Research on Improved DV-HOP Algorithm against Wormhole Attacks in WSN

Xue-Wen WANG[1,a],Feng HU[1],Chun-Xue ZHAI[1],Yuan ZHANG[1],Xing-Xing SU[1], Yan LI[1], Zhao-Ke WU[1], Ting-Ting LI[1] and Zhou-Hu DENG[1]

[1]*School of Information Science and Technology, Northwest University, Xi'an 710127, P. R. China*
Contacting e-mail: 815156932@qq.com
Corresponding author. Xue-Wen WANG Tel: 13488466766

Abstract. The secure location of node is significant in the WSN (Wireless Sensor Networks) of the troop frontier defence system. The wormhole attack is a big threat in the secure location. The credibility of the beacon node was used to determine the malicious nodes produced by wormhole attack in the WSN. The estimated method of multi-beacon nodes was adopted to improve DV-HOP algorithm after excluding the malicious nodes.In this paper,we compared the basic DV-HOP algorithm and the improved DV-HOP algorithm in the coverage percentage and the error of network localization by simulating. The simulation results indicate that the improved DV-HOP algorithm makes the localization coverage percentage can reach 90% on a certain scale of the network,andit makes the error percentage lower when the number of beacons is different.

1 Introduction

WSN (Wireless Sensor Networks) is a compound technology of the combination of sensor technology, wireless communication technology, embedded computer technology, network technology and so on.WSN has very significant application prospect in the troop frontier defence system. Because sensor nodes of WSN in the troop frontier defence system generally have high concealment and the advantages of high safety and reliability and its mobility, node localization is a key technology in sensor network architecture. The DV-HOPalgorithm is also the central issue of positioning technology in WSN localization technology. A series of positioning algorithm was put forward, like Centroid Algorithm, Amorphous Algorithm [1],[2] and so on. However, it cannot be applied to the complex environment of the troop frontier defence system, and it is based on the positioning technology of measuring the distance. So studying in range-free scheme against algorithms which has taken advantage of Network Connectivity or Topology Structures is considerably significant [3]. Since the DV-HOP [4],[5] (Distance Vector-Hop) algorithm has a low cost and high precision, it is a kind of algorithm in WSN which has the moderate node density and topology rules which are easy to achieve. The wormhole attack is one of the most common ways of attacks of the security problem of securing localization. This way of attack has great influence on the positioning precision, and wormhole attack even will endanger the hop counts of positioning DV–HOP algorithm and may cause data packets eavesdropping or denial of service [5], [6].So, compared with the security protocol of wireless sensor network and ultra-low power consumption routing, the research of unmanned border post information platform[7]and DV-Hop algorithm is increasingly important [8]. In this paper, in terms of theestimationof the distance between the unknown node and beacon nodes, we put forward the method to determine the wormhole attack of malicious nodes in WSN and improve the DV-HOP algorithm after the exclusion of malicious nodes.The improved algorithm enhances the precision of positioning and security after comparing the simulation results.

2 WSN in the Troop Frontier Defence System and Wormhole Attack

The WSN of the troop frontier defence system consists of sensor nodes, convergent nodes and terminals[8],[9].When the sensor nodes monitor the change of environment to the frontier, the data is transmitted by wireless transmission along the other nodes. Sensor nodes which are detected could use either single hop or multi-hop mode of communication to send their data to sink node though routing protocol for receiving and processing in the process. Data is transmitted to the terminal through the backbone network based on certain protocol configuration and management.

The wormhole attack, as atypical external attack, can be easily launched by two colluding attackers. One attacker sniffs packets of one point of the network,

tunnels them via the wormhole link to the other attacker which locates at the other point of the network. The wormhole attack affects sensor nodes from the calculation of the beacon nodes hop, forcing the packet of the path of the closer one hop (dotted line) transmission, then accuracy of fixed position can be reduced[13]. So, in the first phase, a sensor may obtain smaller hop counts to beacons. In the second phase, a beacon may calculate an incorrect hop size, which will be flooded with other nodes in the network.

Finally, each sensor may use incorrect hop counts and hop size to estimate the distances to the beacons, based on which the self-localization will be inaccurate. This paper presents an optimized algorithm whichmarked credibility of the beacon node based on DV-HOP localization algorithm.

