THROUGHPUT ENHANCEMENT OF WIRELESS SENSOR NETWORK LOCALIZATION ACCURACY AGAINST JAMMING 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

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 wireless sensor network. Since the wireless sensor network is a shared medium, jamming attacks can be launched by adversary emitting the radio frequency signal. Therefore jamming attacks affect the localization process. Range based methods like received signal strength indication (RSSI) is affected a lot by physical jamming attacks. This paper proposes a solution based on modified multi frequency multi power antenna to provide robust and accurate localization technique .In this paper continuous, random and capture and replay jammers are be simulated to test the localization accuracy of the RSSI algorithm However the access point sends beacons in different frequencies and jammer cannot jam all the frequencies, sensor nodes will be able to receive beacons in spite of the existence of continuous and random jammer. The only problem now is with capture and replay jammer. So that this paper proposes a set of filters to eliminate the replayed beacons The simulation results showed a powerful and improvement in the localization accuracy against jamming attacks through detecting , filtering and eliminating the effect of these attacks.

Keywords: *Wireless Sensor Network, Received Signal Stregnth Indicator (RSSI) ,Trilateration Technique , Jamming Attacks, Localization Accuracy.*

1. INTRODUCTION

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 millitary applications the broad spectrum of wireless sensors is deployed for the purpose of survaillance , exploration and other applications. Information obtained via the monitoring of environmenta 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 ,intrussion , inveatory management , exploration and survielliance .In enterprise domain, facilities have to be delivered to places on need. Accurate position of sensor is important for the success of these applications [1,2]

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 .In wireless sensor networks various methods are used for performing localization. These localization techniques are broadly represented by two categories range based and range free methods. The first method applies complete node to node range estimates (e.g. distance or angle) for estimating location. Range-free algorithms employ other methods to approach the localization problems (e.g. using the hop-count between two nodes as an estimate of the distance between them). Range-based algorithms are generally more accurate because they use physical quantities in measuring distances more accurately [3].

Out of many range based localization mechanisms like Received Signal Strength (RSS), Time of Arrival(TOA), Angel of Arrival(AOA) , RSS is best because we can reuse the existing wireless network without requiring specialized devices such as ultra sound and infrared. This results in cost savings. All of the current radio technologies like 802.11, 802.15.4, Bluetooth have support for RSS measurement [4].

The location of sensors is important for many wireless sensor applications. One of the main challenge in localization is that the process can be made erroneous by launching various attacks.

Radio interference attacks can be easily launched on wireless sensor network because of its shared nature of medium. An adversary continuously transmits on the wireless channel and disrupts the Localization services. The intrusion with an appropriate wireless communication systems is the main goal of the jamming sensor attacks. Many types of these attacks are possible in the wireless networks. Localization methods using range based methods like RSS is severely affected by jamming attacks. The jammer transmits radio waves to the sensor and makes the distance method erroneous which relies on signal from the known anchors for RSS measurement [4].

There are very few works on localization under jamming attack which focusing on locating the jammer or finding the presence of jammer in the wireless sensor network. However most of the previous works investigation related to the wireless sensor network localization over a jamming attack environment emphasized on a certain direction refers to locate or deactivate the jammers with a view to achieve a proper action or alarm the network system.While a few works focused on the location of the sensor in the presence of jamming attacks through using the jammers information itself to locate the sensors, moreover using a proactive and countermeasures techniques against jamming attacks for the wireless sensor network localization .

The essential direction indicated in this paper differs from the previous works by virtue of detecting filtering and eliminating the jammer influence, meanwhile in furtherance of improving localization accuracy for the wireless sensor network.

The goal of this paper is to avoid and overcome the effects of the jamming attacks through using multiple frequency multiple power localization (MFMPL) technique supported by a set of filters in order to enhance the location accuracy for the sensor nodes in the wireless sensor network .

Rest of this paper is outlined into these sections: background details in section two , the related works in section three, the current problem statement in section four . the proposed solution is explained in details in section five, the Performance analysis is given in section six and finally the conclusion is given in section seven.

2. BACKGROUND

2.1 Range Based Received Signal Strength Indicator (RSSI) Technique

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].

Estimating node-to-node distances or angles is called ranging.Latest studies , classify the localization methods 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 [5]. The taxonomy of range based localization methods is shown in Figure 1 .

Wide set of algorithms are commonely using the signal strength in their location estimation getting the advantages 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 , also the measuring capability of recieved signal stregnth is the important feature of most wireless devices [4] . In addition this feature shows enormus saving in costs over prevailing localization particular hardware [6].

