

# TSCD: A Novel Secure Localization Approach for Wireless Sensor Networks

Honglong Chen<sup>1,2</sup>, Wei Lou<sup>2</sup>, Junchao Ma<sup>2</sup>, Zhi Wang<sup>1</sup>

<sup>1</sup>State Key Lab of Industrial Control Technology, Zhejiang University, Hangzhou, China

<sup>2</sup>Department of Computing, The Hong Kong Polytechnic University, Kowloon, Hong Kong  
{cshlchen,csweilou,csjma}@comp.polyu.edu.hk, wangzhi@iipc.zju.edu.cn

## Abstract

*Recent advances in wireless networking technologies, along with ubiquitous sensing and computing, have brought significant convenience for location service. The localization issue in wireless sensor networks under the non-adversarial scenario has already been well studied. However, most existing localization schemes cannot provide satisfied location service under the adversarial scenario. In this paper, we propose an attack-resistant localization scheme, called TSCD secure localization, to overcome the distance-consistent spoofing attack in wireless sensor networks. The main idea of the TSCD scheme is to firstly apply the temporal and spatial properties of locators to detect some attacked locators, and then utilize the consistent properties of the attacked locators and legitimate locators to find out other attacked locators. Simulation results demonstrate that the proposed scheme achieves better performance than existing approaches under the same network parameters.*

## 1. Introduction

Wireless sensor networks (WSNs) have increasingly drawn attentions of researchers in the areas of wireless communication, sensor technology, distributed systems and embedded computing. These sensor networks consist of a large number of low-cost, low-power, and multi-functional sensor nodes that communicate through wireless media. Various WSN applications have been proposed, e.g., military operations, environment monitoring, medical treatment, emergency rescue and smart home. For such applications, one of the fundamental requirements is the location awareness of the system. Therefore, the acquisition of sensors' location becomes an important issue since sensing results without

location information are probably inapplicable. Considering the nature of random deployment of most sensor networks, it is laborious, if not impossible, to predetermine the location of each sensor node before deployment. A common assumption in most localization schemes is the existence of enough special nodes, called *locators* or *beacons*, which can obtain their locations by GPS or from infrastructure. Locations of normal sensor nodes are then estimated by interacting with locators to obtain the distance and angle information. Once the location information of three non-collinear locators is available, the relative positions of the sensors can be transformed into physical positions.

Energy efficiency, accuracy and security account for the major metrics in localization. The former two metrics have already been investigated for nearly a decade and a large amount of achievements [2, 14, 5] have been reported. The security metric, however, has been addressed only in recent years. In practice, localization schemes for WSNs may work under the adversarial scenario where malicious attacks may exist. For example, a simple replay attack [16] may modify the distance measurement, leading to the malfunction of the localization schemes. Therefore, it is important to take the hostile environment into consideration.

In a hostile environment, a WSN may suffer certain attacks conducted by attackers. Generally, attackers in WSNs can be classified into two categories, *external* attacker and *internal* attacker [6]. External attackers can distort the network behavior without passing the system authentication, while internal attackers are authenticated ones, and thus, more dangerous to the system security. Most attacks in WSNs are coming from the aforementioned two types of attackers. For example, the wormhole attack [7] is conducted by two colluding external attackers, and the false position and distance dissemination attack [3] can be accomplished by an internal attacker.

In this paper, the distance-consistent spoofing attack in WSNs is investigated, based on which we propose an attack-resistant localization scheme, called TSCD (Temporal Spatial Consistent based Detection) secure localization. Simulation results demonstrate that the proposed scheme

---

This work is supported in part by grants HKPU A-PH12, Z09M, Z0DF, PolyU-5236/06E, PolyU 5232/07E, NSFC 60434030, NSFC 60773181, the National High-Tech Research and Development Plan of China under Grant No.2006AA01Z218, and Shanghai Science and Technology R&D Program under Grant No.07DZ15012.

achieves better performance than existing approaches under the same network settings.