3 DV-HOP Algorithms andimprovements

3.1 DV-HOP Algorithms

DV-HOP algorithm is a distance independent localization algorithm which is put forward on the basis of distance vectors routing principles. The basic principle is to represent the distance with the product of the average hop distance and the number of hops between the unknown nodes and beacon nodes instead of the distance between them. Then, calculate the unknown nodes coordinate using trilateration method or the method of Maximum Likelihood [10], [11]. The specific process is:

3.1.1 Calculating the Minimum Hops of the Unknown Node and Beacon Node

The beacon node sends information packets to position the nodes around, and the receiving node records the minimum number of hops from itself to each beacon node and forwards itself to its neighbors,adding 1. Thus, all nodes in the network will be able to know the minimum number of hops of each beacon node.

3.1.2 Calculating the Average Hop Distance between the Unknown Nodes and Beacon Nodes

Calculate the average hop distance between the unknown nodes and beacon nodes to broadcast it to the network when the node obtains hops beacon node by formula (1) to calculate the average of each beacon node hop distance, according to the hops of the beacon nodes to themselves and the received average jump distance, we can calculate the distance from each jump to abeacon node.

$$hopSize_i = \frac{\sum_{j \neq i} \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2}}{\sum_{j \neq i} h_i} \quad (1)$$

[Where(x_i,y_i), $(x_j,y_j)$are thebeacon node i,j coordinates, h_i is the number of hops between i and $j(j \neq i)$].

3.1.3 Calculating the Coordinates of Nodes

We can get the jump distance from the second step to each anchor node, and then calculate its own coordinates bytrilateration or maximum likelihood estimation method.

DV-HOP algorithm can position with theinformation of the multi-hop beacon nodes. We cannot consider the attack of malicious nodes on the network during positioning,resulting in positioning errors.

3.2 DV-HOP Algorithm Improvements

Based on the problems, we use the estimation of multi-beacon nodes to improve the accuracy of DV-HOP algorithm. The basic principle of the multi-beacon nodes estimation method is shown in Figure 1. Assuming that the distance of unknown node A away from the nearest beacon node is B, and the node A now can estimate the unknown distance to another beacon node C, d_{AC}. Node A, B and C constitute a triangle. The distance between nodes B and Care known is as a certain value. We can get d_{AC}, the distance from A to C, from the average number of hops of beacon node B and the product of hops.

$$d_{AB} = HopSize_C \times H_1 \quad (2)$$

$$d_{AC} \approx \sqrt{d_{AB}^2 + d_{BC}^2 - \frac{H_1^2 + H_2^2 - H_3^2}{H_1 \times H_2} \times d_{AB} \times d_{BC}} \quad (3)$$

In these formulas above, HopSize$_C$is the average hop distance from the beacon node3.H_1 is the hop count from beacon node B to unknown node. H_2 is the hop count from beacon node B to C, and$H_3$is the hop count from beacon node C to unknown node A.

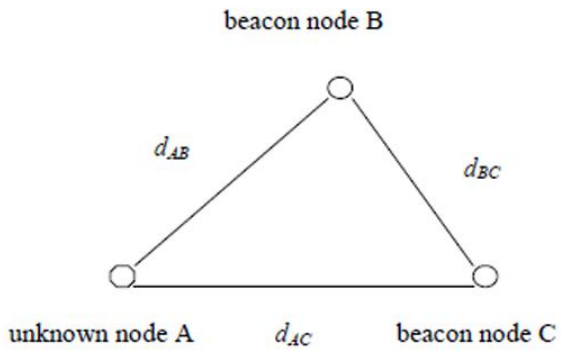

Figure 1. The Estimated Method of Multi-Beacon Nodes.

To make it meet the actual situations better, we used a method of multi-beacon nodes which based on DV-HOP algorithm[12],and corrected thefinal result with the certain valued_{BC}.

