Graduate Research in Engineering and Technology (GRET)

Volume 1 | Issue 2 Article 9

October 2013

IMPERTINENT TRILATERATION: SECURE LOCALIZATION OF WIRELESS SENSOR NETWORK USING GREEDY TECHNIQUE

M. B. NIRMALA
Department of Computer Science and Engineering, Siddaganga Institute of Technology, Tumkur, Karnataka, India, nirmalamb@gmail.com

Mr. NAYANA
Department of Computer Science and Engineering, Siddaganga Institute of Technology, Tumkur, Karnataka, India., nayanaj169@gmail.com

A.S MANJUNATH
Department of Computer Science and Engineering, Siddaganga Institute of Technology, Tumkur, Karnataka, India., asmanju@sit.ac.in

IMPERTINENT TRILATERATION: SECURE LOCALIZATION OF WIRELESS SENSOR NETWORK USING GREEDY TECHNIQUE

NAYANA, M.B.NIRMALA, A.S MANJUNATH

[1,2,3] Department of Computer Science and Engineering, Siddaganga Institute of Technology, Tumkur, Karnataka, India.
Email: nirmalamb@gmail.com,nayanaj169@gmail.com, asmanju@sit.ac.in

Abstract-Wireless sensor network localization is an important area that attracts significant research interest. Current localization algorithms mainly focus to localize as many nodes as possible for a given static set of anchor nodes and distance measurement. In this paper, we discuss a new technique that aims to localize all the sensor nodes in the network using trilateration with greedy technique, and a security protocol is used for providing confidentiality and authentication between anchor nodes and sensor nodes.

Keywords-*Wireless Sensor, Localization, Trilateration, Greedy technique, Security Protocol.*

I. INTRODUCTION

Knowledge of position of the sensing nodes in a Wireless Sensor Network (WSN) is a necessary part of many sensor network operations and applications. Sensors reporting monitored data of the deployed location.

Many localization algorithms have been proposed to localize sensor nodes by exchanging information with anchor nodes.The basic idea is nodes measure distances to their neighbors and share their position information with their neighbors to compute their positions. Sensor node whose position has already been uniquely determined, it can act as a new anchor node to localize other nodes by sharing its position with its neighbors. This iterative process continues until there are no nodes can be further localized.

Many localization algorithms have been designed for wireless sensor networks.Trilateration is a basic localization technique [1, 2], it uses the known locations of multiple anchor nodes and distance measurement to each anchor node to determine the accurate location of a node in a 2D sensor network, and it needs to hear from at least three anchors. Iteratively by applying trilateration it is possible to identify localizable nodes in a network, iterative trilateration is used to localize nodes via multi-hop.

Since trilateration can only recognize a subset of sensors even when the sensor network is globally rigid.. Yang et al. [3] proposed a localization method based on detection of wheel structures to further improve the performance of localization. Their method is based on the following claim made by them that all nodes in a wheel Structure with three anchor nodes is uniquely localizable, since existing localization methods try to

localize more sensor nodes in a network without guarantee of localizing all nodes.

To overcome the limitation of trilateration, this paper proposed a new technique which aims to localize all sensor nodes in a network using minimum number of anchor using trilateration with greedy technique, and analysis the security of the sensor network using RC5 encryption protocol and SHA-1 authentication algorithm.

The rest of this paper is organized as follows: Section II consists of background and related works. Section III consists of proposed algorithm. Section IV analysis the security. Section V analysis the performance of proposed technique. Finally section VI gives the conclusion.

II. BACKGROUND AND RELATED WORKS

A. BACKGROUND

The most of existing location discovery approaches consist of two basic phases: (1) distance (or angle) estimation and (2) distance (or angle) combining. The most popular methods for estimating the distance between two nodes are:

Received Signal Strength Indicator (RSSI) techniques measure the power of the signal at the receiver. Based on the known transmit power, the effective propagation loss can be calculated. Theoretical and empirical models are used to translate this loss into a distance estimate. This method has been used mainly for RF signals.

