A Localization Technique in Wireless Sensor Network based on Angle of Arrival

Deeksha Verma
Dept. of computer Applications
Kanpur Institute of Technology, Kanpur
India

Sachin Umrao
Dept. of computer Applications
Krishna Institute of Engineering and Technology
Ghaziabad, India

Rahul Verma
Dept. of Computer Applications
Kanpur Institute of Technology, Kanpur
India

Arun Kumar Tripathi
Associate professor
Krishna Institute of Engineering and Technology
Ghaziabad, India

ABSTRACT
Wireless sensor network (WSN) consists many sensor nodes across the network. In this paper every sensor node is aware about the physical position of sensor nodes in wireless sensor network. The determination of position of sensor nodes can be released in range measurements including angle of arrival. We proposed a new localization technique based on angle-of-arrival between sensor nodes in a particular area of Wireless sensor network. This technique is derived under the assumption of angle measurement. This article emphasizes the basic localization technique to understand the angle-of-arrival of sensor nodes and to make progress in new and large open area of sensor network localization research.

Index Terms
WSN, mitigation, Ad-hoc, pulse delay attack, intruder, node replication attack, countermeasure, angle-of-arrival, localization technique, security protocol

1. INTRODUCTION
Wireless Sensor network [1] contains number of sensor nodes [2] spread across a geographical area. Each sensor node has wireless communication [3] capability and its own level of intelligence. Sensor nodes can decide the transmission in WSN. Sensor nodes control the processing and decision making by the processor. Signal processor helps the sensor node to decide that which information sends first to the server or to the other sensor nodes. After that sensor node transmitted the information to the other sensor node or to the server. This process also helps to get feedback from the server to the sensor node. The working of sensor nodes is represented in Fig 1.

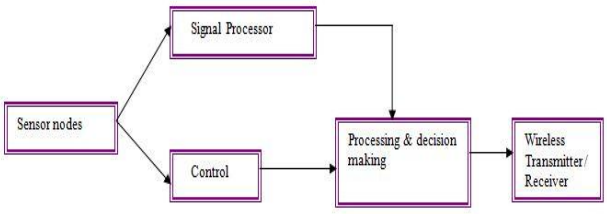

Fig.1: Working of sensor nodes

In wireless sensor network, the number of nodes is present in the network. All the nodes in the network cannot communicate with the server at the same time. If the time of communication of any two nodes is same then the collision occurs. Due to the collision the transmission of whole network is affected. The network will not communicate in a proper manner. Collision occurs when more than one node will transmit at the same time. To avoid the collision in WSN there is two protocols which includes static channel allocation& dynamic channel allocation [4].

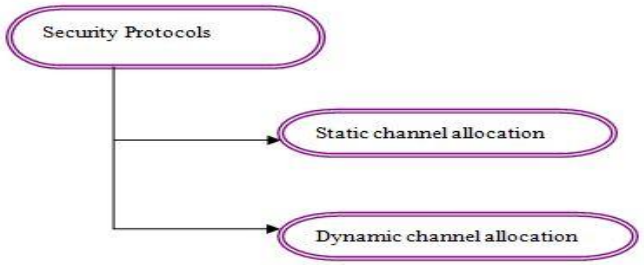

Fig.2: Types of Security Protocols

1.1 Static channel allocation
In static channel allocation, if N nodes are in the network then the bandwidth is divided in N equal partitions. Static channel allocation have the number of nodes is equal to the number of partition of bandwidth.