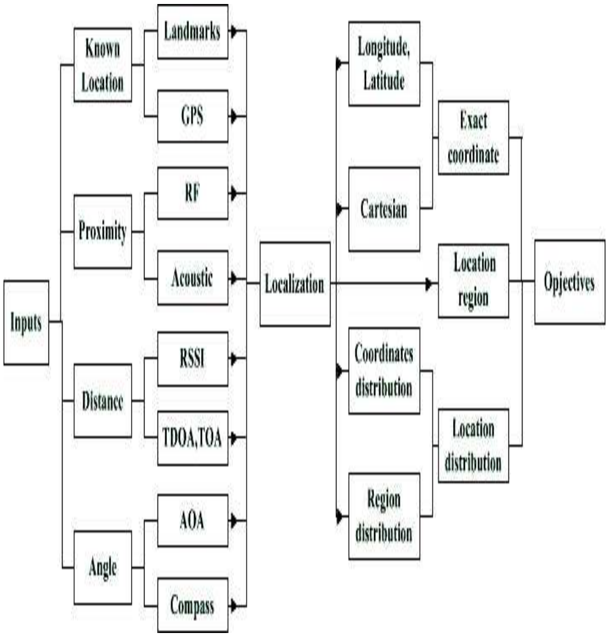

Figure 1: The taxonomy of range based localization methods.

2.2 Trilateration Range Combining Technique

The moment that a position exploration algorithm measures ranges to the other anchor nodes , it attempts to use the measured ranges for estimating the location of the sensor node. The intersection of a three circles can be considerate to locate the sensor node position through applying the trilateration technique as illustrated in Figure 2 . Whether there is any discrepancy, the intersection of the three circles result in two or more points [7].

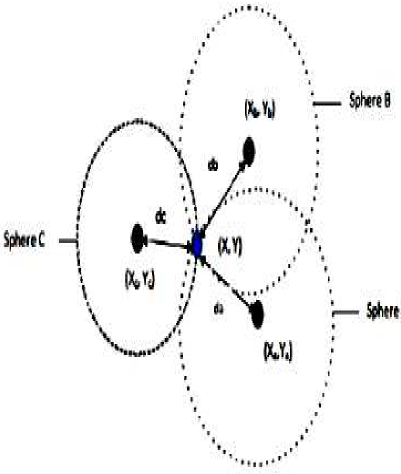

Figure 2: Trilateration :Intersection of three sphere in 2 D

Suppose a ranges of three points will well known positions are given , the equations of the system can be found as follow:

$$(x_i - x_u)^2 + (y_i - y_u)^2 = r_i^2 \text{ for } i = 1, \ldots, 3 \qquad (1)$$

where
(xi,yi) : Anchor coordinates for I = 1,2,3.
ri : Range to anchor i.
(xu, yu) : unknown node coordinates .

Now we get three equations for i = 1,2,3

By subtracting eqation (3) from equation (1) and (2) we get :

$$(x_1 - x_u)^2 - (x_3 - x_u)^2 + (y_1 - y_u)^2 - (y_3 - y_u)^2 = r_1^2 - r_3^2 \qquad (2)$$

$$(x_2 - x_u)^2 - (x_3 - x_u)^2 + (y_2 - y_u)^2 - (y_2 - y_u)^2 = r_2^2 - r_3^2 \qquad (3)$$

Rearranging equation (2) and (3) in terms of a linear way for (xu, yu) we get:

$$2(x_3 - x_1)x_u + 2(y_3 - y_1)y_u = (r_1^2 - r_3^2) - (x_1^2 - x_3^2) - (y_1^2 - y_3^2) \qquad (4)$$

$$2(x_3 - x_2)x_u + 2(y_3 - y_2)y_u = (r_2^2 - r_3^2) - (x_2^2 - x_3^2) - (y_2^2 - y_3^2) \qquad (5)$$

Rewriting equation (4) and (5) to get the coordinate of the nodes (xu, yu)

$$2\begin{bmatrix} x_3 - x_1 & y_3 - y_1 \\ x_3 - x_2 & y_3 - y_2 \end{bmatrix} \begin{bmatrix} x_u \\ y_u \end{bmatrix} = \begin{bmatrix} (r_1^2 - r_3^2) - (x_1^2 - x_3^2) - (y_1^2 - y_3^2) \\ (r_2^2 - r_3^2) - (x_2^2 - x_3^2) - (y_2^2 - y_3^2) \end{bmatrix} \qquad (6)$$

2.3 Jamming Sensor Attack Strategies

The overlapping of wireless communication systems can be achieved through different jamming strategies. Based on the jamming methods jammers are classified into following [8,9].

- Constant Jammer: This kind of jammers continuously emits a radio signal.

- Deceptive Jammer: This type of jammers insert a typical packets continually into the transmission channel without any gap among these packets . As a consequence , an ordinary communication will be duped and trusting that there is an appropraite packets so that it will cheating the receiver to continue receive these fake packets.

- Random Jammer: This kind of jammers continuously alternate between jamming and sleep cycle. The operation of this jammers is to inject a packets into the channel for a certain time tj after that it will switched off it's radio and sleep for a time ts .

