RESEARCH ARTICLE OPEN ACCESS

# Survey on localization of the Sensor nodes in Wireless Sensor Networks

B.Dineshbabu[1], T.Thirunavukarasu[2]
Information Technology, SNS college of Technology, Coimbatore
Anna University, Tamil Nadu-India

**ABSTRACT**
The Wireless Sensor Networks is a group of nodes scattered in the network. Each node has certain processing capacity, memory. It shares the resources and information among the nodes. The example of these services includes mobile services, traffic monitoring, natural calamities, smoke detection and vehicle tracking applications. Sensor networks provides the fast sensing and make necessary actions to provide reliable transfer of information. The sensor node helps to provide the better gathering of data and it provides a backup through which the failure of one node is compensate by the other node. Sensor nodes require less energy, battery power, reduced cost easy node deployment.
***Keywords***- Localization Algorithm, Jamming nodes, Multi-alteration

## I. INTRODUCTION

Sensor Node Localization is the main process in the Wireless Sensor Networks (WSN). Node localization will improve the performance of WSN. To find out the location of the sensor node is the main task, wrong prediction of the location due to attackers will leads to many problematic situations. An attacker can spoof by using another node identity to make an attack which results in the compromise of node and hence finding the location of the attacker will be crucial task. We can find out the location of the sensor node by either two or three dimensional through which the landmark of the node can be identified. One of the main problems is the coverage area where it becomes difficult to cover all the areas in the network. Hence a survey is needed to be taken for localizing the sensor node.

## II. MACHINE LEARNING APPROACH IN LOCALIZATION

In this paper [1] there are various techniques implemented to find out the location of the sensor nodes, machine learning is the different technique used for the localization. The information which is shared by giving the signal strength as the input.SVM is the machine learning approach for classification by getting the input and by having the training sets available, it predicting the corresponding output by accurately predict the location of the sensor node and determine the class of the sensor node. These training methods include only the beacon nodes through which any sensor can find the location without the knowing about other sensors. Exact location based on the size of the training data that we have already gathered. By combining the past and the current information gathered we can find out the location accurately. This will reduce the cost and need for every sensor to run the localization algorithm. The important processes to find out the

## III. JAMMER LOCALIZATION IN WIRELESS SENSOR NETWORKS

In this paper [2] is to find the position of the jamming device is a critical process so as to take the necessary actions in order to the jammer in the network communication. To provide an efficient algorithm called Double Circle Localization (DCL). To deploy DCL in different situations and make contrast with the present jamming localization algorithms by simulation, by comparing with the other methodologies it provides the exactness in localization of jammer. This attack affect the network by stopping the transmitters from transferring the data which results in packet collisions even though the alternatives are choose to counter these attacks like channel surfing. Advanced devices and high standard protocols are required to prevent this attack. To make effective strategies location of the jammer is essential. All nodes are randomly deployed and there is no change in their locations. This device always emit the electromagnetic power by that it can sense the signal and stopping or preventing the data which is transferred. This jamming signal will disturb the communications in the sensor networks. The energy of the jamming will be high to the nodes which are nearer to that jamming node. The nodes which are jammed are to transmit these jammed messages to the nearest node. With the help of the boundary nodes we can detect the presence of the jamming node and then the localization algorithm for the jamming nodes are activated. To measure the landmark of the node can be done by the Received Signal Strength (RSS) and also provide the exact distance between the jamming nodes and nearest nodes. To transfer the node from the predicted location to the jamming location Virtual Force Iterative

Localization(VFIL) to run many times as pull and push by the mutual virtual forces. When the nodes are outside the predicted region it will make the jammed region near to it. And the inside the region will push the unaffected nodes. Centroid Localization will gather the location information about the neighbouring node, weighted centroid localization combine the information of the target node to provide the accurate Jamming node Localization.

## IV. ATTACK DETECTION IN WIRELESS LOCALISATION

In this paper [3], Non-Cryptographic attacks cannot be controlled by the traditional security services and hence it is essential to detect the attack in Wireless Sensor Networks (WSN).At first with the help Statistical Significance Testing attack detection problem can be formulated theoretically. With the help of localization approaches such as Multi-alteration and signal strength to provide solutions for high detection rate for attack detection. When there is any physical attacks localization algorithm performance decreases. The output of the compromised node make a serious risk by affecting the applications, Most used localization approach is the Multialteration which uses the techniques called Least Squares(LQ) to make localization process. Many algorithms use the signal strength to detect the attackers. By measuring the physical properties we can calculate the distance between them with the help of the Range based algorithms. Attack can be detected with the help of signal strength. Attacker can modify the signal strength and change the location of the node with the help of low cost electronic devices. Certain performance metrics can be used to make the high attack detection range. Cumulative Distribution Function (CDF), Detection rate (DR) are the performance metrics used for the attack detection. The RSS has the ability to reuse the wireless network infrastructure, the main benefit in the use of this technique is that it does not depend on the localization algorithms and it performs earlier than the localization process. By selecting the correct threshold to prevent the false detections, Detection of attack in signal authentication provides better performance than the signal attenuation due to its higher detection range when the signal is amplified by the attacker. To make the highest detection range the Area Based Probability (ABP) and Bayesian Networks (BN) which makes the signal strength to further increase the detection range and the location of node can be identified .Bayesian Network provides the probability distribution of finding the unknown locations with the help of Monte-Carlo sampling technique. By using these techniques it will increases high detection rate and providing the less false positive rate.