3.3 The Technology to Find Out Malicious Nodes by Using Credibility of the Beacon Node

To prevent wormhole attacks, this algorithm measured the reliability of beacon nodes when the unknown nodes located, using thecredibility of the beacon node[13],[14].If the number of nodes in sensor networks is X, there are(X-1) average hop distance (Hopsize$_{ij}$, (j=1,2,3,X))between beacon node *i* and other (X-1) nodes. After the result, which normalized the average hop distance of one single path and node *i*, is the credibility of node j relative to node *i*. The formula for calculation is as follows:

$$w_{ij}=\begin{cases}\arctan\left(\dfrac{Hopsize_i}{Hopsize_i-Hopsize_{ij}}\right)\times\dfrac{2}{\pi}, & Hopsize_i\neq Hopsize_{ij}\\ 1, & Hopsize_i=Hopsize_{ij}\end{cases}\quad(4)$$

In formula (4), $Hopsize_i$ is the average hop distance from beacon node *i*. Hopsize$_{ij}$is the hop count away from beacon node *i*to *j*. The formula is as follows:

$$Hopsize_{ij}=\frac{\sqrt{\left(x_i-x_j\right)^2+\left(y_i-y_j\right)^2}}{h_{ij}}\quad(5)$$

W_{ij}will become smallerWhen the difference between $Hopsize_i$ and $Hopsize_{ij}$ becomes larger, which shows that there are some abnormal in the path form node*i*to node *j*, compared with other paths.Therefore, the average hop distance deviation in sensor networks was raised. In this case, we consider that compared with beacon node *i*, the credibility in node *j* is not enough. When the difference between $Hopsize_i$ and $Hopsize_{ij}$ becomes smaller,W_{ij}will tend towards 1, which means that the credibility is higher this time. After locating malicious nodes and excluding them, we use other nodes to locate unknown nodes.

4 Simulation and Results

4.1 Sensor Network Model Parameters Settings

In order to focus on the research of localization algorithm and simplify the simulation model, we make MATLAB as a simulation and data processing software, which only simulates the upper positioning module. The parameters of experiment are set as follows: there are 100 sensor nodes in a100 m * 100 msregion and make them uniform distribution randomly. Each sensor node has the same communication radius R. It adjusts the average network connectivity by adjusting the node communication radius [15]. The experiment data is the average ofmany simulationexperiments. In the simulation test, we measure the performance of the localization algorithm with the following parameters and the beacon nodes density: it means the ratio of beacon nodes and all number of nodes in a network.Beacon node coordinates are known, and there is no error of the location information. The average positioning error: the pending node distance between the actual position byestimating and the real value of node location indicates the error of each node positioning. The defined positioning error of the algorithm is as follows:

$$error=\frac{\sqrt{(\hat{x}_i-x_i)^2+(\hat{y}_i-y_i)^2}}{R}\times 100\%\quad(6)$$

Where (x_i ,y_i) is the actual coordinate of a pending node, and itis the calculated coordinate of the pending node, R is the radius of a communication node. The node localization error of the node localization, compared with the simulation experiment, is the average positioning error after it runs 10 times. The fraction of coverage:we can get the ratio of the number of nodes to be located and the number of all nodes to be located.

4.2 Sensor Network Simulation Process

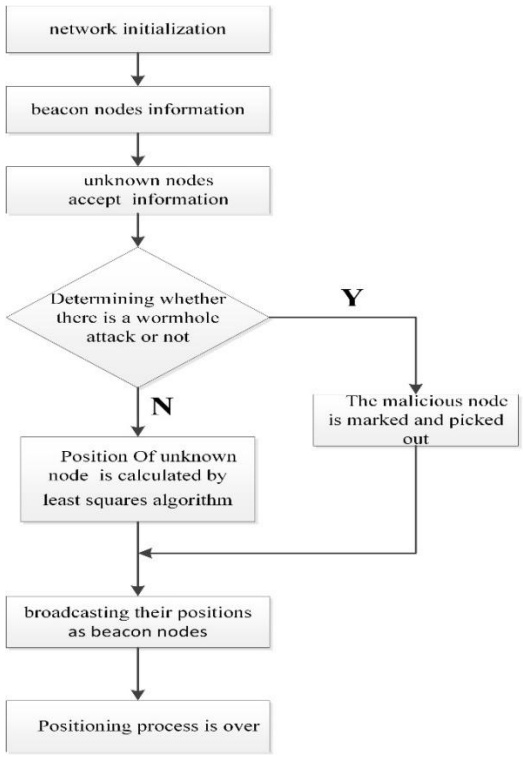

Figure2. The Process Chart of Simulation for Wsn

After the initialization of network, each beacon node will broadcast its own information on the network. When B, one of the positioned nodes, receives the broadcast information about beacon no descent by A, it will check the information if there is a wormhole attack.If there is an exsit of wormhole attack whenit broadcast information sent by the beacon node, the network will use the trust degree of beacon nodes to make sure the wormhole attack of malicious nodes and make the beacon node as a

malicious beacon node, which is excluded from the network. If there is no existence of the wormhole attack, we use the least squares method to calculate the position of the positioned node B,which makes the node B become a beacon node to continue to broadcast their own location and proceed to localise the next time.

