International Journal of Scientific Engineering and Applied Science (IJSEAS) – Volume-2, Issue-2, February 2016
ISSN: 2395-3470
www.ijseas.com

Finding Cheating Beacon for Secure Localization In Wireless Networks

Prakruthi M.K, Dept. of CSE, SJBIT,Bangalore, Chaitra.M, Dept. of CSE, SJBIT,Bangalore

Abstract— secure distance-based localization in the presence of cheating beacon (anchor) nodes is an important problem in mobile wireless ad hoc and sensor networks. Despite significant research efforts in this direction, some fundamental questions still remain unaddressed. When the number of cheating beacon nodes is greater than or equal to a given threshold, no two-dimensional distance-based localization algorithms exist that can guarantee a bounded error. In this project, the problem of robust distance-based localization in the presence of malicious beacon nodes will assume theoretically that the number of malicious beacon nodes are below threshold and derive a necessary and sufficient condition for having a bounded localization error and use heuristic algorithm that can achieve a bounded error. Suppose if the number of cheating beacons is equal or more than the threshold will use the suspicious message detection by signal strength for detecting and eliminating malicious beacon nodes. This project verifies their accuracy and efficiency. The primary goal here is to conduct a thorough analytical study of the distance-based localization problem in the presence of cheating beacons. Finally, it shows that the heuristic-based algorithm provides good localization precision with a very small time cost.

Index Terms—Wireless sensor networks, distance-based localization, security, beacon.

1 INTRODUCTION

The Wireless sensor networks (WSNs) are shaping many activities in our society, as they have become the epitome of pervasive technology. WSNs have an endless array of potential applications in both military and civilian applications, including robotic land-mine detection, battlefield surveillance, target tracking, environmental monitoring, wildfire detection, and traffic regulation, to name just a few. One common feature shared by all of these critical applications is the vitality of sensor location. The core function of a WSN is to detect and report events which can be meaningfully assimilated and responded to only if the accurate location of the event is known. Also, in any WSN, the location information of nodes plays a vital role in understanding the application context. There are three visible advantages of knowing the location information of sensor nodes. First, location information is needed to identify the location of an event of interest. For instance, the location of an intruder, the location of a fire, or the location of enemy tanks in a battlefield is of critical importance for deploying rescue and relief troops. Second, location awareness facilitates numerous application services, such as location directory services that provide doctors with the information of nearby medical equipment and personnel in a smart hospital, target-tracking applications for locating survivors in debris, or enemy tanks in a battlefield. Third, location information can assist in various system functionalities, such as geographical routing [1, 2], network coverage checking [3], and location-based information querying [4]. Hence, with these advantages and much more, it is but natural for location-aware sensor devices to become the defacto standard in WSNs in all application domains that provide location-based service.

A straightforward solution is to equip each sensor with a GPS receiver that can accurately provide the sensors with their exact location. This, however, is not a feasible solution from an economic perspective since sensors are often deployed in very large numbers and manual configuration is too cumbersome and hence not feasible. Therefore, localization in sensor networks is very challenging. Over the years, many protocols have been devised to enable the location discovery process in WSNs to be autonomous and able to function independently of GPS and other manual techniques [5, 6]. In all these literatures, the focal point of location discovery has been a set of specialty nodes known as *beacon nodes*, which have been referred to by some researchers as anchor, locator, or seed nodes. These beacon nodes know their location, either through a GPS receiver or through manual configuration, which they provide to other sensor nodes. Using this location of beacon nodes, sensor nodes compute their location using various techniques is discussed. It is, therefore, critical that malicious beacon nodes be prevented from providing false location information since sensor

nodes completely rely on the information provided to them for computing their location The rest of the paper is organized as follows: In Section 2, we provide some background on secure localization and discuss the related work, and in Section 3, we present the network and adversary model. In Section 4, we derive the conditions for secure distance-based localization and define the class of bounded error distance-based localization algorithm. In Section 5, we propose an algorithm that belongs to this class. In Section 6, we extend the existing localization framework to include more practical distance estimation error models. We conclude the paper with a summary of contributions.