- Reactive Jammer: This kind of jammers remains silent through the idle status of the channel and will sending packets directly after the sensing of the channel activity .

3. RELATED WORK

Several schemes have been proposed for the localization techniques , while most of these works focus on the location of jammer or detecting the presence of jammer.

A Virtual Force Iterative Localization (VFIL) algorithm [10] has been proposed to find the location of the jammer. This work uses the network topology information to get the approximate location of the jammer.

K.Pelechrinis [11] presented a light weight jamming detection method based on packet delivery ratio. They used gradient descent minimization based scheme to locate the jammer. This approach is based on assumption that sensor nodes location is already known and the jammer location must be identified.

Both of the works [10] and [11] does not consider localization of sensor nodes under the influence of jammer. These works can be used only for checking if the localization using lateration or other techniques is affected due to presence of jammer.

Yu Seung Kim [12] proposed a scheme to locate the position of the sensor node by getting the benefits of jamming attacks for the network.in the first step , this work employing the power adaptation technique to locate the jammer and utilize these characteristics to localize the sensor node. The assumption of this approach is based on a high transmission power for the sensor node which is not always the case for energy constrained sensor nodes.

An efficient scheme for deactivating the jammed nodes for reactive jammers was proposed in [13]. The main concept of this work is based on the consideration of the received signal strength and the packet delivery ratio investigation to determine the sufferer sensor nodes in the network and then arranged these nodes in to a various verification units.Once the group verification program is done by the base station and transferred to all victims nodes , a trigger or non trigger of the verification will be classified. The outcome of the classification process can be gathered and used to localize the jammer position. The base station sets the classified trigger nodes to the checking status , so that the trigger nodes will transmit beacon signals till the jammer node energy does not have the ability of the deactivation. But localization of sensor node is not considered in this work.

Aristides Mpitziopoulos and Damianos Gavalas [14] proposed an approach based on frequency hopping spread spectrum (FHSS) and direct sequence spread spectrum (DSSS), where both of them are considered to be a powerful corrective techniques against jamming . The main concept of this work is to employ the channel diversity by the jammer nodes in consideration of providing the communication with the other nodes out of the jammed region. But this approach is proposed for the case of routing and localization is not considered.

Liu D. [15] proposed a two mechanisms for range based localization algorithm in order to stan for the malicious attacks. The first mechanism is using the fundamental of identification to separate the malicious node signals from various beacon signals . As long as the second mechanism separates the malicious beacon signal by approving iterative voting strategy . Both of these two mechanisms can be out of malicious attacks in spite of the attackers can be avoid the authentication, on the condition of that most of the beacon signal in the network should be benign. These solutions work for the case if the anchor node is jammed, but if the jamming attacker is disrupting the beacon signals these solutions fails.

A non-iterative algorithm to localize a jammer has been presented in [16], this work takes the advantage of schedule differences for the node's neighbor which is induced by the jamming attacks . But this work requires each node must be knows its neighbors but in the network model in which we work, a random distribution is used for the sensor nodes in the network region, so the neighbor list at each node is not possible to be kept.

Zhenhua Liu [17] proposed a method to find the position of the jamming sensor node straight way through the jamming signal strength (JSS). The determination of JSS is a big challenge because of it will be a part of other interference signals . This approach devised an estimation mechanism depend on the ambient noise to filter out the JSS. But the work focuses on localizing the jammer and not the sensor nodes.

4. PROBLEM STATEMENT

Jammer transmit radio signal in their configured frequency range and disrupt the beacon packets from reaching the sensor nodes. Every sensor node must receive a minimum of three beacons from different access points for localization of sensor node through applying a trilateration technique. The objective of the proposed system is to detect jamming beacons attack and eliminate these invalid beacons , inorder to enable each sensor node to receive a minimum of three valid beacons from different anchors / access points.

5. PROPOSED SOLUTION

5.1 Overview of the Proposed Solution

We propose a solution based on multi frequency multi power transmission. All the sensors are already coded with the knowledge on expected frequencies and the power level from the AP. The proposed scheme can be overcome the effect of the constant and random jamming because of these two types of jamming sensors can be broadcasting in only one frequency range and will jam the packets sent in that frequency range. In order to avoid the estimation getting affected by interference caused by capture and reply jamming sensor which is the more dangerous type of jamming attacks we propose a technique to filter out those invalid beacons by using a three stages of filters.Therefore the received beacons will be checked by the frequency filter , power level filter and duplicated filter to remove the replyed beacons and this will be lead to improve the localization accuracy.

5.2 *Network and Adversary Model*

In this network system model, a sensor node N exists in a non trust worthy medium needs to determine its own position through the distance estimation to a group of anchors/access points(APs). Multi frequency Multi power access point devices whose locations are known are deployed in the network. Each access point transmits beacon signal consistently including it's position coordinates (x, y) with a multiple frequency and power transmission.The sensors will receive these beacons from these APs and construct it's location refference (x , y , d') , where d' is the distance range from the sensor to the APs which can be estimated from the received signal strength (RSS) . Once a location refference of a three valid beacons are constructed the sensor position can be estimated by using trilateration technique.

