Research Journal of Recent Sciences ____ ISSN 2277-2502
Vol. **3(11),** 103-109, November **(2014)** *Res.J.Recent Sci.*

A Survey on Secure Range Based Localization Algorithms in Wireless Sensor Networks

Ahmed Abdulqader Hussein AL-Qaysi[1,2] and Tharek A. Rahman[1]
[1]Faculty of Electrical Engineering, University Teknologi Malaysia, UTM Skudai, Johor 81310, MALAYSIA
[2]University of Technology, Baghdad, IRAQ

Available online at: www.isca.in, www.isca.me
Received 2nd December 2013, revised 29th March 2014, accepted 27th July 2014

Abstract

Localization refers to locating the position or area in which the sensor or object to be tracked. Based on the localization, many applications are emerging in the sensor network. Localization schemes are broadly divided into Range based and Range free. As localization is becoming popular, many attacks on the localization process are also on a rise. These attacks confuse the localization process and cause location estimation errors. The Range Based and Range free localization methods are available for obtaining the location of the sensor nodes. One of main challenge in localization is that the process can be made erroneous by launching various attacks. In this paper, we analyze the attacks on the Range Based methods and survey the current work on attack detection and resolution.

Keywords: Secure localization, wireless sensor network, localization attacks, range based methods.

Introduction

It is a reality that much research activities have been developed into wireless sensor networks because to its importance. Sensors with the following performance indices such as inexpensive, low power consumption, small size, and multipurpose and small coverage area are direct function of the advancement in electronics and communications.

Homes, cities and general environmental control have been achievable to the wireless networking of several sensors regarded as been smart and affordable. In military applications the broad spectrum of wireless sensors is deployed for the purpose of surveillance, exploration and other applications.

Information obtained via the monitoring of environmental events such as agricultural precision, bush burnings , inspection and monitoring of water are not so significant without the knowledge od the data source location. In addition, the ability to estimate a location enhances the following: monitoring of the road traffic, health care, intrusion, inventory management, exploration and surveillance.

In enterprise domain, facilities have to be delivered to places on need. Accurate position of sensor is important for the success of these applications.

To estimate the location of a sensor which is not known before a localization algorithms utilize information such as distance and absolute positions of other sensors.

Anchors are sensors whose both location and information are known and can be gotten through the use of global positioning system (Gps) or by placing anchors at points whose coordinates are known (Sensors that are otherwise are referred to as non-anchor nodes).

Anchors determine the location of sensor networks in global coordinate system and define the local coordinate system which sensors referred to as location coordinate system suffices.

The location of sensors remains unknown by most of the sensors themselves; this is as a result of of the limitations created by cost, energy consumption, sensor size and deployment and the environment for implementation. Sensor network algorithm estimates the coordinates of non-anchor nodes.

Recently many secure localization systems have been to established to secure the positioning of WSNs. Most of these techniques obtain the security using cryptography by blocking and detecting the information, performing statistical decisions or filtering this information as a procedure for position computations [1]. Also attackers can launch signal strength attacks on the range based methods. By attacking they introduce errors in the localization process[2].

In this paper, we explore the range based localization methods and the attacks on those methods. We explore the current security mechanisms in the range based methods against attackers. The aim of this paper is identify the areas on further research on the secure range based localization methods.

Range based localization: Localization can be defined as the position estimation for whole or some sensor nodes in the network, specified the measurements of each locative connection among the sensors. At present, the accurate location is the meaning by any way of the position allocation. However, the measurements on locative connection as it may be on the closeness the angle or distance among sensor nodes[3].

Localization methods are organized into two kinds Range based and Range free localization methods. Range based methods are based on RSSI, TOA, TDOA, AOA of the signal from the sensors. Range free mechanism are based on certain anchor nodes with locations known communicate beacons to other nodes and determine their location relative to the anchor node[4]. The taxonomy of range based localization methods is shown in figure-1

Wide set of algorithms are commonly using the signal strength in their location estimation getting the advantages its physical properties? Most approaches like fingerprinting and multilateration use it as well. The reuse of existing wireless infrastructure is the main advantage of applying the RSS algorithm, in addition this feature shows enormous saving in costs over prevailing localization particular hardware[5].