2 BACKGROUND AND RELATED WORK

In this section, we survey some earlier research efforts toward securing distance-based localization schemes. Most of the prior works in this area have followed one of the following two themes: 1) detection and elimination of cheating nodes or 2) localization in the presence of cheating nodes and large errors.

2.1 Malicious Node Detection and Elimination

One approach followed by researchers to secure distance-based localization approaches is to detect the cheating nodes and eliminate them from consideration during the localization process. Liu et al. [7] propose a method for securing beacon-based localization by eliminating malicious data. This technique, called attack-resistant Minimum Mean Square Estimation (MMSE), takes advantage of the fact that malicious location references introduced by cheating beacons are usually inconsistent with the benign ones. Similarly, the Echo location verification protocol proposed by Sastry et al. [8] can securely verify location claims by computing the relative distance between a prover and a verifier node using the time of propagation of ultrasound signals.Capkun and Hubaux [9] shortlist various attacks related to node localization in wireless sensor networks and propose mechanisms such as authenticated distance estimation, authenticated distance bounding, verifiable trilateration, and verifiable time difference of arrival to secure localization. Pires et al. [10] propose protocols to detect malicious nodes in distance-based localization approaches by detecting message transmissions whose signal strength is incompatible with its originator's geographical position. In another similar work by Liu et al. [11], the authors propose techniques to detect malicious beacon nodes by employing special detector nodes. Other nodes first compute the distance (or angle) estimates to a set of neighboring beacons and then estimate their own location using basic trilateration (or triangulation). The working of a two-dimensional beacon-based localization scheme using distance estimates to neighboring beacons. In Figure 1(a), nodes B1, B2, B3, and B4 located at positions (x1, y1), (x2, y2), (x3, y3), and (x4, y4) respectively, act as beacon nodes. The target node T estimates distances z1, z2, z3, and z4, respectively, to these beacon nodes and computes its own location by trilateration. Efficient techniques for estimating distances such as Received Signal Strength Indicator (RSSI), Time of Arrival (ToA), and Time Difference of Arrival (TDoA) exist and have been successfully used in the various beacon-based localization protocols listed above. Although beacon-based techniques are very popular in most wireless systems, they have one shortcoming. Most beacon-based techniques in the literature assume that the nodes acting as beacons always behave honestly. It is not surprising that beacon-based methods perform well when all the beacon nodes are honest. But their accuracy suffers considerably in the presence of malicious or cheating beacon nodes. Beacons can cheat by broadcasting their own locations inaccurately or by manipulating the distance estimation process, thus, adversely affecting the location computation by the other nodes. This is depicted in Figure 1(b). In this figure, we can see that beacon nodes B1, B2, and B4 behave honestly, whereas beacons B'3 and B3 cheat. This causes the target node T to compute its location incorrectly.

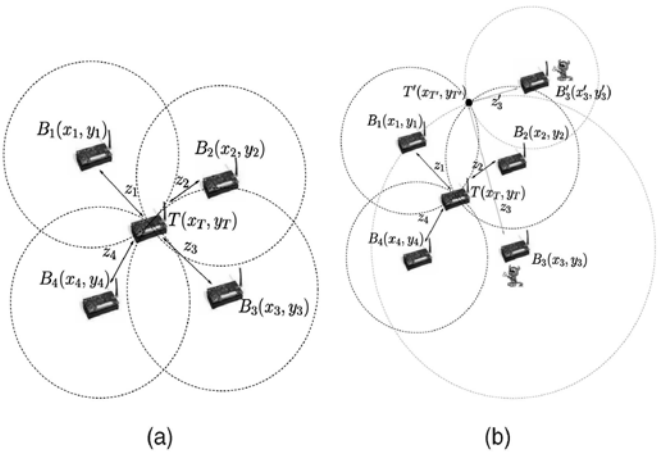

Figure 1. Distance-based (range-based) localization. (a) Trilateration. (b) Cheating beacons.