The main contributions of this paper are summarized as follows: 1) We first summarize four secure properties of locators under the distance-consistent spoofing attack; 2) We then propose the TSCD secure localization scheme to yield good performance under the presence of the distance-consistent spoofing attack; 3) We analyze the effects of network parameters to the performance and compare our scheme with existing methods.

## 2. Related Work

There have been some recent achievements [16] on secure localization. Lazos et al. proposed a robust positioning system called ROPE [10] that provides a location verification mechanism to verify the location claims of the sensors before data collection. However, the requirement of the counter with nanoseconds precision makes it unsuitable in low cost sensor networks. DRBTS [15] is a distributed reputation-based beacon trust security protocol aimed at providing secure localization in sensor networks. Based on a quorum voting approach, DRBTS drives beacons to monitor each other and then enables them to decide which should be trusted. However it requires extra memory to store the message of NRT and TBN.

To provide secure location services, [13] introduces a method to detect malicious beacon signals, techniques to detect replayed beacon signals, identification of malicious beacons, avoidance of false detection and the revoking of malicious beacons. By clustering of benign location reference beacons, Wang et al. [17] proposes a resilient localization scheme that is computational efficiency. In [11], robust statistical methods are proposed, including triangulation and RF-based fingerprinting, to make localization attack-tolerant. SPINE [3] is a range-based positioning system that enables verifiable multilateration and verification of positions of mobile devices for secure computation in the presence of attackers. In [1], a secure localization scheme is presented to make the location estimation of the sensor secure, by transmission of nonces at different power levels from the beacon nodes. As all the computation is implemented on the base station, it will cause a significant bottleneck.

By localizing the sensor node with directional antennae equipped on locators, SeRLoc [8] is robust against wormhole attacks, sybil attacks and sensor compromise. On the basis of SeRLoc, HiRLoc [9] further utilizes antenna rotations and multiple transmit power levels to provide richer information for higher localization resolution. Liu et al. [12] proposed two secure localization schemes. The first one is attack-resistant Minimum Mean Square Estimation, which filters out malicious beacon signals by the

consistency check. The other one is voting-based location estimation. However, SeRLoc requires directional antennae which are complex in real deployment. The schemes in [12] would fail when the majority of location references are malicious colluding ones. The TSCD secure localization scheme, proposed in this paper, is able to conquer both the two limitations. It does not require any complex hardware, and works well even when the majority of locators are attacked. In addition, it consumes less time than that of [12] while obtaining better performance.

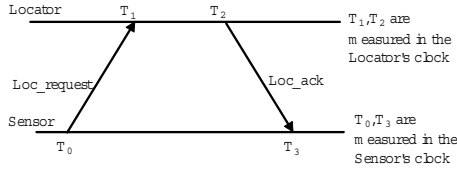
## 3. Problem Statement

In this section, the network model and related assumptions as well as the localization approach are given, followed by the attack model which we focus on.

**Network model** We assume that there are three types of nodes in a WSN, including locators, sensors, and attackers. The locators are fixed nodes with their locations known in advance. The sensors, while continuously moving around, estimate their own locations by measuring distances to neighboring locators. Each sensor and locator has its own unique identification. The attackers, known as adversarial nodes, intentionally disturb the localization process. The attackers may collude to spoof a sensor in the network. We assume that all the nodes in the network have the same transmission range of  $R$ , and there is no package loss for the in-range communications. However, the communication range between two colluded attackers is unlimited as they can communicate with each other using certain communication technique.

The locators are deployed independently with a density of  $\rho_l$ , and the probability that a sensor hears  $k$  locators can be obtained by the Poisson distribution:  $P(L_S = k) = \frac{(\pi R^2 \rho_l)^k}{k!} e^{-\pi R^2 \rho_l}$ . Each sensor is able to measure the distances to neighboring locators. The measurement error follows a Normal distribution  $N(\mu, \sigma^2)$ , where the mean  $\mu$  is 0 and the standard deviation  $\sigma$  is within a threshold. The attackers also measure the distances to neighboring locators and send the distance measurements to its colluder – another attacker – to replay the measurements to a sensor in another region, thus providing faulty measurements.