RADAR[6] is a point based RSS scheme, which is a duplicated base stations are distributed to provide interfere coverage area. Therefore the know position host mobile broadcasting beacons periodically during the setting up. So that the measurement of a signal strength readings at a fixed landmark has been set. A radio map can be provided by collecting the readings of the signal strength for different transmitter locations of each landmark. After training the measuring of the wireless device's RSS at each landmarks has been applies to determine the localization and the make a comparison of the RSS vector values to the radio map. The vector of the signal strength record in such a radio map has been impending in the eucidean sense to the noted signal strength vector is announced to match the transmitter location[7]. Variation of this scheme, such as Average RADAR which provides the average of the nearest two fingerprints. Moreover Gridded RADAR that applies a set of additional fingerprints by using the basis of the interpolated map grid (IMG) to perform the location estimation[7].

As a rule various technologies have been utilized to obtain the estimation of the node location such as Time of Arrival (TOA), Time Difference of Arrival (TDOA) and Angle of Arrival (AOA) required additional hardware which is too expensive to be implemented in a large scale sensor networks[8]. The localization system of (TOA) is based on usage of GPS; actually it has been required expensive and extra electronic devices which consume high energy to obtain the synchronization of satellite's clock precisely. The limitations in hardware for implemented such a sensor networks should be considered with energy constraints. Similar to this algorithm (TDOA) and (AOA) schemes extensive hardware and it is not suitable for low power sensor networks. In addition (TDOA) applies ultrasound signal in the transmission even it can be propagated just a few feets only, and (AOA) algorithm needs a special antenna design[9].

The simulations and environmental controlled labratories show that more efficiency for the solutions to estimate the node location based on Recieved Signal Stregnth Indicator (RSSI) scheme.Since the measuring capability of recieved signal stregnth is the important feature of most wireless devices[2] However, fading and propagating pattern models remenant dubitable requiring a new solutions for localization that is being freelance of these suppositions [10].

Attacks Affecting Localization: Angle and Distance estimation Attacks: The range based schemes such as recieved signal strength , time of arrival and hop counts are the main techniques of the sensor location estimation . In the signal strength case, the sending packets of a sensor nodes affected by the attackers through increasing or decreasing the received power with reference to the real power transmission, so that it makes the estimation of the sensor position to be near or far away from the exact location. In the time of arrival case, the delaying of the packets transmission time for both TOA and TDOA techniques has been affected on the system localization accuracy.