2.2 Robust Localization Schemes

The second approach toward securing localization is to design techniques that are robust enough to tolerate the cheating effect of malicious nodes (or beacons), rather than explicitly detecting and eliminating them. Priyantha et al. [12] propose the CRICKET system that eliminates the dependence on beacon nodes by using communication hops to estimate the network's global layout, and then apply force-based relaxation to optimize this layout. Some other research attempts also to solve the secure localization problem by formulating it as a global optimization problem. For example, Li et al. [13] develop robust statistical methods such as adaptive least squares and least median squares to make beacon-based localization attacktolerant.

Alternatively, Doherty et al. [6] address the problem of beacon-based localization in the presence of large range measurement errors and describe a localization method using connectivity constraints and covex optimization. Moore et al. [14] formulate the localization problem in wireless sensor networks as a two-dimensional graph realization problem and describe a beaconless (anhorfree), distributed, linear-time algorithm for localizing nodes in the presence of large range measurement noise. Liu et al. [7] design an intelligent strategy, called votingbased scheme, where the deployment area is divided into a grid of cells such that the target node resides in one of the cells. Every beacon node votes on each cell depending on the distance between the target node and itself and the location of the target node is estimated as being within the cell that had the maximum number of beacon votes. In another approach, Shang et al. [15] and Ji and Zha [16] apply efficient data analysis techniques such as Multi-Dimensional Scaling (MDS) using connectivity information and distances between neighboring nodes to infer target locations. Fang et al. [17] model the localization problem as a statistical estimation problem. The authors use Maximum Likelihood Estimation (MLE) in order to estimate the most probable node location, given a set of neighborhood observations. Recently, ideas from coding theory have also been applied to achieve robust localization, for example, [18], [19]. In another work, Lazos and Poovendran [20] propose a range-independent distributed localization algorithm using sectored antennas, called SeRLoc, which does not require any communication among nodes. However, SeRLoc is based on the assumption that jamming of the wireless medium is not feasible. To overcome this problem, Lazos et al. [21] also present a hybrid approach, called RObust Position Estimation (ROPE), which unlike SeRLoc provides robust location computation and verification without centralized management and vulnerability to jamming. In another recent research effort by Misra et al. [22], the authors propose a convex optimization-based scheme to secure the distancebased localization process, which uses Barrier's method to solve the optimization problem.

2.3 Discussion

Malicious node detection and elimination strategies, as dicussed in Section 2.1, take into account the inconsistency (caused by cheating behavior) in measurement of a particular network parameter in order to detect cheating nodes. One shortcoming of such an approach is the requirement that verifier nodes have to be completely honest. Moreover, these solutions do not provide any fixed guarantees of the number of detected cheating beacon nodes or the accuracy of the ensuing localization algorithms. Any undetected cheating beacon node will only add to the error of the localization algorithm.

On the contrary, a majority of the localization schemes discussed in Section 2.2 attempts to improve the robustness of the localization procedure by employing optimization techniques. The main focus of these schemes is to minimize the effect of inconsistent or erroneous data on the overall localization accuracy. Some shortcomings of such a strategy include the complexity of the proposed solutions, e.g., [16], [15], or sometimes the requirement of special hardware and equipment, e.g., [20]. Moreover, most of the research efforts in this direction have failed to study the feasibility of the distance-based localization problem under adverse conditions.

In view of the above, our primary goal here is to conduct a thorough analytical study of the distance-based localization problem in the presence of cheating beacons. The secure distance-based localization framework and the associated results that we present in this paper are very general. The algorithms for secure localization that we propose achieve provable security and are computationally feasible and efficient. As a matter of fact, it will be clear later that the class of bounded error distance-based localization algorithms proposed in this paper also includes other algorithms such as the optimization-based scheme by Misra et al. [22] and the voting-based technique by Liu et al. [7]. Next, we first outline the network and adversary model for the secure distance-based localization framework.