**Localization approach** As sensors may move around all the time, their locations are continuously changing. Whenever needed, a sensor can rely on the localization process to determine its current position. The localization process is as follows: The sensor maneuvers in the region, stops and broadcasts a requesting signal *Loc\_request* to its neighboring nodes whenever it needs localization. Upon receiving the *Loc\_request* signal, each locator, within the communication range of the sensor, replies a *Loc\_ack* signal to the sensor including the corresponding ID. The sensor estimates the distances to all the locators based on the *Loc\_ack*



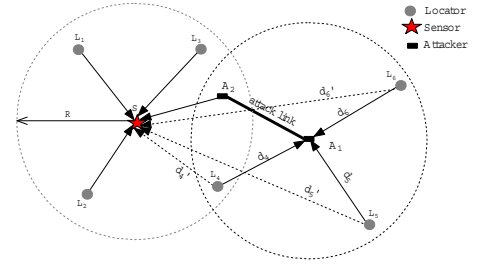
**Figure 1. Two-way message exchange between Sensor and Locator.**

signal (e.g. TDoA or RSSI).

The sensor also measures the response time of each locator during the above process. As the response time is highly affected by the random delay at the MAC layer, we make use of the scheme proposed in [4] to countervail this random delay. As shown in Fig. 1, when broadcasting the *Loc\_request* signal, the sensor records the local time as  $T_0$ . Every locator gets the local time as  $T_1$  by time-stamping the packet at the MAC layer (i.e. the time when the packet is received at the MAC layer) instead of time-stamping the packet at the application layer. Similarly, when responding the *Loc\_ack* packet, the locator registers the local time as  $T_2$  at the MAC layer, both  $T_1$  and  $T_2$  are included in the *Loc\_ack* packet. After receiving the *Loc\_ack*, the sensor gets its local time as  $T_3$ , and calculates the response time of the locator as  $(T_3 - T_0) - (T_2 - T_1)$ . Note that this response time only eliminates the random delay at the MAC layer of the locators.

Once enough distance measurements obtained, the sensor starts location estimation using the maximum likelihood estimation (MLE) method.

**Attack model** In this paper, we consider an adversarial environment where a pair of colluding attackers can launch a so-called *distance-consistent spoofing attack*. Unlike the wormhole attack [7] that two colluding attackers just relay the signals they received with no modification, the colluding attackers in the distance-consistent spoofing attack are able to revise the distance measurement information of the message to spoof a distance consistency check. The distance consistency check proposed in [12] assumes that all distance measurements from neighboring locators to a sensor are consistent, i.e., these distance measurements can converge to an identical location. Therefore, the distance consistency check can be used to detect a wormhole attack effectively because the malicious distance measurements generated by the wormhole attack will be inconsistent. However, for a distance-consistent spoofing attack, as the colluding attackers can deliberately manipulate the distance measurement messages sent from all the attacked locators to fake a virtual location, the distance consistency check scheme loses its efficacy. An example of the distance-consistent spoofing attack is shown in Fig. 2. As two



**Figure 2. The attack model in range-based localization.**

colluding attackers  $A_1$  and  $A_2$  can communicate with each other via an *attack link*, locators  $L_4$ ,  $L_5$  and  $L_6$  can, therefore, communicate with the sensor  $S$  through the attack link. For  $L_6$ , the *Loc\_request* signal sent from  $S$  travels through the attack link to reach  $L_6$ , and  $L_6$  responds a *Loc\_ack* signal. Attacker  $A_1$  measures the distance to  $L_6$  as  $d_6$  after receiving the *Loc\_ack* signal.  $A_1$  forwards the *Loc\_ack* signal with the distance measurement information to  $A_2$  through the attack link.  $A_2$  modifies the distance measurement information in the *Loc\_ack* signal to make it consistent with others. For example, if  $A_2$  modifies the distance measurement information in the signal sent from  $L_6$  to  $S$  to be  $d_6$ ,  $S$  will consider the distance to  $L_6$  as  $d_6$  instead of the actual distance  $d_6'$ . Similarly,  $S$  considers the distances to  $L_4$  and  $L_5$  as  $d_4$  and  $d_5$ , respectively, instead of the actual distances  $d_4'$  and  $d_5'$ .