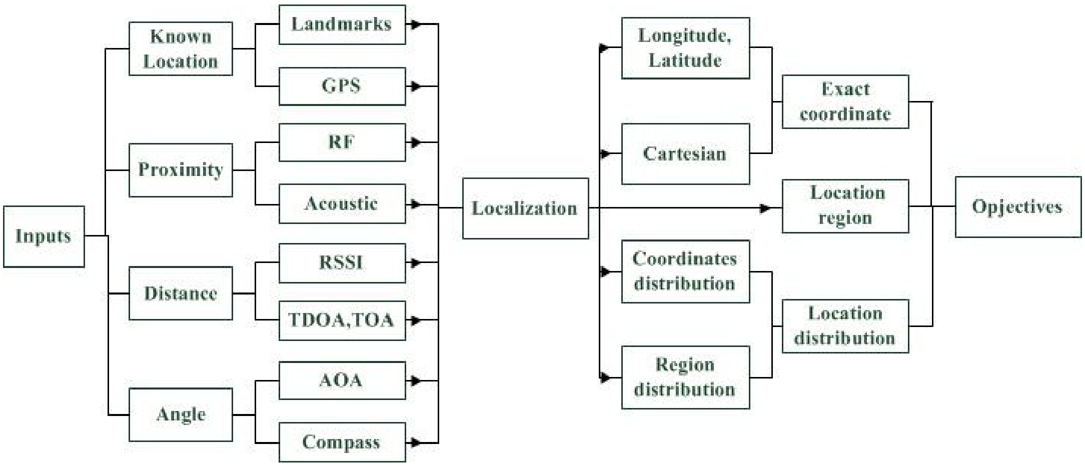


Figure-1
Taxonomy of range based localization

The hop counts case, the distance estimation can be disturbed through the hop counts computations which is lead to make the localization accuracy be incorrect. In general environment and for both signal strength and time of arrival techniques the attacks also can be focus on changing the medium physical characteristics by inserting a barrier , noise etc. Also the position estimation of the systems stated on the angle of arrival (AOA) can be influenced by diffusing a magnets in the sensor coverage area[11,12].

Position Computation Attacks: Definitely the sensor node location computations require at least a three known positions and distance estimations.The main aim of any attacker is to affecting at once the position computations by broadcasting untrue recognized location.The erroneous broadcasted position can be produce incorrect position computations in spite of the correct distance estimation, in this case the sensor node will send not only it's own information with improper location but also will send further information for a various nodes in various locations.In general environment the presence of jamming action can be attacking the GPS signal which leads to improper or unattainable sensor node position estimation[12,13].

Effects of Attacks on Localization: As more location based services getting deployed, there are a growing number of malicious attacks on the localization schemes. Most of attacks aim to affect the localization process so that the applications will be severely affected. Location infrastructure is subjected to various attacks from conventional to non-cryptographic attacks[14,15].

Conventional attacks are launched by injecting false messages into the network. These attacks can be seperated and authenticated by using cryptographic techniques. The non – cryptographic attacks are launched in such a way the processing of measurement has been deviated by attackers. This attacker can insert an absorbing obstruction between transmitter and the target changing the signal measurements. Wormhole attack tunnel can be established to confuse the reception units. These kinds of signal based attacks have not been studied deeply in literature. We focus on these kinds of attacks for the RSS based localization schemes to open the door for the researchers to propose effective methods to detect and eliminate the effect of these attacks on the localization process[16].

Attack detection in Wireless Localization[17] have been experimented with signal strength attacks by placing barrier. According to this experiment, the effect of different barrier on the signal strength is shown in figure-2.

We see that attacker can easily targeting the spotted signal strength by placing various materials. The attack on the RSS is measure by this scheme against the RSS mechanisms. The observation on the signal strength attack on these parameters is given in figure-3.

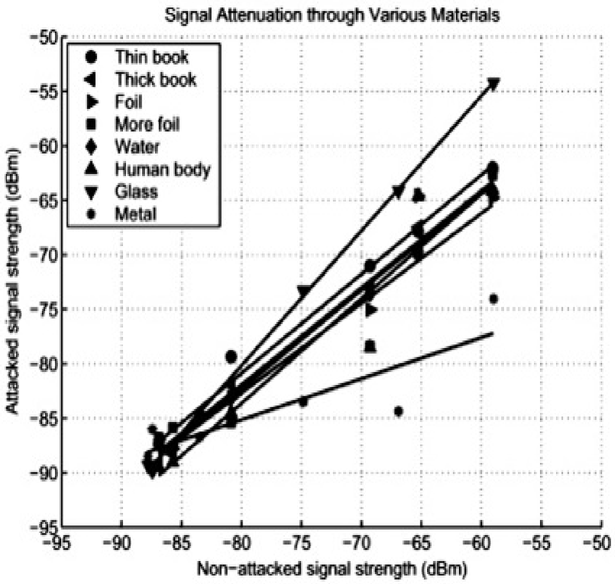


Figure-2
Signal strength passing through a barrier.