All the sensor nodes and the access point nodes are 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 [18,19].

There are some jammers placed randomly in the network. A uniform power strength antenna is supplied to the jammer node . The coverage area of the jammer node transmission can be considered as a circle fixed at the point of the jammer node, when the fact that the transmission range of the jammer node should be wider than the range of the sensor node . Figure 3 shows a network with AP's, sensors and the jamming sensors. To simulate an influential and fuctional jamming sensor nodes system ,there are a three kinds of jammers in the network.

1. Continous jammer
2. Random jammer
3. Capture and replay jammer

Each jammer work in only one frequency range and will jam the packets sent in that frequency range. Capture and replay jammer will capture the beacon packets and continuously jam the network with those beacons. By this way, sensors taking these beacons and using this for localization will calculate their position inaccurately. This attack is more dangerous and can make the entire localization process erroneous.So that the effect of this jammer must also be stopped.

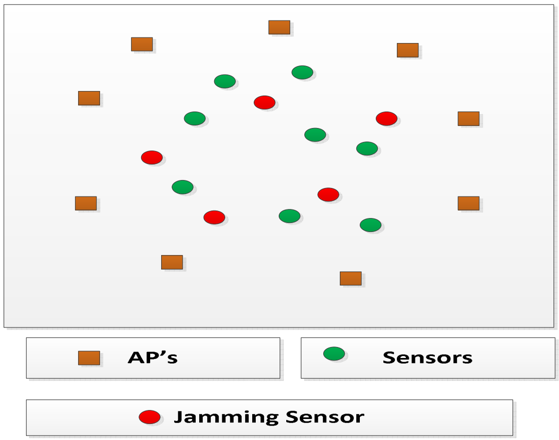

Figure 3: Network System Model

5.3 Proposed System Based on Multi frequency Multi power Localization (MFMPL) Approch

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. 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 jamming in the path of the signal.

Trilateration 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 , three stages of filters are found. Figure 4 shows the functional block diagram of the proposed solution.

The proposed solution Multi Freq Multi Power Localization (MFMPL) consist of two phases:

1. Initialization phase
2. Localization phase

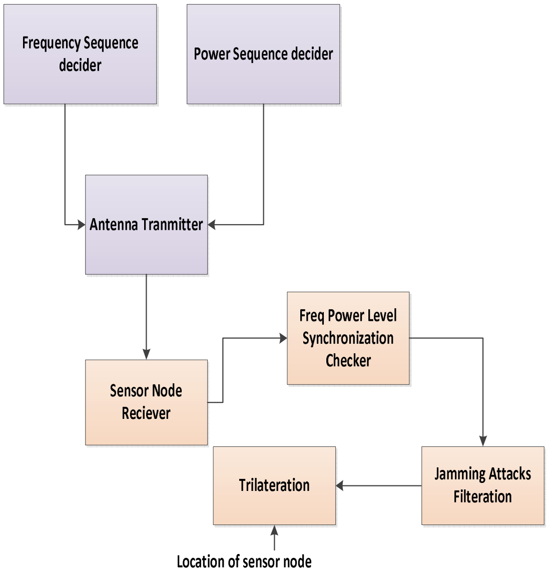

Figure 4: The functional block diagram of the proposed solution .

1. Initialization phase

In Initialization phase, each access point will choose a random seed and using it to design a frequency calculation function.

$$Freq(t) = F\ (t,St(seed)) \qquad (7)$$

Frequency calculation function is a function of this random seed at the current time. The frequency calculation function will return the frequency at which the access point must send the beacon in that time. St is the seed generation function which generates the seed at a particular time stand on the present time and the initial seed value.

The function F, St, initial seed for each access point is kept in secure memory area of sensor nodes so it is difficult for attackers to know these values.

The access point node also transmits in different power levels in a sequential pattern. The sensor node must know the number of power level in advance.

Each AP (access point) is assigned by a function of frequency and power level in a step wise over the possible values of transmission. The step function with in a step duration is kept different for different AP's. A sample of a step function is shown in Figure 5 . This function has three values a,b,c representing the frequency and power level for the transmission. 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.

$$f(t) = \begin{cases} a & 0 \le t \le 3T \\ b & 3T < t \le 7T \\ c & 7T < t \le 8T \end{cases} \qquad (8)$$

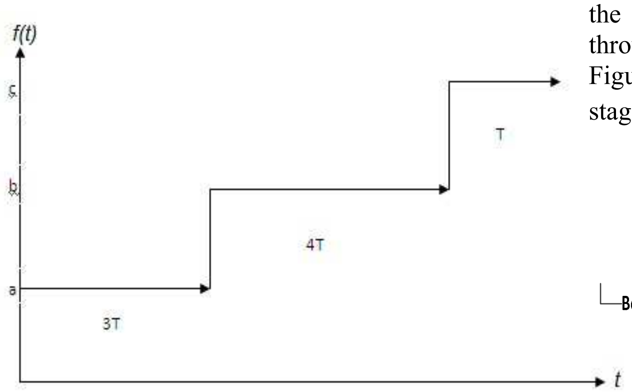

Figure 5:A step function for a frequency and power decider .