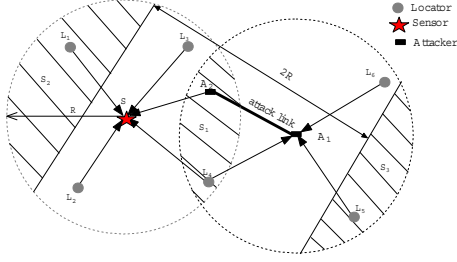
Although the attackers may be able to modify other contents of the messages, such as the IDs of the locators, or even fake messages for non-existent locators, to launch a much more complicated attack, this does not belong to the distance-consistent spoofing attack we discuss. In this paper, our proposed techniques only concentrate on solving the distance-consistent spoofing attack problem.

## 4. Secure Properties and Corresponding Detection Schemes

In this section, we summarize the characteristics of WSNs as four secure properties: temporal property of the locators, spatial property of the locators, consistent property of the legitimate locators and consistent property of the attacked locators. The detection schemes using corresponding properties are also provided. The detection schemes based on the temporal and spatial properties have been used in [8] while the detection scheme based on the consistent property of legitimate locators has been used in [12].

### 4.1. Secure properties in WSNs

WSNs have the four following secure properties:



**Figure 3. Attacked locators with temporal and spatial properties.**

**Property 1 (temporal property):** The sensor can receive at most one message from the same locator for each localization process. That is, the locator from which the sensor has received more than one signal is an attacked one.

**Property 2 (spatial property):** The sensor cannot receive messages from two different locators for each localization process if the distance between these two locators are larger than  $2R$ . That is, if the sensor has received messages from two locators between which the distance is larger than  $2R$ , one of these two locators is attacked.

**Property 3 (consistent property of legitimate locators):** We assume a set of locators is  $\mathbb{L} = \{(x_1, y_1, \delta_1), (x_2, y_2, \delta_2), \dots, (x_m, y_m, \delta_m)\}$ , where  $(x_i, y_i)$  is the 2-D location of locator  $L_i$  and  $\delta_i$  is the measured distance from the sensor to  $L_i$ . Based on  $\mathbb{L}$ , the estimated location of the sensor is  $(\tilde{x}_0, \tilde{y}_0)$ . The mean square error of the location estimation  $\delta^2 = \sum_{i=1}^m \frac{(\delta_i - \sqrt{(\tilde{x}_0 - x_i)^2 + (\tilde{y}_0 - y_i)^2})^2}{m}$ . The consistent property of legitimate locators means that the mean square error of the location estimation, generated from legitimate distance measurements, is lower than that containing malicious distance measurements.

**Property 4 (consistent property of attacked locators):** Under the distance-consistent spoofing attack, the distance measurements to the attacked locators are consistent. That is, the estimation location based only on the attacked locators will have a low mean square error.

#### 4.2. Detection schemes based on secure properties

The following schemes use the above secure properties to detect attacked locators:

**Detection scheme 1 based on Property 1:** As shown in Fig. 3, suppose an attacked locator is in the shading domain  $S_1$ , which is the common transmission area of sensor  $S$  and attacker  $A_1$ . When  $S$  broadcasts the *Loc\_request* signal,  $L_4$  can hear it twice, one directly from  $S$ , and the other from  $A_1$  which is replayed by  $A_2$  to  $A_1$  through the attack link.  $L_4$  will also reply the *Loc\_ack* signal through these two paths.

Therefore,  $S$  will receive more than one messages from  $L_4$ , based on which  $S$  can determine that  $L_4$  is attacked.

The sensor  $S$  can also differentiate the correct distance message from incorrect one based on the following scheme: As the localization approach only countervails the time delay at the MAC layer of the locators when measuring the response time of the message, if the message goes through the attack link, the MAC layer delay introduced by the two attackers still exists. Therefore, the response time of the revised *Loc\_ack* signal from  $L_4$  to  $S$ , which travels through the attack link, will be longer than that of the original *Loc\_ack* signal which travels from  $L_4$  to  $S$  directly.  $S$  will consider the *Loc\_ack* signal with a shorter response time from a locator to be correct while treating the other to be attacked.

