International Journal of Control and Automation
Vol. 11, No. 4 (2018), pp.31-44
http//dx.doi.org/10.14257/ijca.2018.11.4.04

An Approach for Location Verification using Atomic Localization in Wireless Sensor Networks

Gulshan Kumar[1], Thirumalaraju Vamsi Krishna[2], Mritunjay Kumar Rai[3], Rahul Saha[4] and Hye-Jin Kim[5]

[1,2,4]*School of Computer Science and Engineering, Lovely Professional University, Punjab, India*
[3]*School of Electronics and Communication Engineering, Lovely Professional University, Punjab, India*
[5]*Business Administration Research Institute, Sungshin W. University, Seoul, Republic of Korea*
[*]*rsahaaot@gmail.com*

Abstract

We propose a location verification mechanism, for localization of wireless sensor networks through atomic localization. Atomic localization shows remarkable change in ability to localize in case of low density networks. It is a range based localization technique that forms groups where each node will be able to share beacon signals to its adjacent neighbour. Detection of malicious locators, whose locations are tampered with, is more accurate and any node can verify its location by checking for consistency. Checking for consistency can eliminate the complexity of digital signatures and authentication mechanisms, assuming the number of malicious locators is less than benign locators. This method also reduces the number of left alone nodes which cannot receive beacon signal directly from locators. Over all the mean square estimation error and number of left alone nodes when using atomic localization is considerably low.

Keywords: *Localization, atomic, WSNs, security, wormhole*

1. Introdution

Wireless sensor networks are defined as a network of tiny sensor nodes. These sensor nodes are deployed in the field independently and they operate co-ordinately through wireless links. There might be different kinds of sensor nodes in a network, some nodes with basic functionalities and some with expensive special functionalities. The network may be distributed over a small field, in a household, in an industry, or it can be a operating over a large forest [1], deep oceans[2], health care[3] or a traffic monitoring[2] network in a city. Wireless sensor networks are not limited by the type of data they monitor. The data can be seismographic readings or humidity levels or sounds in the forest or traffic camera recordings of a city.

Wireless sensor networks have become cost effective and small in size, thanks to the speed of evolution of technology. Flexibility, Scalability, Accuracy of sensor networks have made its manufacturing rapid, which in turn reduced the cost of development. Deployment of monitoring nodes has become simple with robust and reliable low cost nodes.

Sensor networks cannot have a single design because, incorporating all the features in one design makes the nodes costly and size cannot be small. Design of wireless sensor networks has become application specific as the requirements are different in each

Received (January 4, 2018), Review Result (March 1, 2018), Accepted (March 5, 2018)
* Corresponding Author

ISSN: 2005-4297 IJCA

application. A military application demands secure communication[4], A healthcare application demands accuracy[3], An environmental monitoring scheme demands for robustness, A traffic monitoring scheme demands for longer lifetime. This might be the reason that the sensor networks are attracting attention of researchers to address these design constraints, improving existing protocols.

Localization is referred to the process of identifying the location of sensors with the help of anchor/beacon nodes. Wireless sensor networks as stated above, have limited resources. All the sensor nodes cannot have location awareness independently as they are deployed ad hoc in the network and some other factors such as cost, power constraints, size etc. In some cases, the GPS systems cannot be employed as the environmental conditions[6] restrict the communication with satellites *e. g.*, monitoring applications in deep forests, ocean depths, household application in case of basements and dense concrete structures. Location of sensor node is very important in many applications. Without the location information, the data collected is of no use. Thus the sensor localization is an important domain in WSN. Mobility is an important indicator of development. Mobile sensor nodes are required to have location awareness. To identify the location of all the nodes in the network, some of the nodes in the network must be self-aware of their own location either by placing them in a fixed known location or by providing them with GPS like systems. These nodes are referred to as Anchor/Beacon nodes. A sensor node to identify its own location, it communicates with the in-range anchor nodes. The beacon signals send the location of beacon nodes. The sensor nodes find the distance and/or angle between anchor node and sensor node. From all the information of anchor nodes' locations and distances, sensor nodes calculate their own location. For finding the distance and angle, many range based localization techniques were discovered, such as ToA (Time of Arrival), RSS (Received Signal Strength), TDoA (Time Difference of Arrival), AoA (Angle of Arrival), Directional Antennas[6], [7].Connectivity based localization algorithms were a great success where the accuracy is not a critical requirement. Localization of sensor nodes with of use of connectivity information of nodes is called Range free localization[8], [9]. Some popular algorithms are DV-Hop localization algorithm[7], [10]–[12], LCB (Localizable Collaborative Body) algorithm[6] and centroid localization algorithm[6], [7], [10], [11].

2. Secure Localization

Wireless sensor networks are usually installed/deployed in unattended and insecure locations. Nodes cannot be made completely tamper proof, as it increases cost[2], [6], [13]. The importance of localization process and the need of accuracy is an attractive target to attackers[2], [6], [14][29][30]. Attacks on localization process can cause significant confusion and may also degrade routing mechanisms.

Attackers can jeopardize the localization process which in turn affects the monitoring tasks[13]. For example, a sensor at the summit of a mountain is misleading into believing that it is located at the bay of ocean. This misleading information can make most of the routes in the routing table, invalid. It is well known that, stale routes and inefficient routes consequently cause energy consumption. The localization issue in under no specific adversary has already been well studied. No specific adversary scenarios include ranging errors and computational errors. Ranging errors can be overcome by Distance Bounding Techniques, VerfiableMultilateration technique[8], [13], [15], Directional Antennae-Based Schemes, Transmission Range Variation-Based Schemes, Hybrid Schemes. Many algorithms were introduced to overcome computational errors as such Mean square error estimation[13], Maximum likelihood estimation, Gradient descent based estimation[8], Kalman filter algorithm[7], Cuckoo search algorithm[16]. However, adversary is a problem to be addressed when the network is under attacks. Non coordinated attacks such as Rushing, Masquerading (Sybil attack), Misuse, Anomaly attacks[17] and coordinated

attacks such as Distance consistent spoofing attack[14], wormhole attack are still needed to be overcome.