Using this function, the current frequency and power at which the APs transmit the signal can be known at any sensor node.

2. Localization phase

Localization involves two stages ranging and trilateration. Ranging estimates the distance d from the position of the sensor node to the AP .RSS can be expressed as shown in equation (9).

$$RSS = Po - 10\ \alpha \log_{10} d \qquad (9)$$

Therefore the distance can be determined from equation (10) as follow:

$$d = 10^{(Po - RSS / 10*\alpha)} \qquad (10)$$

Where

Po - is the power received in dBm at 1m distance.

d - distance between node and the AP.

α – is the path loss component.

In the localization phase, each sensor will receive beacons from different access points. Since the access point sends beacons in different frequencies and jammer cannot jam all the frequencies, sensor nodes will receive beacons even in spite of presence of continuous and random jammer. The only problem now is with capture and replay jammer.

Valid beacons from the access points will be captured and replayed by jammer. This will affect the distance calculation using RSS and the effect is cascaded to location estimation. For this problem we propose a set of filtering techniques at the sensor nodes. Whenever the sensor node receives the beacons it will be forwarded consistently through these filters to drop the replayed beacons. Figure 6 show the block diagram of the filtering stages.

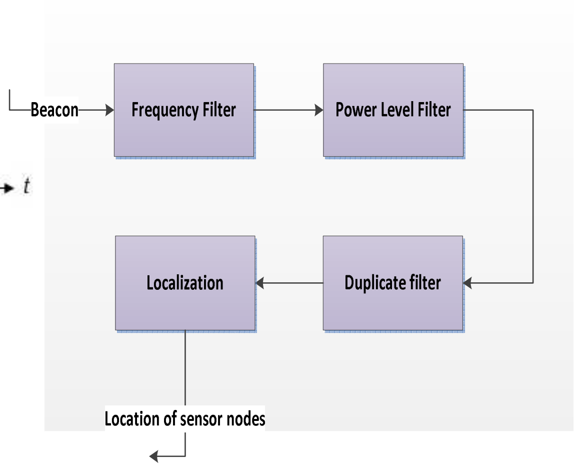

Figure 6: Proposed beacon signal filters technique.

Frequency Filter: This filter will estimate the frequency of transmission for the access point and match it with the frequency of the received beacon from the access point.

$$ESS = \text{Estimated Frequency} - \text{Actual Frequency} \qquad (11)$$

Non zero ESS value indicates error and the beacon will be dropped.

Power Filter: When the frequency validated beacons comes to Power filter, the received signal strength is calculated and the packet is buffered. For the subsequent beacon from the access point, the power level is checked for lying in proportion with respect to the power level. The beacons not in proportion to the power level are just dropped and one packet passing the power level test is given to the duplicate filter.

Duplicate filter: If one more than one valid beacon is received from same access point only one is kept and other is dropped. When three different beacons are received, the received beacon is given to the localization component.

Localization: Using the beacons from three different anchor points, the localization module will extract the location of the anchor points from the beacons and estimate the distance to the anchor points using the RSS value. With this information, we can apply the trilateration to determine the sensor nodes position.
The algorithm code for the proposed solution is given below:

Algorithm: Proposed Solution

```
1) APs send beacons with multi frequency and
   power levels
2) Sensor received beacons from APs
3) Beacons will be pass to frequency filter
    Calculate
 ESS = Estimated frequency – Actual frequency
      If  $ESS \neq 0$
      Then  drop this beacon
      Else  ESS =0  Go to power level filter
4) Sensor calculate RSS for received beacons
   and packet is buffered
    Drop beacons that is not within the
   propotion level
    Keep the other beacons
    Go to duplicated filter
5) If  more than one valid beacon received from
   the same AP
    Then only one is kept and drop the other
6) Three valid beacons received from different
   APs
7) Do localization by trilateration technique
8) Estimate the location of the sensor
    End
```

6. PERFORMANCE ANALYSIS

We simulated the proposed solution in MATLAB. A two dimensional terrain with 1000 * 1000 m is applied for the network area simulation. We suppose a few but logical number for a beacon nodes distribution of 20 access point (almost 5 in each direction), These APs dispersed in a uniform distribution over an area of 1000 * 1000 m.There are 15 jammers and 100 sensor nodes placed randomly in the network. The localization must be done for these sensor nodes. Table 1 shows the system model specification.

