# Secure Localization in Wireless Sensor Networks

You-Sheng Fan, Yu-Kai Hsiao[1] and Chueh Wang[2]
*Department of computer Science and Information Engineering, Tamkang University, Tamsui, Taipei, Taiwan 251, R.O.C*

[1] *shiaukae@gmail.com* ,[2] *ufjl1785@ms7.hinet.net*

***Abstract.*** *In wireless sensor networks, location information of sensor nodes is very important. However, in a self-configurable wireless sensor network, the randomly deployed sensor nodes cannot know their own locations a priori. Localization methods are needed to allow sensors to determine their locations. Global position system (GPS) is a widely used localization technique, but it is not suitable for sensor nodes, since sensor nodes are low-cost and hardware-limited devices. Therefore, many studies of localization method for wireless sensor networks have been proposed. Security issues are also very important in wireless sensor networks. Yet, studies have mostly assumed that they locate sensors in a trusted environment. These methods are in fact vulnerable to malicious attacks. In this paper, we propose a secure localization scheme, which is not only able to locate sensors with high accuracy, but also to fully solve the security problem. Our scheme is robust against several known attacks, such as Wormhole attack and Sybil attack. Since sensor nodes are low-cost and hardware-limited, one of our goals is to improve the performance of the entire network by reducing the overhead of sensor nodes, such as energy and storage.*

*Keywords: wireless sensor network, secure localization*

## 1. Introduction

Wireless sensor networks have been widely used in many applications, such as military, home, health, traffic, weather, industry, and commerce. A wireless sensor network is composed of a large number of sensor nodes with high density in the sensing field. Each sensor node would sense data from the environment, depending on different task requirements. The data that the sensors collect will be transmitted to the sink, and thereby to the network controller, which then collects the data and acquires useful information.

Many issues of wireless sensor networks have been discussed, such as localization, routing protocol, and key management. Localization is one of the most important issues. Location information is a major requisite for many mechanisms and applications in wireless sensor networks, including geographic routing, data forwarding, location service, object detection, target tracking, environmental monitoring, and rescue system. In these applications, the higher accuracy of location can always have the better performance and result. For example, in geographic routing based on an end-to-end distance, the higher accuracy of location can find the routing path as desired. However, in a self-configurable wireless sensor network, the randomly deployed sensors do not know their own locations. Therefore, a localization scheme is required for a wireless sensor network.

GPS (global position system)[17] has been widely used in localization; yet, it is too expensive for sensors, which are low-cost devices. To solve this problem, a number of localization schemes have been proposed. One of their objectives is to reduce the requirements of GPS, especially the cost of a localization scheme in sensor networks. Most of these localization studies assume that there is a special device called locator. Locators can know their own locations via some methods; for example, GPS locators can help sensors estimate their locations.

Localization methods can be classified into two types: range-based and range-free. Range-based methods determine a location by distance estimation, such as time of arrival (TOA), time difference of arrival, (TDOA) [12], [15], angle of arrival (AOA) [10], [11], and received signal strength indicator (RSSI) [1], [5]. On the other hand, range-free methods determine a location only by the information transmitted from locators. Range-based methods are accurate but expensive, due to their requirement of special hardware to estimate end-to-end distances. Range-free methods cannot work as precisely as range-based methods do, but they are cost-effective and therefore suitable for sensor networks.

As sensor networks can work in a hostile environment, such as a battlefield, security issues become very important. Localization scheme is mostly the first step to take when sensors are deployed, and it should be followed by consideration of the security issues in localization. Otherwise, when a localization scheme is under attack and the location information is modified, the working process will become incorrect.

However, most studies of localization have assumed a trusted network environment. Although a few of them have shown concerns with security problems [2], [7], [8], [9], they still cannot provide protections against some malicious attacks. We will discuss this part in section 2.

In this paper, we propose a secure localization scheme suitable for wireless sensor networks. Our proposed scheme can resist several known attacks, such as Wormhole attack [2], [6], [7], Sybil attack [3], [7] and Silence attack [4]. Even when under attack, our proposed scheme can still work with high accuracy. As we explain how our proposed scheme resists these malicious attacks, we will suggest solutions to the security problem . Moreover, due to constraints of sensor devices, we will also concern the energy efficiency and storage usage.