3. Atomic Localization

Atomic Localization is a local process of sensor nodes to identify its surrounding nodes locations in reference to its own. This local mapping of neighbours for each node helps to verify a node's location once it has acquired its location estimation with the help of beacon nodes.

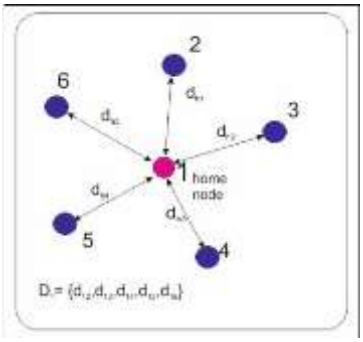

Figure 1. Formation of Distance Vector at each Node

A sensor node, when it wakes from the sleep state, sends Dist_Est (Distance Estimation) packets to its neighbour sensor nodes. The sensor nodes respond with an Ack packet. The round trip time of the two signals will be used to calculate the distance[14] between the two nodes. This process is done at each node as shown in Figure 1, to identify its distance vector, $D_i = \{d_{ia}, d_{ib}, d_{ic}, d_{id}, d_{ie}, d_{if}, \ldots\}$. When a node sends Dist_est signal, the receiver responds with Ack signal. The sender node calculates the total round trip time period including processing and buffering delay in the mac layer. The responding node, when it receives the Dist_Est signal, it starts a clock in its mac layer and stops when sent back the response. This delay time is included in Ack signal to the sender. The delay time subtracted from total round trip time to estimate the actual time of travel as shown in Figure 2. The TOT mechanism is prone to errors, interferences and attacks. But this is the simplest technique without the need of extra hardware functionalities. One can always go for RSSI[28] with variable power antennas that are more accurate ranging mechanism. But it needs special hardware functionalities which could increase the cost of network.

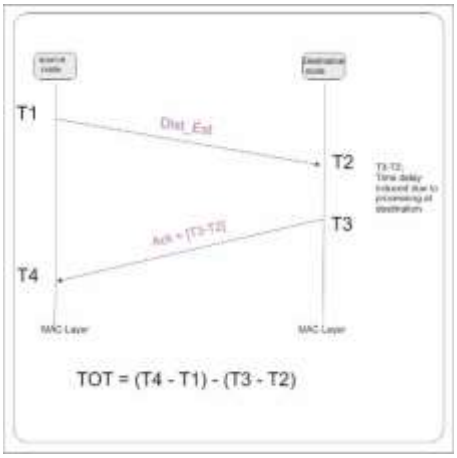

Figure 2. TOT Mechanism with Secure Round Trip Time Estimation

Once the distances to all the neighbours are known, the sensor node selects a node at random. A distance vector table is created as shown in Table 1, the distance vector of home node (say node-1) is added to the table. The distance vector from the new node (say D6 = {d_{61}, d_{62}, d_{63}, d_{64}, d_{65}}) is received and is added to the table. If the nodes are not in direct range, the distance will be represented as infinity. In practice, it can be a large value compared to the maximum range of a node.

Table 1. Distance Vector Table of a Node

Distance Vectors	D1	D2	D3	D4	D5	D6
D1	0	d12	d13	d14	d15	d16
D2	d21	0	d23	d24	d25	d26
D3	d31	d32	0	d34	d35	d36
D4	d41	d42	d43	0	d45	d46
D5	d41	d41	d43	d44	0	d46
D6	d61	d62	d63	d64	d65	0

Then the next node chosen is the node which is in direct rage of node 6. Similarly, distance vectors of all the nodes are added to the table. This procedure at each node forms a set of distances to all its neighbours and their mutual distances to perform atomic localization. The distance vectors are exchanged between neighbours. When node 1 receives distance vectors from its neighbours, it forms the atomic graph of its neighbours.

Atomic localization can be explained with the help of a simple example. Showing in the Figure 3, is a node 1, performing atomic localization. The node 1 selects a node at random, and assumes it to be the reference or at 0 degrees.

In step 3, as shown in Figure 4, the next node chosen is the common node for node 1 and 2. From the distance vectors D1 and D2, the distances d16 and d26 are extracted and reference location of node 6 is identified.

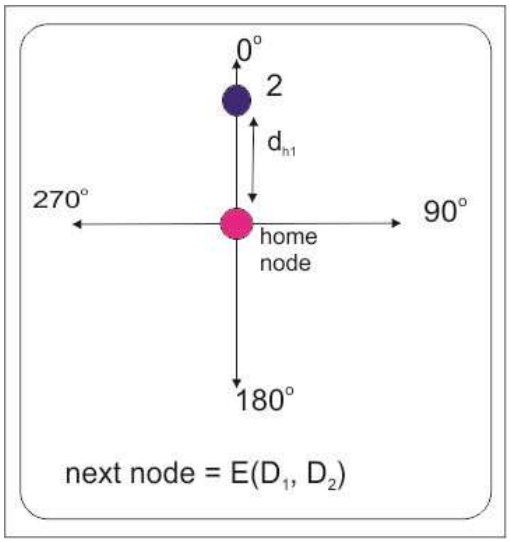

Figure 3. Atomic Localization Process Step 2

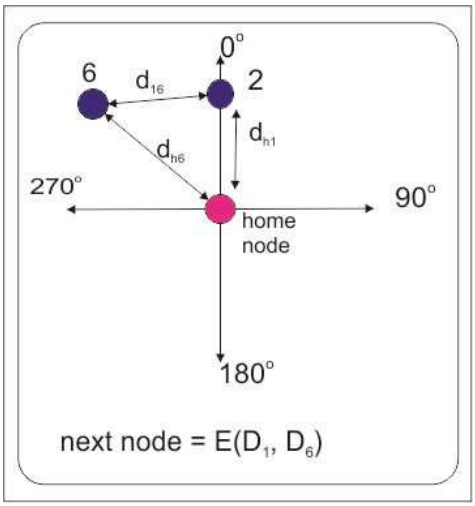

Figure 4. Atomic Localization Process Step 3

Similarly, the next node selected is the common node of node 1 and 6 and is not already a part of the network. This process as shown in Figure 5, will be continued till all the nodes in range of node 1 are added to network.