Table 1 : System Model Specification

Network Area	1000 * 1000 m
No of sensor	100
No of APs	20
No. of random jammers	2-5
No. of continuous jammers	2-5
No. of capture replay jammer	2-5
Frequency Used by AP	400, 600,800 MHZ
Power Used by AP	2, 4,6, 8 dB
Sensor and jammer nodes Placement	Random
Radio signal propagation	Free space

The average localization error is calculated between the actual and the estimated locations for all sensor nodes. The average localization error is applied to determine the performance measurement by varying the number of jammers in the network as shown in Figure 7. We compare the performance with TMT technique [20].

In the TMT technique, the localization error increases at faster phase when compared to our solution. The reason for error reduction is due the proposed filtering logic at the sensor nodes and most sensor nodes are able to receive beacons for localization.

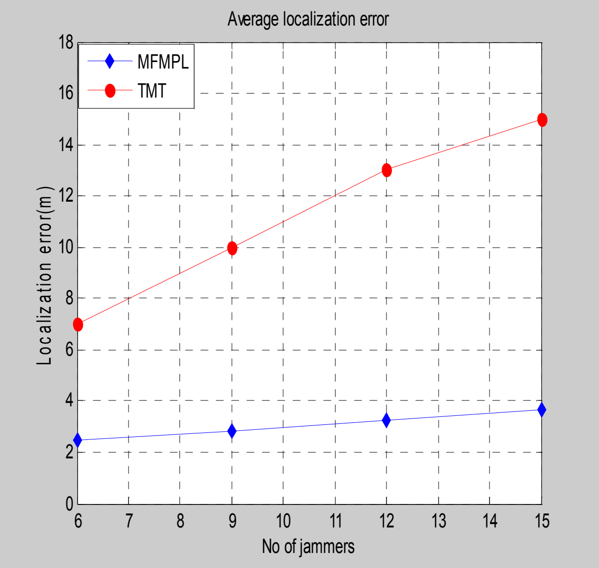

Figure 7. Average localization error for different number of jammers.

We increased the number of jammers and measure the availability of beacons for localization process as shown in Figure 8. We observe that while increasing the number of jammers then the number of sensor nodes for which beacons are available for localization in TMT technique depletes faster but in our approach it is almost constant.

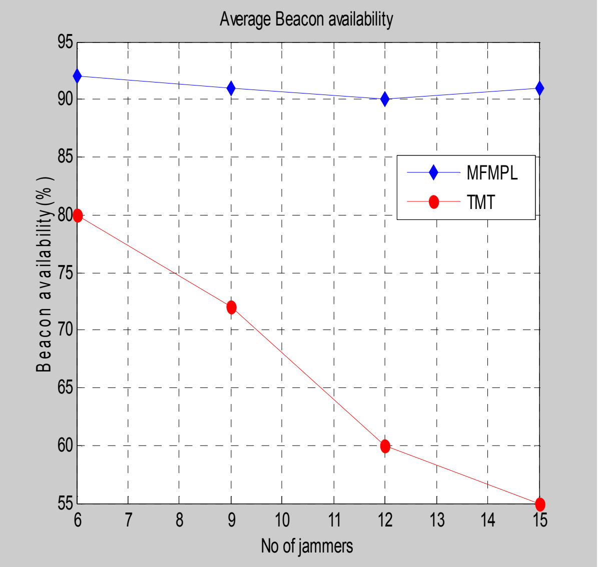

Figure 8. Average beacon availability for different number of jammers.

Figure 9 shows another important performance metric is the accuracy of dropping the invalid beacon packets. This accuracy is measured in terms of drop ratio by increasing the number of jammers.

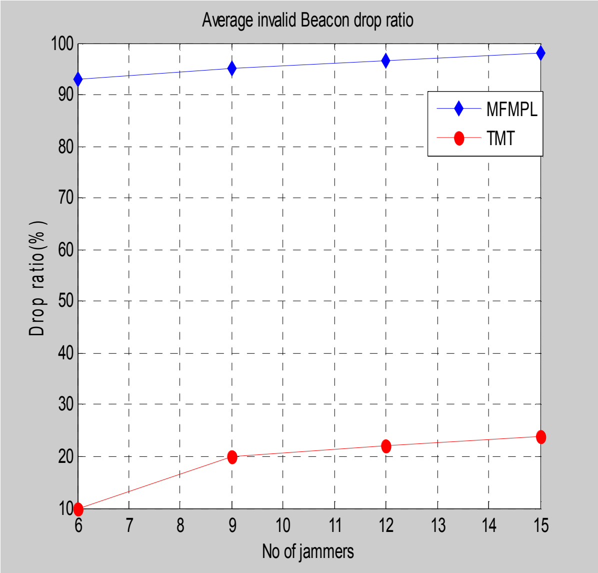

Figure 9. Average invalid beacon drop ratio.