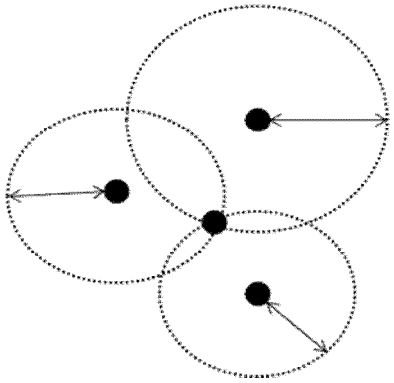
Time based methods (ToA, TDoA) record the time of-arrival (ToA) or time-difference-of-arrival (TDoA).The propagation time can be directly translated into distance, based on the known signal propagation speed. These methods can be applied to many different signals, such as RF, acoustic, infrared and ultrasound.

Angle -of -Arrival (AoA) systems estimate the angle at which signals are received and use simple geometric relationships to calculate node positions.

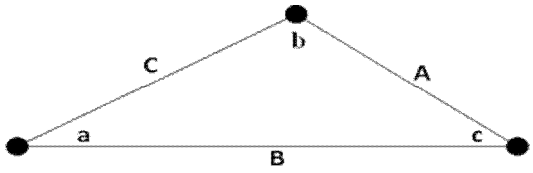
A detailed discussion of these methods can be found in. For the combining phase, the most popular alternatives are:

- The most basic and intuitive method is called hyperbolic trilateration. It locates a node by calculating the intersection of 3 circles (figure 1a).

- Triangulation is used when the direction of the node instead of the distance is estimated, as in AoA systems. The node positions are calculated in this case by using the trigonometry laws of sines and cosines.(figure 1b)



(a)



(b)

$$sine\ Rule = \frac{A}{sina} + \frac{B}{sinb} + \frac{C}{sinc}$$

$$C^2 = A^2 + B^2 + 2AB_{cos\,(c)}$$

$$Cosine\ Rule \quad B^2 = A^2 + C^2 + 2BC_{cos\,(b)}$$

$$A^2 = B^2 + C^2 + 2BC_{cos\,(a)}$$

Figure1. Localization Basics a) Hyperbolic Trilateration b) Multilateration

B. RELATED WORK.

In this section, we analyze some of the basic theorem and recent works on localization in wireless sensor network.

1. Trilateration

Trilateration is the most basic technique for positioning system and has been used for thousands of years. It uses the known locations of multiple anchor nodes and the measured distance to each anchor node. In [4] proposed a new distributed technique that only requires a limited fraction of the nodes to know their exact location (either through GPS or manual configuration) and that nevertheless can attain network-wide fine-grain location awareness. The technique, which is called AHLoS (Ad-Hoc Localization System).

2. Rigidity theory.

In many network localization systems recently have been proposed and evaluated, there has been no systematic study of partially localizable networks, networks in which there exist nodes whose positions cannot be uniquely determined. There is no existing study which identifies which nodes in a network are uniquely localizable and which are not. In [5] proposed the framework for two dimensional network localization to determine which nodes are localizable and which are not. This system is implemented to conduct comprehensive evaluations of network localizability. In [6] proposed a theoretical foundation for the problem of network localization in which some nodes know their location and other nodes determine their location by measuring the distance to their neighbors.

Theorem 1: Given a formation graph G with $n>=2$ vertices in the plane (resp. $n>=3$ vertices in 3-space) the following are equivalent:

1) for some formation *Fp* with this graph, rank $R(Fp) = 2n - 3$ (resp. rank $R(Fp) = 3n - 6$ in 3-space);

2) for all $q \in IR^{2n}$ in an open neighborhood of *p*, the formation *Fq* on the graph G is first-order rigid in the plane (resp. $q \in IR^{3n}$, *Fq* is first-order rigisd in 3-space);

3) for all *q* in an open dense subset of IR^{2n}, the formation *Fq* on the same graph G is first-order rigid in the plane (resp. open dense subset of IR^{3n}, *Fq* is first-order rigid in 3-space).

When property 3) holds, we say that the graph G of *Fp* is generically rigid in the space. It is well known that first-order rigidity implies all of the other standard forms of rigidity for a formation, but the converse can fail [7], [8], [9].

For the plane we have a strong combinatorial characterization of the generically rigid graphs. We

note that this leads to a fast $(O(|V|^2)$ algorithm for generic rigidity testing [10].