The remainder of this paper is organized as follows. In section 2, we review the related works on localization. In section 3, we propose a secure localization scheme. In section 4, we discuss and analyze our proposed scheme. In section 5, we simulate our scheme. Finally, we make a brief conclusion in section 6.

## 2. Related works

There have been many studies of localization. By different methods, localization schemes are classified into range-based [1],[5],[10],[11],[12],[15] and range-free [7],[14],[16].

In [7], Lazos and Poovenrdan proposed a range-free localization scheme called HiRLoc. They assumed that each locator is equipped with several transmitters, and that accuracy can be improved by transmitter rotation and communication range variation. They also discussed about some known attacks. However, their scheme is vulnerable to some attacks, such as Wormhole attack and Sybil attack. The attacker may be able to control the location computed by sensors.

In [2], Capkun and Hubaux proposed a range-based localization scheme called SPINE. They used timer with nanosecond of precision to estimate the end-to-end distance. Based on their proposed method called verifiable multilateration, a sensor within communication range of at least three locators can compute its location. The drawback of SPINE is that the performance depends on the number of locators and thus needs a large number of locators to accomplish high accuracy. In [9], Liu et al. proposed a range-free localization function. They used minimum mean square estimation (MMSE) to drop incorrect information and compute a location by the consistency of range estimates. However, if the attacker can compromise with more than half the range estimates, the scheme would not be able to find a correct result. In [8], Li et al. proposed localization scheme using least median square (LMS) to drop wrong messages from external attacks. However, their scheme cannot resist some malicious attacks, such as Wormhole attack.

### 3. Our proposed scheme

In this section, we propose a secure localization scheme. In our scheme, sensors can estimate their own locations with high accuracy, malicious attacks can be detected, and errors can be corrected. Moreover, we can also save energy by reducing the broadcast times of each sensor. Table 1 lists the notation we use in this paper.

Table 1. Notation

| *$ID_U$* | *U*'s Identity |
|---|---|
| $S_{Li}$ | $L_i$‘s secret value |
| H() | Hash function |
| SECTOR( ($X_1$,$Y_1$), ($X_2$,$Y_2$), ($X_3$,$Y_3$) ) | Convert coordinates ($X_1$,$Y_1$), ($X_2$,$Y_2$), ($X_3$,$Y_3$) into a coordinate set, which represents a sector |
| CIRCLE( ($X_1$,$Y_1$) ) | Convert coordinate ($X_1$,$Y_1$) into a coordinate set, which represents a circle |
| *INTERSECTION* | Coordinate set maintained by each sensor |
| *K* | Preload global shared key |
| $\{M\}_K$ | Encrypt *M* by key *K* |

### 3.1 Network model and assumption

In the sensor network we define two components: sensor node and locator. Sensors and locators are randomly deployed in the network. The density of sensors is far larger than that of locators. When sensors are deployed, they do not know their own locations, yet, locators can know their own locations by some methods, such as GPS. As long as locators transmit localization information in the network, sensors can estimate their locations by the information.

We assume that each sensor and each locator has a unique identity. All sensors and locators have a globally shared key *K*. Each locator has a secret value $S_{Li}$ and a hashing chain $H^1(S_{Li})\ldots H^m(S_{Li})$. All sensors will preload identities of all locators and corresponding $H^m(S_{Li})$. Locators transmit different hash value, depending on round time. Sensors can authenticate locators by checking the correctness of hash values. We further assume that both locators and sensors are static.

Locators are special devices equipped with several transmitters. The transmitter can rotate orientations and change communication range. Given that locators would rotate orientations and change communication ranges, we have to set some system parameters. We assume that each locator has *V* transmitters. There will be *D* different directions for each transmitter and *Z* different communication ranges for each direction. In other words, each transmitter will rotate *D*-1 times directions and change *Z*-1 times communication ranges. The rotation angle will be $2\pi/DV$. Therefore, each transmitter will transmit $Z\times D$ times messages, and each locator will broadcast $Z\times D\times V$ messages. We define that $m=Z\times D$ is the number of total rounds in the whole localization process.