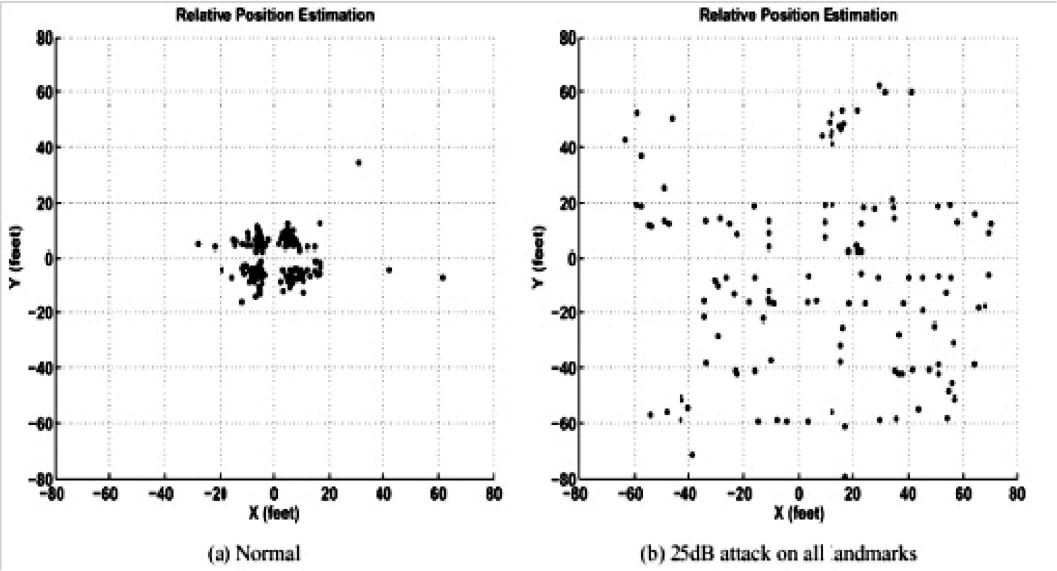
The cumulative distance function across the algorithms with and without attack is given in figure-4.

The error in current range based algorithm for varying signal attenuation is shown in figure-5, from this we observe as the signal attenuation increases the error in localization also increases linearly. From this test, the scheme under attacking has been clearly shows the error in position estimation.

Localization algorithms are built on ranging functionalities like RSS, TOA, AOA, hop count. Most of these methods base on the wireless system's physical properties. Attackers can stratify non-cryptographic attacks to attenuate or amplify signal strength. By using such simple mechanisms attacker can make the entire localization results erroneous. Trappe W. and Nath B.[18] summarize of different ways to launch such attacks methods for securing wireless localization in sensor networks.

Current Secure Localization Methods and Problems: Many secure localization algorithms have been proposed. However, most of them are range-free localization schemes which are based on securing the communication between anchor nodes, hence requiring special antennas.

