results from attacked access points.

After the localization results are partitioned into two clusters, we then use the averaged coordinates in the cluster with smaller $\{D_i\}$ to represent the final localization result of the wireless device. We call this result as the *cluster* result. Moreover, since 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.

IV. Experimental Evaluation

In this section, we first describe our experiment methodology using an IEEE 802.11 network. We then present the experimental results that validate our attack-resistant localization approach using lateration methods.

A. Experimental Methodology

In order to evaluate the effectiveness of our approach, we conducted experiments using the ORBIT testbed in the Wireless Information Network Laboratory (WINLAB) at Rutgers University. The ORBIT testbed simulates a large-scale wireless network using an IEEE 802.11 (Wi-Fi) network. The size of the ORBIT room is 60x60ft. Figure 3 shows the layout of the ORBIT room and the deployment of 10 access points, shown in red stars, in the 802.11(Wi-Fi) network. The small dots in the map are the locations used for testing. There are totally 100 locations in our experiments.

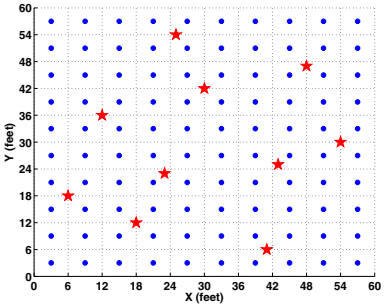
To evaluate the localization accuracy, we use the leave-one-out method, which means we choose one location as the testing node whereas the rest of the locations as the training data. Thus, the size of the training data used to estimate the parameters in the signal propagation model in lateration algorithms is 99 locations.

B. Experimental Results

We evaluate the performance of our attack-resistant localization method in terms of localization error which is the distance between the estimated position and the true position of the wireless device. Figures 4, 5 and 6 present the Cumulative Distribution Function (CDF) of the localization error of both NLS and LLS methods when the number of attacked access points varying from 10% to 20% and further to 30%, respectively. The resulted curves are presented in four categories: normal situations without attack, without using our attack-resistant method, using our attack-resistant method with the cluster result, and using our attack-resistant method with the single result.

10% access points are attacked: Figure 4 shows the localization results when 10% of access points are attacked. Particularly, in our experiments one of the ten access points is

(a) Wireless nodes lay out in ORBIT room



(b) Deployment of access points

Fig. 3. The lay out of Orbit room and the deployment of access points.

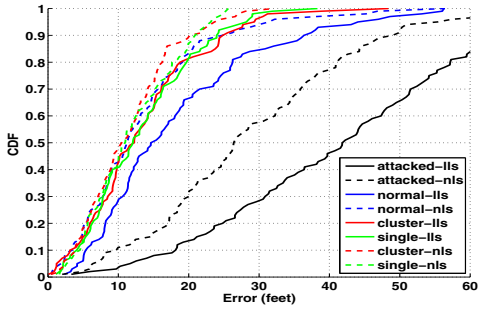


Fig. 4. Localization error CDFs when 10% access points are attacked.

attacked by 20dB. From Figure 4, the key observation is that the CDF curves of the localization error of our attack-resistant method are mixed with those under normal situations, and the *single* result is comparable to the *cluster* result. This indicates that our attack-resistant method achieves similar performance as under normal situations. In particular, for the NLS method, the median error can be improved from 26 feet to about 10.5 feet under an access-point attack, while it is 11 feet for a normal situation. For the LLS algorithm, the median error can be improved from 42 feet to 12 feet, compared to 15 feet under normal situations. Surprisingly, the localization results obtained from the attack-resistant method when attacks are present on access points outperform those under normal situations. This is because under normal situations sometimes the RSS measurements may contain outliers. The RSS outliers are similar to the corrupted RSS readings under attack. Therefore, the localization results can be affected by RSS outliers under normal situations, whereas under attack situations, our attack-resistant method has removed the effects of the corrupted RSS from the attacked access points and may achieve better localization accuracy.

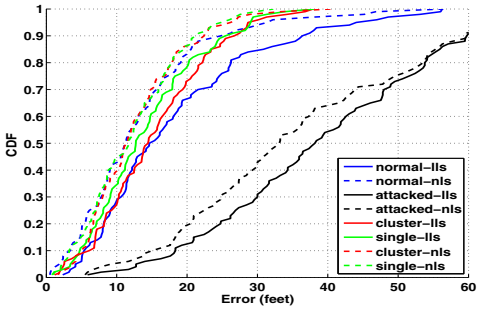


Fig. 5. Localization error CDFs when 20% access points are attacked.

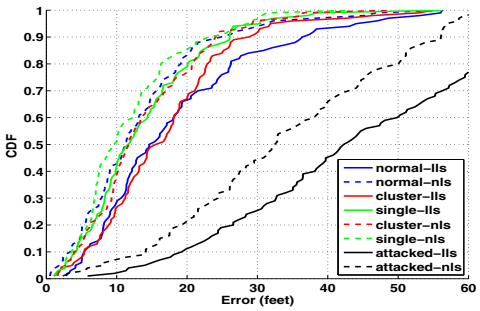


Fig. 6. Localization error CDFs when 30% access points are attacked.