3 NETWORK AND ADVERSARY MODEL

In our network model, a device M in a nontrustworthy environment wants to compute its own location by using distance estimates to a set of beacon nodes. These beacons nodes know their own locations and may or may not cheat about their locations to the other nodes. The target node M and the beacon nodes are currently assumed to be located on a two-dimensional area (plane), i.e., the location of each of these entities can be represented as two-dimensional coordinates (x, y).

Suppose that the target node M has a total of n beacon nodes available for localization. Let these beacon nodes be denoted by B1, B2, B3. . . ,Bn. Among these n beacons, some beacons are malicious (or cheating beacons). Let k denote the number of malicious or cheating beacons. It is important to note that k is not necessarily known to the target node or to any of the honest beacons. However, the value of k clearly has a great influence on whether a bounded localization error can be achieved or not. Let kmax (<=n) be an upper bound on the number of malicious nodes, i.e., kmax is the maximum number of malicious nodes that can exist in the network at any time. The parameter kmax is a system or environment-dependent constant and is assumed to be known to the localization algorithm.

Beacons that are not malicious are honest, i.e., they fully cooperate with the localization protocol by disclosing the information as truthfully as possible. More details on the cheating behavior by the beacon nodes will follow shortly. Regardless of being honest or dishonest, each beacon Bi provides M with a measurement di of the distance between Bi and M. The precise distance between Bi and M is the euclidean distance between the position coordinates of Bi and M, and is denoted by dst (Bi, M). Let the set of honest beacons be denoted by H. Then, for each beacon Bi beloogs to H, di is a random variable that follows some probability distribution, denoted by msr(dst(Bi,M)), such that E[di]=dst(Bi,M),i.e., the expected (mean) value of the estimated distance di for each beacon Bi in H, is the precise distance between the beacon Bi and the node M. In the case when Bi is honest, the difference between the estimated and the true distance is very small, i.e.,

$$|\tilde{d}_i - dst(B_i, M)| < \epsilon, \quad (1)$$

Where ϵ is the maximum distance estimation error. Ideally, this difference should be zero, but such discrepancies in distance estimates can occur due to measurement errors, either at the source or target. Currently, ε can be assumed to be a small constant. Later, we extend the current network model to include a more practical representation for the distance estimation error.

For each beacon Bi doesnot belongs to H, i.e., a cheating beacon, the corresponding di is a value selected (possibly arbitrarily) by the adversary such that it may or may not follow (1). Note that we allow colluding attacks in this model, i.e., we assume that a single adversary controls all the malicious beacon nodes (all Bi doesnot belongs to H) and decides di for them. This is a very strong adversary model that in addition to independent adversaries also covers all possibilities of collusion.

As a distance-based localization strategy is assumed here, the output O of the corresponding localization algorithm can be defined by a function F of the measured distances (di) from the device M to every available beacon node, i.e., O=F(d1, . . . , dn).

The error e of the localization algorithm is the expected value of the euclidean distance between the actual position of M and the one output by the algorithm, i.e., e = E[dst(M,O)].

In the next section, we outline the framework for bounded error distance-based localization in the presence of malicious beacon nodes.

4 BOUNDED ERROR DISTANCE-BASED LOCALIZATION

Before describing our secure localization framework, we derive the necessary condition for bounded error localization in the presence of cheating beacons. This condition fixes the minmum number of beacons required to correctly compute the target node location by using just the distance information, assuming that some of the beacon nodes will cheat during localization.

4.1 Necessary Condition

In order to achieve a bounded localization error, the first step is to derive a threshold for the number of malicious beacons k (in terms of the total number of available beacons n) such that if k is greater than or equal to this threshold, then no algorithm would be able to guarantee a bounded localization error just based on the distances to the beacon nodes. Consequently, having the number of malicious beacons below this threshold is a necessary condition for getting a bounded localization error out of any distance-based localization algorithm. This condition is given by Theorem 4.1.