Theorem 2 Given a non-degenerate formation *Fp* with a non-trivial flex *q*, the formations F_{p+tq} and F_{p-tq} on the same graph, for all $t > 0$, have the same edge lengths for all links but are not congruent.

We say that a formation *Fq* is generically globally rigid if every sufficiently small perturbation *q* of *p* creates a globally rigid formation *Fq*. The result above shows that any non- degenerate generically globally rigid formation *Fp* must be first-order rigid. However, as Fig.2 illustrates, the converse is not true.

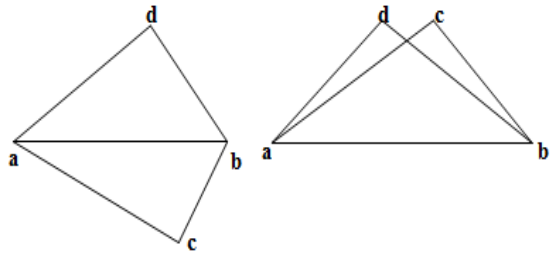


Figure 2 Two first-order rigid formations with the same graph and the same distance value

A graph *G* is redundantly rigid in IR^d if the removal of any single edge results in a graph that is also generically rigid in IR^d. As Fig. 3 suggests, we need the graph to be generically redundantly rigid to ensure generic global rigidity.

Recall that a graph *G* is k-connected if it remains connected upon removal of any set of $< k$ vertices. The k-connectivity of a complete graph with *n* vertices is defined to be *n*.

1. A simple mental check also confirms that for more than

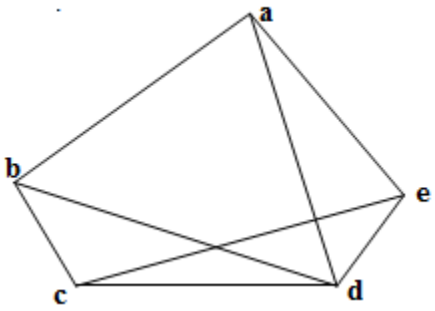


Figure 3 A globally rigid formation in the plane

$d + 1$ vertices in dimension d, we need at least $d + 1$ vertex connectivity, to avoid a reflection of one component through a mirror placed on a disconnecting set of size *d*.

An graph G = *{V, £}* with *n* vertices is generically globally rigid in IR^d if there is an open dense set of points $p \in IR^{dn}$ at which *Fp* is a globally rigid formation with link set *L*. In the plane, a recent result gives a complete characterization of generically globally rigid graphs.

III. PROPOSED SYSTEM

In this section we propose a new technique to overcome the limitation of trilateration. Figure 4, illustrates the set of sensor nodes that have been deployed to illustrate the localization of sensor nodes in wireless sensor network. In this network anchor nodes need to propagate the whole network for localizing the sensor nodes. Hence more number of anchor nodes is required for localization of sensor nodes. To minimize number of anchor nodes involved in the localization of network new technique Impertinent Trilateration have proposed which aims to localize more number of sensor nodes using trilateration with greedy technique.

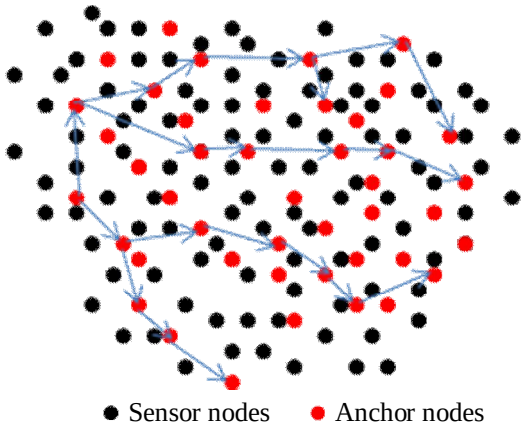


Figure 4 Set of nodes deployed in the network.