20% access points are attacked: Figure 5 shows the localization results when two of ten access points are attacked by 20dB. Our observation in Figure 5 is similar to that of Figure 4. Our attack-resistant method can significantly improve the localization accuracy when attacks are present on access points. For both lateration methods, we can clearly see that the results of our method are better than those under normal situations. In particular, for NLS, the median error is improved from 32 feet to 11 feet under access-point attacks. Whereas the median error is improved from 38 feet to 13 feet for LLS, compared to 15 feet under normal situations.

30% access points are attacked: Figure 6 shows the localization results when three of ten access points are attacked by 20dB. We observed consistent behavior of our attack-resistant method: achieving the similar localization accuracy when there are access point attacks present to that of normal situations. Further, the *single* result slightly outperforms the *cluster* result. Again, our method can achieve better localization accuracy than those under normal situations. In particular, our attack-resistant method can improve the localization accuracy from 33 feet to 10 feet for NLS algorithm, whereas the median error can be improved from 43 feet to 13 feet for LLS algorithm.

V. Conclusion

In this work, we proposed a robust localization method to achieve accurate location estimation when attacks present on access points. We investigated the effects of access-point attacks on localization accuracy. Based on the clustering effects of the localization results from the non-attacked access points versus the scattering effects of the localization results from the attacked access points, we derived an attack-resistant scheme, which is localization algorithm independent and can be integrated with the existing algorithms.

To validate the effectiveness of our method, we conducted experiment in the ORBIT testbed using an IEEE 802.11 (Wi-Fi) network. We examined our robust localization scheme based on the widely used lateration-based algorithms, non-linear least squares and linear least squares methods. Our experimental results show that our method can achieve similar location accuracy when attacks are present on access points to that under normal situations, and thus provide strong evidence of the robustness of our approach under attacks.

Acknowledgments

This work is supported in part by NSF grant CNS-0847211 and by US Army Armament Research Development and Engineering Center Contract W15QKN-05-D-0011.

References

[1] K. Akkaya and M. Younis, "A survey on routing protocols for wireless sensor networks," *Ad Hoc Networks*, vol. 3, pp. 525–349.

[2] Y. Chen, K. Kleisouris, X. Li, W. Trappe, and R. P. Martin, "A security and robustness performance analysis of localization algorithms to signal strength attacks," *ACM Transactions on Sensor Networks (ACM TOSN)*, vol. 5, no. 1, February 2009.

[3] Z. Li, W. Trappe, Y. Zhang, and B. Nath, "Robust statistical methods for securing wireless localization in sensor networks," in *Proceedings of the Fourth International Symposium on Information Processing in Sensor Networks (IPSN 2005)*, 2005, pp. 91–98.

[4] D. Liu, P. Ning, and W. Du, "Attack-resistant location estimation in sensor networks," in *Proceedings of the Fourth International Symposium on Information Processing in Sensor Networks (IPSN 2005)*, 2005, pp. 99–106.

[5] R. Want, A. Hopper, V. Falcao, and J. Gibbons, "The active badge location system," *ACM Transactions on Information Systems*, vol. 10, no. 1, pp. 91–102, Jan. 1992.

[6] N. Priyantha, A. Chakraborty, and H. Balakrishnan, "The cricket location-support system," in *Proceedings of the ACM International Conference on Mobile Computing and Networking (MobiCom)*, Aug 2000, pp. 32–43.

[7] P. Bahl and V. N. Padmanabhan, "RADAR: An in-building RF-based user location and tracking system," in *Proceedings of the IEEE International Conference on Computer Communications (INFOCOM)*, March 2000, pp. 775–784.

[8] Y. Chen, J. Francisco, W. Trappe, and R. P. Martin, "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)*, September 2006.

[9] J. Yang and Y. Chen, "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.

[10] N. Patwari, J. N. Ash, S. Kyperountas, A. O. Hero, R. L. Moses, and N. S. Correal, "Locating the nodes," *IEEE Signal Processing Magazine*, July 2005.

[11] T. He, C. Huang, B. Blum, J. A. Stankovic, and T. Abdelzaher, "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)*, 2003.

[12] D. Niculescu and B. Nath, "Ad hoc positioning system (APS)," in *Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM)*, 2001, pp. 2926–2931.

[13] K. Langendoen and N. Reijers, "Distributed localization in wireless sensor networks: a quantitative comparison," *Comput. Networks*, vol. 43, no. 4, pp. 499–518, 2003.

[14] N. Sastry, U. Shankar, and D. Wagner, "Secure verification of location claims," in *Proceedings of the ACM workshop on wireless security*, 2003, pp. 1–10.

[15] S. Capkun and J. P. Hubaux, "Secure positioning of wireless devices with application to sensor networks," in *Proceedings of the IEEE International Conference on Computer Communications (INFOCOM)*, 2005, pp. 1917–1928.

[16] S. Capkun and J. Hubaux, "Securing localization with hidden and mobile base stations," in *Proceedings of the IEEE International Conference on Computer Communications (INFOCOM)*, March 2006.

[17] T. Hastie, R. Tibshirani, and J. Friedman, *The Elements of Statistical Learning, Data Mining Inference, and Prediction*. Springer, 2001.