LOCATION DISCOVERY WITH SECURITY IN WIRELESS SENSOR NETWORK

Mahadevi G

Assistant Professor,
Department of Computer Science & Engineering
Karpagam University, Coimbatore

ABSTRACT : Localization is one of the supporting technologies in wireless sensor networks. To identify the exact location of each and every sensor may not be feasible. In most of the sensor network application gathered by sensor will be meaningless without the location of sensor nodes. The researchers involve identifying localization of sensor node for the past years. The localization places a vital role in wireless sensor network. Exchange information with the environment through sensor and implement the function of collecting and delaying with data. Various techniques are available to locate the sensor node from the network. As sensor node is tiny device, it is not easy to develop an application for wireless sensor network security. In this paper we describe the different type of approaches of node localization discovery in wireless sensor networks and we describe the architecture of elliptic curve cryptography processor for network security.

Keywords-WSN, Localization, ToA, TDoA, RSSI, Angle Estimation, Distance Estimation

I. INTRODUCTION

In the recent past, development of network technologies had prompted researchers to opt wireless sensor networks as an effective alternative for data collection, which reduced the cost and complexity of the network. Wireless sensor network works properly only based on the position information. A large scale wireless sensor network is a large collection of wireless sensor nodes that are resource constrained and are distributed spatially in an area of interest [1]. Some of the potential applications of wireless sensor networks include; environmental monitoring, military surveillance, etc. [2]. Wireless sensor nodes must operate in a cooperative and distributed manner. Such nodes are usually embedded in a physical environment to report sensed data to a central base station [3]. For example in monitoring a forest for fire detection, thousands of wireless sensors are deployed randomly and equipped with heat sensors which can detect a fire. Based on the sensor collected information, a base station generates approximate picture of the event and trigger an alarm for immediate action [4]. Another example is when thousands of tiny wireless sensor nodes are deployed to monitor the activities in a battlefield. By forming self-organizing wireless sensor network, the sensor nodes can collect and filter out raw data for relevance and report events to a base station [3]. For a sensor network to be useful, it is vital to identify positions of its sensor nodes. Localization of sensor network is one of the supporting technologies in sensor nodes. The problem of sensor localization is defined as to estimate the positions or spatial coordinates of wireless sensor nodes. Localization is an inevitable challenge when dealing with large-scale wireless sensor networks.

II. SENSOR LOCALIZATION TECHNIQUE

A sensor node from the wireless sensor network can be identified by the two phase: -

A. Distance or Angle Estimation
B. Distance or Angle Combination

A. Distance or Angle Estimation

The distance between one node to another node has been declared as d1, d2,… dn. From the figure 1 n1 transmit the signal to the bacon node n2. Filled circle is a co-ordinator node and hallow circle is bacon node) n2 finds the approximate distance d1 between n1 and n2 by auto configuration. Now n2 acts as a co-coordinator and passes the signal to n3and n3 finds the distance d3 between n2 and n3.

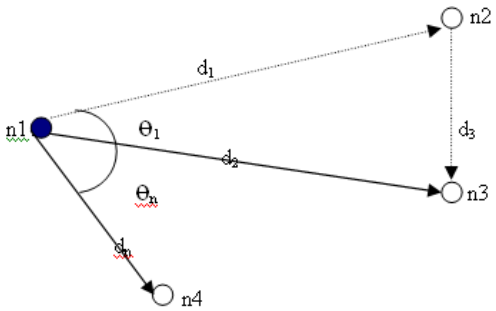

Figure 1. Distance or Angle estimation

All the nodes find the distance between them and neighbor node. Based on the distance between the co-ordinator node and bacon node the bacon node identifies the nearest node and transmits the signals. When the signal passes from one node to another node it is not transmitted in a string line as the wireless sensor network is in a mesh network. It passes the signals randomly with ɵ degree. So the identification of localization is much useful using distance estimation technique.