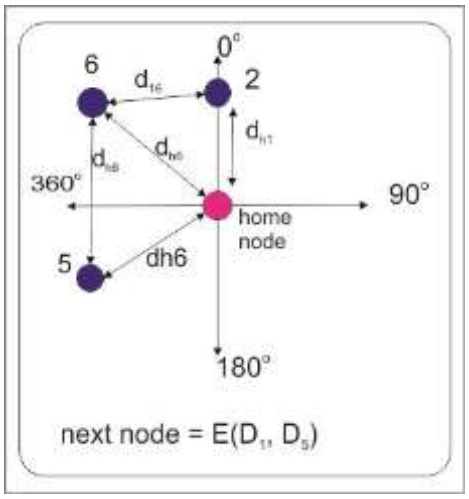

Figure 5. Atomic Localization Process Step 4

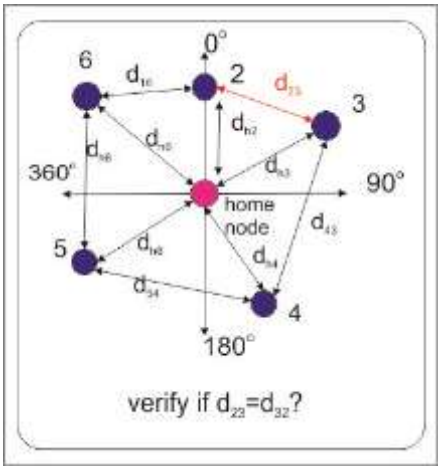

Figure 6. Atomic Localization Process, Verification of Closure

The mutual distances of unchecked pairs are checked to verify closure of the graph. As shown in Figure 6. When all the nodes are added to the distance vector table, the upper diagonal and lower diagonal matrices are not always symmetric. In the table, the distance between any two nodes (say i, j), $d_{ij}$is not always equal to d_{ji}. This error need to be corrected.

4. Related Work

Atomic localization is performed by distance estimation at node to node level using distance estimation techniques such as time of travel. Time of travel can be error prone and processing delay may increase the estimated distance than actual distance. A technique discussed in [14] can be used to eliminate such errors. The mac layer protocols are used to eliminate processing delays in mac layer and above from total round trip time as shown in Figure 2.The concept of atomic localization was inspired from kcdlocation algorithm[18] where any node can act as anchor node after estimating its location with the help of neighbouring locators. In the algorithm the authors illustrated an atomic localization algorithm (in Section 3.1) where one or more nodes can estimate their location where they are within one hop distance from an anchor and meet appropriate requirements.

Wormhole attack (simplex and duplex[15], [19]) is a very difficult attack to detect. The use of atomic localization data to resist against the wormhole attack is described in following sections. A simplex wormhole attack is where the attacker eavesdrop the beacon signals and retransmit to neighbouring nodes. Since the captured packets and retransmitted packets are in the range of same nodes, such attack is rather easy to detect with simple mechanisms. A duplex wormhole attack is a set of attacker nodes maintaining a tunnel/channel between the nodes. The packets eavesdropping at one end are broadcasted at the other end. Many solutions to such attacks are discussed in [15], [19], [12], [20].

In [21],[9],[10],[2]and [18] various localization algorithms were analysed and compared in different scenarios such as mobility of anchor nodes, mobility of sensor nodes and range based or range free techniques etc. Gradient descent localization discussed in [9] is an optimization technique to reduce the estimation error in localization process. Cuckoo search algorithm inspired by bird nesting habits as in [16] and Bat algorithm discussed in [23] for localization are optimization techniques to minimize estimation error in localization of wireless sensor networks.

In [24]–[27] security mechanisms for localization of wireless sensor networks are analysed and compared. Security mechanisms such as TSCD [14], where the temporal, special properties of the network are verified to detect the wormhole attacks on localization process. And SeRLoc[20] explains a defence mechanism against wormhole attack using hashing and locator verification.

5. Proposed Work

Location Correction in Case of Tampered Locators

Once the atomic localization process is completed, this data can be used to verify the accuracy of localization. Localization of sensor nodes is achieved with the help of beacon nodes. Beacon signals [B1=(d1, x1, y1) and B2=(d2, x2, y2)] is used to find a node's location.