We assume that each sensor receives at least one correct message from locators in the whole localization process. When sensors receive messages from neighboring sensors, more than half these messages will be correct.

### 3.2 Secure localization scheme

$T_1$ is the period of time in which sensors collect information from locators; $T_2$ is the period of time in which sensors collect information from neighboring sensors; and $T_3$ is the period of time in which sensors wait for neighboring sensors to begin broadcasting. The three periods of time should be predefined with the following steps:

Step 1: Each locator $L_i$ broadcasts: $\{(X_1,Y_1)\ ||\ (X_2,Y_2)\ ||\ (X_3,Y_3)\ ||\ \mathrm{H}^{m-j}(S_{Li})\ ||\ j\ ||\ ID_{Li}\}_K$, $j$ is the round number. $(X_1,Y_1)$ is location of the locator. $(X_2,Y_2)$ and $(X_3,Y_3)$ are the two points on the circle of the information coverage area.

Step 2: Each sensor $N_i$ detects anomalism for received information and compute *INTERSECTION*.

Step 2-1: For each message, the sensor checks if $\mathrm{H}^{\Delta j}(\mathrm{H}^{m-j}(S_{Li}))$ is equal to the stored hash value. If it is not, the message would be dropped. Otherwise, the message will be considered valid, and the sensor will store the correct new hash value.

Step 2-2: Each sensor checks messages. If there exist two locators $L_i$ and $L_j$ and the distance between them is farther than $R_{Li}+R_{Lj,}$ then there is anomalism. The sensor will execute Step 2-4.

Step 2-3: Each sensor generates *INTERSECTION*.

Step 2-3-1: For each message, the sensor computes SECTOR($(X_1,Y_1)$,$(X_2,Y_2)$,$(X_3,Y_3)$).

Step 2-3-2: The sensor stores $SECTOR_1$, $SECTOR_2$, …, $SECTOR_p$.

Step 2-3-3: The sensor checks if $SECTOR_1 \cap SECTOR_2 \cap\ldots\cap SECTOR_p$ is an empty set. If it is true, then there is anomalism. The sensor will execute Step 2-4.

Step 2-4: If the sensor detects anomalism or drops all messages, it will fall into sleep mode until it receives messages from neighboring sensors. We assume that all sensors will compute and store $SECTOR_1$, $SECTOR_2$, …, $SECTOR_p$.

Step 3: Each sensor $N_i$ computes the initial location.

Step 3-1: The sensor will compute $INTERSECTION = SECTOR_1 \cap SECTOR_2 \cap\ldots\cap SECTOR_p$.

Step 3-2: Assume that *INTERSECTION* is $(X_1,Y_1)$ ,…, $(X_n,Y_n)\}$. The sensor computes $(X,Y)$:
$X=\lfloor(X_1+\ldots+X_n)/n\rfloor$, $Y=\lfloor(Y_1+\ldots+Y_n)/n\rfloor$

Step 4:Each sensor broadcasts: $\{(X,Y)\ ||\ ID_{Ni}\}_K$

Step 5:Each sensor computes the final location

Step 5-1: For each message, computes CIRCLE($(X,Y)$).

Step 5-2: The sensor stores: $CIRCLE_1$, $CIRCLE_2$, ….

Step 5-3: The sensor computes *INTERSECTION* according to different situations:

Case 1: The sensor that passed the detection in Step 2 checks if $INTERSECTION \cap CIRCLE_c$, $1 \leqq c \leqq q$, is an empty set. If it is true, the sensor updates $INTERSECTION = INTERSECTION \cap CIRCLE_c$, or ignores the message.

Case 2: The sensor that fell into sleep mode in Step 2 will execute the following steps.

Step 5-3-1: The sensor computes $INTERSECTION = CIRCLE_1 \cap CIRCLE_2 \cap\ldots\cap CIRCLE_q$. If the result shows an empty set, the sensor will choose the intersection area with the highest number of neighboring sensors to be *INTERSECTION*.