The followings are using for estimating the distance between two nodes :

1) Received Signal Strength Indicator (RSSI)

The power of the signal in the receiver measures by RSSI. The transmission poser and strength identifies by RSSI and the effective movement of signals through sensor loss can be calculated [3]. There is a option to translate this loss in to distance by using theoretical models. RSSI only gives the better solution with out any devices. When compare with ranging techniques, this is not good due to multipath propagation of radio signals [7]. In [8] the authors describe to measure algorithm for RSSI

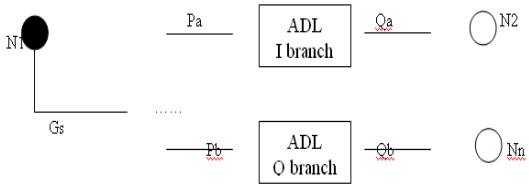

Figure 2. Received Signal Strength Indicator (RSSI)

The signal is passed from node N1 through Gs. The input signal strength is Pa. Pa is converted from analog to digital and passed as Qa . Like that, when the signal passes to the node it has been converted from Pb to Qb. So the following expression can be used to measure the strength of the signal

$\sigma Pa2 = \sigma Pb2 = \sigma P2$ and $\sigma Qa2 = \sigma Qb2$

2) Time Based Methods (ToA, TDoA)

The time based methods records the Time of Arrival or Time- Difference-of-Arrival(TDoA). According to sensor network each and every sensor transmits the signals to neighbor nodes. The travel time of the signal can be directly translated into distance, based on the known signal propagation speed. The carrier frequency of the signal and speed in air measures the distance between transmitter and receiver. The system has to be synchronous to find the range estimation using ToA.

3) Angle of Arrival

Angle of Arrival is a angle between propagation direction of the signal and some reference direction given by the nodes. If the position in a particular direction ɵ , the AoA is absolute otherwise it is relative. Generally an antenna array on sensor node measure AoA.

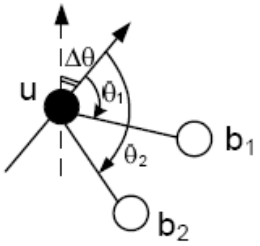

Figure 3. Angle of Arrival (AoA)

[6] Hence ɵ1 , ɵ2 are angles of bacon node b1, b2 respectively . It is measure by u. An antenna array is Δɵ are the relative AOAs of the signals sent from beacons b1 and b2. Now b1, b2 can be calculated as ɵi + Δɵ(mod 2π)

While two or more non-collinear are available, U intersect all the rays with particular angle. If the AoA cannot be obtained, the AoA difference can be used.

B. Distance or Angle Combining

According to the distance or Angle combining, the nodes used all the estimated distance to detect the actual location. It combines the distance or angle , based on that finds the localization in wireless sensor networks. The combining phase categorized as followings

a) Hyperbolic Trilateration
b) Triangulation
c) Maximum Likelihood estimation

1) Hyperbolic Trilateration

This estimation estimates the position of a node y minimizing the difference between measure distance and estimated distance. It is multilateration process. According to this different types of hyperbole generated, based on that the Time difference of Arrival (TDoA). Each and every hyperbole intersect in a place. From the intersected point this process calculated. Time difference of arrival of a signal emitted by the sensor to in three or more neighbor node. The neighbor node which receives the signal is calculated with tightly synchronized clocks. If N nodes are used as a receiver it results N-1 hyperboles and the position of the nodes intersects in a three dimensional space. If many number of receivers are used it can be solved by least square method.

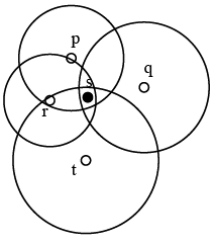

Figure 4. Hyperbolic Trilateration

2) Triangulation

This method gathers Angle of Arrivle (AoA) measurement at the sensor network from least three nodes. It identifies the location of node only when direction of the node instead of the distance is estimated. Using trigonometry laws the position of node will be calculated.