**Detection scheme 2 based on Property 2:** When an attacked locator lies farther than  $2R$  away from one of the legitimate locators, the sensor can detect the attack based on the spatial property. As shown in Fig. 3,  $L_5$  is an attacked locator which lies farther than  $2R$  away from  $L_1$ .  $S$  can detect that one of the two locators is attacked. To differentiate the attacked locator from these two locators, observing that the MAC layer delay introduced by the attackers will increase the response time of the *Loc\_ack* signal from the attacked locator, the response time of the message from the attacked locator will be longer than the one from the legitimate locator. Therefore, by comparing the response time of the two locators,  $S$  can further determine that the locator with a longer response time is the attacked one, which is  $L_5$  in this case.

**Detection scheme 3 based on Property 3:** To detect the attacked locators, a predefined threshold  $\tau^2$  of the mean square error is selected in advance. The sensor estimates its location based on distance measurements to all the locators, and determines whether the mean square error based on the estimation result is lower than the threshold. If yes, it accepts the estimated result; otherwise it considers all subsets of the locators with one fewer locator, and chooses the subset with the least mean square error while eliminates the locator which is out of the subset. The sensor repeats the above process until a consistent estimation is obtained or there are only 3 remaining locators. Note that this scheme works only when majority of locators are legitimate.

**Detection scheme 4 based on Property 4:** If the sensor has already detected no less than two attacked locators, it can identify other attacked locators using the consistent property of attacked locators based on the detected ones. We assume the set of already detected locators is  $L_{ts}$  and the set of other remaining locators is  $L_r$ . The sensor first detects a set of attacked locators  $L_r$  by using the temporal and spatial properties. Then, the sensor repeats to select one locator from  $L_r$  each time and calculates the mean square error based on  $L_{ts}$  plus the selected locator. If the mean square error is lower than the threshold  $\tau^2$ , the selected locator is

considered as an attacked one; otherwise, the selected locator is considered as a legitimate one. The sensor repeats this until all locators in  $L_r$  are checked.

## 5. TSCD Secure Localization Scheme

The main idea of the TSCD scheme is to apply the temporal property, spatial property, consistent property of legitimate locators and consistent property of attacked locators to detect all attacked locators. The sensor first applies both temporal and spatial properties to detect attacked locators. If no less than two attacked locators are successfully detected, the sensor can identify other attacked locators based on their consistency. However, if the sensor detects less than 2 attacked locators, it can use the consistent property of legitimate locators to detect other attacked ones. After attacked locators are removed, the sensor can conduct the localization based on the remaining locators. The procedure of the TSCD scheme is shown as follows:

- 1: Broadcast the *Loc\_request* message
- 2: Wait for the *Loc\_ack* message, conduct the distance estimation and calculate the response time of each locator
- 3: Use the detection schemes 1 and 2 to detect attacked locators
- 4: **if** the detected attacked locators  $\geq 2$  **then**
- 5: Use the detection scheme 4 to detect other attacked locators
- 6: **else**
- 7: Use the detection scheme 3 to detect other attacked locators
- 8: **end if**
- 9: Conduct the MLE localization based on the remaining locators

In this algorithm, when the sensor requires the location estimation, it broadcasts the *Loc\_request* message to the network, and waits for the *Loc\_ack* messages from neighboring locators. If it receives *Loc\_ack* messages from the same locator more than once, it uses the detection scheme 1 to distinguish the correct distance measurement and the spoofing distance measurement. Meanwhile, when it receives *Loc\_ack* signals from neighboring locators, it checks whether there are two locators between which the distance is larger than  $2R$ . If it detects, it uses the detection scheme 2 to identify which is a legitimate locator and which is an attacked one. If the sensor has detected at least two attacked locators, it can continue using the detection scheme 4 to detect all the other locators, otherwise, the sensor uses the detection scheme 3 to eliminate other attacked locators. The sensor conducts the MLE localization based on the remaining locators after the detection.

