ROBUSTNESS OF LOCALIZATION ACCURACY FOR WIRELESS SENSOR NETWORKS UNDER PHYSICAL ATTACKS

[1,2]AHMED ABDULQADER HUSSEIN, [1]THAREK A. RAHMAN, [1]CHEE YEN LEOW

[1] Wireless Communication Centre (WCC), Faculty of Electrical Engineering, Universiti Teknologi Malaysia, UTM Skudai, Johor 81310, Malaysia

[2] University of Technology,Baghdad,Iraq

E-mail: ahmedabdulqaderhussein@gmail.com, tharek@fke.utm.my,bruceleow@fke.utm.my

ABSTRACT

Wireless sensor network localization is an important area that attracted significant research interest. This interest is expected to grow further with the proliferation of wireless sensor network applications. 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. Range based methods like received signal strength indication (RSSI) is affected a lot by physical attacks. This paper proposes a solution based on multi frequency multi power antenna to provide robust and accurate localization technique . In addition this paper proposes a grid coloring algorithm to detect the signal hole map in the network which is refer to the attack prone regions in order to take a corrective actions . The simulation results showed improvement in the localization accuracy in the presence of barrier attacks through detecting , filtering and eliminating the effect of these attacks.

Keywords: *Wireless Sensor Networks WSNs, Robust Localization, Received Signal Strength Indication(RSSI) algorithm, Physical Attacks.*

1. INTRODUCTION

Many applications are designed based on localization of nodes in the sensor networks. These applications require accurate position of the nodes in the network. Location information can be describes as a railway tracks, a floor in a building and a multi level in mall for one , two and three dimensional respectevely . It is a reality that much research activities have been developed into wireless sensor networks because to it's importance . sensors with the following performance indices such as inexpensive , low power consumption , small size , multipupose and small coverage area are direct function of the advancement in electronics and communications.

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.

In wireless sensor networks various methods are used for performing localization.These mechanisms are affected by two kinds of attacks non cryptographic signal strength based attacks and cryptographic attacks.Therefore these attacks have been introduce errors in the localization process.

In this paper, we explore the RSSI range based localization method, the physical attacks on this method and a current powerful mechanism associated with this algorithm against attackers. We propose a new solution for robust localization against attackers using multi frequency multi power antenna constructed after these physical attacks have to be filtered . The solution is effective for the RSS technique based on the signal strength physical attacks.

2. BACKGROUND

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 the beacons to other nodes and determine their location relative to the anchor node.[1]

The location of sensors is important for many wireless sensor applications. Range Based and Range Free localization methods are available for obtaining the location of the sensor nodes. One of the main challenges in localization is that the process can be made erroneous by launching various attacks.[2]

2.1 Localization Process

The process of the localization algorithm is to estimate the location of the sensors based on input data. Absulute localization refer to anchor based groups have been an absolute coordinate output.In some cases , the absolute location can be determined from the relative locations by using linear transmission and some references. In the other hand relative localization of the anchor free scheme outputs are relative coordinates. Hence relative location is the relationship between distance and angle of nodes in the network and it can be also transform to the absolute localization [3]. Figure 1 shows the process of localization algorithms.

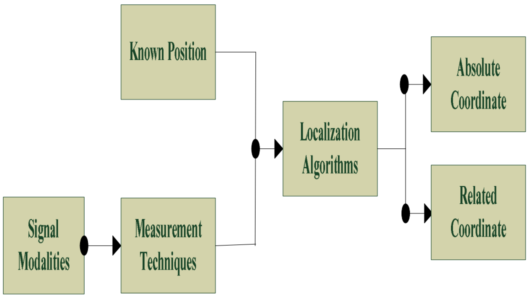

Figure 1:The Process Of Localization Algorithms.

2.1 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 [4]. Localization system requires to take out the range estimates from fixed anchors or reference points with a view to estimate the location of the node . The range estimation can be acquired using various metrics such as RSS , AOA and TOA techniques [5]. Figure 2 show anarchitecture of a typical positioning system.

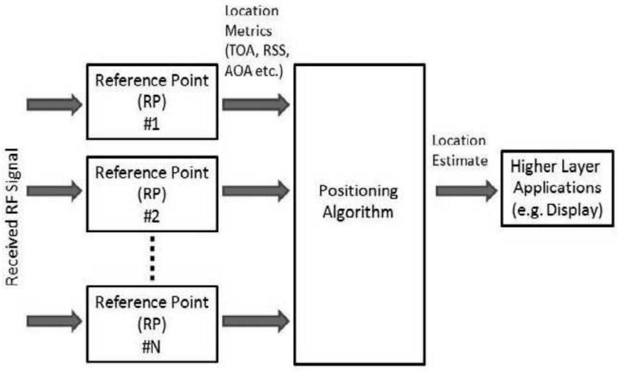

Figure 2: Architecture Of A Typical Positioning System.