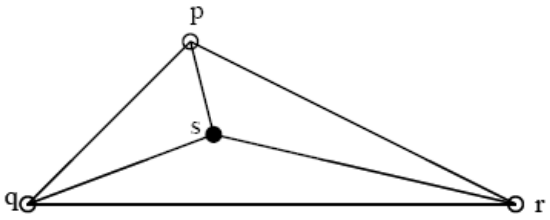

Figure 5.

3) Maximum Likelihood estimation:

It is a basic method of determining the relative positions of nodes using geometry of triangles. It locates the node by calculating the intersection of three circles. It gathers three number of reference in tuble form (x, y, d) where d is a distance between x and y. There are three reference points needed for accurate detection of location and find the relative location.

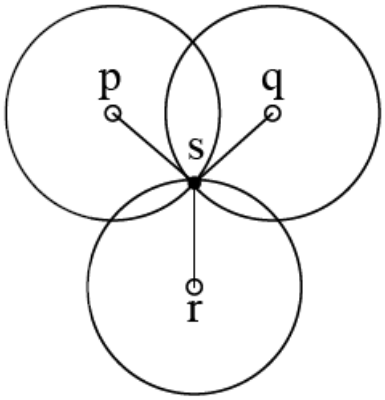

Figure 6. Maximum Likelihood estimation

III. SECURITY FOR WSN

As sensor is a tiny device, the application of security should be small. Then only the security application not affects performance of node in Wireless sensor Network. According to security the recent Elliptic Curve Cryptography can be applied.

A. General Architecture for Elliptic Curve Cryptography

The Elliptic Curve processor (ECP) is shown figures. The operational blocks of ECC processor consist of Control Unit, Arithmetic unit, ROM and RAM. All the parameters and constant values of ECC stored in Read Only Memory. RAM communicates with ROM and ALU, it contains input and output variables. Control Unit directs ALU for addition, multiplication and squaring. [18] algorithm only used point multiplication. When the START signal is set the bits of K= $\sum_{i=0}^{nk-1} k_i 2^i, k_i : \{0,1\}, n_k = [\log_2 K]$ is calculated and new value stored in P1 and P2. An internal counter END the signal after all bits has been evaluated. The result of Pl calculation is written into the output register and VALID output is set. The control units consist of many simple state machine with encounter.

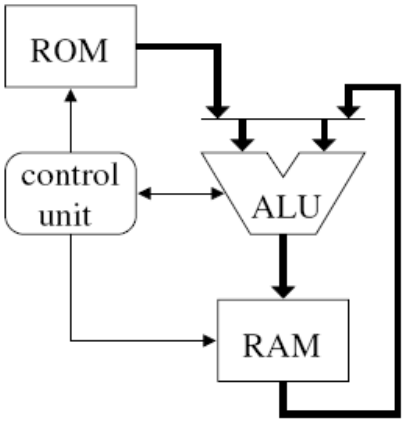

Figure 7. Elliptic Curve Cryptograph Processor

The processor memory comprises of the equivalent to five n-bit (n=p) register. In [20] the author used a Modular Arithmetic Logic Unit (MALU). It reduces the power less than 30µW if the frequency is 500kHz.

IV. CONCLUSION AND FUTURE WORK

This paper presented the approaches of different location ideitifaction of sensor node from wireless network and security applied into sensor nodes. It describes to identify the nodes in two methods that the Distance or Angles of arrival and distance or Angles combinations. According to the security appllication we discussed elliptic curve cryptography and explained about the architecrue of Elliptic Curve Cryptograph process. In the future work it can be implement and test with various frequency.