Step 5-3-2: For each $SECTOR_w$, the sensor computes $INTERSECTION \cap SECTOR_W$, $1 \leqq w \leqq p$. If the result does not show an empty set, the sensor will update $INTERSECTION = INTERSECTION \cap SECTOR_W$; otherwise, the sensor will ignore the message.

Step 5-4: The sensor computes the final location. Assume *INTERSECTION* is $(X_1,Y_1)$ ,…, $(X_n,Y_n)\}$. The sensor computes $(X,Y)$:
$X=\lfloor(X_1+\ldots+X_n)/n\rfloor$, $Y=\lfloor(Y_1+\ldots+Y_n)/n\rfloor$

## 4. Analysis and discussions

In this section, we analyze our scheme in different aspects, such as security, communication overhead, and storage overhead.

### 4.1 Security analysis

Localization is usually the initial process. If the localization process is under attack and the location information is modified, the following applications using the location information would be affected. Indeed, secure localization is a requisite in a robust wireless sensor network.

We now introduce several known attacks on localization, such as Wormhole attack, Sybil attack and Silence attack. We will explain how our scheme can resist these malicious attacks.

**4.1.1 Wormhole attack** Wormhole attack generally means the attack that creates a high quality path called Wormhole so as to make messages in the network gather inside the Wormhole. In localization, Wormhole attack means the attack that transmits information far away [7]. In figure 1, the attacker transmits messages from $L_3$, $L_4$ and $L_5$, so the sensor $N_1$ would receive messages from $L_1$ to $L_5$. This will have different effects, depending on localization methods. Lazos and Poovedran [7] used a voting mechanism, so the Wormhole attack can totally control the location that the sensor computes.

In our scheme, Wormhole attack will be detected in Step 2-2 and Step 2-3. In Step 5, the sensor under Wormhole attack will use messages from neighboring sensors to compute the correct location. These messages from neighboring sensors are correct because only sensors that have passed the anomaly detection in Step 2 can broadcast messages. Therefore, the effect of Wormhole attack in our scheme is limited.

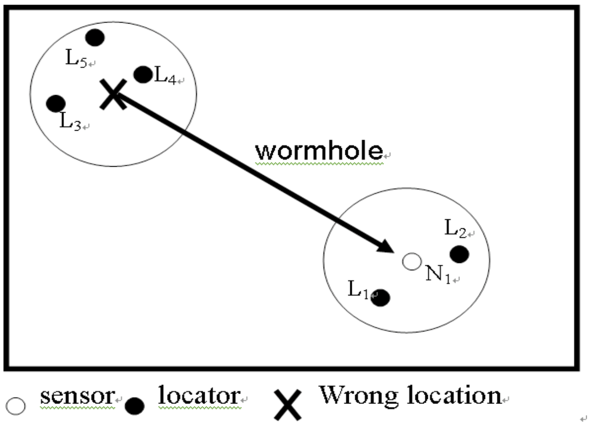

Figure 1. Wormhole attack

**4.1.2 Sybil attack** Sybil attack generally means the attacker that impersonates multiple identities. In localization, Sybil attack is the attacker that compromises K [7]. The attacker could collect valid hash values to impersonate several locators and then transmit false beacons to make sensors compute wrong locations.

Similar to Wormhole attack, in our scheme, the sensor under Sybil attack can use messages from neighboring sensors to compute correct locations. Consequently, the effect of Sybil attack in our scheme is limited.

**4.1.3 Silence attack** In Silence attack, the attacker compromises several locators and stop them from broadcasting any location information. This will decrease location accuracy because the average number of messages received by each sensor would decrease. Moreover, some sensors may receive no message and fail to compute any location—localization failure.

In our scheme, sensors that have passed anomaly detection in Step 2 will broadcast location information in Step 4. These messages can help improve location accuracy.