The RF signal for the received signal strength RSS algorithm that is transmitted by a transmitter has an energy loss proportional to the distance signal travels. A model based on single – path radio propagation is given by equation (1) [2].

$$\Pr(dB) = Pt(dB) - 10\,\alpha \log_{10} d \qquad (1)$$

Where
Pr(dB) is the received signal power in dB.
Pt(dB) is the transmitt signal power in dB.
α is the distance power gradients.
d is the distance.

Wide set of algorithms are commonely using the signal strength in their location estimation getting the advantages of it's 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 enormus saving in costs over prevailing localization particular hardware.

RSS-based localization is an 802.11 physical location estimation depending on signal strength only. This algorithm is typically using statistical/machine learning techniques due to the noisy nature of RSS measurments. Two phases are inherent in this algorithm [6]:

1) An offline training phase is the readings of received signal strength indication (RSSI)!ti = (ri1, ..., rin) are gathered over a set of n passive receivers and are labeled with the transmitter's true physical location and orientation pi = (xi, yi, "i).
2) Through the phase of online localization, the readings are applied RSSI oj = (rj1, ..., rjn) are used to get the output of the device's estimated location ˆ pj = (ˆ xj , ˆ yj) .

2.3 Attacks Affecting 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 [7].

2.3.1 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 recieved 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.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 attackes 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 [8,9].

2.3.2Position 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.[9,10]

2.3.3 Effects of Attack on Localization

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 a non-cryptographic attacks to attenuate or amplify signal strength. By using such simple mechanisms attacker can make the entire localization results erroneous. Summary of different ways to launch such attacks can be found in.[11]

Conventional attacks are launched by injecting false messages in 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 on the RSS based localization schemes and propose effective methods to detect and eliminate the effect of these attacks on the localization process.[12,13]

3. RELATED WORK

A localization scheme for wireless sensor networks has been presented in [14]. This approach requires sensors to determine their location based on beacon information transmitted by locators. Each transmitted beacon contains the following:

(a) the locator's coordinates, and (b) the angles of the antenna boundary lines with respect to a common global axis. 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.

A related range-independet localization scheme is presented in [15]. 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.

Secure verification of device position is provided for in the SPINE algorithm [16]. 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 [17]. Malicious nodes are detected in a step-wise fashion, begining 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.

A novel ratio-based signal strength metric (RSM)[18] 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.

In [19], the improvement of localization accuracy has been proposed by applying multiple frequencies and power transmission. 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.

Murtuza Jadliwala [20] proposed a scheme to ensure secure localization in the presence of cheating beacon nodes has been proposed. 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 [21] 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 can not be scaled to bigger networks.

4. 4. CURRENT PROBLEMS AND OPEN ISSUES

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 implimented in a large scale sensor networks. The localization system of (TOA) is based on the usage of GPS , actually it has bee required expensive and extra electronic devices which consume high energy to obtain the synchronization of satellite's clock precisely. The limitations in hardware for implimented such a sensor networks should be considered with energy constraints [3]. Similar to (TOA) algorithm, (TDOA) and (AOA) schemes necessitate to an 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, furthermore (AOA) algorithm needs a special antenna design [22].In the other hand the simulations and environmental controlled labratories show more efficiencient 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].

As we see from the related work we notice that Most solutions are range free authenticated methods which cannot be used for range based localization, also involve complex hardware and tight time synchronization, which cannot be run on power constrained devices.

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 [7].

Moreover a physical attacks can be launched on these mechanisms by merely causing signal attenuation or amplification, delaying the signal arrival time etc. The attacks results lead to a great deviation in the estimated location values causing bigger measurement errors. Due to this errors, the application built on localization is affected.

The challenge is to accepting and dealing with the presence of these attacks in the network , this open issues motivate us to propose an effective robust localization scheme and powerful position computations using filtering and statistical techniques in order to detect and eliminate these attacks.

5. PROPOSED SOLUTION

5.1 Overview of the Proposed Solution

We propose a solution based on multi frequency multi power transmission. In our solution, the anchor or access point(AP) nodes will transmit signals in multi frequencies at multiple power levels. Sensor nodes receive these signals and construct a RSS fingerprint from it. All the sensor are already coded with the knowledge on expected frequencies and the power level from the AP. By the observing the RSS fingerprint that is expected, the sensor will be able to find if there is a barrier which attenuates or degrades the signal. Sensor will reject the RSS finger prints which it doubts as attenuation or degradation. Leaving those corrupted RSS fingerprints , sensor nodes will choose the remaining RSS fingerprints from the uncorrupted and does the lateration using non linear least squares to get the location of the sensor node.

In order to avoid the estimation getting affected by interference and reflection we propose a technique to filter those signals by estimating the approximate angle of arrival of the signal. In addition we also propose the method to get the estimation of attack area in the network. By estimating the attack area and alerting the network administrator, it can remove those barriers effect and improve the localization accuracy.