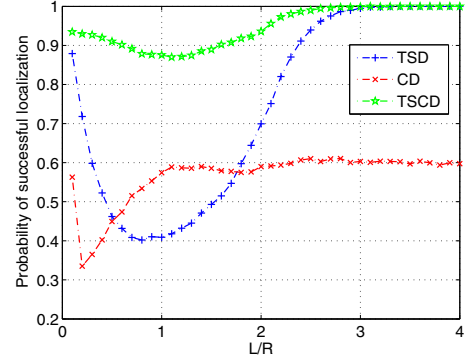


Figure 4. Performance of existing schemes and the TSCD scheme.

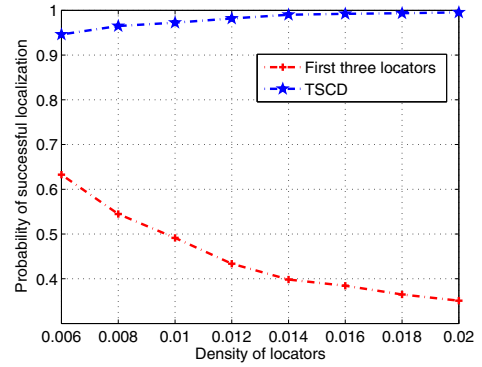


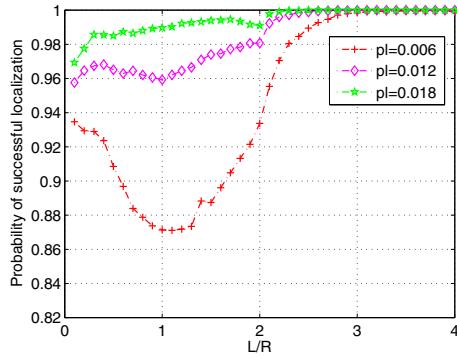
Figure 5. Performance of the first three locators scheme and the TSCD scheme.

## 6. Simulation Evaluation

In this section, we evaluate the performance of our proposed scheme in terms of the probability of successful localization. Let the distance between the estimated position without attack and the real position be  $d_1$ , and the distance between the estimated position with attack detection and the real position be  $d_2$ . The localization is considered successful if  $d_2 \leq 2d_1$ .

We adopt the following parameters in our simulation: the transmission range  $R = 15m$ ; the density of locators  $\rho_l = 0.006/m^2$ ; the standard deviation of the distance measurement error  $\sigma = 0.5$ ; the threshold of the mean square error used in the consistent property is 1. The label  $L/R$  of the  $x$  axis denotes the ratio of the distance between the sensor  $S$  and the locator  $A_1$  (shown in Fig. 2) to the transmission range.

Fig. 4 shows the performance comparison of the following schemes: the scheme using only temporal and spatial properties (TSD), the scheme using only consistency property of legitimate locators (CD) [12], and the TSCD scheme.



**Figure 6. The effect of  $\rho_l$  on the TSCD scheme.**

We can see that the TSCD scheme yields much better performance than the other two schemes.

As the malicious signals always come later than the legitimate ones, an intuitive approach can only take the first three signals from neighboring locators into account for determining the sensor's location. However, as the existence of distance measurement errors, the first three locators scheme will deteriorate the localization accuracy remarkably. The reason is that it takes no account of the remaining legitimate locators if there exist more than three legitimate locators. Fig. 5 shows the performance comparison of the first three locators scheme and the TSCD scheme at different densities of locators. The simulation result shows that the TSCD scheme outperforms the first three locators scheme approach dramatically throughout all densities of locators.

The effects of  $\rho_l$  on the performance of the TSCD are shown in Fig. 6. From the figure, we can find that as the  $\rho_l$  increases, better performance is obtained. This is mainly because the increase of  $\rho_l$  will enlarge the probability of detecting at least 2 attacked locators by temporal and spatial properties. However, when  $\rho_l$  is large enough, the improvement by increasing it will be inconspicuous.