We see that as the number of capture and replay jammer increases more number of invalid beacons will appear in the network and drop ratio is very high in our approach contributing to lesser localization error.

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 and measured the localization error as shown in Figure 10. we observed that localization error is reduced at the 100% increasing which is twice the base frequency.

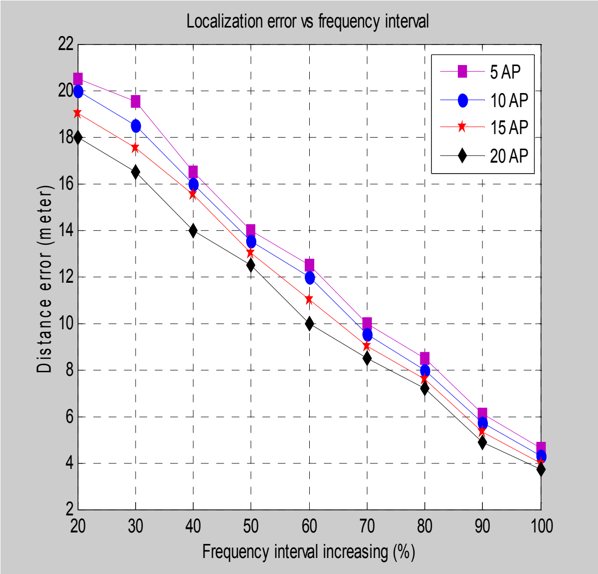

Figure 10. Localization error with different frequency interval percentage.

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

Another important parameter affecting on the localization accuracy is the number of the access points (APs) in the network . However , the placement and number of the anchors / access points (APs) in the network play a significant parameter for localization process . In fact more numbers of the access points that being deployed in the network will leads to accurate and efficient results for the location of each sensor.

The simulation results for our approach (MFMPL) showed an accurate and powerful localization accuracy with minimal number of APs as compared to TMT technique . Figure 11 illustarte the localization accuracy for different access points (APs) for both (MFMPL) and TMT techniques .

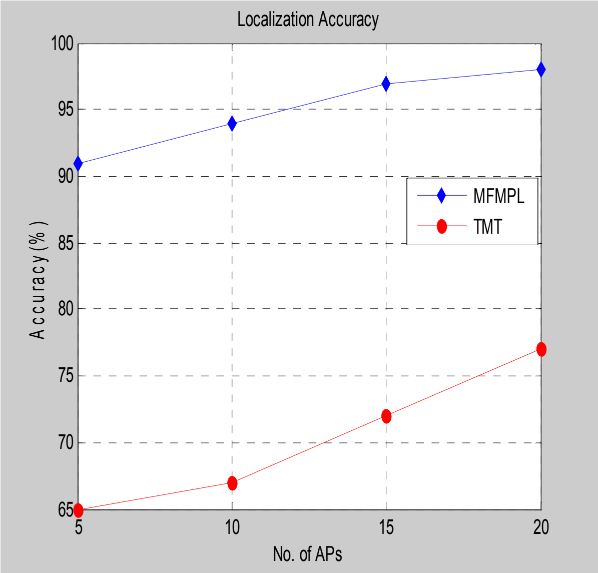

Figure 11. Localization accuracy versus number of APs.

We measured the localization error percentage for different signal degradation by the jamming attackers. The signal degradation is varied from 40% to 80 % of the original signal from the AP as shown in Figure 12.

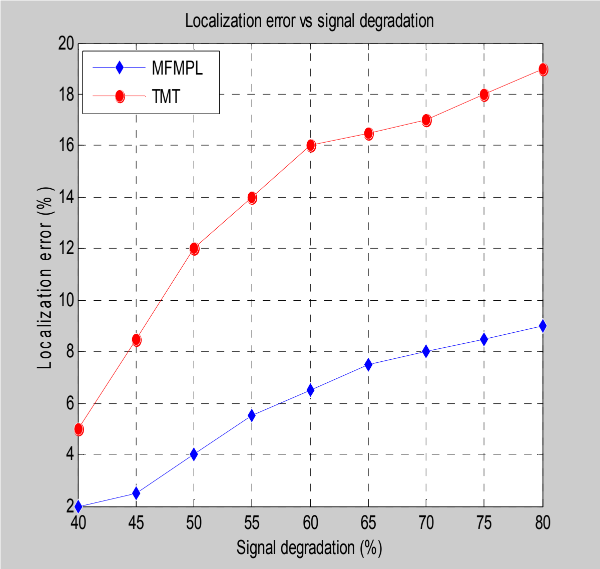

Figure. 12 The effect of signal degradation on the Localization accuracy.

.

From the results, we see that as the signal degradation increases our proposed multi frequency multi power localization (MFMPL) performs better than the TMT method.