5.2 Proposed Robust Localization Based on Multi Frequency Multi Power approach

Location is achieved with the aid of multi frequency multi power antenna. The knowledge what frequency and power level from the expected antenna is known priori at the sensor. When this deviation across, the sensor can know easily there is some barrier. By cooperating with all sensors the sensor is able to identify the area of barrier attack. Each antenna sends its signal in a programmed fashion with different frequencies and power level. By using linear lateration method, the accurate position of sensor node is estimated, skipping the antenna position values of barrier attacked antenna reading.

The Frequency, Power level sequence decider will give the next frequency, power level to use for the antenna. The antenna will transmit at that power level and frequency. The receiver at sensor node will try to synchronize and check the expected power level and frequency for checking if there is any signal degradation or attenuation in the path of the signal. Lateration technique is applied on the position of the sensor and distance measurement to get the location of the sensors. In addition ,based on the signal irregularities at all sensor , attack map of the region of attack is found.The functional block diagram of the solution is shown in Figure 3.

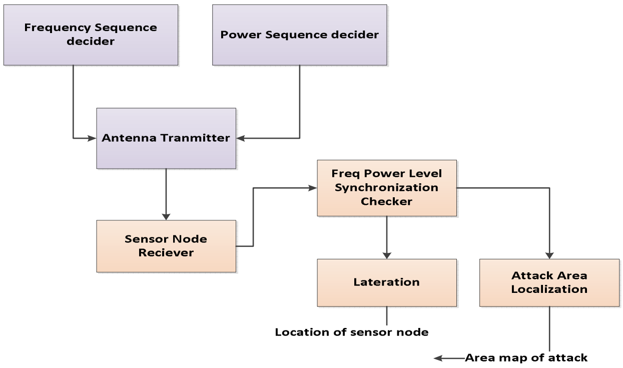

Figure 3: Block Diagram Of Proposed Secure Localization Solution.

5.3 Network and Adversary Model

In our network model, a sensor device M in a non trust worthy environment wants to compute its own location by using the distance estimates to a set of access points(AP). These access points transmit signals in multi frequency and multi power.

The sensor device estimates the distance based on RSS of the signal from the landmarks. Signal strength attack can be launched by the attackers by placing barriers. Due to this there is an error in distance measurement as well as the result of the localization is erroneous. The sensor device is assumed to have the knowledge about the AP's position and the approximate angle of AP's location. Knowing the approximate angle range in which the AP is located helps to avoid any faulty measurements due to signal reflection by the barriers.

In addition , Knowing the approximate angle of arrival of signals from the AP will help the sensor to avoid any interference or reflected signals from the barrier. Since the sensor nodes are placed randomly in the network ,so that knowing the angle of arrival of signal from the AP is done by sensor tuning in each direction till maximal power is received. This process has to be done for each AP at the initial deployment time.

The sensor and the AP are strictly time synchronized. This can be done by running a quartz crystal clock in all the sensors and AP. With the help of quartz crystal, all of them are time synchronized. Quartz crystal based time synchronization is easy to implement and it is cheap.For more information about other time synchronization in wireless sensor networks can be found in [23,24].

5.4 RSS Measurement

Each AP (access point) is assigned by two functions:

yf = Ff(t) (2)

yp = Fp(t) (3)

The Function Ff and Fp is a step wise function over the possible values of frequency and power. The step function with in a step duration is kept different for different AP's.

A sample step function is shown in Figure (4). The step function has three values a,b,c. The time duration for the step function is given as 3T for a, 4T for b and T for c. The step will repeat after one full cycle of 8T. the T duration can be different for each AP.

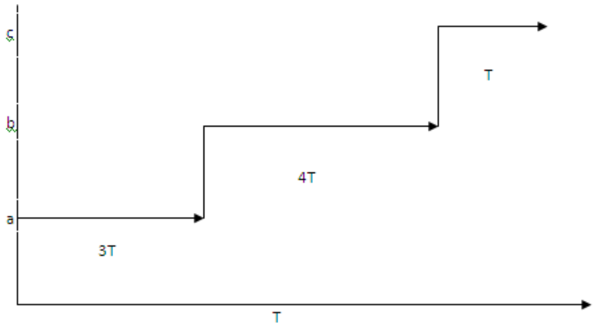

Figure 4:A Step Function For A Frequency And Power Decider .

Using these functions, the current frequency and power at which the AP transmit the signal can be known at any sensor node.The sensors are pre- distributed with these two functions. Also the AP 'a antenna follows this functions for the frequency and power at which the signals are transmitted.

Before starting localization, each sensor node tune to the approximate angle in which an AP is located to capture the signal and measure the RSS. By tuning to the approximate angle, we are able to filter out the RSS measurement errors due to reflection and interference signals from other directions.

