ZDBL: Zippy Distance-Based Localization for Malignant Beacons

[1]D.Poovizhi, [2]Selva Ganapathy Ram.R, [3]Santhiya R.
[1]Assistant Professor, [2,3]UG Scholar
Cse,Care School Of Engineering, Thiruchirapalli, India
[1]poo.akshaya@gmail.com, [2]selvarganapathy@gmail.com, [3]santhiyaragavan.r@gmail.com

***Abstract*: Secure distance-based localization in the presence of cheating beacon (or 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: In the presence of cheating beacon nodes, what are the necessary and sufficient conditions to guarantee a bounded error during a two-dimensional distance-based location estimation? Under these necessary and sufficient conditions, what class of localization algorithms can provide this error bound? In this paper, we attempt to answer these and other related questions by following a careful analytical approach. Specifically, we first show that when the number of cheating beacon nodes is greater than or equal to a given threshold, there do not exist any two-dimensional distance-based localization algorithms that can guarantee a bounded error. Furthermore, when the number of cheating beacons is below this threshold, we identify a class of distance-based localization algorithms that can always guarantee a bounded localization error.**

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

1. INTRODUCTION

Localization or location discovery in distributed wireless networks is the problem of determining the location, with respect to some global or local coordinate system of a (mobile) device in the network in an efficient and accurate fashion. Distributed localization protocols in such networks can be broadly classified into range-based and range-free techniques. Range-based techniques can be further classified into broad categories, viz., 1) Beacon-based techniques and 2) Beacon-free techniques. Beacon-based algorithms require the presence of special nodes, called Beacon or anchor nodes, which know their own location and are strategically placed in the network. The working of a two-dimensional beacon-based localization scheme using distance estimates to neighboring beacons as shown in the figure.

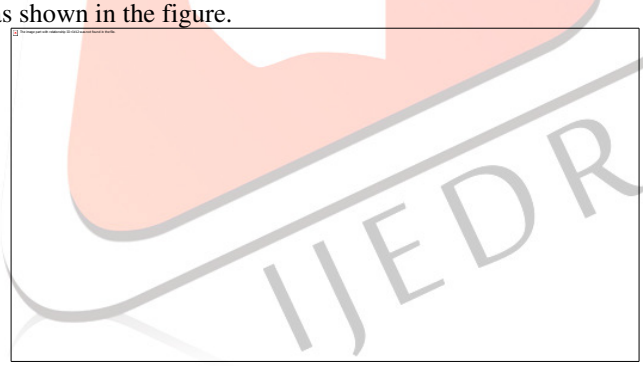


Fig1a. Distance-based (Range-based) localization a)Trilateration. b)Cheating Beacons.

2. MALICIOUS NODE DETECTION AND ELIMINATION

One approach followed by researchers to secure distance-based localization approaches is to detect the cheating beacon nodes and eliminate them from consideration during the localization process. 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.

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. 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. In another approach, Shang et al. and Ji and Zha apply efficient data analysis techniques such as Multi-Dimensional Scaling (MDS) using connectivity information and distances between neighboring nodes to infer target locations. The authors use Maximum Likelihood Estimation (MLE) in order to estimate the most probable node location, given a set of neighborhood observations. In another work, Lazos and Poovendran propose a range-independent distributed localization algorithm using sectored antennas, called SeRLoc, that 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. 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.

3. BOUNDED ERROR ALGORITHMS

The class of robust localization algorithms, as defined contains algorithms that output the location of a target in the continuous region of at least k þ 3 rings. In this section, we propose three algorithms that belong to this class. The first algorithm, called the Polynomial-Time algorithm, has a polynomial-time (in terms of number n of available beacons) worst-case computational complexity, which is much faster than an exhaustive search of all the grid points [17]. However, in practice, it is still very slow. We also propose two heuristic-based algorithms. It is not known if their worst-case complexity is any better than that of the Polynomial-Time 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 all the three algorithms work under the condition k _ n_3 2 . Thus, an upper bound for k (number of malicious beacons) can be defined as kmax ¼ n_3 2 . All the algorithms presented here output a point within the continuous region r in the intersection of kmax þ 3 rings as the location of the target node, but they differ in the way they determine this point.