4.3 The Analysis of Experimental Simulation Results

First of all, we compare the positioning coverage of the DV-HOP algorithm and the improved DV-HOP algorithm. If the number of the beacon node is 14,the simulation experiment performed by changing the node communication radius. The results are as follows in Figure 3, Figure 4 and Figure 5.

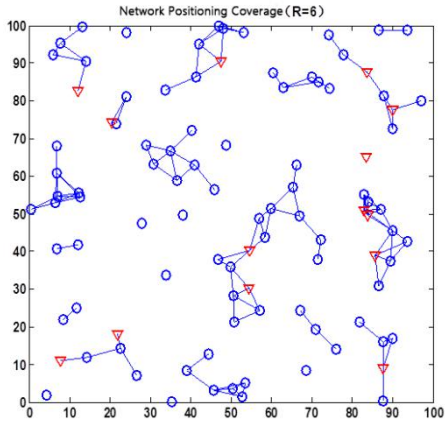

Figure 3. The Network Location Overlays Under 6-Meterradius of The Node Communication

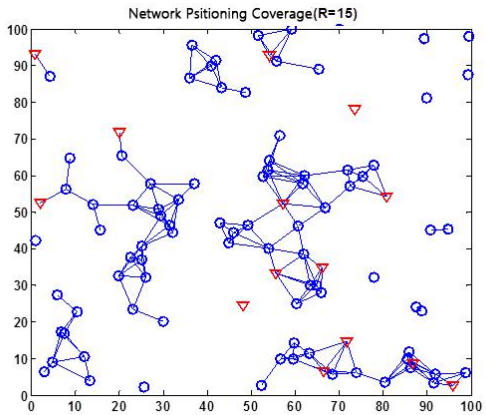

Figure 4.The Networklocation Overlays Under 15-Meter Radius of The Node Communication

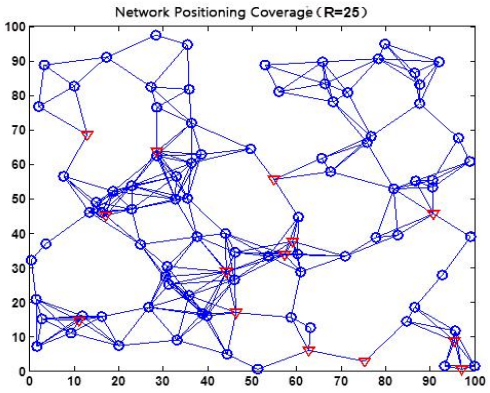

Figure 5. The Network Location Overlays Under 25-Meterradius Of The Node Communication

Figure 3, Figure 4 and Figure 5 give us the network coverage figure of the improved DV-HOP algorithm and the node communication radius of themareR=6,R=15, R=25 respectively.The red triangle represents the beacon nodes, blue circle represents the location undetermined nodes, a wired node that represents this part of the node is positioned.

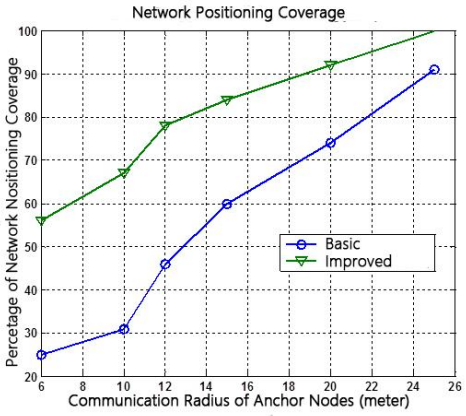

Figure 6.The Comparison Of The Positioning Coverage About The Improved Dv-Hop Algorithm And The Basic Dv-Hop Algorithm

Figure 6 shows that after the positioning coverage difference between the improved and unimproved DV-HOP algorithm under the same node communication radius, we can conclude that from the same beacon nodes, the improved algorithm is better than the basic DV-HOP algorithm in the network coverage. When the beacon node communication radius is small, the algorithm Coverage Percentage improved is nearly twice bigger than the Coverage Percentage of basic DV-HOP algorithm, and with the increase of the beacon node communication radius, the improved algorithm can quickly cover the whole network while the basic DV-HOP algorithm cannot. From the DV-HOP algorithm principle, we can know that the positioning accuracy of the algorithm is closely related to the beacon node density.