Each sensor calculates the estimated signal frequency and power by using the functions with it. According to equation (4) and (5) the tuning is done in a way to minimize the error between the actual transmitted frequency and the power .

Ef = abs(yf - yaf) (4)
Ep = abs(yp - yap) (5)

If the deviation in error within the approximate angle is greater than threshold, the RSS value from that AP must be rejected, as it is an indication of signal attenuation or degradation by the attacker the deviation in error can be calculated from equation (6) and (7).

Df = min(Ef) $\alpha\min < \alpha < \alpha \max$ (6)

Dp = min(Ep) $\alpha\min < \alpha < \alpha \max$ (7)

Df and Dp must be less than threshold λ for the RSS value in order to be accepted. Every Sensor must measure the RSS value for different frequencies for the same AP. The best value of RSS with lower most value for Df and Dp must be taken. The AP's location (x,y) together with its

RSS value measured constitute the RSS finger print for that AP.Each sensor node must calculate the RSS finger print all the AP who's Df and Dp is less than the threshold λ .

Threshold is the amount of tolerance between the estimated and actual . It can be measured by placing the a small obstacle for signal degradation in different points in the network and measure the error. The size of obstacle will be the maximum obstacle size that our network can tolerate. This is done to accommodate certain infrastructure provisions made by administrator in the network.

5.5 Localization

Localization involves two stages ranging and lateration.Ranging estimates the distance ρ from the position of the sensor node to the AP.RSS received can be expressed as shown in equation (8).

RSS = Po – 10 α log10 d – v (8)

Therefore the distance can be determined from equation (9) as follow:

ρ=10(Po–RSS/10*α) (9)

Where

Po - is the power received in dBm at 1m distance.
d - distance between node and the AP.
α – is the path loss component.
v – is the log normal shadow fading effects .
ρ – distance estimate.

Lateration gets the position of the sensor node from the distance measurement for different AP and their locations.There are two popular methods to get the location estimate Non linear least squares (NLS) and linear least squares (LLS).In NLS , from the estimated distance di and known positions Li = (xi,yi) of the landmarks , the position (x,y) of the target device can be estimated by finding (x^,y^) satisfying the equation (10).

$$(\hat{x},\hat{y}) = argmin_{x,y}\sum_{i=1}^{n}[\sqrt{(xi-x)^2+(yi-y)^2}\_\hat{d}i]^2 \qquad (10)$$

Where i=1…n for n total landmarks.

Since solving this equation is computationally complex, we can approximate this relation as shown in equation (11).

A P^ = b (11)

Where

$$A=\begin{pmatrix} x1-\frac{1}{n}\sum_{i=1}^{n}xi & xn-\frac{1}{n}\sum_{i=1}^{n}xi \\ y1-\frac{1}{n}\sum_{i=1}^{n}yi & yn-\frac{1}{n}\sum_{i=1}^{n}yi \end{pmatrix} \qquad (12)$$

And

$$b=\frac{1}{2}\begin{pmatrix} (x_1^2-\frac{1}{n}\sum_{i=1}^{n}x_i^2+(y_1^2-\frac{1}{n}\sum_{i=1}^{n}y_i^2) \\ (x_n^2-\frac{1}{n}\sum_{i=1}^{n}x_i^2)+(y_i^2-\frac{1}{n}\sum_{i=1}^{n}y_i^2)-(\hat{d}_n^2-\frac{1}{n}\sum_{i=1}^{n}\hat{d}_i^2) \end{pmatrix} \qquad (13)$$

A is described by the coordinates of landmarks and b is composed of estimated distance to landmarks. The position estimation is solved by equation (14) .

$$\hat{P}=(A^T A)^{-1}A^T b \qquad (14)$$

5.6 Detecting Attack Prone Regions

One of the important advantages in our solution is that we can find the region of attack and take some corrective action.In our solution, each sensor node can identify the AP which has barriers in the path to the sensor node. Each sensor node sends to a central signal fusion centre which marks the boundary of attack region and handles it by removing the barriers effect.

Figure 5 shows a network with AP's, sensors and the barriers. The accepted AP (whose error deviation is less than threshold),the rejected AP (whose error deviation is above the threshold) , the sensor node location estimated is provided to the signal fusion center. Signal fusion center is also aware of the direction of propagation of signal from the AP to the sensor nodes.

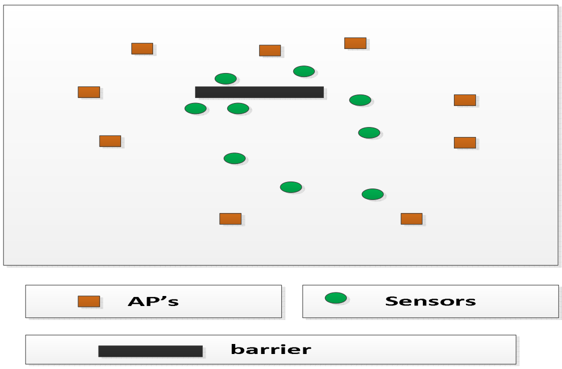

Figure 5 :Wireless Sensor Network System With AP's, Sensors And The Barriers.