7. CONCLUSION

This paper presents the robust range based RSSI localization algorithm in the presence of jamming attacks. The jamming attacks have a deep effect on the communication process and the localization procedure to make it erroneous. The proposed algorithm based on multiple frequencies and power levels transmission including trilateration based showed efficient and accurate localization technique for wireless sensor network.

In fact of continous and random jammers can broadcasting signals in only single frequency range, therfore the proposed scheme based on multi frequency range transmission is able to overcome the effect of these jammers . Also in this paper the high accuracy of the proposed filtering technique showed a crucial and powerful results to drop the invalid received beacon packets caused by capture and replay jamming attacks which is definitely leads to minimize the error in the localization process and improve the accuracy of the sensor position estimation. Through simulation results we have proved the effectiveness of our approach.

The future work directions in the simulation for testing our approach will take into consideration the improvement of the localization accuracy under log normal shadowing environment besides the jamming attacks.

REFRENCES:

[1] Reza Zekavat , R. Michael Buehrer, " Handbook of Position Location: Theory, Practice and Advances " , John Wiley and Sons, october 2011.

[2] Chee-Yee Chong; Kumar, S.P., "Sensor networks: evolution, opportunities, and challenges," Proceedings of the IEEE , vol.91, no.8, 2003, pp. 1247-1256.

[3] Wang, J. , Ghosh R. K. and Das S. K., " A survey on sensor localization" , J. Control Theory Appl., vol 8, 2010, pp. 2–11 .

[4] Mao G .and Fidan B. , " Localization Algorithms and Strategies for Wireless Sensor Networks" ,United States of America by Information Science Reference IGI Global ,2009.

[5] 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

[6] XuYang Ding; Hai Zhao; Jian Zhu; Kuan Zhang; DaZhou Li, "A Novel Localization Algorithm Based on RSSI for Wireless Sensor Networks," Wireless Communications, Networking and Mobile Computing (WiCOM), 2011 7th International Conference on , vol. 1, no. 4, 2011, pp. 23-25.

[7] Oguejiofor O.S, Aniedu A.N, Ejiofor H.C, Okolibe A.U," Tilateration Based Localization Algorithm for Wireless Sensor Network ", International Journal of Science and Modern Engineering (IJISME), Vol. 1, Issue-10, 2013 , pp. 21-27.

[8] Prakash J. Parmar, Sachin D. Babar," Survey of Jamming Attacks and Techniques in Wireless Sensor Networks",INDIAN JOURNAL OF APPLIED RESEARCH, Volume : 3, Issue : 8 ,Aug 2013 .

[9] Faraz Ahsan , Ali Zahir, Sajjad Mohsin, Khalid Hussain, " Survey On Survival Approaches In Wireless Network Against Jamming Attack" . Journal of Theoretical and Applied Information Technology, vol. 30 , no. 1 ,2011, pp. 55-67 .

[10] Hongbo Liu; Wenyuan X; Yingying Chen; Zhenhua Liu, "Localizing jammers in wireless networks," Pervasive Computing and Communications, 2009. PerCom 2009. IEEE International Conference , 2009, pp.1-6.

[11] Pelechrinis, K.; Koutsopoulos, I; Broustis, I; Krishnamurthy, S.V., "Lightweight Jammer Localization in Wireless Networks: System Design and Implementation," Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE ,2009, pp.1-6.

[12] Yu Seung Kim; Mokaya, F.; Chen, E.; Tague, P., "All your jammers belong to us — Localization of wireless sensors under jamming attack," Communications (ICC), 2012 IEEE International Conference, vol. 949, no. 954, 10-15.

[13] Supreetha Patel, K.N. Sereen A. "An Energy Effcient Deactivation Technique For Reactive Jammers In Wireless Sensor Networks".Graduate Research in Engineering and Technology (GRET) An International Journal vol. 1, no. 2, 2013.

[14] Aristides Mpitziopoulos and Damianos Gavalas , " An effective defensive node

against jamming attacks in sensor networks " , Security and Communication Networks, Security Comm. Networks, John Wiley & Sons, 2008.

[15] Liu, D.; Peng Ning; Du, W.K., "Attack-resistant location estimation in sensor networks," Information Processing in Sensor Networks, 2005. IPSN 2005. Fourth International Symposium 2005, pp. 99,106-15.

[16] Zhenhua Liu; Hongbo Liu; Wenyuan Xu; Yingying Chen, "Exploiting Jamming-Caused Neighbor Changes for Jammer Localization," Parallel and Distributed Systems, IEEE Transactions on , vol.23, no.3, 2012, pp.547-555 .

[17] Zhenhua Liu; Hongbo Liu; Wenyuan Xu; Yingying Chen, "An Error-Minimizing Framework for Localizing Jammers in Wireless Networks," Parallel and Distributed Systems, IEEE Transactions on , vol.25, no.2, 2014, pp. 508-517 .

[18] 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 .

[19] 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 .

[20] 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.