Table 2. Broadcasting time of each sensor

| | HiRLoc | Our scheme |
|---|---|---|
| Normal situation | 0 | 1 |
| Under attack | Received locator numbers | 1 |

**4.2 Communication overheads**

In table 2, we compare the numbers of broadcasting in our scheme with HiRLoc[7]. There are two cases in HiRLoc. If no attack is detected, the sensor will not broadcast. If any attack is detected, the number of sensor broadcasting will be determined by the number of locators received. The sensor in our scheme needs to broadcast at least once even if there is no attack. To assume that there is no attack at all in a real environment is not a practical thing to do. Judging from this, our scheme is more practical and efficient than HiRLoc.

Figure 2 shows the relation of locator number and average locator number received by a sensor. This simulation shows that a sensor would receive 2 to 15 locators when there are 5 to 45 locators in the network. This simulation does not consider the situation under attack. If there is any attack, the number of locators received by a sensor will increase, because the attacker needs to broadcast a large number of false beacons to confuse the sensor. Hence, our scheme is efficient when attacks exit and the number of locators is great.

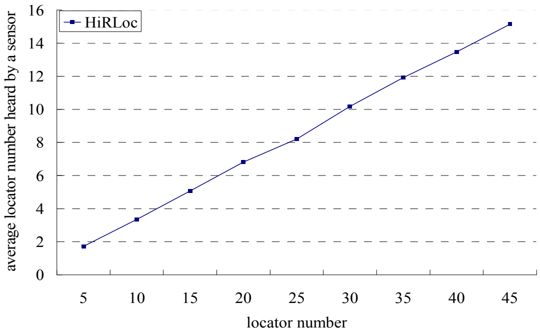

Figure 2. Locator numbers v.s. average received locator numbers

Table 3. Sensors storage

| HiRLoc | Our scheme |
|---|---|
| *1. K*<br>2. hash value list<br>*3.* $K_{SLi}$ × locator numbers | *1. K*<br>2. hash value list |

**4.3 Storage overheads**

In table 3, we compare our scheme with HiRLoc in terms of sensor storage. $K_{SLi}$ is the pair-wise key shared by each sensor-locator pair in HiRLoc. If there are 5,000 sensors and 40 locators in a network, there must be 400,000 pair-wise keys. In our scheme, we do not use pair-wise keys.

Table 4. Parameters

| | |
|---|---|
| Area | 100*100 $m^2$ |
| Sensor number | 5000 |
| Locator number | 5-45 |
| Sensor transmission range | 5 m |
| Locator transmission range | 40,20 m |
| Number of transmitter of each locator | 3 |
| Rotation time of each transmitter | 1 |
| Reduction time of transmission range of each transmitter | 1 |

**5. Simulations**

We use C++ program to simulate our scheme. Every result is the average of 100 times simulations. Table 4 shows the default parameters.

**5.1 average localization error**

Here, we define the average localization error as follows:

$$\frac{1}{|\mathrm{N}|}\sum_{k=1}^{|N|}|E_{Nk}-A_{Nk}|$$

$|N|$ is the number of sensors in the network. $E_{Nk}$ is the estimated location computed by the sensor $N_k$. $A_{Nk}$ is the actual location of the sensor $N_k$. The equation represents the average distance error of all sensors.

**5.1.1 Average localization errors v.s. locator numbers** Figure 3 shows the relation of locator number and the average localization error. In the simulation, the greater number of locators leads to lower average localization error. This is because *INTERSECTION* would become smaller if the number of messages received by a sensor is increasing. If *INTERSECTION* is smaller, the localization will usually be lower. Owing to its random deployment, there would be some special cases. Yet, the greater number of locators generally brings the lower error.