Based on this information, the signal fusion center constructs a signal map. The signal map is the representation of points where the signals from the AP's are able to traverse in the network. The signal map holes are places where the places in which signal from AP are not accepted at the sensor node due to larger error deviation in the signal power as shown in Figure 6.

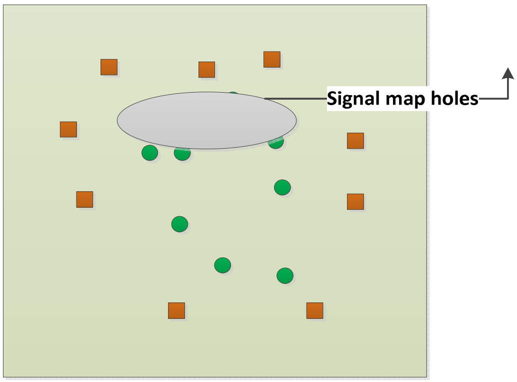

Figure 6: Signal Map At The Fusion Center.

Through construction of signal map, we are able to identify the signal holes in the network. Signal holes are region of attack in the network and must be corrected. The usual corrective action is to remove the barrier manually.

To detect the signal hole, we propose a grid coloring algorithm. The algorithm split the entire network into small equal sized grids. Initially all the grids are white. The sensor locations are marked in the grids. When a sensor accepts the AP' RSS value (since the error deviation in signal power is less than threshold), the grids in the direction from the AP to the sensor node along the direction of the signal is colored gray. This process is done for all sensors for all the accepted AP. Once the process is complete, all the grids still in white are the signal holes.

The algorithm code is given below:

Algorithm: Signal Hole detection

```
GM[][]  ← Split  network into small grids
N*N

For i=1: N
  For j=1: N
      GM[i][j] = White;
  End
End

For i=1: No_of_Sensor
  For j=1:No_of_AP
    If error_deviation(AP) < threshold

         For X=1: N
            For Y=1: N
               If  Grid(X,Y) is in direction of
AP,sensor(i)
                  GM(X,Y)← gray;
               End
            End
         End
    End
  End
End
```

Error in estimated attack area is calculated by equation (15).

$$E = nGAct - nGF \tag{15}$$

Where

nGAct is the No. of Gray squares actually in the attack area.
nGF is the No. of Gray squares estimated in the attack area.

6. PERFORMANCE ANALYSIS

We simulated the proposed solution in MATLAB. The simulation area consists of a 1000 * 1000 m two dimensional terrain. The optimal number and placement of AP is important. We assume a small but reasonable beacon node population of 20 beacon nodes (approximately 5 beacon in each direction), which is scattered uniformly over the 1000 m * 1000 m area.We place a maximum of 10 barriers of length 1m and width 0.5 m randomly in the network. The barriers will cause signal strength attack degrades the signal and affect the RSS.Table 1 shows the system model specification.

Table 1 : System Model Specification

Network Area	1000 * 1000 m
Frequency Used by AP	400, 600,800 MHZ
Power Used by AP	2, 4,6, 8 dB
Barrier dimension	1 * 0.5 m
Node Placement	Random
APs Placement	Random , Around Perimeter

The average localization error is calculated between the actual and the estimated locations for all sensor nodes. The performance is measured in-terms of average localization error by varying the number of barriers in the network as shown in Figure 7. Also measure the localization error by varying the number of AP's in the network. We compare the performance with TMT technique proposed in [25].

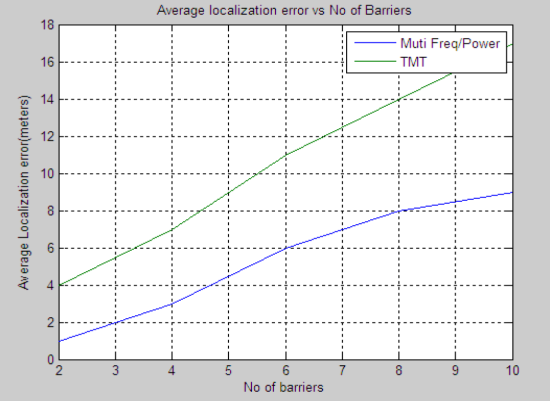

Figure 7 Average Localization Error Versus Number Of Barriers.

We kept the number of barriers as 10 and varied the no of APs and measured the localization error as shown in Figure 8.