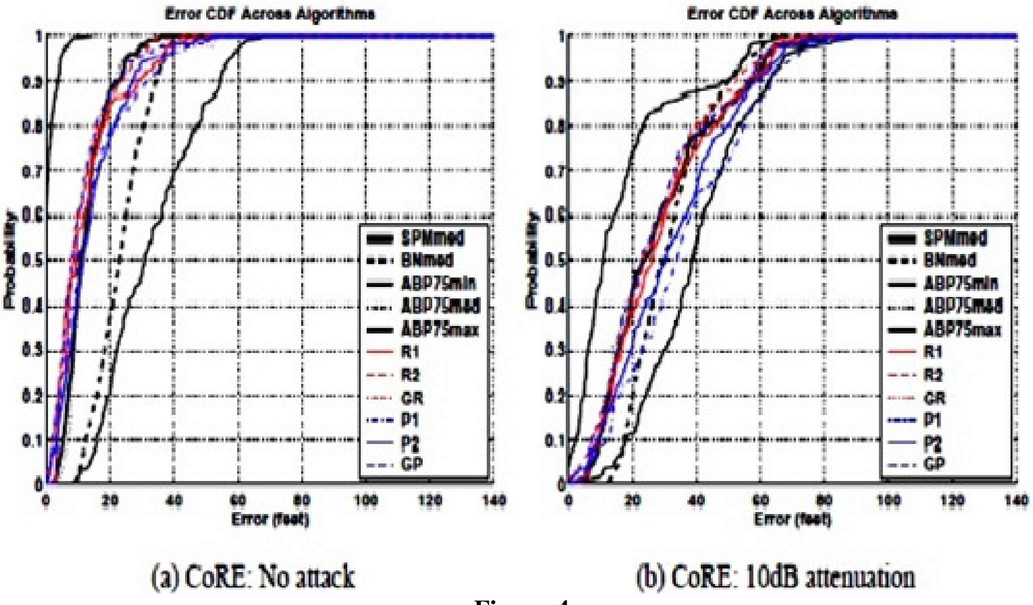
A localization scheme known as SeRLoc[19] presents a solution for wireless sensor networks. This approach requires sensors to determine their location based on beacon information transmitted by locators. Each transmitted beacon contains the following: i. the locator’s coordinates, and ii. the angles of the antenna boundary lines with respect to a common global axis.



(a) Normal

(b) 25dB attack on all 'andmarks

Figure-3
Localization estimation comparative to the proper positions



(a) CoRE: No attack

(b) CoRE: 10dB attenuation

Figure-4
Error CDF across localization algorithms

A locator is included within a particular sector if a sensor receives the beacon transmitted at that specific antenna sector. The location of each sensor is determined as the center of gravity (CoG) of the overlap of the different sectors. This position is computed on the basis of the locator-to-sensor communication range, the coordinates of the transmitting locators, and the sector boundary lines established by the beacons. The communication between locators to sensors is encrypted and secure. This approach needs specialized antenna called Locators to transmit beacons. This will increase the cost for localization.

HiRLoc[20] is a related range-independent localization scheme has been proposed for wireless sensor networks.This scheme lets sensors passively estimate their location with high resolution. The algorithm, known as HiRLoc, enables sensors determine their location by using the intersection of coverage area by the transmitted beacons from multiple reference points. Beacon transmission is secured by using computationally efficient cryptographic primitives in tandem with the physical medium constraints to provide localization. HiRLoc requires directional antenna for localization increasing the cost for localization.

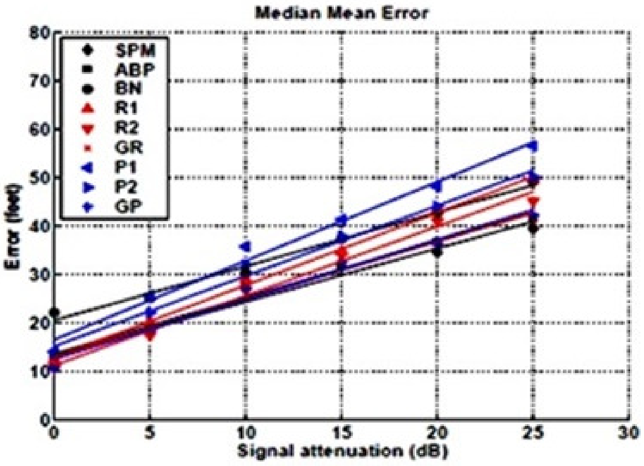


Figure-5
Average location estimation error across localization algorithms

Secure verification of device position is provided in the SPINE algorithm[21]. This scheme is based on Verifiable Multilateration. This mechanism, based on the measurement of radio propagation time, enhances conventional multilateration with distance estimation by verifying node positions using a set of (at least three) base stations. However, this method requires complex time synchronization logic, and extra hardware for its implementation.

