HCTL Open Int. J. of Technology Innovations and Research
HCTL Open IJTIR, Volume 9, May 2014
e-ISSN: 2321-1814
ISBN (Print): 978-1-62951-521-2

Security Framework in WSNs: Location Discovery

***Roma Sharma*[*] *and Dr. Rama Sushil*[†]**
roma28.sharma@gmail.com

Abstract

Wireless Sensor Networks (WSNs) have pulled a great deal of recognition in recent years. They have a promising future to a ample variety of military and civilians operations. Location of sensor nodes structures the basis of many applications i.e., many operation. WSNs rely on the physical location of sensor nodes. Ensuring that the sensor nodes locations are protected from destructive attacks it is necessary that the attackers are unaware of the presence of sensor nodes. In this paper we have first proposed a new Genetic Algorithm (GA) for encrypting the sensor nodes location, and then also compared the proposed algorithm with the AES algorithm.

Keywords

Wireless Sensor Networks, Security, Algorithm.

[*]Department of Computer Science and Engineering, DIT University, Dehradun, Uttarakhand, India
[†]Professor, Department of Computer Science and Engineering, DIT University, Dehradun, Uttarakhand, India.

HCTL Open Int. J. of Technology Innovations and Research
HCTL Open IJTIR, Volume 9, May 2014
e-ISSN: 2321-1814
ISBN (Print): 978-1-62951-521-2

Introduction

Wireless sensor networks (WSNs) derive from the technology of sensor, wireless transmission, tiny embedded devices and the use of distributed computing. These sensor networks consist of a large number of low-cost, low-power, and multifunctional sensor nodes that communicate via wireless media. They interchange data with the environment through sensors and put into effect the function of collecting and dealing with data.

Localization is amongst the widely discussed topic in Wireless Sensor Networks (WSNs) since several fundamental methods of WSNs, e.g., geographical routing [1], geographic key distribution [2], and site-based authentication [3] demands the positions of unknown nodes. Also, the positions of unknown nodes play an important role in numerous WSNs applications, for example monitoring applications include environmental monitoring, health monitoring, and tracking applications include tracking objects, animals, humans, and vehicles [4]. Using the random deployment on most sensor networks, it is hard, in any other case impossible, to predetermine the positioning of each one sensor node before deployment. A simple and easy solution in order to get nodes location is to provide each sensor with a GPS receiver that can precisely provide the sensors with their exact location. This, however, is not a viable solution from an economic aspect since sensors are often deployed in very large numbers and manual configuration is unmanageable and thus not feasible. Therefore, localization in sensor networks is very challenging. Over the years, many protocols have been formulated to enable the location discovery process in WSNs to be autonomous and able to function distinct to GPS and other manual techniques.

Also, when a WSN is deployed in malicious environments, it is endangered to threats and risks. Many attacks exist, e.g., wormhole, sinkhole and sybil attacks, to make the approximated positions incorrect. Particularly for some applications, e.g., military applications like battlefield surveillance or environmental applications like forest fire detection [5], incorrect positions can lead to drastic consequences, e.g., wrong military decisions about the battlefield and false alarms to people [6]. Hence, the down sides of secure localization has to be addressed in WSNs.

The rest of the paper is organized as follows. In section II we review the related work on localization in WSNs. In section III we propose a method for encrypting nodes location. In section IV we have presented the simulation results. In section V we have conclusion.

HCTL Open Int. J. of Technology Innovations and Research
HCTL Open IJTIR, Volume 9, May 2014
e-ISSN: 2321-1814
ISBN (Print): 978-1-62951-521-2

Related Work

In majority of applications of WSNs, the data gathered by a sensor node are not very useful without the position information. Therefore, localization is important for many WSNs applications. WSNs localization techniques can be classified into two classes: range-free and range-based. Both categories make an effort to localize sensor nodes through several anchors that are likely to know their particular locations, e.g., through GPS receivers or manual configuration.

Range-based localization algorithms involve calculating physical properties which you can use to get the distance between a sensor node and an anchor point whose location is well known. Arrival time (ToA) can be a range based method that utilises the connection between beacon-node distance plus the TRM that the signal needs to travel between sender and beacon. Should the velocity of the signal is well known and let's assume that the sender and receptor know the dimensions and time when a transmission starts, then this time of arrival on the signal is an indicative of the beacon node distance and this distance might be computed when using the propagation time by either the beacon or node [7]. Time Difference of Arrival (TDoA) measurements in the transmitter's signal at the volume of receivers with known location information to estimate the position of the transmitter. Angle of Arrival (AOA) method is made up of the angle obtained between a reference node and the node which wishes to know its position. The AOA is normally assembled using radio-chips or microphones array, allowing a listening node to look for the angular direction of your transmitting node [8]. Received Signal Strength Indicator (RSSI) category of distance related measurement techniques estimates the distance between neighbouring sensors from the received signal strength measurements.