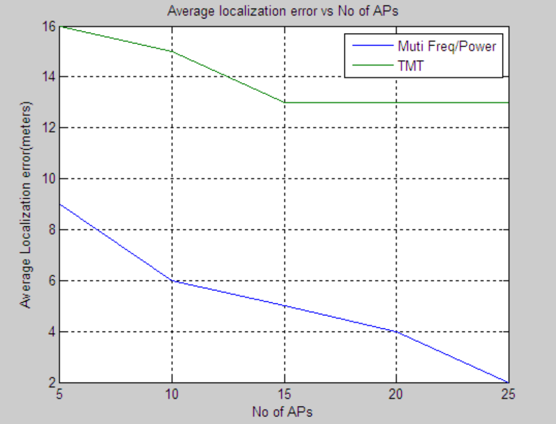

Figure 8 :Average Localization Error Versus Number Of Aps.

The simulation results observe that as the number of AP increases the localization error falls very rapidly in our approach because of the number of variables used in non linear regression increases.

Another important performance metric is the accuracy of detected area of attack. This accuracy is measured in terms of difference between the actual area the barrier occupies and the detected area of signal holes. We vary the number of AP's and measure the accuracy as shown in Figure 9.

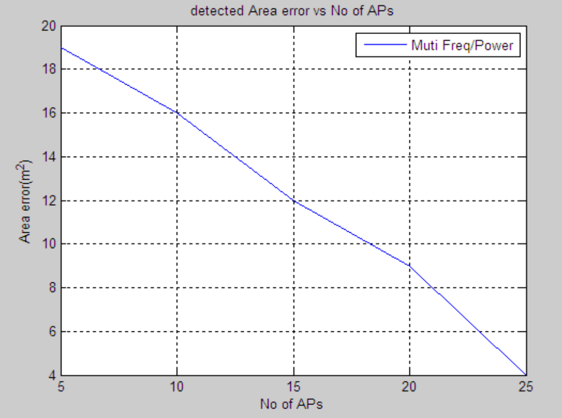

Figure 9 :Detected Area Error Versus Number Of Aps.

We see that as the number of AP increases the area error reduces a lot. We have followed uniform placement of AP's ,but if more optimum placement of AP is done , it will reduce the Area error and identifying the attack area with great precision.

We measured the effect of placing the AP on the network to determine the optimum placement positions. We simulated for two different configurations:

1. Random

2. Around the perimeter

The measurement of the detected area error against number of Aps for the two configuration of placing the Aps in the network can be seen in Figure 10.

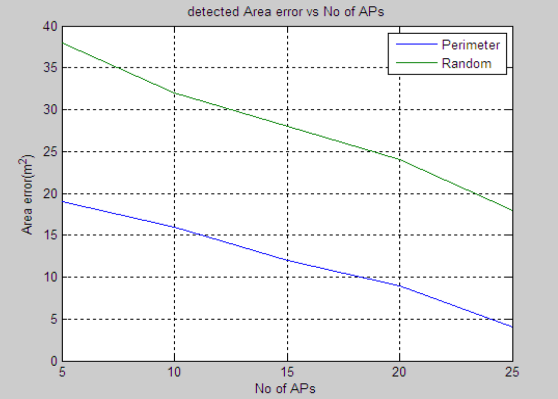

Figure 10: Detected Area Eerror Versus Number Of Aps For Random And Perimeter Placement Configuration Of Aps.

From the simulation results, we conclude that placing the AP around the perimeter gives the better estimation of attack location than the random placing .

The localization error for the two placement configuration is measured as shown in Figure 11.From the results we see that in case placing the AP around perimeter the localization error is minimum and better than the case of random Aps placing in the network.

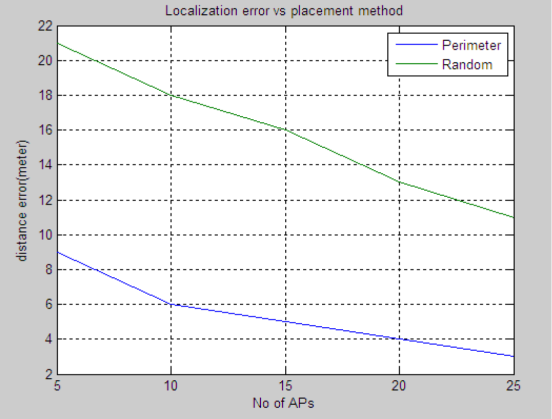

Figure 11: Localization Error Versus Number Of Aps For Random And Perimeter Placement Configuration Of Aps.

The choice of frequencies to use also affects the localization accuracy. We used a following guideline in choosing the frequencies

1. The base frequency to be used must be chosen from unused spectrum range.

2. The multiple frequencies must be separated by twice for a better accuracy.

We varied the difference in frequencies from 20% to 100% increase as shown in Figure 12, and measured the localization error and observed that localization error is reduced at the 100% increase which is twice the base frequency.

The reduced in the localization error as the frequency interval between the multiple frequencies increase is due to the fact the interference between the frequencies is reduced and the effect of reflected signal from the attacker was easily identifiable.