## 7. Conclusion

In this paper, we analyze the distance-consistent spoofing attack in hostile wireless sensor networks and illuminate the drawbacks of the existing secure schemes. We summarize the properties of locators under the distance-consistent spoofing attack and propose the TSCD secure localization scheme. We also evaluate the performance of our proposed scheme and compare it with existing schemes by simulations. The simulation results demonstrate that our scheme outperforms the existing schemes.

## References

- [1] F. Anjum, S. Pandey, and P. Agrawal. Secure Localization in Sensor Networks using Transmission Range Variation. In *Proc. of the IEEE Int'l Conf. on Mobile Adhoc and Sensor Systems*, pages 195–203, 2005.
- [2] P. Bahl and V. N. Padmanabhan. RADAR: An In-building RF-based User Location and Tracking System. In *Proc. of IEEE Infocom*, pages 775–784, 2000.
- [3] S. Capkun and J. P. Hubaux. Secure Positioning of Wireless Devices with Application to Sensor Networks. In *Proc. of IEEE Infocom*, 2005.
- [4] S. Ganeriwal, R. Kumar, and M. B. Srivastava. Timing-sync Protocol for Sensor Networks. In *Proc. of the 1st int'l conf. on Embedded networked sensor systems*, pages 138–149, 2003.
- [5] T. He, C. Huang, B. M. Blum, J. A. Stankovic, and T. Abdelzaher. Range-free Localization Schemes for Large Scale Sensor Networks. In *Proc. of ACM MOBICOM*, pages 81–95, 2003.
- [6] Y. C. Hu, A. Perrig, and D. B. Johnson. Ariadne: A Secure On-demand Routing Protocol for Ad Hoc Networks. In *Proc. of ACM MOBICOM*, pages 12–23, 2002.
- [7] Y. C. Hu, A. Perrig, and D. B. Johnson. Packet Leashes: A Defense Against Wormhole Attacks in Wireless Networks. In *Proc. of IEEE Infocom*, pages 1976–1986, 2003.
- [8] L. Lazos and R. Poovendran. SeRLoc: Robust Localization for Wireless Sensor Networks. *ACM Transactions on Sensor Networks*, pages 73–100, 2005.
- [9] L. Lazos and R. Poovendran. HiRLoc: High-Resolution Robust Localization for Wireless Sensor Networks. *IEEE Journal on Selected Areas in Communications*, 24(2), 2006.
- [10] L. Lazos, R. Poovendran, and S. Capkun. ROPE: Robust Position Estimation in Wireless Sensor Networks. In *Proc. of IEEE IPSN*, pages 324–331, 2005.
- [11] Z. Li, W. Trappe, Y. Zhang, and B. Nath. Robust Statistical Methods for Securing Wireless Localization in Sensor Networks. In *Proc. of IEEE IPSN*, pages 91–98, 2005.
- [12] D. Liu, P. Ning, and W. Du. Attack-Resistant Location Estimation in Sensor Networks. In *Proc. of IEEE IPSN*, pages 99–106, 2005.
- [13] D. Liu, P. Ning, and W. Du. Detecting Malicious Beacon Nodes for Secure Localization Discovery in Wireless Sensor Networks. In *Proc. of IEEE ICDCS*, pages 609–619, 2005.
- [14] A. Savvides, C. Han, and M. Srivastava. Dynamic Fine-Grained Localization in Ad-hoc Networks of Sensors. In *Proc. of ACM MOBICOM*, pages 166–179, 2001.
- [15] A. Srinivasan, J. Teitelbaum, and J. Wu. DRBTS: Distributed Reputation-based Beacon Trust System. In *Proc. of the 2nd IEEE Int'l Symposium on Dependable, Autonomic and Secure Computing*, pages 277–283, 2006.
- [16] A. Srinivasan and J. Wu. A Survey on Secure Localization in Wireless Sensor Networks. *Encyclopedia of Wireless and Mobile Communications*, 2007.
- [17] C. Wang, A. Liu, and P. Ning. Cluster-Based Minimum Mean Square Estimation for Secure and Resilient Localization in Wireless Sensor Networks. In *Proc. of the Int'l Conf. on Wireless Algorithms, Systems and Applications*, pages 29–37, 2007.