Algorithm: Impertinent Trilateration

1: Consider group *G (V, E)* in a network
2: ∀ V_i in *G (V, E)* is anchor node
3: ∀ *V* in *G[V]*
4: **if** *Vi* € anchor nodes then
5: V_i←Visited
//Apply prim's algorithm
6: *T* := a minimum-weight edge
7: **for** i = 1 to $n - 2$
8: begin
9: *e* := an edge of minimum weight incident to a vertex in *T* and not forming a circuit in *T* if added to *T*
10: *T* := *T* with *e* added
11: **end for**
12: return(*T*)
13: **end if**
14: ∀ V_i in Spanning tree (*G'[V]*)
15: Apply trilateration to the constructed Spanning tree
16: **end**

The algorithm proclaims the working of proposed technique. This algorithm works in an iterative manner, firstly the network region is divided into four part as illustrated in Figure 5, and in each region the anchor nodes are involved in the construction of spanning tree. As in line 2 for every vertex V_i it checks whether the node is anchor node, if node is an anchor node it is marked as visited in line 5. From line 6 to line 11 and spanning tree is constructed for visited anchor nodes for a minimum weighted edge. For the constructed spanning tree trilateration is applied at line 15 until all the nodes in the network is localized. This is done parallel in all four regions of a network. This procedure from line 5 to line 15 repeats until all the sensor nodes are localized in the network. The deployed nodes in the network marked in the current iteration acts as an anchor node. Localizability information diffuses step by step and covers the entire network after several iteration.

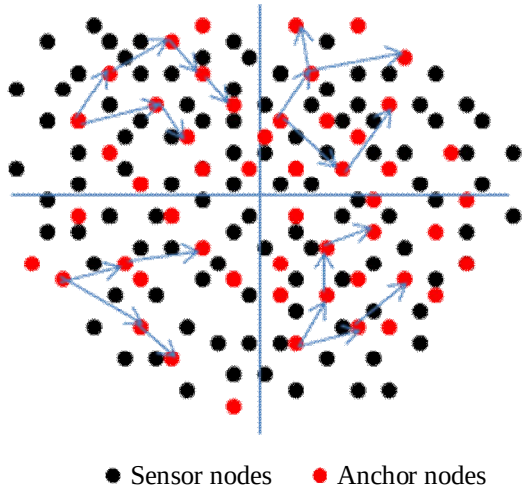


Fig 5 Network divided into four region.

The figure 5 illustrates that on dividing the network into four regions the number of anchor nodes involved in localizing the network is less, and also construction of spanning tree in the network for the anchor nodes can localize the network using minimum number of anchor nodes when compare to traditional technique.

IV. SECURITY ANALYSIS.

Security has become a challenge in wireless sensor network. In order to design a secure network, several aspect need to be consider like Key establishment, trustsetup, secrecy, authentication, and privacy. A secure and efficient key distribution mechanism is needed for large scale sensor networks. Once every node has its own keys, these are used to authenticate and encrypt the message they exchange. Several protocols have been proposed in the literature related to authentication and privacy [11][12] and key distribution [13][14][15].

For the proposed technique Impertinent Trilateration we analyze the security of the network by providing confidentiality and authentication between anchor nodes and sensor nodes. Initially the anchor nodes of the sensor network will generate the random numbers and forwards to all sensor nodes in the network. Similarly all sensor nodes generate an unique ID and send back to anchor nodes. After anchor node receive the ID's of sensor nodes which will be used as an encryption key and will send the encrypted message to the respective sensor node.

Each message includes a Message Authentication Code (MAC). It is computed once for each package. When an agent receives a message, it computes the message MAC and compares with the received MAC.

If they are equal, the message is accepted. The MAC allows endpoints to prevent modifications of the message in transit. It also allows them to authenticate data origin because it share symmetric key between sender and receiver.

The following notation are used to describe the protocol

Km	Master key shared between the node and the base station
Kenc	Encryption key derived from the master key
Kmac	MAC computing key derived from the master key
Ctr	Shared counter between transmitter and receiver
MAC (M)	Message Authentication Code function computed over message M
$\{M\}_K$	Message M encrypted with key K

A message M between two nodes S and R secured with
RC 5 and SHA 1 is the following:

$S \rightarrow R: \{Ctr\}_{Kenc} \oplus M, MAC(K_{mac}, \{\{Ctr\}_{Kenc} \oplus M\})$

Where Kenc and Kmac are derived keys from a master key Km. This master key is shared with the anchor node and sensor node before its deployment. The rest of keys are derived from the master key by means of a pseudo-random function.