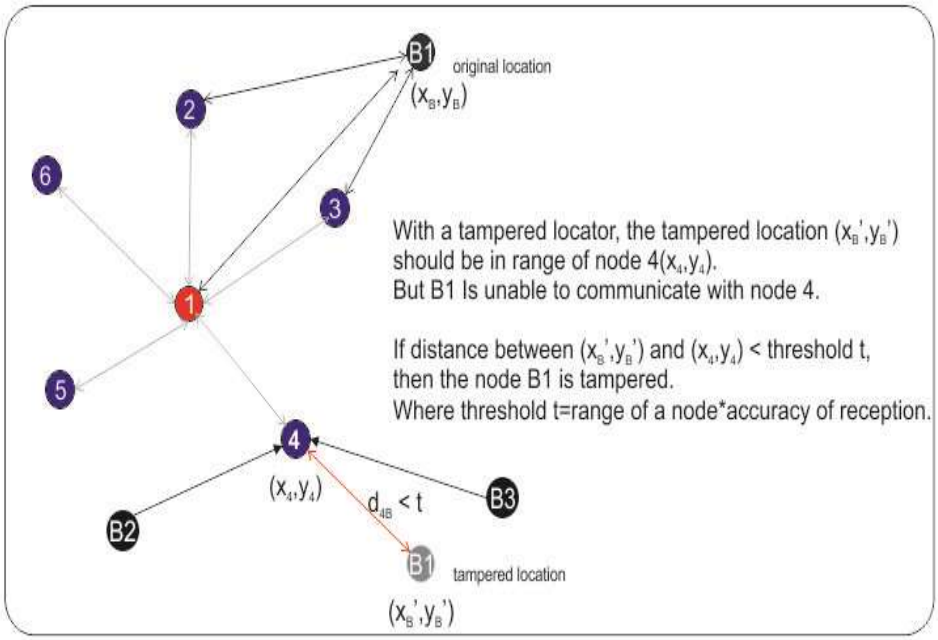

Figure 7. Verifying Consistence of Locator with Nodes in a Single Atom

A beacon which is tampered with and is sending a false location is not consistent with the neighbours of the node (shown in Figure7).The node 1 is receiving information from B1 which is claiming a false location. The false location B1'= (x', y') is verified by checking consistency with the neighbours which are supposed to be in range of B1. The (x', y') of B1 if it is true, must be in range of node 4 (considering node-4 already has accurate location information). The node 4 identified its own location with the help of beacons B3 and B4 as shown in Figure 7. When node 1 receives beacon signal form B1, if identifies the sensor nodes (in its atomic graph) which are close to the claimed location of B1. As in Figure 7, the claimed location of B1 is close to node 4. But node 4 is not actually in range of B1. This inconsistence can be identified as attack by tampering the beacon location. A locator, if it is detected to be tampered with, can be black listed and this information will be broadcasted through the network. Black listing a node can be a serious issue, if the number of beacon nodes is scarce. The beacon location can be corrected with the new location by sending a correction signal digitally signed by the legitimate nodes.

Secure Localization Against Wormhole Attack

Considering a wormhole link, which captures packets at one end of the atom and broadcast at the other end. As show in Figure 8, the node-3 and node-2 are in range of W2 (Broadcasting end of wormhole link) which is tunnelling the packets from beacon B1. The location information of nodes under attack (nodes 3, 2) is disrupted. But the rest of the nodes are not under any attack. They have accurate location information. To verify the location accuracy, the location information should be verified with atomic graph. Distance between node 1 and 6 (d_{16}) if nearly equal to the distance d_{16}' calculated from beacon signal $(d_{16}')^2= (x_1-x_6)^2+(y_1-y_6)^2$thenthe location is accurate. If the difference between d_{16} and d_{16}' exceeds the threshold error, then the node is under wormhole attack. This verification is done with all the nodes in the atomic graph of 1. A set of nodes which are consistent with 1 and a set of nodes which are inconsistent with 1 are present in the network (with the presence of wormhole link). Multiple beacons in range of an atom can simplify this problem as shown in Figure 8.

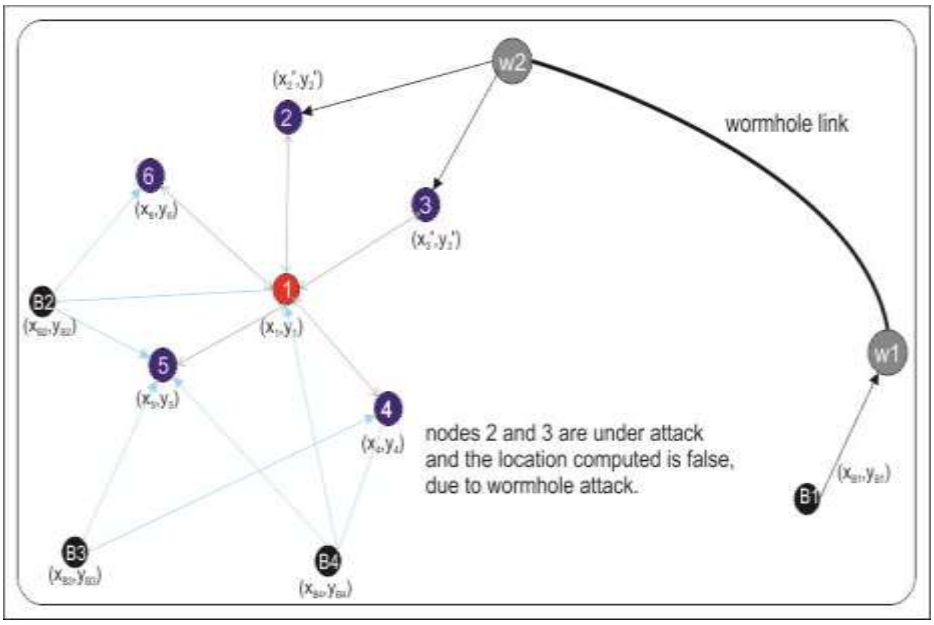

Figure 8. Securing Against Wormhole Attack

The nodes 2, and 3 are consistent with each other, and nodes 5, 6, 2 are consistent with each other. The set of nodes which are in range of a common locator are the nodes which are under attack. The probability of other consistent set, to be in range with other single locator is inversely proportional to the number of sensor nodes in a single atom. More the number of nodes in an atom, less the probability of being in range of single locator, as the range of locatorsare limited. Considering the assumption that, the range of locators and sensor nodes is same.

Low Density of Beacon Nodes

Low density of locator nodes is a severe issue in wireless sensor networks, especially in case of mobile locators (due to power constraints and physiological issues). The mobile nodes drain the power because of continuous change of location, altering neighbour nodes, path calculations *etc.*, which cause them to die-off the network and this causes low density of mobile beacons in the network. Such low density could cause many sensor nodes to waste resources on Loc_req requests and long awaken time. Atomic localization can provide reliable solution for such problems.

A node can use the location information from its neighbours to identify its location. When a node has received enough beacon signals to compute its location, it can act as beacon for its neighbours. A node in an atom can use its neighbour's location to compute its own location. In general, in wireless sensor networks, a sensor node's location is not used for localization of other sensor nodes, because the error propagates in further steps. But in atomic localization, only nodes in same atom are used to get beacon signal, and also the accuracy is not reduces because multiple nodes in the atom are already consistent with each other. Thus the probability of achieving location information accurately with a low density of beacon nodes increases with atomic localization.