Range-free localization algorithms do not require the measurement of physical distance-related properties. For example, In [9] Centroid algorithm all anchors first sends their locations to all sensor nodes within their transmission range. Each unknown node listens for the pre-determined time frame t and collects all of the beacon signals it receives from various reference points. Secondly, all unknown sensor nodes positions are calculated with a centroid determination from all n positions in the anchors in range. In [10] DV-Hop localization algorithm, one anchor transmits a beacon to be flooded through the network containing the anchors location having a hop-count variable initialized to a single. In order to transform hop count into physical distance, the system evaluates the average distance per hop without range based techniques. Each node can calculate the gap estimation to a lot more than 3 anchors in the plane; it uses triangulation

e-ISSN: 2321-1814
ISBN (Print): 978-1-62951-521-2

to estimate its location. APIT [11] is another area based range free method that uses beacons from anchors, and does location estimation by separating the environment into triangular regions between anchor nodes.

Proposed Work

In our proposed work we have simulated 25 sensor nodes in a large geographical area following a random distribution model. For security reasons or some areas marked as sensitive by government we have encrypted the location of those areas so that no one is able to get the location of sensors present in those areas by our proposed genetic algorithm and shown the location of rest areas.

When we access these sensor nodes for the first time we can see the spatial spectrum (Figure 1) of these sensors. However, when these sensors are again accessed to get their locations, we are able to see the location as well as the spatial spectrum of only those sensors which are present in the areas which are not sensitive or which are open i.e., not encrypted. However, the location of rest of the sensors cannot be seen, as the location of the sensors in this case has been encrypted.

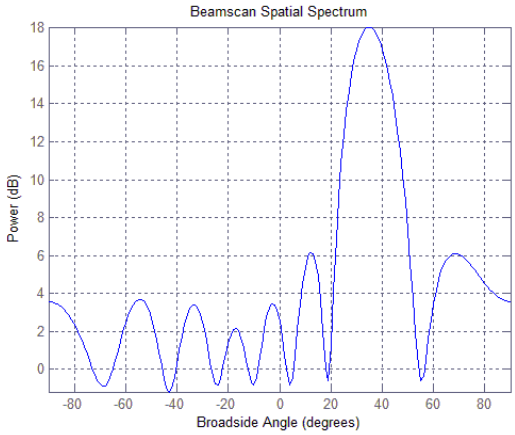

Figure 1: *Spatial Spectrum*

e-ISSN: 2321-1814
ISBN (Print): 978-1-62951-521-2

Algorithm for Encrypting Sensors Location

Algorithm 1 Algorithm for Encrypting Sensors Location.

Require: For all the sensor nodes deployed. Simulate the signal received from each sensor. Store the direction of arrival of signal i.e., angle at which the sensor is located.

Ensure: To define latitude & longitude.

1: Start clock to measure performance.
2: Obtain GPS positions of sensors using extended kalman filter.
3: `Perform mutation`
4: initialize bb, enbeq
5: enbeq = bb + dist.
6: Calculate the length of enbeq and store it to variable l.
7: for k < − 1 to l-1.
8: Select a solution and mutate each bit of k from population.
9: End of for loop.
10: `Perform crossover`
11: Select a solution k from the population.
12: Flip each bit of k and generate a new matrix.
13: For decryption follow the reverse of above process.
14: Display the location of unencrypted sensors.
15: Stop and store timer.
16: Calculate remaining bandwidth.
17: Plot time taken to encrypt the locations.
18: Plot the remaining bandwidth.

Analysis and Simulation Results

We have encrypted the locations first using the AES algorithm and our proposed Genetic Algorithm. The following results were observed: (Figure 2) A plot between the number of nodes and time shows that the time taken by proposed algorithm is less compared to AES. Figure 3 shows that the bandwidth consumed by the proposed algorithm is less compared to AES.