The detection of malicious nodes has also received some attention, with the TSSL proposed as a solution[22]. Malicious nodes are detected in a step-wise fashion, beginning with anchor nodes collaborating by checking their coordinates, identities and time of sending information. This step is used to identify suspicious nodes. The WSA is partitioned into sub-areas of different trust grades by using a mesh generation algorithm to segregate malicious nodes. Further research has led to a novel algorithm for the computation of locations of unknown nodes based on differences in arrival time of localization information. In this method, while calculating the coordinates, if signal strength attacks are launched, the distance estimation will be erroneous and the error is cascaded to all successive stages.

Jian. L[23] proposed a localization scheme based on sifting noisy and outlier distance measurements. This work proposes a bilateration generic cycles-based outlier detection algorithm for identifying malicious nodes. But this algorithm is complex to be realized in low power sensors.

A novel ratio-based signal strength metric (RSM)[24] has been proposed a new solution for wireless sensor network localization.This metric directly maps to information about distance to a set of landmarks. It is thus ratio-based, with a goal to achieve robust localization inspite of attacks. However their method assumes that attack on all the landmarks are uniform, under variation in the attack on the landmarks their method performs poorly.

The improvement of localization accuracy has been proposed by applying multiple frequencies and power transmission [25]. By using deviations of RSS readings and residuals, the algorithm forms high quality RSS fingerprints. These fingerprints are derived from multiple dimensions resulting from the use of multi-frequency and multi-power. Although this method improved the localization accuracy, it however did not consider the effect of the attacks.

Xiaoyan Li [26] proposed an algorithm which simply aggregates a set of point-based algorithms, returning the union of their estimated locations as the final result. For every location, as long as there is a point-based algorithm that can correctly localize, the aggregation algorithm will be capable of locating the point. Thus, aggregation harnesses the strengths of all the algorithms. The performance enhacement derived from such aggregation, depends on the performance of participating algorithms and their complementing of one another at the locations. This work proves that the aggregation improves the localization performance. However, once again, this work did not consider the effect of attacks. The error also gets aggregated in presence of signal strength attacks.

Long XIAO[27] proposed an alternative cost-effective indoor localization system based on off-the-shelf active RFID technology. Besides being compatible with the future smart spaces and ubiquitous computing systems, this system is also appropriate for large-scale indoor localization. It is based on the low-complexity Gaussian Filter (GF), Wheel Graph Model (WGM) and Probabilistic Localization Algorithm (PLA), making it robust to uncertainty. It is suitable for large-scale indoor positioning, and self-adjusting to varying indoor environments. However, the solution is not secure against signal strength attacks.

Murtuza Jadliwala[28] proposed a scheme to ensure secure localization in the presence of cheating beacon nodes. This method is based on known error bounds. Unfortunately, the problem with this solution is that it is based on fixing the location of beacons based on distribution of nodes.

Chunxia Li[29] is concerned with a secure location verification. The proposed algorithm is reported to be well suited to a service restricted region. The algorithm works by considering nodes whose signal strength is imcompatible with the in-region as adversaries. However, this requires the deployment knowledge at all sensors, and this approach cannot be scaled to bigger networks.

Yongzhao Zhan[30] proposed an alternative secure localization scheme based on the time congruity. Time synchronization between user nodes and base stations is not required in this method. Congruity of time is computed according to the

Table-1
Summary of the range base localization analysis

Method	**Problems**
SeRLoc [19]	Costly to install special antenna
HiRLoc [20]	Works only with directional antenna
SPINE [21]	Time synchronization needed
TSSL [22]	Signal strength attack can be easily launched
Outlier detection [23]	Algorithm is complex and energy consuming
RSM [24]	Fails under differential attack
Multi Frequency Multi Power RSS fingerprinting [25]	Effect of Attack not considered
Xiaoyan Li [26]	Effect of Attack not considered and error also gets aggregated in presence of signal strength attacks
Long XIAO [27]	The solution is not secure against signal strength attacks.
Secure distance based localization [28]	Dependent on deployment model
Chunxia Li [29]	Need to know deployment knowledge and not suitable for large networks
Yongzhao Zhan [30]	Not secure against time varying attacks

communication delay between nodes, which enables the estimation of the location of the user node. However this method can be attacked by launching varying time of arrival attack. We summarize the analysis of existing methods for range based localization in table-1.