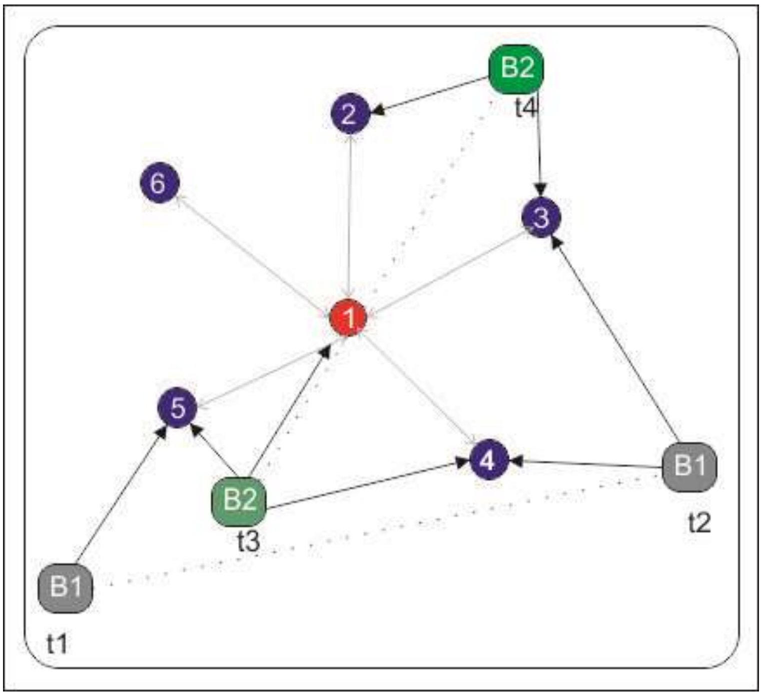

Figure 9. Localization at Low Density of Beacon Nodes Condition

Considering a case of mobile beacons in a network, where it is broadcasting the beacon signal periodically. As shown in Figure 9, the beacon B1 at time t1 communicates with node-5, and as time passes, the beacon B1 moves to a different location as sown in figure. Similarly, considering another beacon B2, and it moves from one location to other from time t3 to t4. In such scenario, node 5 and node 4 can perform localization process as they are able to receive two beacon signals from B1 and B2, but the nodes 1 and 3 has only one beacon signal, and nodes 6 and 2 received no beacon signal. Thus the nodes 1, 3, 2 and 6 are still waiting for beacon signal and resources are being wasted. To avoid this problem, the sensor nodes 5 and 4 (which are aware of their location) can be used for further localization process of remaining nodes.

6. System Model

We assume that the system consists of a set of sensor nodes (s nodes) with unknown location and a set of locator nodes (l nodes) with known location, position can be acquired through GPS receivers. We assume that all the nodes are deployed randomly in the network in a region A. Random distribution of nodes is assumed to be following the Gaussian distribution. As shown in equation 1.

$$f(x|\mu,\sigma) = \frac{1}{\sigma\sqrt{2\mu}} e^{-\frac{(x-\mu)^2}{2\sigma^2}} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (1)$$

χ is the random variable with normal distribution or Gaussian distribution, σ is the standard deviation of input data, σ^2 is variance and μ is the mean or median or mode as applied by the user. The l-nodes are assumed to be moving randomly with constant speed and the density of the nodes is not uniform. The random motion is assumed to be gauss-markov random motion. The speed of a moving node is defined in equation 2, and direction of motion is defined in equation 3.

$$S_N = (\alpha * S_{N-1}) + \left((1-\sigma) * S_{mean}\right) + \sqrt{(1-\alpha^2)S_{mean} - 1} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (2)$$

$$D_N = (\alpha * D_{N-1}) + \left((1-\sigma) * D_{mean}\right) + \sqrt{(1-\alpha^2)D_{mean} - 1} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (3)$$

σ is the turning parameter, S_{MEAN} and D_{MEAN} are mean values of speed and direction. The values of S_{XN} and D_{XN} are random values determined by Gaussian distribution. When the value of α is zero, the function generates random movements, and when α value equals 1, we get complete linear node movement. The transmission range of all the nodes (s nodes and l nodes) is assumed to be same. The number of locators in range of a sensor node is defined in equation 4.

Number of l-nodes in range of an s-node= (total no of l-nodes/A)(πR^2)…………......(4)

A is the area of network, R is the radial range of a node, thus ($\pi *R^2$) represents area of coverage of a node. In a network with 200 locator nodes distributed randomly in an area of 100 square meters, if the radial range of a node is 1 meter, the number of locator nodes in range of an s-node is (200/100)*($\pi *1^2$)=2π =~ 6 or 7 For a given system, with the use of atomic localization; the area of control of a node increases due to the atomic nature of all the s-nodes in an atom. Thus the coverage of an s-node increases with the use of atomic localization. The increase in probability of localization with the use of atomic localization is described in equation 7.

$$\theta = 2cos^{-1}\left(\frac{d}{2r}\right) \dots \dots \dots \dots \dots \dots \dots \dots \dots \dots \dots \dots \dots \dots \dots \dots \dots \dots \dots \dots \dots \dots \dots \dots (5)$$

Where d is the distance between two nodes; r is the radio coverage of nodes;

$$\text{Overlapping area of any two nodes,} \quad A_0 = \theta\left(\frac{r^2}{2}\right) - \left(\frac{1}{2}\right) r^2 \sin(\theta) \dots \dots \dots \dots \dots \dots (6)$$

$$\text{Total area of an atom,} A = n(\pi r^2) - A_0 \quad \dots \dots \dots \dots \dots \dots \dots \dots \dots \dots \dots \dots \dots \dots \dots \dots \dots (7)$$

The probability of detection of wormhole link using the property "single message from single locator", also increases by same factor as shown equation 7 and in above example 1. Increase in probability of localization and detection of a wormhole can be derived as

Increase in probability of detecting a wormhole is given by equation 8, Where N is number of nodes in an atom, and Θ is in radians.

$$\Delta P = N\left(\pi - \frac{\theta}{2}\right) - \frac{\left(\frac{1}{2}\sin(\theta)\right)}{2\pi} \dots \dots \dots \dots \dots \dots \dots \dots \dots \dots \dots \dots \dots \dots \dots \dots \dots . (8)$$

7. Results

The localization problem is simulated in MATLAB in 2D space. We assume that all the nodes; sensor nodes, benign locator nodes and malicious locators have same radio range. All the nodes were distributed randomly. It is also assumed that the node density is not uniform throughout the region. Error free TOA measurements are assumed. After applying algorithm 1; with area 100m X 100m, range r=15m, number of sensor nodes=100, number of benign locators=45, number of malicious locators=10. Distribution of locators, sensors and malicious nodes is shown in figure 10. The mean square error estimation of all the nodes is observed to be 38.79m. Of all the 100 nodes in the network, it is observed that only 60 nodes were able to have accuracy of localization less than 1m. This is shown in Figure 11.