Theorem 4.1. Suppose that $k \geq \frac{n-2}{2}$. *Then, for any distance based localization algorithm, for any locations of the beacons, there exists a scenario in which e is unbounded.*

For the sake of brevity, we skip the proof of this theorem. Interested readers can find the proof in [31]. Theorem 4.1 proves that having $\frac{n-2}{2}$ or more cheating beacons makes it impossible to compute the location of the target node M with a bounded error. In the next set of results, we establish that having $\frac{n-3}{2}$ or fewer cheating beacons makes it possible to compute the location of M with a bounded error. This condition can also be regarded as a *sufficient* condition for secure and robust distance based localization.

4.2 Class of Robust Localization Algorithm

Before defining the class of algorithms that can achieve bounded error localization in the presence of cheating beacons, let us introduce some terminology used for its definition (see Fig. 2). For each beacon Bi, define a ring[2] Ri using the following inequality:

$$\tilde{d}_i - \epsilon < dist(B_i, X) < \tilde{d}_i + \epsilon.$$

As mentioned in Section 3, ϵ is assumed to be a constant denoting some (small) maximum distance estimation error.Clearly, there are altogether n rings. The boundaries of these n rings consist of 2n circles called the boundary circles. In particular, the inner circle of the ring is called an inner boundary circle and the outer circle is called an outer boundary circle.

Definition 4.1. A point is a critical point if it is the intersection of at least two boundary circles.

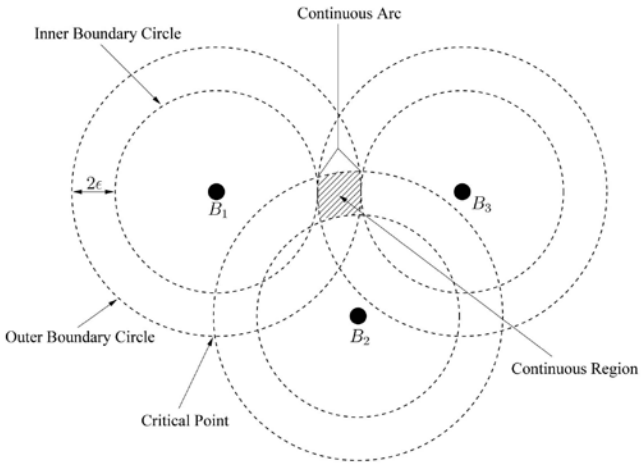

Fig. 2. Terminology for the class of robust localization algorithms.

Definition 4.2. An arc is a continuous arc if it satisfies the following three conditions:

- The arc is part of a boundary circle.

It is either a complete circle or an arc with two distinct endpoints, both of which are critical points.

- There is no other critical point inside the arc.

Definition 4.3. An area is a continuous region if it satisfies the following two conditions:

- The boundary of this area is one or more continuous arcs.

There is no other continuous arc inside the area

Definition 4.4. A localization algorithm is in the class of robust localization algorithms if its output is a point in a continuous region r such that r is contained in the intersection of at least k+3 rings.

5 BOUNDED ERROR ALGORITHM

The class of robust localization algorithms, as defined in Definition 4.4, contains algorithms that output the loc tion of a target in the continuous region of at least k+3 rings. In this section, we propose an algorithm that belongs to this class and it is much faster than an exhaustive search of all the grid points [17] is heuristic-based algorithm.Yet, the probability of reaching the worst-case is less and the heuristic-based algorithms run efficiently in most cases and for most network topologies. Recall that the algorithm work under the condition $k \leq \frac{n-3}{2}$. Thus, an upper bound for k (number of malicious beacons) can be defined as $k_{max} = \frac{n-3}{2}$.The algorithm presented here output a point within the continuous region r in the intersection of kmax+3 rings as the location of the target node, but they differ in the way they determine this point.