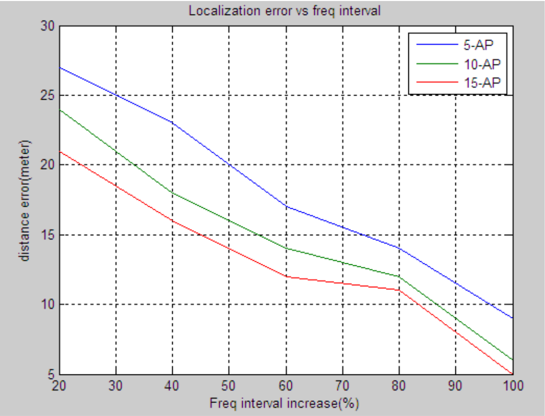

Figure 12 : Localization Error With Different Frequencies Pecentage Increasing.

The measurement of the localization error percentage for different signal degradation by the attackers take into consideration . The signal degradation is varied from 40% to 80 % of the original signal from the AP as shown in Figure 13.

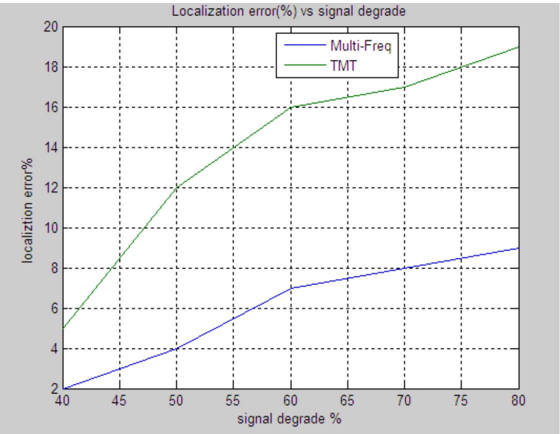

Figure 13: The Effect Of Signal Degradation On The Localization Accuracy.

From the results, we see that as the signal degradation increases , our proposed algorithm based on multi frequency – multi power transmission performs better than the TMT method.

We measure the accuracy in the attack area estimation for different RSS error threshold values as shown in Figure 14. From the results we observe that if the threshold value is high, the accuracy is low because the estimated area is bigger than the attack area, otherwise if the threshold value is low, the accuracy is low because the estimated area is lower than the attack area.

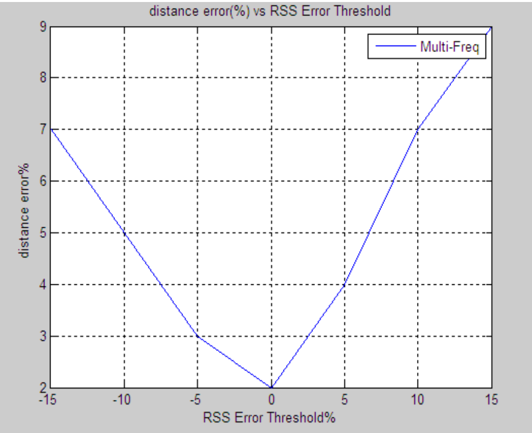

Figure 14: The Accuracy In The Attack Error Estimation For Different RSS Error Threshold Values.

The localization error also depends on the shape and dimension of the attack barrier introduced in the network. We introduced a rectangular barrier of various dimension and measured the localization error as shown in Figure 15.

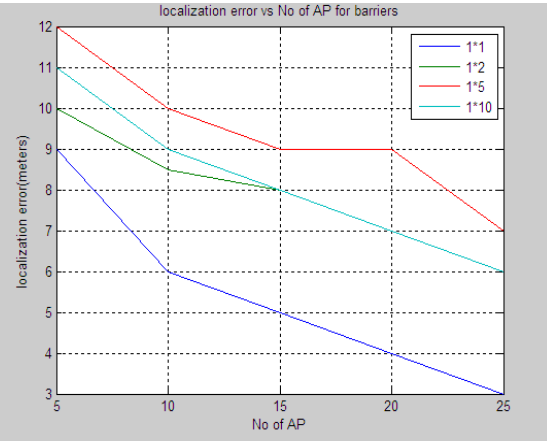

Figure 15:The Effect Of The Shape And Dimension Of The Attack Barrier On The Localization Error.

From the results, we see that initially when the barrier size increases error also increases, but after a certain amount increasing of the threshold the error increasing is very low.

7. CONCLUSION

This paper presents the robust range based RSSI localization algorithm in the presence of barrier attacks. These attacks affecting on the localization process to make it erroneous. The proposed algorithm based on multiple frequencies and power levels including lateration based and fingerprint matching showed efficient and accurate localization technique for wireless sensor network. Also in this paper the detection and identification of the attack area has been achieved through applying a grid coloring algorithm with the aid of the angle of arrival of the received signal from the access points (APs) and the suitable choice of the threshold error value between the actual and the estimated received signal strength. By identifying the attack area, the network operators take action to clear this attack and improve the localization accuracy .Through simulation results we have proved the effectiveness of our approach.