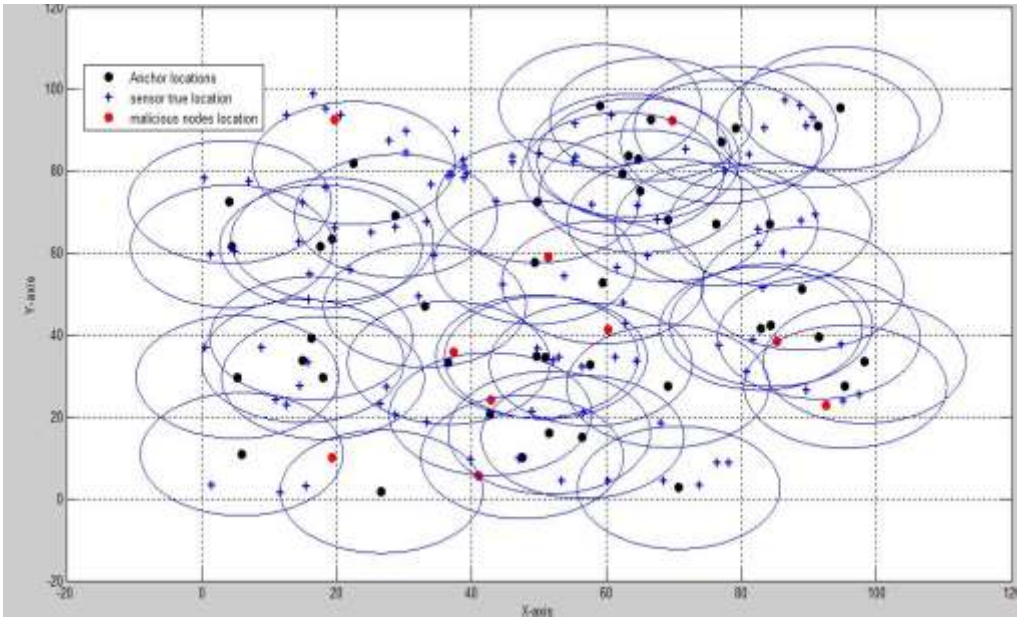

Figure 10. Network with Area 100 Square Meters

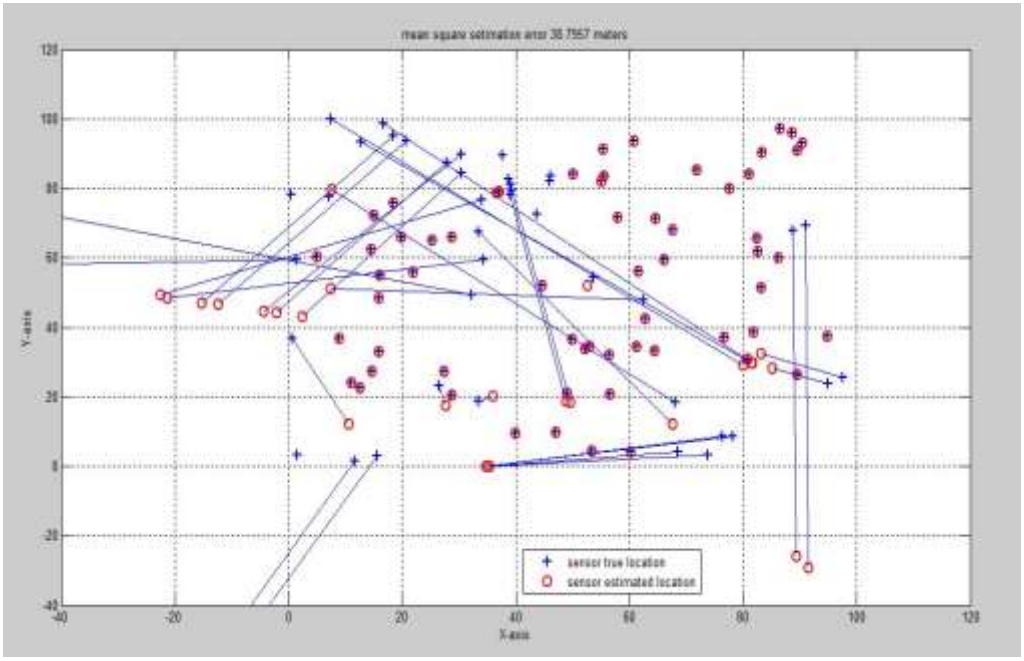

Figure 11. Location Estimation without using Atomic Localization

It is observed that the location error is high and many nodes were under attack. With the use of atomic localization and algorithm 2; the localization error is greatly reduced and more number of nodes are able to achieve accurate location. The comparative output of localization result with and without atomic localization technique is as follows.

With respect to area of distribution, the accuracy of localization in both cases, and the percentage of nodes that were able to localize accurately is identified. The parameters for the simulation are area=100 X 100 m^2, range of each node= 20m, number of benign locators = 35, number of malicious locators= 10. For the above parameters, the mean square estimation error and successful localized sensors is plotter in Figure 12, 13.