1.2 Dynamic channel allocation
In dynamic channel allocation, no fixed distribution of bandwidth for the nodes is given.

In WSN, the sensor nodes are connected with the base station this base station act as a gateway between the sensor nodes and the end user as they typically forward the data from the WSN to the server. The connection of sensor nodes, gateway and the end user is represented below-

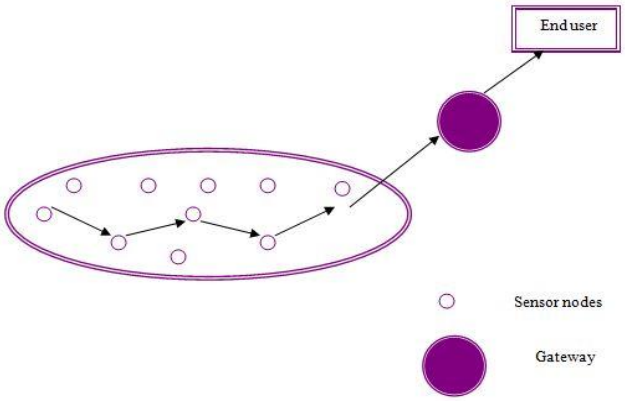

Fig.3: Wireless sensor network

WSN have some characteristics that make them different from other networks such as wired network. These characteristics are given below-

- Ability to handle with node failure.
- Mobility of node.
- All the nodes in network are different type.
- Easy to use.
- Secure communication.
- Scalability of large scale of deployment
- Transmission may fail between the nodes.
- Power consumption constraints for nodes using batteries or energy harvesting.

2. RELATED WORKS

There are many sender- receiver based [5] protocol and node replication attack in secure pair wise synchronization [6]. In SPS all the sensor nodes are synchronized with the server. Server will match the activation time of all sensor nodes. If activation time is same for all sensor nodes then transmission will start. If activation time of any one sensor node is not same as majority of sensor nodes then that node is malicious node and server will not communicate with that sensor node.

Where as in [7] server calculates the time taken in transmission and finds the message delay [8]. Sender and receiver synchronized with each other by using time stamp and sender- receiver [8, 9] is intended by measuring the total time taken, from the time a receiver request a time stamp to receiving a response.

Where as in [10] server recognizes the pulse-delay attack [11] and malicious node in WSN. In routing algorithm [10,12] is used to overcome the node replication attack and pulse delay attack. This algorithm detects the replicated node and finds the message delay in transmission between two nodes. It differentiates between the original node and its replicated copy.

In the routing algorithm [10] all types of attacks in wireless sensor network are discussed with their effects. the proposed algorithm[8] isto overcome the node replication attack. This algorithm detects the replicated node and then differentiates among the original node and its replicated copy. After finding the replicated copy it will terminate the communication with replicated copy.

3. PROPOSED WORK

Many techniques are used for limited number of nodes, they are aware about their positions like GPS [15],these nodes are referred to as beacons [16] and rest nodes are referred to as unknowns [16]. Depending upon the mechanism of positioning schemes can be classified into two categories:

(1) Range-free or proximity based [17].
(2) Range based [17].

In order to overcome the problem of security in wireless sensor network we use the Range based scheme. In Range based scheme the transmission between nodes and server is handled by the Range measurement (Receive signal strength (RSS), time of arrival (TOA), Time difference of arrival (TDOA) [18] and angle of arrival (AOA) [19]) between the nodes. The proposed method helps to find the genuine node and provide the security to the transmission of message. This method finds the genuine node in the network. All the sensor nodes in the WSN follow the pattern and they are placed in equal distance from each other and also from the server. This synchronization of the sensor nodes and the server is represented bellow-

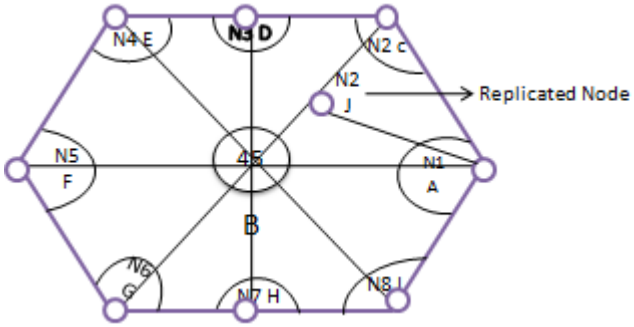

Fig.4: Proposed Algorithm

In Fig.5. We use the localization technique [20] to find the position of sensor nodes. Here we explain the procedure to locating the sensor nodes in wireless sensor network based on the angle of arrival. Angle of arrival focuses on the mathematical concepts for localization. This technique needs an anchor node [21] which accurately knows their position and help to locate other sensor nodes in the network. The most successful strategies implement on methods to reduce the errors and increase the accuracy of the network.