V. PERFORMANCE ANALYSIS.

The localization is one the most important issue since sensing data without locations is almost meaningless.

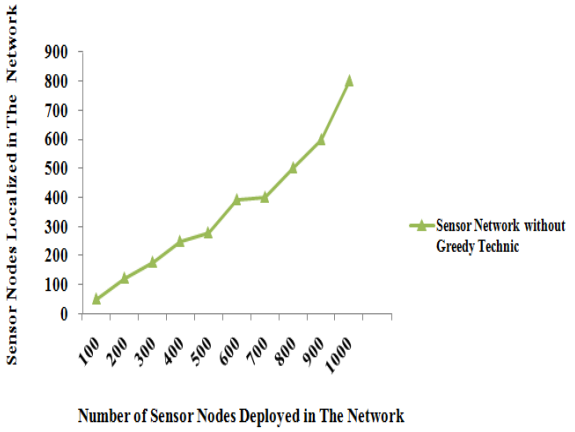


Figure 6 Sensor Network without Greedy Technique

Both Fig 6 and Fig 7 gives plot of number of sensor nodes localized in the network. Where in Fig 6 denotes number of nodes localized without using greedy technique, it illustrate the localization of nodes in the localizable network Only 50% of the nodes are localized when 500 nodes are deployed where in Fig 7 which denotes number of nodes localized using greedy technique around 80% of the nodes are localized.

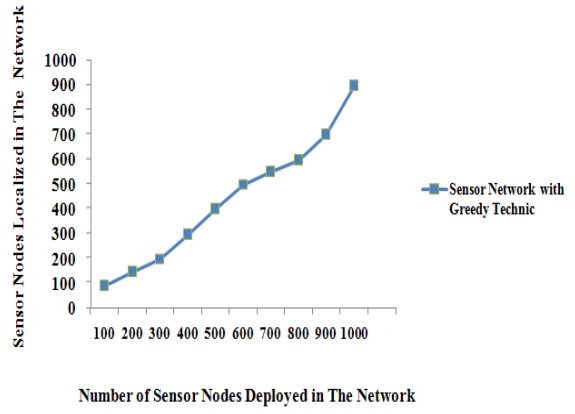


Figure 7 Sensor Network with Greedy Technique

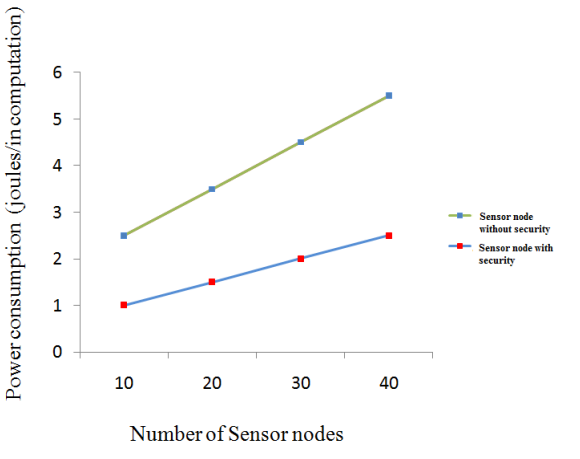


Figure 8 Energy Consumption for Sensor nodes

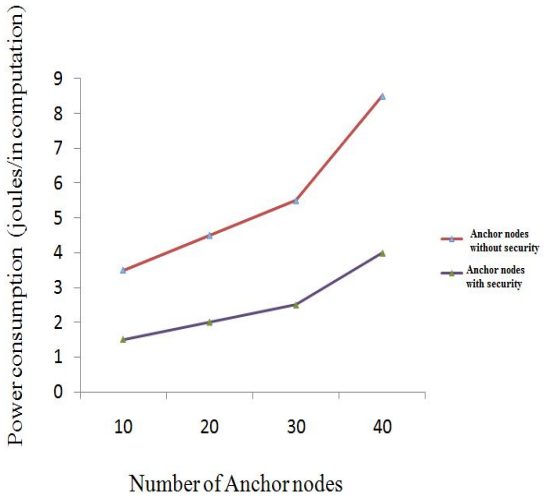


Figure 9 Energy Consumption of Anchor nodes

From the figure 8 gives the plot of energy consumption of the sensor nodes in the network after each decryption and authentication of the sensor node. It illustrate that there won't be much variation in the energy consumption in the network after providing the confidentiality and authentication.
Similarly the figure 9 gives the plot of energy consumption of the anchor nodes in the network.