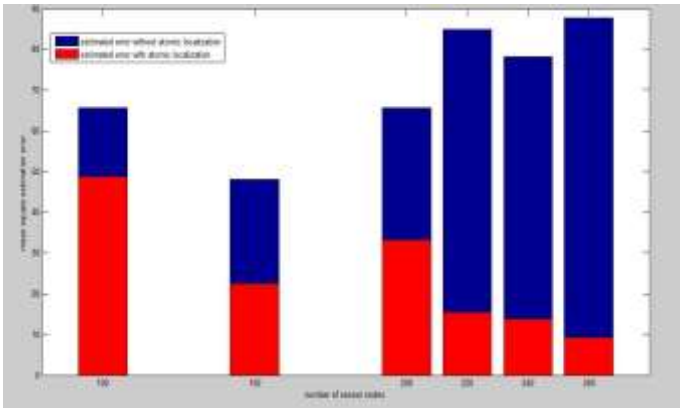

Figure 12. Mean Square Error Estimation for Varying Density of Sensor Nodes

It is observed that, the mean square error is not dependent on the density of nodes when the atomic localization is not used. But, with the use of algorithm 2, the mean square error is constantly decreasing with respect to increasing density of sensor nodes. The coordinated operation of nodes in atomic localization results in better performance with high density of sensor nodes.

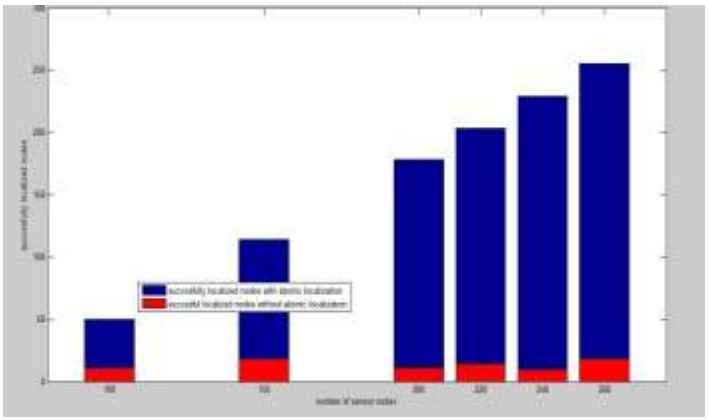

Figure 13. Number of Successful Localizations with Respect to Varying Density of Sensor Nodes

The above Figure 13 shows the number of successful localizations with respect to varying density of sensor nodes. It is again clear that the latter case shows better performance with increasing density of sensor nodes. Without using atomic localization, the number of nodes with successful location estimation is constant, because even though the density of nodes is increased, the number of locators is unchanged, and the sensor noes are not in coordinated operation.

The bar-chart in Figure 14 shows the estimation error plotted against number of locator nodes in the network. In the case without atomic localization, the estimation error with increasing locator density is not decreasing. As all the sensor nodes are working independently, the estimation error is dependent on malicious nodes, but not very much influenced by density of locator nodes. In the latter case, where the sensor nodes are working in co-ordinated manner, the mean square error is consistently reducing with the increased density of locators. As the locator density is increasing, as described in our proposal, the sensor nodes are able to distinguish between the benign and malicious nodes. Thus, the accuracy of localization increases.

The parameters taken for this case are as follows. Area 100m X 100m; range, r=15m; number of sensor nodes=100, number of malicious nodes=10.

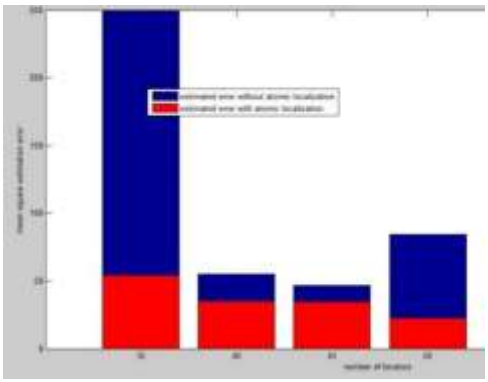

Figure 14. Mean Square Error with Respect to Varying Locator Density

The Figure 15 shows the number of successfully localized nodes with respect to varying density lo locators. It can be seen that, irrespective of the density of locators, the atomic localization is able to provide the location for many sensor nodes. With the formation of atoms, and communication with neighbours, sensor nodes are able to identify their location with sufficient number of locators. In previous case, without coordination of sensor nodes, the successful localization of nodes is dependent on locator density, and is also very less as compared to atomic localization.

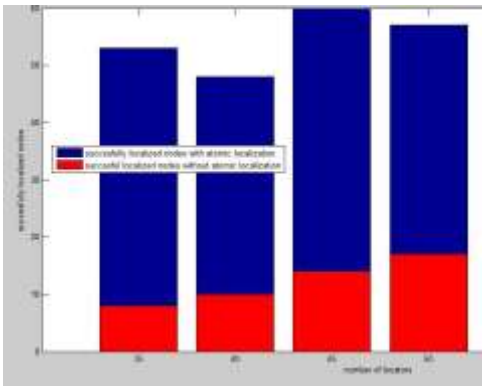

Figure 15. Number of Successful Localized Sensors with Respect to Varying Locators

Noisy TOA measurements can reduce the accuracy of localization. But in general, atomic localization retains its accuracy, high probability of localization and high probability of anomaly detection. Location correction using atomic localization is complex when compared to non-coordinated operation due to high connectivity and message exchange between neighbours. But as the communication is limited to its neighbours *i.e.*, only one step, the complexity of message exchange does not become a burden.