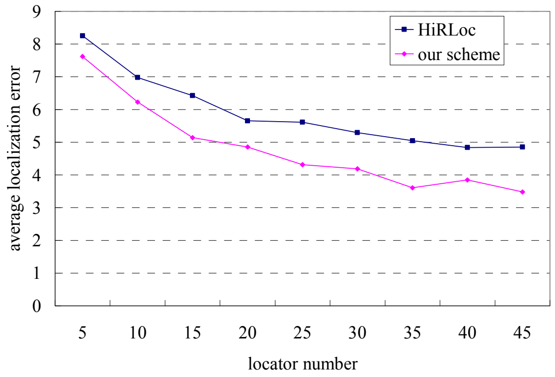

Figure 3. Locator number v.s. average localization error

The simulation shows that our scheme has lower error when compared with HiRLoc, no matter how many locators there are. Moreover, compared with HiRLoc, our scheme can achieve lower error even with a smaller number of locators. The error made by 20 locators in our scheme is almost the same with the error made by 40 locators in HiRLoc. This shows that, when the error is about 5 m, our scheme compares much favorably with HiRLoc, for it is efficient enough to cut down the number of locators at a 50% rate. Since locators are special devices with high cost, our scheme can reduce the cost of a network as it reduce the number of locators.

**5.1.2 Average localization error v.s. average received locator number** Figure 4 shows the relation of localization error and average locator number received by a sensor. In this simulation, there are 45 locators, and the communication range of the sensor is 5m.

The simulation result shows that the greater number of locators received by a sensor will lead to lower error. Almost all the results show that our scheme has lower error when compared with HiRLoc. Moreover, the error that sensors receive from 10 locators in our scheme is almost the same with the error that sensors receivefrom 27 locators in HiRLoc. Hence, the requirement of locators in our scheme is far lower than HiRLoc.

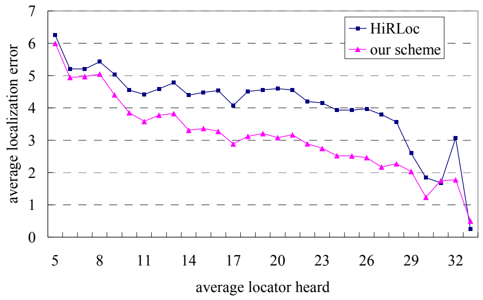

Figure 4. Received locator number v.s. average localization error

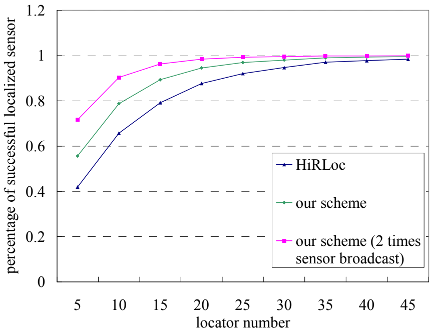

Figure 5. Locator number v.s. percentage of successful localization (200×200 m$^2$)

## 5.2 Percentage of successful localization

Although almost all localization schemes assume that there will be at least one message received by a sensor in whole process, in a real environment, randomly deployed locators and sensors may hamper some sensors from receiving any message from locators in the whole process. In our scheme, sensors that have received no messages from locators can utilize the messages from neighboring sensors. Because the density of sensors is much higher than that of locators, using broadcasting between sensors can lead to high percentage of successful localization. Our scheme has better performance especially when the network grows and the density of locators decreases,

Figure 5 shows the percentage of successful localization when the network field is 200×200 m$^2$. The simulation result shows that our scheme can locate almost all sensors when there are 30 locators in the network. In contrast, HiRLoc needs 40 locators to locate almost all sensors. If we allow sensors to broadcast twice (i.e. to execute Step 4 and Step 5 twice), our scheme will be able to locate all sensors when there are only 20 locators in the network. This simulation shows that, compared with HiRLoc, our scheme can locate more sensors even with fewer locators and in a larger network field.

## 6. Conclusions

We propose a secure localization scheme in wireless sensor networks. In our scheme, sensors can estimate their locations with high accuracy. Furthermore, our scheme can resist several known attacks, such as Wormhole attack, Sybil attack, and Silence attack. Simulations show that the requirement of locators is very low in our scheme, which means that we can reduce the cost required by the whole network. Moreover, in our scheme, each sensor broadcasts only once, whether under attack or not, which means that our scheme is efficient in terms of energy.

## Acknowledgements

This work was partially supported by the iCAST project sponsored by the National Science Council, Taiwan, under the grants no. NSC97-2745-P-001-001.