## V. SECURE ATTACK DETECTION AND LOCALIZATION IN WIRELESS SENSOR NETWORKS

In this paper [4] to make a secure Localization module which makes the particular clusters as a reference points and by knowing the positions and by having the centroid to provide the reference points. It must be needed to eliminate the intrusion, the cryptographic authentication used were it share the key which is unique, it provides malicious node detector which is installed in beacon nodes and the regular node, each sensor node must know about the position of the beacon before the actual deployment. The malicious beacons have to be filtered first due to the inconsistency among the multiple beacon signals. It provides the Petri net provides an Enhanced Secure Localization Scheme which protects not only to the distance reduction attacks and also by the distance enlargement attacks and also ensured to find the beacon nodes which have been compromised this cryptographic authentication and encryption does not completely prevent the localization of the Wireless Sensor Networks (WSN). Hence the costs of the sensors are less and the algorithms that we are developing should be less weight. By using the triangle based method we can detect an attack, some protocols adjust to failures and by the multiple inclusion of the sensors which results in the possibility of misguiding of the signals, even though by implementing several technologies are used there will be the compromise of the beacon nodes which shows the different locations. Mostly sensors are static which provides the trialteration localization method to detect the sensor nodes, where the position of the regular node on the plane can be find out the distances of the three different beacons, by the availability of the resources to improve the precision of the localization is called the multialteration. Certain authentication schemes are needed to deploy like tesla, but this authentication will not guarantee about the security. It is essential to separate the beacon and compromised beacons and since the sensor nodes are prone to errors and make them identifies the suspicious location references. There is no need for double check for the energy conservation the combining of the nodes based on the secure communication. Attacks against discovery of the location can be made to assist other types of attacks which give the network topology; example of this is the sinkhole attack.

## VI. LOCALIZATION OF MULTIPLE MOBILE AGENTS ON DISTRIBUTED SENSOR NETWORK

In this paper [5] locating the mobile agents is needed to make an interaction where the sensors are deployed on the machines and it cannot be used for the multiple mobile agents. Solutions are provided to locating the mobile nodes; At first the multiple agent localization for the architectural design, by using the RFID system combines with the target system, implementing the localization algorithm will provide the exact prediction of the multiple agents. Mobile agents contain the sensor nodes by the help of these sensors which are installed is to find out the location and the classic localization algorithm is used by the sensors installed in the mobile agents. It works perfectly to find out the position and the main purpose is to improve the accuracy determination of the location of the nodes. In the hybrid network it uses the

localization algorithm to find out positions inside the particular region through which the moving objects are also getting concerned. The node which has the control over particular space knows the position of the mobile agent; all the mobile agents know their positions in the network. RFID tags stores the ID and the positions of the data through which the infected data and the wrong readings will not occur. These tags are stored in a particular value and the distance between them is calculated, the position of the node is continuously updated and the position is calculated based on the data gathered. But the distribution of the tags affects the localization. Tags are usable through which the correctness is obtained and the algorithms are compared through which the performance is measured.

## VII. CONCLUSION

Machine learning approach is the different technique which is used to find out the location of the node by giving the Signal Strength as input and by having the already gathered data, the position of the jamming node in the network is difficult to find out and that can be find out by using the Double Circle Localization. Non-Cryptographic methods are difficult to control where the traditional methods are not efficient and by using the Least Squares (LQ) which was used by the multi-alteration method to point out the attacker location, the accuracy of the algorithm results in the accuracy of locating the attackers, Enhanced Signal Localization scheme will be against the distance enlargement attacks and the distance reduction attacks and results in the accuracy of locating the attackers.

## REFERENCES


[1] A.Tran, XuanLong Nguyen, and Thinh Nguyen,"Localization Algorithms and Strategies for Wireless Sensor Networks" (Eds: Guoqiang Mao and Baris Fidan, IGI Global)

[2] Zhenhua Liu, Hongbo Liu, Wenyuan Xu, and Yingying Chen *Exploiting Jamming-Caused Neighbor Changes for Jammer Localization*,"IEEE Transactionson Parallel and distributed Systems. Vol: 23, March 2012.

[3] Yingying Chen, Wade Trappe and Martin, R.P. "Attack Detection in Wireless Localization," *IEEE Infocom.*2007.

[4] Wen Tao Zhu · Yang Xiang · Jianying Zhou "Secure localization with attack detection in wireless sensor networks," Int. J. Inf. Secur. 2011.

[5] Byoung-Suk Choi, Joon-Woo Lee, Ju-Jang Lee, Kyoung-Taik Park "Distributed Sensor Network Based on RFID System," *Wireless Sensor Network*, 2011.