References

[1] D. Gao, Y. Liu, F. Zhang and J. Song, "Data Aggregation Routing for Rechargeable Wireless Sensor Networks in Forest Monitoring", Wirel. Pers. Commun., vol. 79, no. 1, **(2014)**, pp. 773-788.
[2] P. Rawat, K. D. Singh, H. Chaouchi and J. M. Bonnin, "Wireless sensor networks: a survey on recent developments and potential synergies", J. Supercomput., vol. 68, no. 1, **(2014)**, pp. 1-48.
[3] M. H. Yaghmaee, N. F. Bahalgardi and D. Adjeroh, "A prioritization based congestion control protocol

for healthcare monitoring application in wireless sensor networks", Wirel. Pers. Commun., vol. 72, no. 4, **(2013)**, pp. 2605-2631.
[4] A. Boukerche, H. A. B. F. Oliveira, E. F. Nakamura and A. A. F. Loureiro, "Secure Localization Algorithms for Wireless Sensor Networks", IEEE Commun. Mag., no. April, **(2008)**, pp. 96-101.
[5] M. Bala Krishna and M. N. Doja, "Multi-Objective Meta-Heuristic Approach for Energy-Efficient Secure Data Aggregation in Wireless Sensor Networks", Wirel. Pers. Commun., vol. 81, no. 1, **(2015)**, pp. 1-16.
[6] D. Ma, M. J. Er, B. Wang and H. B. Lim, "Range-free wireless sensor networks localization based on hop-count quantization", Telecommun. Syst., vol. 50, no. 3, **(2010)**, pp. 199-213.
[7] J. Wang, R. K. Ghosh and S. K. Das, "A survey on sensor localization", Journal of Control Theory Appl., vol. 8, no. 1, **(2010)**, pp. 2-11.
[8] M. Mofarreh-Bonab and S. A. Ghorashi, "A low complexity and high speed gradient descent based secure localization in Wireless Sensor Networks", Iccke 2013, no. Iccke, **(2013)**, pp. 300-303.
[9] N. A. S. Alwan and A. S. Mahmood, "Distributed Gradient Descent Localization in Wireless Sensor Networks", Arab. J. Sci. Eng., vol. 40, no. 3, pp. 893-899, **(2015)**.
[10] D. Niculescu and B. Nath, "DV based positioning in ad hoc networks", Telecommun. Syst., vol. 22, no. 1-4, pp. 267-280, **(2003)**.
[11] Y. Hu and X. Li, "An improvement of DV-Hop localization algorithm for wireless sensor networks", Telecommun. Syst., vol. 53, no. 1, **(2013)**, pp. 13-18.
[12] X. Yang and Q. Song, "An Improved DV-Hop Algorithm for Resisting Wormhole Attack", no. 1, **(2015)**, pp. 1443-1448.
[13] W. T. Zhu, Y. Xiang, J. Zhou, R. H. Deng and F. Bao, "Secure localization with attack detection in wireless sensor networks", Int. J. Inf. Secur., vol. 10, no. 3, **(2011)** June, pp. 155-171.
[14] H. Chen, W. Lou, J. Ma and Z. Wang, "TSCD: A Novel Secure Localization Approach for Wireless Sensor Networks", 2008 Second Int. Conf. Sens. Technol. Appl. (sensorcomm 2008), **(2008)**, pp. 661-666.
[15] J. W. J. Wu, H. C. H. Chen, W. L. W. Lou, Z. W. Z. Wang and Z. W. Z. Wang, "Label-Based DV-Hop Localization Against Wormhole Attacks in Wireless Sensor Networks", Networking, Archit. Storage (NAS), 2010 IEEE Fifth Int. Conf., **(2010)**.
[16] S. Goyal and M. S. Patterh, "Wireless Sensor Network Localization Based on Cuckoo Search Algorithm", Wirel. Pers. Commun., vol. 79, no. 1, **(2014)** November, pp. 223-234.
[17] B. Soediono, "Security for Wireless AD Hoc Networks", vol. 53, **(1989)**.
[18] Z. Fang, Z. Zhao, X. Cui, D. Geng, L. Du and C. Pang, "Localization in wireless sensor networks with known coordinate database", Eurasip J. Wirel. Commun. Netw., vol. 2010, **(2010)**.
[19] Z. Wang, H. Chen, W. Lou and X. Sun, "A secure localization approach against wormhole attacks using distance consistency", Eurasip J. Wirel. Commun. Netw., vol. 2010, **(2010)**.
[20] L. Lazos and R. Poovendran, "SeRLoc: Secure Range-Independent Localization for Wireless Sensor Networks", Netw. Secur., **(2004)**, pp. 21-30.
[21] S. Halder and A. Ghosal, "A survey on mobile anchor assisted localization techniques in wireless sensor networks", Wirel. Networks, **(2015)** October.
[22] G. Han, H. Xu, T. Q. Duong, J. Jiang and T. Hara, "Localization algorithms of Wireless Sensor Networks: a survey", Telecommun. Syst., vol. 52, no. 4, **(2013)**, pp. 2419-2436.
[23] S. Goyal and M. S. Patterh, "Modified Bat Algorithm for Localization of Wireless Sensor Network", Wirel. Pers. Commun., vol. 86, no. 2, **(2016)** January, pp. 657-670.
[24] Y. Zeng, J. Cao, J. Hong, S. Zhang and L. Xie, "Secure localization and location verification in wireless sensor networks: a survey", Journal of Supercomput., vol. 64, no. 3, **(2013)**, pp. 685-701.
[25] A. Ahmed, K. A. B. U. Bakar, M. I. Channa, K. Haseeb and A. W. Khan, "A survey on trust based detection and isolation of malicious nodes in ad-hoc and sensor networks", vol. 9, no. 2, **(2015)**, pp. 280-296.
[26] D. G. Padmavathi and M. D. Shanmugapriya, "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks", vol. 4, no. 1, **(2009)**, pp. 9.
[27] K. Venkatraman, J. V. Daniel and G. Murugaboopathi, "Various Attacks in Wireless Sensor Network : Survey", no. 1, **(2013)**, pp. 208-211.
[28] W. Mardini, Y. Khamayseh, A. A. Almodawar and E. Elmallah, "Adaptive RSSI-based localization scheme for wireless sensor networks", Peer-to-Peer Netw. Appl., **(2015)** June.
[29] G. Kumar, M. Kumar Rai, H.-j. Kim and R. Saha, "A Secure Localization Approach Using Mutual Authentication and Insider Node Validation in Wireless Sensor Networks", Mobile Information Systems, vol. 2017, Article ID 3243570, 12 pages, 2017. doi:10.1155/2017/3243570.
[30] G. Kumar, M. Kumar Rai and R. Saha, "Securing range free localization against wormhole attack using distance estimation and maximum likelihood estimation in Wireless Sensor Networks", Journal of Network and Computer Applications, vol. 99, **(2017)**, pp. 10-16.