The heuristic tries to guess the location of the target closer to the center (or centroid) of the continuous region of at least kmax+3 intersecting rings. This is because the actual location of the target is more likely to be near the center of the continuous region than near the boundary. Thus, assuming that the continuous region is convex, we first compute three distinct critical points, instead of just one, that lie on the intersection of a large number of rings. If (x1,y1),(x2,y2) and (x3,y3) are the coordinates of these critical points, the coordinates (xM, yM) of the target location are guessed by computing the centroid of the triangle formed by (x1,y1),(x2,y2) and (x3,y3) as shown below:

$$x_M = \frac{x_1 + x_2 + x_3}{3},$$
$$y_M = \frac{y_1 + y_2 + y_3}{3}.$$

If this guessed point (xM,yM) lies in the intersection of kmax+3 rings, then it is output as the location of the target, otherwise, the procedure is repeated for a new set of critical points. Details of this heuristic are outlined in Algorithm (or Heuristic) shown below

Heuristic Algorithm.

1: Count the number of rings intersecting with each ring
2: **for** each ring R_i, in the order of decreasing number of rings intersecting with it **do**
3: **for** each ring $R_j, R_{j+1}, R_{j+2} | R_j, R_{j+1}, R_{j+2} \neq R_i$, in the order of decreasing number of rings intersecting with it **do**
4: Compute the intersection points of the boundary circles of R_i and R_j, R_i and R_{j+1} and R_i and R_{j+2}
5: Choose a point (x_1, y_1) from the intersection of the ring pair R_i, R_j at random. Similarly, choose intersection points (x_2, y_2) and (x_3, y_3) from the other two pairs
6: Compute $\overline{O} = (\frac{x_1+x_2+x_3}{3}, \frac{y_1+y_2+y_3}{3})$
7: Count the number of rings containing $\overline{O}$
8: **if** there are at least $k_{max} + 3$ rings containing $\overline{O}$ **then**
9: Output $\overline{O}$
10: Stop the Algorithm
11: **end if**
12: **end for**
13: **end for**

6 Conclusion

The research on securing localization services presented in this paper targets a very specific type of localization technique, referred to as the beacon-based technique. Unlike previous techniques on securing beacon-based localization, this paper takes a two-pronged approach. Rather than directly going out for a solution based on some heuristic, this project conducts a detailed mathematical analysis of the problem using a practical network model and a strong adversary model. The necessary and sufficient conditions and the bounds on the worst case localization errors obtained by this study may help in understanding how best any distance-based algorithm could perform. Such bounds are also useful to other researchers and algorithm designers, because they provide a reference scale to compare the solution quality of new algorithms in this area. The class of robust localization algorithm defined for secure distance-based localization approaches.

References

[1] J. C. Navas and T. Imielinski. Geographic Addres ing and Routing. *In Proceedings of MOBICOM '97*, Budapest, Hungary, September 26, 1997.

[2] Y.-B. Ko and N. H. Vaidya. Location-Aided Routing (LAR) in Mobile Ad Hoc Networks. *In the Proceedings of MobiCom '98*, 1998.

[3] T. Yan, T. He, and J. A. Stankovic. Differentiated Surveillance Service for Sensor Networks. *In Proceeding of First ACM Conference on Embedded Networked Sensor Systems (SenSys '03)*, Los Angeles, CA 2003.

[4] H. Gupta, S. R. Das, and Q. Gu. Connected Sensor Cover: Self-Organization of Sensor Networks for Efficient Query Execution. *In Proceeding of MobiHoc '03*, Annapolis, Maryland, June 2003.

[5] N. Bulusu, J. Heidemann, and D. Estrin. GPS-less low cost outdoor localization for very small devices. *In IEEE Personal Communications Magazine*, 7(5):28-34, October 2000.