e-ISSN: 2321-1814
ISBN (Print): 978-1-62951-521-2

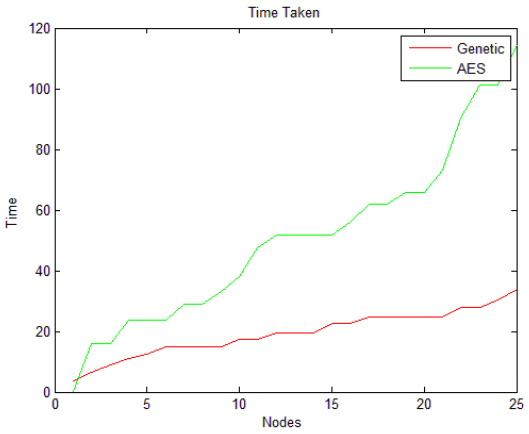

Figure 2: *Time Calculation*

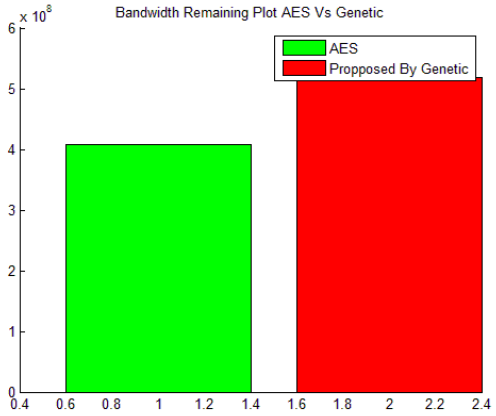

Figure 3: *Bandwidth Remaining*

Conclusion

In this paper, we have discussed localization technology in WSNs, and how this is important to various applications. The paper also discusses various techniques to discover the sensors location. Since we are focussing on securing the location of those areas where the sensors are present so that no one can access them. The paper discusses a method to encrypt those areas.

e-ISSN: 2321-1814
ISBN (Print): 978-1-62951-521-2

References

[1] B. Karp and H. T. Kung, **GPSR: Greedy Perimeter Stateless Routing for wireless networks**, in Proceedings of the 6th Annual International Conference on Mobile Computing and Network, pp. 243-354,2000.

[2] D. Liu and P. Ning, **Location-based pairwise key establishments for static sensor networks**, in Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks, pp. 72-82,2003.

[3] S. U. Sastry, N. and D. Wagner, **Secure verification of location claims**, in Proceedings of the 2nd ACM workshop on Wireless security, September 2003.

[4] J. Yick, B. Mukherjee, and D. Ghosal, **Wireless sensor networks: a survey**, Computer Networks, vol. 52, no. 12, pp. 2292-2330, August 2008.

[5] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, **Wireless sensor networks: a survey**, Computer Networks, vol. 38, no. 4, pp. 393-422, March 2002.

[6] Y. Zeng, J. Cao, J. Hong, and L. Xie, **Secure localization and location verification in wireless sensor networks,** in IEEE 6th International Conference on Mobile Adhoc and Sensor Systems, pp. 864-869, October 2009.

[7] Bible S, Zyda M, Brutzman D; **Using Spread Spectrum Ranging Techniques for Position Tracking in a Virtual Environment**. Second IEEE Workshop Networked. 2000.

[8] Steggles P, Gschwind S; **The Ubisense Smart Space Platform**. In Proceedings of the Third International Conference on Pervasive Computing, 2005.

[9] Bulusu N, Heidemann J, Estrin D; **GPS-less low cost outdoor localization for very small devices**. IEEE Personal Communications Magazine 7. 5. 2000.

[10] Nicolescu D, Nath B; **Ad-Hoc Positioning Systems**. In Proceedings of IEEE GLOBECOM. 01 November 2001.

[11] He T, Huang C., Blum B, Stankovic JA, Abdelzaher T; **Range-Free localization schemes in large scale sensor networks**. In ACM International Conference on Mobile Computing and Networking (Mobicom). 2003.

e-ISSN: 2321-1814
ISBN (Print): 978-1-62951-521-2 *References*

[12] Preetam Suman and Amrit Suman, **An Enhanced TCP Corruption Control Mechanism For Wireless Network**, HCTL Open International Journal of Technology Innovations and Research, Volume 1, January 2013, Pages 27-40, ISSN: 2321-1814, ISBN: 978-1-62776-012-6.

[13] Arvind Kumar and Tanmay De, **A Survey on Routing Protocols for Mobile Ad-hoc Networks (MANETs)**, HCTL Open International Journal of Technology Innovations and Research, Volume 5, Sept 2013, ISSN: 2321-1814, ISBN: 978-1-62840-986-4.

[14] Anil Kumar Khurana and Vishal Srivastava, **QoS and Energy Efficient Routing Protocols in WSN**, Edition on Wired and Wireless Networks: Advances and Applications, Volume 3 - November 2013 of HCTL Open Science and Technology Letters (STL), ISSN: 2321-6980, ISBN: 978-1-62951-015-6.