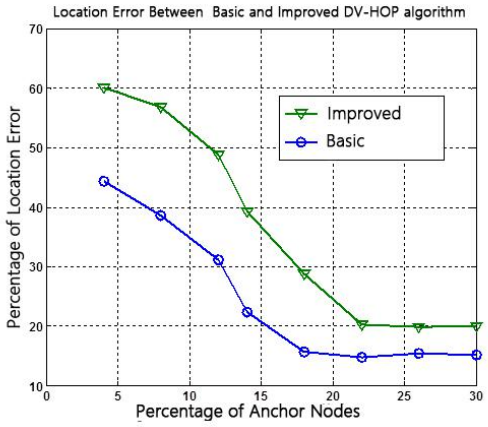

Figure 7. The Comparison About Positioning Error Of The Improved Dv-Hop Algorithm And The Basic Dv-Hop Algorithm

Figure 7 shows the relationship between the positioning error of DV-HOP algorithm and the beacon node proportion. The picture shows that when the beacon node number is 4, the average position error percentage of the DV-HOP algorithm is 60%, while the average position error percentage of the improved algorithm is 43%. As we increase the number of beacon nodes, the positioning accuracy is higher and higher. However, when the number of the beacon nodes is 22 or more, the positioning error percentageof two algorithms is kept in a relatively balanced state, the error percentage is maintained at about 20%. Since the localization process of the undetermined location node is determined by several key beacon nodes location information on its communication range which belongs to the public areas of the multi-coordinate system. It is not necessary to use the position information on all beacon nodes in its communication range. Therefore, after the beacon node density reaching a certain extent, positioning error is basically unchanged. We can conclude that the positioning accuracy of the improved algorithm will not rely too much on the number of beacon nodes, so in the condition that the beacon nodes is less, this algorithm can greatly improve the location accuracy than the former algorithm.

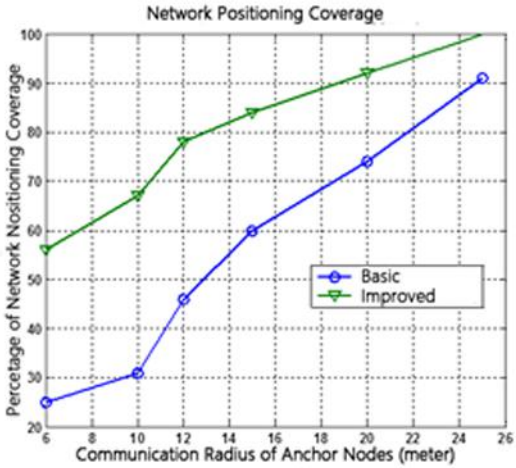

Figure 8.The Comparison About Affection Of The Beacon Nodes Ratio Attacking To The Positioning Node Proportion

In this figure, the ratio of the locatable nodes for basic DV-HOP algorithm and the improved DV-HOP algorithm are reduced when improvement for the percentage of attacked beacon nodes.The percentage of the located node improved is higher than the basic DV-HOP algorithm in the same case where the percentage of attacked beacon nodes is same.More proportion of malicious beacon node increase around the Node,unknown location,as augment for proportion of the attacked node.Position coordinates information produce large error in the process of node localization.Malicious nodes are eliminated by credibility of the beacon node through the improved DV-HOP algorithm. Therefore,the ratios of the referred beacon nodes and located node are descended.However, the accuracy of node being unknown location is stable.At last, under the condition of the mobile beacon nodes, the situation will become more complex, therefore algorithms need to be further improved[16].

Acknowledgments

This work was supported by the National Natural Science Foundation of China (No. 61405159), the National Natural Science Foundation ofChina (No. 61076002) and the Natural Science Foundation of Education Commission of Shaanxi Province (Grant No. 2012JK848).