To localize the sensor nodes we use the angle of arrival. Angle of arrival is the angle between the direction of a signal transmission and some reference direction. By the arrangement of sensor nodes is represented in above figure, the M sensor nodes are distributed with constant spacing with each and every node of d meters distance. Letα(t) represent the value of source of signals, at time t:

$$\alpha(t) = A(t).\cos(\mathcal{E}t + \theta(t)) \quad (1)$$

Where A(t) represents amplitude, θ(t) represent the phase shift and Ɛt represent the carrier frequency of the sensor nodes. We assume that Ti represent the time of signal to (i =1, 2……M). Then the value of emitted signal when signal reach to the sensor node M represent as:

$$\alpha(t\text{-}Ti) = A(t\text{-}Ti).\cos(\mathcal{E}(t\text{-}Ti) + \theta(t\text{-}Ti))$$

$$\alpha(t\text{-}Ti)\theta \approx A(t).\cos(\mathcal{E}t\text{-}\mathcal{E}Ti + \theta t) \quad (2)$$

The transmission delay Ti can also be represented as phase shift of carrier frequency ƐTi. In order to signal assumption and taking sensor node B as a reference point, the transmission delay Ti can be written in terms of AoAx:

$$Ti = (i\text{-}1)\, d \sin x / Vp \quad (3)$$

For $x \in [-\pi/2, \pi/2]$

Where Vp is the velocity of signals transmission, since the arrangement of sensor nodes represented in the above figure

cannot allow to transmit the information by any replicated node and the value of x is lies in between the -π/2,π /2.d is the distance of the network in which the nodes can transmit with each other. By the range based localization technique we have limited distance for node transmission, where the value of d is constant and we assume that the value of d= 1 Km.Then the equation is written as

$$Ti=(i-1)\ \text{Sin}\ x/\ Vp \qquad (4)$$

Where Vp is the velocity of signal transmission and the value of Vp may vary by different node. The value of Vp is

Vp= (1,2,3,……)

We find the transmission delay where velocity of signal transmission Vp = 1, then

$$Ti=(i-1)\ \text{Sin}\ x$$

Where i = (1,2,3,4,5,6…….)

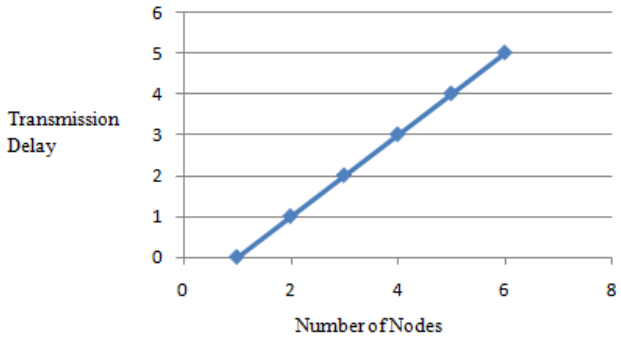

Fig.5: Graphical representation for Vp=1

Above graph represent that the transmission delay between sensor node is increased where the velocity of signal transmission Vp = 1.