Open Issues: As we see the literature survey we notice following problems in the solutions: i. Most solutions are range free cryptographic authentication methods which cannot be used for range based localization. ii. The solutions involve complex hardware and tight time synchronization. iii. The solution cannot be run on power constrained devices. iv. The solutions work on assumptions only certain number of attackers present. v. Most solutions are for point based localization. vi. The use of multi frequency, multi power methods for secure localization is not explored much.

This open issue motivates researchers to propose efficient solutions addressing this concern.

Conclusion

The paper summarizes the range based localization methods and the different attacks on localization process to make localization erroneous. There is no single localization algorithm secure against all the attacks which we have explained. Also use of single approach to localization will be difficult to secure under all the attacks. We have identified the areas for further research on range based localization in the wireless sensor networks.

References

1. Morteza J, Hossein M, Kasra M and Mohammad F., A Method in Security of Wireless Sensor Network based on Optimized Artificial immune system in Multi-Agent Environments, *Res. J. Recent Sci.*, **2**(**10**), 99–106 (**2013)**

2. Mao G. and Fidan B., Localization Algorithms and Strategies for Wireless Sensor Networks; United States of America by Information Science Reference IGI Global **(2009)**

3. Wang J., Ghosh R.K. and Das S.K., A survey on sensor localization., *J. Control Theory Appl.*, **8,** 2–11 **(2010)**

4. Youssef A and Youssef M., A Taxonomy of Localization Schemes for Wireless Sensor Networks ,International Conference on Wireless Networks (ICWN’07), Las Vegas, Nevada, 25–28 **(2007)**

5. Ding X, Zhao H, Zhu J, Zhang K and Li D., A Novel Localization Algorithm Based on RSSI for Wireless Sensor Networks, *7th Int. Conf. Wirel. Commun. Netw. Mob. Comput.*,**1(4),** 23–25 **(2011)**

6. Paramvir B. and Venkata N.P., RADAR : An in-building RF-based user location and tracking system, In IEEE International Conference on Computer Communications (INFOCOM), 775–784 **(2000)**

7. Elnahrawy E. and Martin R.P., The limits of localization using signal strength: a comparative study , First Annu. IEEE Commun. Soc. Conf. Sens. Ad Hoc Commun. Networks, 406–414 **(2004)**

8. Afzal S., A Review of Localization Techniques for Wireless Sensor Networks, *Journal of Basic and Applied Scientific Research,* **2**, 7795–7801 **(2012)**

9. Alrajeh N.A., Bashir M. and Shams B., Localization Techniques in Wireless Sensor Networks, *Int. J. Distrib. Sens. Networks*, 1–9 **(2013)**

10. Fink A, Beikirch H., Analysis of RSS-based Location Estimation Techniques in Fading Environments., International Conference on Indoor Positioning And Indoor Navigation (IPIN), 21–23 **(2011)**

11. Yang Jie and Ying Y.C., Toward attack-resistant localization under infrastructure attacks, *Security and Communication Networks,* **5(4),** 384–403 **(2011)**

12. Neve KN, Phegade SG and Kirange DY., Secure

Localization : The Review on Possible Attacks of WSN and Their Remedy, *Int. J. Eng. Res. Technol.*, **2(8), 2085–2090 (2013)**

13. Zhu WT, Xiang Y, Zhou J, Deng RH and Bao F, Secure localization with attack detection in wireless sensor networks, *Int. J. Inf. Secur.*, **10(3),** 155–171 **(2011)**