VI. CONCLUSION.

Trilateration is basic building block of many existing localization algorithms, often wrongly recognizes localizable graphs as non-localizable. To address the issue, we analyze the limitation of trilateration based approaches and proposed a new technique which aims to localize more number of sensor nodes using trilateration with greedy technique. Performance analysis is made to test the localizability of the sensor network when compare to traditional technique, and further RC5 and SHA1 protocols is used to achive the confidentiality and authentication between anchor nodes and sensor nodes. So from the results we conclude that energy consumption is increased that the cost of security which vary is much required for many application.

REFERENCES.

[1] A. Savvides, C.C. Han, M.B. Strivastava, Dynamic fine-grained localization in ad-hoc networks of sensors, in: ACM MobiCom, 2001.

[2] A. Savvides, H. Park, M.B. Srivastava, The bits and flops of the n-hop multilateration primitive for node localization problems, in: Proc. Of ACM Int'l W. on Wireless Sensor Networks & Applications, 2002.

[3] Z. Yang, Y. Liu, X.-Y. Li, Beyond trilateration: On the localizability of wireless ad-hoc networks, in: Proc. of IEEE INFOCOM, 2009.

[4] A. Savvides, C. C. Han and M. B. Srivastava Dynamic Fine-grained Localization in Ad-Hoc Networks of Sensors,Proceedings of the seventh annual international conference on Mobile computing and networking, Mobicom 2001, pp 166-179,Rome, Italy, July 2001

[5] D.K. Goldenberg, A. Krishnamurthy, W.C. Maness, Y.R. Yang, A.S. Morse, A. Savvides, Network localization in partially localizable networks, in: Proc. of IEEE INFOCOM, 2005.

[6] J. Aspnes, T. Eren, D.K. Goldenberg, A.S. Morse, W. Whiteley, Y.R. Yang, B.D.O. Anderson, P.N. Belhumeur, A theory of network localization, IEEE Trans. Mob. Comput. 5 (12) (2006) 1–15.

[7] B. Roth, "Rigid and flexible frameworks," American Mathematical Monthly, vol. 88, pp. 6–21, 1981.

[8] W. Whiteley, "Some matroids from discrete applied geometry," in Contemporary Mathematics, James G. Oxley Joseph E. Bonin and Brigitte Servatius, Eds., vol. 197. American Mathematical Society, 1996.

[9] T. Eren, W. Whiteley, A.S. Morse, and P.N. Belhumeur, "Sensor and network topologies of formations with distance-direction-angle constraints," Submitted to the 42nd IEEE Conference on Decision and Control, Hawaii, 2002.

[10] B. Hendrickson, "Conditions for unique graph realizations," SIAM J. Comput., vol. 21(1), pp. 65–84, 1992.

[11] C. Karlof, N. Sastry, and D. Wagner, "TinySec: a link layer security architecture for wireless sensor networks." in Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems, SenSys 2004, Baltimore, MD, USA, November 3-5, 2004. ACM, 2004, pp. 162–175.

[12] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler, "SPINS: Security protocols for sensor networks." Wireless Networks, vol. 8, no. 5, pp. 521–534, 2002.

[13] S. Zhu, S. Setia, and S. Jajodia, "LEAP: efficient security mechanisms for large-scale distributed sensor networks." in ACM Conference on Computer and Communications Security, S. Jajodia, V. Atluri, and T. Jaeger, Eds. ACM, 2003, pp. 62–72.

[14] H. Chan, A. Perrig, and D. X. Song, "Random key predistribution schemes for sensor networks." in IEEE Symposium on Security and Privacy. IEEE Computer Society, 2003, p. 197.

[15] L. Eschenauer and V. Gligor, "A key-management scheme for distributed sensor networks." in ACM Conference on Computer and Communications Security, V. Atluri, Ed. ACM, 2002, pp. 41–47.

[16] A. Perrig, R. Szewczyk, V. Wen, D. E. Culler, and J. D. Tygar, "SPINS: security protocols for sensor netowrks," in Mobile Computing and Networking.