REFRENCES:

[1] Youssef A, Youssef M. "A Taxonomy of Localization Schemes for Wireless Sensor Networks" ,International Conference on Wireless Networks (ICWN'07). Las Vegas, Nevada, 2007,pp. 25–28.

[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] Afzal S. " A Review of Localization Techniques for Wireless Sensor Networks", Journal of Basic and Applied Scientific Research, vol. 2, 2012, pp.7795–7801.

[4] Wang, J. etal" A survey on sensor localization", J. Control Theory Appl.,vol. 8,2010, pp2–11.

[5] Javad Rezazadeh etal. "Fundamental Metrics for Wireless Sensor Networks localization" , International Journal of Electrical and Computer Engineering (IJECE), Vol.2, No.4,2012, pp452-455.

[6] Zàruba, G. V. et al "Indoor location tracking using RSSI readings from a single Wi-Fi access point", Wireless Networks, vol.13,no. 2, 2006, pp221–235.

[7] 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, vol. 5, 2009, pp. 1–37.

[8] Jie Yang nd Ying Y. C. "Toward attack-resistant localization under infrastructure attacks", Security and Communication Networks, vol.5 , no. 4,2011, pp. 384–403.

[9] Neve KN, Phegade SG, Kirange DY." Secure Localization: The Review on Possible Attacks of WSN and Their Remedy". Int. J. Eng. Res. Technol.,vol.2, no. 8, 2013, pp. 2085–2090.

[10] Zhu WT, Xiang Y, Zhou J, Deng RH, Bao F. "Secure localization with attack detection in wireless sensor networks". Int. J. Inf. Secur.,vol. 10 , no. 3, 2011, pp. 155–171.

[11] Li,.Z etal "Robust statistical methods for securing wireless localization in sensor network",Proceedings of the Fourth International Symposium on InformationbProcessing in Sensor neetwork, October 2005 , pp. 91-98.

[12] Chen Y., Yang J., Member S., Trappe W.and M artin, R. P." Detecting and Localizing Identity-Based Attacks in Wireless and Sensor Networks",IEEE Transactions on vehicular Technology, vol. 59 , no. 5, 2010, pp. 2418–2434.

[13] Población A." Performance of Robust Algorithms for Secure Localization in Wireless Sensor Networks", International Conference on Localization and GNSS, vol.1, no.4, 2012, pp. 25-27.

[14] Lazos L. and Poovendran R. " SeRLoc : Robust Localization for Wireless Sensor Networks", ACM Transactions on Sensor Networks, vol. 1, no.1, 2005, pp. 73–100.

[15] Lazos, L. , Poovendran R." HiRLoc: high-resolution robust localization for wireless sensor networks", IEEE J. Sel. Areas Commun., vol. 24 , no. 2, 2006, pp. 233–246 .

[16] Capkun S.and Hubaux J."Secure positioning of wireless devices with application to sensor networks", Proc. IEEE 24th Annu. It. Conf. IEEE Comput. Commun. Soc. , vol. 3, 2005, pp. 13-17.

[17] Guangjie H.,Jinfang J., Lei S., mohsen G. and Shojiro N. " A Two-Step Secure Localization for Wireless Sensor Networks" , The computer Journal, vol. 56, no. 10,2012, pp. 1154–1166.

[18] Li X. , Chen Y. , Yang J. and Zheng X. "Achieving robust wireless localization resilient to signal strength attacks. Wireessl Networks" , vol. 18 , no. 1, 2012 ,pp.45–58.

[19] 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., 2010, pp. 156–165.

[20] Jadliwala M. , Upadhyaya S. J. and Hubaux J. " Secure Distance-Based Localization in the Presence of Cheating Beacon Nodes", IEEE Trans. Mob. Comput., vol. 9 , no.6, 2010 , pp. 810–823.

[21] 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), vol.1, no.4, 2010, pp. 23-25.

[22] Alrajeh, N. A., Bashir, M.and Shams B." Localization Techniques in Wireless Sensor Networks", Int. J. Distrib. Sens. Networks , 2013, 1–9.

[23] Keun Rhee , Jaehan Lee, Jangsub Kim, Erchin Serpedin and Yik-Chung Wu"Clock Synchronization in Wireless Sensor Networks: An Overview",Sensors,vol. 9,2009,pp.56-85.

[24] Shiu Kuma, Yeonwoo Lee, and Seong Ro Lee " Time Synchronization in Wireless Sensor Networks: Estimating Packet Delay", Proceedings, The 1st International Conference on Convergence and it's Application ICCA, vol. 24, 2013, pp. 68-71.

[25] Iqbal, Murshed, M. " Attack-Resistant Sensor Localization under Realistic Wireless Signal Fading", Wireless Communications and Networking Conference (WCNC), vol.1, no.6 , 2010, pp. 18-21.