Now, we find the transmission delay where velocity of signal transmission Vp = 2, then

$$Ti= (i-1)\ \text{Sin}\ x / 2 \qquad (5)$$

Where i= (1, 2, 3, 4, 5, 6 ……)

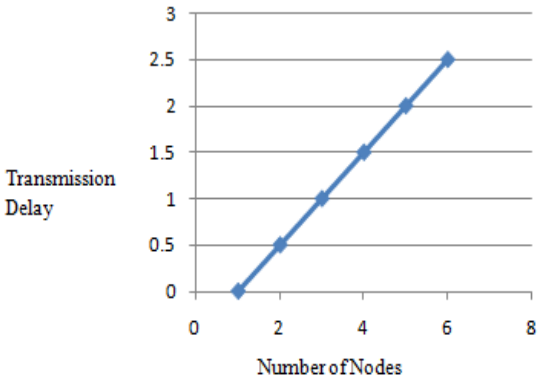

Fig.6: Graphical representation for Vp=2

Above graph represent that the transmission delay between sensor node is decreased where the velocity of velocity of signal transmission Vp = 2 in comparison to the graph of fig.6.

Now we find the transmission delay where velocity of signal transmission Vp = 3, then

$$Ti= (i-1)\ \text{Sin}\ x / 3 \qquad (6)$$

Where i=(1,2,3,4,5,6,……)

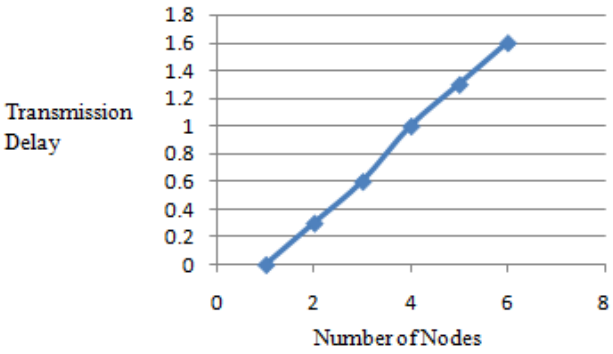

Fig.7: Graphical representation for Vp=3

This graph represent that the transmission delay between sensor node is more decreased where the velocity of signal transmission Vp = 3 in comparison to the graph of fig.6 and fig.7.

The algorithm for node replication attack [10] typically focus on the detection of replicated based on the arrival time of sensor node in the network but in this paper we assign a position based on angle of arrival of localization for all sensor nodes. It explains that each and every sensor node has its own place in the network so any mobile replicated node will not be able to communicate with any sensor node and interfere in the transmission of sensor nodes. When mobile replicated node communicate with each other and share information with each other, they can make the detection technique fail very easily. Thus, we can use this technique to determine the mobile replicated node from the network. With this technique the amount of sensor node is also increases in the network and sensor nodes in this network can communicate easily with each other.

4. CONCLUSION AND FUTURE WORK

By using this proposed approach the problem of replication of node or clone attack can be avoided. In this approach the location of every node is predefined or we can say every genuine node follows the predefined pattern of the server. This approach will make the wireless communication secure and reliable. In this paper, we represented a localization technique based on angle of arrival for Wireless Sensor Networks. We assume that all sensor nodes are capable to detect angle of incident signal from neighboring sensor nodes. This approach is helpful to achieve much better localization coverage in comparison to last existing approach in [10]. This type of efforts can increase security of wireless sensor networks.

In future researchers may focus on the implementation of this algorithm in network simulation tools and also try to make it energy efficient, better, secure and cost efficient.

5. REFERENCES

[1] Mukherjee, B, Ghoshal, D., Yick, J.: Wireless Sensor network survey. Computer Network 52(12), 2292-2330(2008)

[2] Al-Sakib Khan Pathan, Hyung-Woo Lee, Choong Scon Hong, "Security in wireless Sensor Network: Issues and Challenges". International Conference on advanced computing Technologies, Page 1043-1045, year 2006

[3] Zhenwei Yu, Jeffrey J.P. Tsai.A Framework of Machine Learning Based Instruction Detection for Wireless Sensor Networks, IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing.2008