5 Conclusions

To prevent the main network attacks of DV-HOP algorithm which named wormhole attack, this paper proposed a new technology to pick out malicious nodes by using the credibility of the beacon node. Furthermore, this paper has improved the original scheme after ruling some malicious peers.In terms of estimating the distance form an unknown node to a beacon node, this technology improved method by calculating more than one node. After all of this, we build a simulation platform in MATLAB to compare the difference between this improved DV-HOP algorithm and the basic DV-HOP

algorithm in network positioning coverage and location error. The simulation results show that under certain network size, network positioning coverage percentage can reach 90% using this new DV-HOP algorithm. When the number of beacon nodes is different, the improved DV-HOP algorithm is always better than the basic one in location error. In a word, the improved algorithm improved the safety and accuracy of location.

References

[1] Kirci, P.; Chaouchi, H., Recursive and ad hoc routing based localization in wireless sensor networks. Computer Standards & Interfaces (2016), 44, 258-263.

[2] FuBao, W.; Long, S.; Fengyuan, R. Self-Localization Syste`ms and Algorithms for Wireless Sensor Networks Self-localization systems and algorithms for wireless sensor networks. Journal of Software 2005, 16 (5), 857-868.

[3] Shi, X.; Ran, Q.; Fan, M.; Yu, H.; Wang, L.; University, C., Dynamic weighted DV-Distance algorithm for wireless sensor networks. Chinese Journal of Scientific Instrument (2013), 34 (9), 1975-1981.

[4] Gui, L.; Val, T.; Wei, A.; Dalce, R., Improvement of range-free localization technology by a novel DV-hop protocol in wireless sensor networks. Ad Hoc Networks(2014), 24, 55-73.

[5] Zhang, A.; Ye, X.; Hu, H.; Ding, X., Improved DV-HOP positioning algorithm based on one-hop subdivision and average hopping distance modification. Yi Qi Yi Biao Xue Bao/chinese Journal of Scientific Instrument (2012), 33 (11), 2552-2559.

[6] Zonghai, L. I.; Liu, S.; Wang, Y., Defending against wormhole attacks in wireless sensor networks. Computer Engineering & Applications (2012), 48 (27), 94-98.

[7] Yang, J.; Zhong, Y., The Research on unmanned border outposts Information Platform based on Wireless multimedia sensor networks. Network Security Technology & Application (2013).

[8] Huang, C. Z.; Li, X. U.; A-Yong, Y. E.; Zhong, J. F., Secure DV-Hop Algorithm Against Malicious Beacon Nodes. Computer Systems & Applications (2011).

[9] Sun, Y.; Shen, M.; Zhou, L.; Xiong, Y.; Lin, X., Simulation and realization of farmland wireless sensor networks nodes deployment. Transactions of the Chinese Society of Agricultural Engineering (2010), volume 26 (8), 211-215(5).

[10] Liu, X. S.; Chen, J. X.; Liu, Z. H.; Gai-Yan, L. I., Security localization based on DV-Hop in wireless sensor network. Journal of Computer Applications (2012), 32 (1),107-98.

[11] Hui, L. I.; Xiong, S.; Duan, P., An Improvement of DV-Hop Localization Algorithm for Wireless Sensor Network. Chinese Journal of Sensors & Actuators(2011).

[12] Liu, H.; Cui, J., Multivariate Classification-Based Malicious Node Detection for Wireless Sensor Network. Chinese Journal of Sensors &With the change of parameter r Actuators(2011), 24 (5), 771-777.

[13] Chen, H.; Lou, W.; Wang, Z.; Wu, J.; Wang, Z.; Xia, A., Securing DV-Hop localization against wormhole attacks in wireless sensor networks. Pervasive & Mobile Computing (2014), 16, 22–35.

[14] Labraoui, N.; Gueroui, M.; Aliouat, M., Secure DV-Hop localization scheme against wormhole attacks in wireless sensor networks. Springer Berlin Heidelberg: (2012); p 303–316.

[15] Amish, P.; Vaghela, V. B., Detection and Prevention of Wormhole Attack in Wireless Sensor Network using AOMDV Protocol. Procedia Computer Science(2016),79, 700-707.

[16] Han, G.; Chao, J.; Zhang, C.; Shu, L.; Li, Q., The impacts of mobility models on DV-hop based localization in Mobile Wireless Sensor Networks. Journal of Network & Computer Applications (2014), 42 (6), 70-79.