## References

[1] Paramvir Bahl; Venkata N. Padmanabhan, "RADER: an in-building RF-based user location and tracking system," *Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies*, vol.2, pp. 775-84

[2] Srdjan Capkun and Jean-Pierre Hubaux, "Secure Positioning in Wireless Sensor Networks," *IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS*, VOL. 24, NO. 2, pp. 221-232,FERURARY 2006.

[3] John Douceur, "The Sybil Attack,"In: *1st International Workshop on Peer-to-Peer System (IPTPS'02).* Springer, 2002.

[4] Wenlian Du, Lei Fang, Ning Peng, "LAD: localization anomaly detection for wireless sensor networks," *Journal of Parallel and Distributed Computing (JPDC).* Volume 66, Issue 7, pp. 874-886, July 2006.

[5] Jeffrey Hightower, Roy Want, and Gaetano Borriello, "SpotON: An indoor 3D location sensing technology based on RF signal strength," UW CSE 00-02-02, *University of Washington, Department of Computer Science and Engineering*, Seattle, WA, Feb. 2000.

[6] Yih-Chun Hu, Adrian Perrig, and David Johnson, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks," *Proceedings of IEEE INFOCOM*, San Francisco, CA, USA, pp. 1976-1986, April 2003.

[7] Loukas Lazos and Radha Poovendran, "HiRLoc: High-Resolution Localization for Wireless Sensor Networks," *IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS*, VOL. 24, NO. 2, pp. 233-246, FERURARY 2006.

[8] Zang Li, Wade Trappe, Yanyong Zhang, and Badri Nath, "Robust statistical methods for securing wireless localization in sensor networks," *Proceedings of The Fourth International Symposium on Information Processing in sensor networks (IPSN '05)*, pp. 91-98,April 2005.

[9] Donggang Liu, Peng Ning, and Wenliang Kevin Du, "Attack-resistant location estimation in sensor networks," *Proceedings of The Fourth International Symposium on Information Processing in sensor networks (IPSN '05)*, pp. 99-106 ,April 2005.

[10] Asis Nasipuri, Kai L, "A directionality based location discovery scheme for wireless sensor networks," *WSNA*, pp. 105-111, *2002*.

[11] Dragoş Niculescu and Badri Nath, "Ad Hoc Positioning System (APS) using AoA," *Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies*, Vol. 3, pp. 1734-1743,2003.

[12] Nissanka B. Priyantha, Anit Chakraborty, and Hari Balakrishnan, "The Cricket location-support system," *Proceedings of the 6th annual international conference on Mobile computing and networking*, pp. 32-43, 2000,.

[13] Naveen Sastry, Umesh Shankar, and David Wagner, "Secure verification of Location Claims," *ACM Workshop on Wireless Security (WiSe 2003)*, pp. 1-10,September 19, 2003.

[14] Kuo-Feng Ssu, Chia-Ho Ou, and Hewifin Christine Jiau, "Localization With Mobile Anchor Points in Wireless Sensor Networks," *IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY*, VOL. 54, NO. 3, pp. 1187-1197, MAY 2005.

[15] Ariel Tamches, Barton P. Miller, "Dynamic fine-grained localization in Ad-Hoc networks of sensors," *Proceedings of the 7th annual international conference on Mobile computing and networking*, pp. 166-179,2001.

[16] Sheng-Shih Wang, Kuei-Ping Shish, and Chih-Yung Chang, "Distributed direction-based localization in wireless sensor networks," *Computer Communications*, Volume 30, Issue 6, pp.1424-1439, MARCH 2007.

[17] Bernhard Hofmann-Wellenhof, Herbert Lichtenegger, James Collins,."Global Positioning System: Theory and Practicr," *4th ed.New York: Springer-Verlag*, 1997.

[18] Yan-Chao Zhang, Wei Liu, Yu-Guang Fang, and Da-Peng Wu, "Secure Localization and Authentication in Ultra-wideband Sensor Networks," *IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS*, VOL. 24, NO. 4, pp. 829-835 , APRIL 2006.