[4] www.enggpedia.com/computer-engineering encyclopedia/dictionary/computer-network/1617-channel-allocation-dynamic-a-static-channel-allocation

[5] Wang, C., Ning,P., Sun, K.: Secure and resilient clock synchronization in Wireless Sensor Networks. IEEE Journal on selected areas in Communications 24(2),395-408(2006)

[6] Ganeriwal, S., Propper, C., Capkun, S., Srivastava, M.B.: Secure Time Synchronization in Sensor Networks, ACM Transactions on information and System Security, Article No. 23,11(4)(2008)

[7] Sachin Umrao and A.K.Tripathi "Time Synchronization Protocol in wireless Sensor Network based on Hash Code" International Journal of Computer Application (IJCA), vol-68 Number 23, Article No. 6,2012.

[8] Song, H., Zhu, G.C.S.: Attack resilient time synchronization for wireless sensor network In: IEEE International conference on Mobile Adhoc and Sensor System Conference, p. 772(2005)

[9] Li, H., Chen, K., Wen, M., Zheng, Y.: A Secure Time Synchronization Protocol for sensor network. In: Washio, T., Zhou, Z., -H, Huang, J.Z., Hu, X., Li, J., Xie, C., He, J., Zou, D., Li, K., -C., Freire, M.M.(eds.) PAKDD 2007. LNCS(LNAI), vol. 4819, pp. 515-526, Springer, Heidelberg(2007)

[10] Sachin Umrao, Deeksha Verma and A.K. Tripathi "Node Replication and Pulse Delay Attack in Wireless Sensor Network". IEEE International conference in MOOC, ISBN: 978-1-4799-1625-2, pp390-392, 2013

[11] Arun Kumar Tripathi, Ajay Agarwal, "Approach towards Time Synchronization Based Secure Protocol for Wireless Sensor Network", International Conference at NDT'2010, published by the "Communications in Computer and Information Science" (CCIS) Series of Springer LNCS, Springer, Vol. CCIS-88, Issue-2, pp: 321-332(2010).

[12] Sachin Umrao, Deeksha Verma and A.K. Tripathi "Node Replication and Pulse Delay Attack in Wireless Sensor Network". IEEE International conference in MOOC, ISBN: 978-1-4799-1625-2, pp390-392, 2013

[13] Hu, H., Atakli, I.M., Chen, Y., Ku, W.S, Su, Z., Malicious Node Detection in Wireless Sensor Networks. In: The Symposium on Simulation of Systems Security, pp. 836-843(2008)

[14] Kopetz, H., Ochsenreiter, W.: Clock Synchronization in Distributed Real- Time System. IEEE Transaction on Computers 36(8),933-940(1987)

[15] D. Niculescu and B.Nath, "Ad hoc positioning system (APS) using AOA," in IEEE INFOCOM, Apr, 2003.

[16] C.Savarese, J.M. Rabaey, and J.Beutel, "Locationing in distributed Ad hoc wireless sensor network," in Proc. Of ICASSP' 01, vol. 4, 2001, pp. 2037-2040.

[17] Rong Peng and Mihail L.Sichitiu, "Robust, Probabilistic, constraint- based Localization for wireless sensor network," in Proc. Of SECON 2005, Santa Clara, CA, Sept. 2005.

[18] D.Niculescu and B.Nath, "Ad hoc Positioning system (APS) using AOA," in IEEE INFOCOM, Apr.2003.

[19] J.B. Andersen and K.I.Pedersen, "Angle of arrival statistics for low resolution antennas," in IEEE Transactions of Antennas and Propagation, vol.50, no.3, Bern, Switzerland, Mar.2002.

[20] Francisco Santos, "Localization in wireless sensor networks", ACM Journal, Vol 5, November 2008.

[21] Bonnet, P., Gehrke, J., and Senhadri, P. "Towards database systems," International conference on mobile data management. ACM Journal Vol.5. Springer- Verlag, London, UK, 3-14. November 2008.