14. Chen Y., Kleisouris K., Li X., Trappe W. and Martin R.P., A security and robustness performance analysis of localization algorithms to signal strength attacks, *ACM Trans. Sens. Networks*, **5,** 1–37 **(2009)**

15. Chen Y., Yang J., Member S., Trappe W. and Martin R.P., Detecting and Localizing Identity-Based Attacks in Wireless and Sensor Networks, *IEEE Transactions on vehicular Technology,* **59(5),** 2418–2434 **(2010)**

16. Población A., Performance of Robust Algorithms for Secure Localization in Wireless Sensor Networks, *International Conference on Localization and GNSS,* **1(4), 25-27(2012)**

17. Chen Y. ,Trappe W. and Martin R., Attack Detection in Wireless Localization, In *26th IEEE International Conference on Computer Communications*, **1964,** 1972 **(2007)**

18. Trappe W. and Nath B., Robust statistical methods for securing wireless localization in sensor networks, *Fourth Int. Symp. Inf. Process. Sens. Networks,* 91–98, **(2005)**

19. Lazos L. and Poovendran R., SeRLoc : Robust Localization for Wireless Sensor Networks, *ACM Transactions on Sensor Networks,* **1(1),** 73–100, **(2005)**

20. Lazos L., Poovendran R., HiRLoc: high-resolution robust localization for wireless sensor networks, *IEEE J. Sel. Areas Commun.*, **24**(**2**), 233–246 **(2006)**

21. Capkun S. and Hubaux J., Secure positioning of wireless devices with application to sensor networks, *Proc. IEEE 24th Annu. Jt. Conf. IEEE Comput. Commun. Soc.,* **3**, 13-17 **(2005)**

22. Guangjie H., Jinfang J., Lei S., mohsen G. and Shojiro N., A Two-Step Secure Localization for Wireless Sensor Networks, *The computer Journal,* **56(10),** 1154–1166 **(2012)**

23. Jian L., Yang Z. and Liu Y, Beyond Triangle Inequality : Sifting Noisy and Outlier Distance Measurements for Localization, *Proc. IEEE INFOCOM*, **1(9),** 14-19 **(2010)**

24. Li X., Chen Y., Yang J. and Zheng X., Achieving robust wireless localization resilient to signal strength attacks, *Wireessl Networks*, **18(1),** 45–58, **(2012)**

25. Zheng X., Liu H., Yang J., Chen Y., Francisco J., Martin R. and Li X, Characterizing the impact of multi-frequency and multi-power on localization accuracy, *7th IEEE Int. Conf. Mob. Ad-hoc Sens. Syst.*, 156–165 **(2010)**

26. Xiaoyan Li and Martin R., Simple algorithm aggregation improves signal strength based localization, *In 3rd International Symposium on Wireless Pervasive Computing*, **540 (544),**7-9 **(2008)**

27. Xiao L., Yin Y., Wu X. and Wang J., A Large-scale RF-based Indoor Localization System Using Low-complexity Gaussian Filter and Improved Bayesian Inference, *Radioengineering Journal,* **22(1),** 371–380 **(2013)**

28. Jadliwala M. , Upadhyaya S.J. and Hubaux J., Secure Distance-Based Localization in the Presence of Cheating Beacon Nodes, *IEEE Trans. Mob. Comput.,* **9(6),** 810–823 **(2010)**

29. Li C., Chen F., Zhan Y. and Wang L., Security Verification of Location Estimate in Wireless Sensor Networks , 6th International Conference on Wireless Communications Networking and Mobile Computing (WiCOM), **1(4), 23-25 (2010)**

30. Zhan Y. , Li C., Wang X., Zhou Y., Liu L. and Al-Aqrabi H., A Secure Node Localization Method Based on the Congruity of Time in Wireless Sensor Networks, *IEEE 11th Int. Conf. Trust. Secur. Priv. Comput. Commun.*, **884**(**889**), **25-27 (2012)**