REFERENCE

[1] P. Bahl and V. N. Padmanabhan. RADAR: An In-Building RF-Based User Location and Tracking System. In Proceedings of the IEEE INFOCOM ’00, March 2000.
[2] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “Wireless sensor networks:Asurvey,” Comput. Netw., vol. 38, no. 4, pp. 393–422, 2002.
[3] A. A. Ahmed, H. Shi, and Y. Shang, “Sharp: A new approach to relative localization in wireless sensor networks,” in Proceedings of IEEE ICDCS, 2005.
[4] C. Savarese, J. Rabaey, and J. Beutel, “Locationing in distributed ad-hoc wireless sensor networks”, in Proceedings of IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP'01), May 2001, Salt Lake City, Utah, USA, vol. 4, pp. 2037-2040.
[5] Y. Xu, J. Heidemann and D. Estrin. Geography-Informed Energy Conservation for Ad Hoc Routing. In Proceedings of MOBICOM ’01, Rome, Italy, July 2001.
[6] Network Protocols and Algorithms ISSN 1943-3581 2010, Vol. 2, No. 1 Rui Huang, Gergely V. Zaruba, and Manfred Huber, “Complexity and Error Propagation of Localization Using Interferometric Ranging”, in Proceedings of IEEE International Conference on Communications ICC 2007, pp. 3063-3069, Glasgow, Scotland, June 2007
[7] J. J. Cho, Y. Chen, and Y. Ding, “On the (co)girth of connected matroids,” Discrete Appl. Math., vol. 155, pp. 2456–2470, 2007.
[8] C. Aykanat, A. Pinar, and Ü. V. Çatalyürek, “Permuting sparse rectangular matrices into block-diagonal form,” SIAM J. Sci. Comput., vol. 25, pp. 1860–1879, 2004.
[9] [Online]. Available: http://www.splus.com
[10] [Online]. Available: http://www.sas.com
[11] A. Srinivasan, J. Teitelbaum, J. Wu. DRBTS, “Distributed Reputation-based Beacon Trust System”, 2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing (DASC ’06), September 2006, Indianapolis, USA, pp. 277-283.
[12] J. Bachrach and C. Taylor, "Localization in Sensor Networks," in Handbook of Sensor Networks:Algorithms and Architectures, I. Stojmenovic, Ed., 2005.
[13] Available HTTP : http://www.cse.ust.hk/~yangzh/yang_pqe.pdf.
[14] Yi Shang, Hongchi Shi and A. Ahmed, “Performance study of localization methods for ad-hoc sensor networks”, in proceedings of IEEE International Conference of Mobile Ad-hoc and Sensor Systems, Fort Lauderdale, FL, October 2004.
[15] Eiman Elnahrawy, Xiaoyan Li and Richard P. Martin, “ The Limits of Localization Using Signal Strength: A Comparative Study, in Proceedings of IEEE SECON, pp. 406-414, Santa Clara,
[16] California, USA, October 2004.Jaime Lloret, Jesus Tomas, Miguel Garcia, Alejandro Canovas, “A Hybrid Stochastic Approach for Self-Location of Wireless Sensors in Indoor Environments” Sensors 9, no. 5: 3695-3712.
[17] 2. G. Gaubatz, J.-P. Kaps, E. ¨Ozt¨urk, and B. Sunar. State of the Art in Ultra-Low Power Public Key Cryptography for Wireless Sensor Networks. In 2nd IEEE International Workshop on Pervasive Computing and Communication Security (PerSec 2005), Kauai Island, Hawaii, March 2005.
[18] 3. G. Gaubatz, J.-P. Kaps, and B. Sunar. Public Key Cryptography in Sensor Networks - Revisited. In 1st European Workshop on Security in Ad-Hoc and Sensor Networks (ESAS 2004), Heidelberg, Germany, August 2004.

[19] 4. IEEE P1363. Standard specifications for public key cryptography, 1999.
[20] L. Buttyan, V. Gligor, and D. Westhoff (Eds.): ESAS 2006, LNCS 4357, pp. 6-17, 2006. Springer-Verlag Berlin Heidelberg 2006