[6] L. Doherty, K. S. Pister, and L. E. Ghaoui. Convex optimization methods for sensor node position estimation. *In Proceedings of IEEE INFOCOM '01*, 2001.

[12] N. Priyantha, A. Chakraborty, and H. Balakrishnan, "The Cricket Location-Support System," Proc. ACM MobiCom, 2000.

[16] X. Ji and H. Zha, "Sensor Positioning in Wireless Ad-Hoc Sensor Networks Using Multidimensional Scaling," Proc. IEEE INFOCOM, 2004.

[17] L. Fang, W. Du, and P. Ning, "A Beacon-Less Location Discovery Scheme for Wireless Sensor Networks," Proc. IEEE INFOCOM, 2005.

[13] Z. Li, W. Trappe, Y. Zhang, and B. Nath, "Robust Statistical Methods for Securing Wireless Localization in Sensor Networks," Proc. Fourth Int'l Symp. Information Processing in Sensor Networks (IPSN '05), 2005.
822 IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 9, NO. 6, JUNE 2010

[7] D. Liu, P. Ning, and W. Du, "Attack-Resistant Location Estimation in Sensor Networks," Proc. Fourth Int'l Symp. Information Processing in Sensor Networks (IPSN '05), 2005.

[8] N. Sastry, U. Shankar, and D. Wagner, "Secure Verification of Location Claims," Proc. Second ACM Workshop Wireless Security (WiSe '03), 2003.

[9] S. Capkun and J.-P. Hubaux, "Secure Positioning in Wireless Networks," IEEE J. Selected Areas Comm., vol. 24, no. 2, pp. 221-232, Feb. 2006.

[10] W. Pires, T.H. de Paula Figueiredo, H.C. Wong, and A.A. Loureiro, "Malicious Node Detection in Wireless Sensor Networks," Proc. 18th Int'l Parallel and Distributed Processing Symp. (IPDPS '04), 2004.

[11] D. Liu, P. Ning, and W. Du, "Detecting Malicious Beacon Nodes for Secure Location Discovery in Wireless Sensor Networks," Proc. 25th Int'l Conf. Distributed Computing Systems (ICDCS '05), 2005.

[14] D. Moore, J. Leonard, D. Rus, and S. Teller, "Robust Distributed Network Localization with Noisy Range Measurements," Proc. Second Int'l Conf. Embedded Networked Sensor Systems (SenSys '04), 2004.

[15] Y. Shang, W. Ruml, Y. Zhang, and M. Fromherz, "Localization from Connectivity in Sensor Networks," IEEE Trans. Parallel and Distributed Systems, vol. 15, no. 11, pp. 961-974, Nov. 2004.

[18] S. Ray, R. Ungrangsi, F. de Pellegrini, A. Trachtenberg, and D. Starobinski, "Robust Location Detection in Emergency Sensor Networks," Proc. IEEE INFOCOM, 2003.

[19] K. Yedavalli, B. Krishnamachari, S. Ravula, and B. Srinivasan, "Ecolocation: A Sequence Based Technique for RF-Only Localization in Wireless Sensor Networks," Proc. Fourth Int'l Conf. Information Processing in Sensor Networks (IPSN '05), 2005.

[20] L. Lazos and R. Poovendran, "SeRLoc: Secure Range Independent Localization for Wireless Sensor Networks," Proc. ACM Workshop Wireless Security (WiSe '04), 2004.

[21] L. Lazos, R. Poovendran, and S. _Capkun, "ROPE: RObust Position Estimation in Wireless Sensor Networks," Proc. Fourth Int'l Symp. Information Processing in Sensor Networks (IPSN '05), 2005.

[22] S. Misra, G. Xue, and S. Bhardwaj, "Secure and Robust Localization in a Wireless Ad Hoc Environment," IEEE Trans. Vehicular Technology, vol. 58, no. 3, pp. 1480-1489, Mar. 2009.