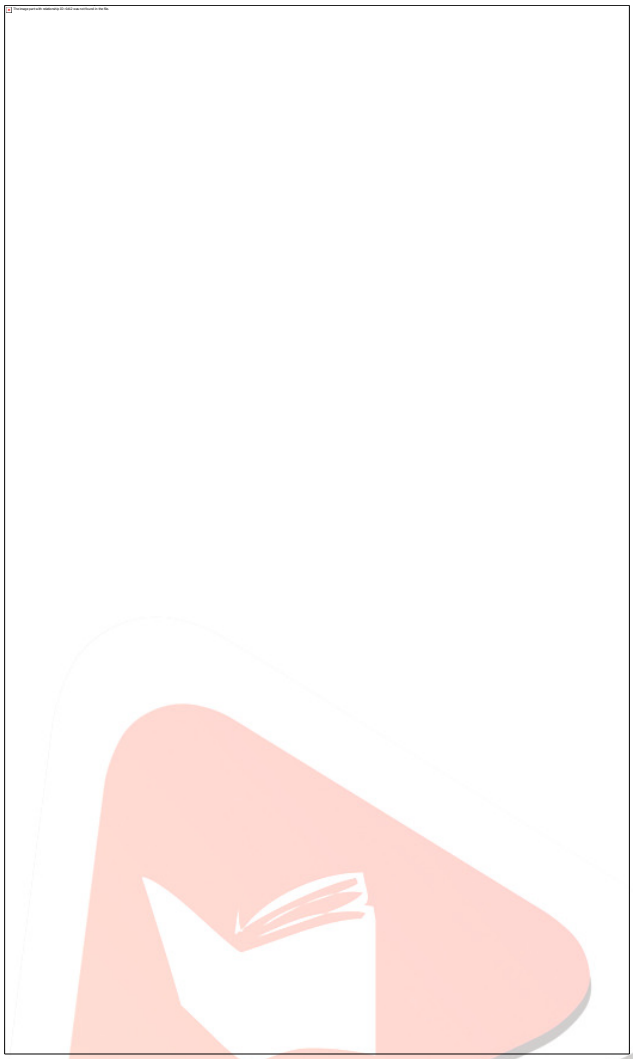
3.1 Polynomial-Time Algorithm

Before outlining details of the Polynomial-Time algorithm, we give a lemma that defines the relationship between a continuous region and a continuous arc.

Definition 3.1. A ring is related to a continuous arc if the continuous arc is inside, but not on the boundary of this ring.

Lemma 3.1. Suppose that r is a continuous region and c is a continuous arc on the boundary of r. Then r is in the intersection of at least k þ 3 rings if and only if at least k þ 2 rings are related to c. (We skip the proof of Lemma 4.1 as it is very straightforward.) The main idea behind the Polynomial-Time algorithm is that in order to determine a continuous region in the intersection of at least kmax þ 3 rings, it is sufficient to count the number of rings related to each continuous arc, and then find a continuous arc such that at least kmax þ 2 rings are related to it (it is easy to check whether a ring is related to a continuous arc by comparing the distance between the arc's endpoints and the center of the ring to the inner and outer radii of the ring). Once such an arc is found, depending on whether the arc is on an outer boundary circle or an inner boundary circle, a point can be picked from either the inner region or the outer region of the arc, respectively. The details of the Polynomial-Time algorithm are shown in Algorithm 1.

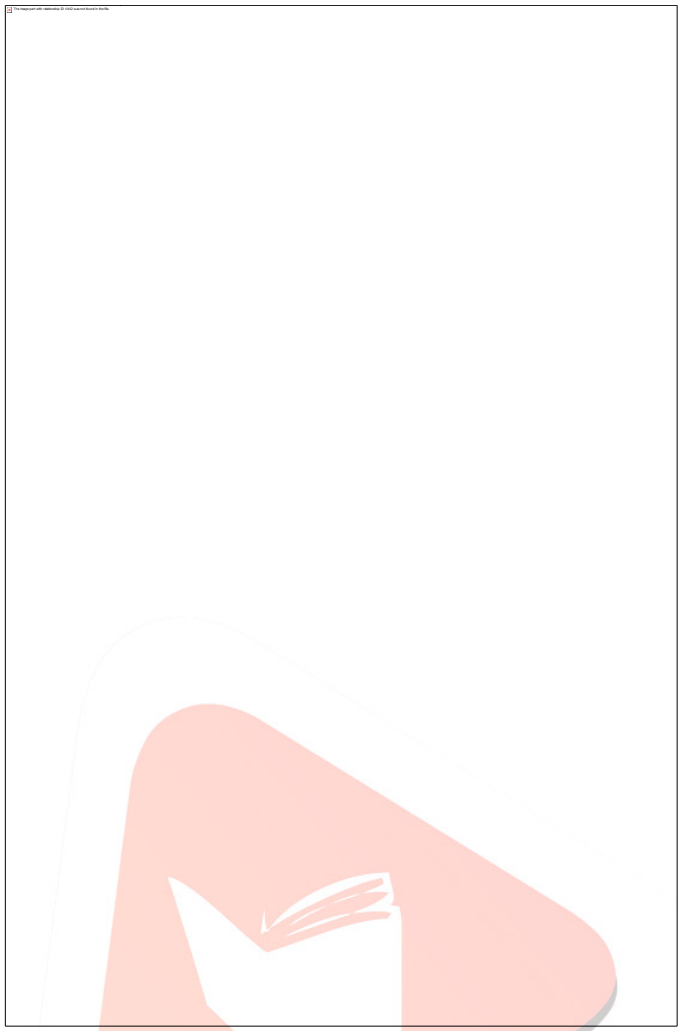
Algorithm 1.Polynomial-Time Algorithm.



3.2 Heuristic 1

The first heuristic attempts to estimate the target location around a critical point that lies on the intersection of a large number of rings. It can be observed that kmax þ 3 is already a large number of rings (more than half of the total number of rings in the network). We need to determine the region r contained in at least kmax þ 3 rings. It is highly probable that the rings containing such a region r are intersecting with large numbers of other rings. In other words, if a ring, say, Ri, is intersecting with a large number of rings, then it is very likely that Ri contains r. Therefore, the heuristic first considers the rings intersecting with a large number of other rings in order to determine the critical point around which the target location is guessed. This continues until a target location within the continuous region in the intersection of at least kmax þ 3 rings is estimated. The details of Heuristic 1 are outlined in Algorithm 2, as shown below.

Algorithm 2. Heuristic 1.



The next heuristic attempts to further improve the quality of localization, by trying to estimate a point closer to the center of the continuous region formed by kmax þ 3 intersecting rings.

4. SIMULATION

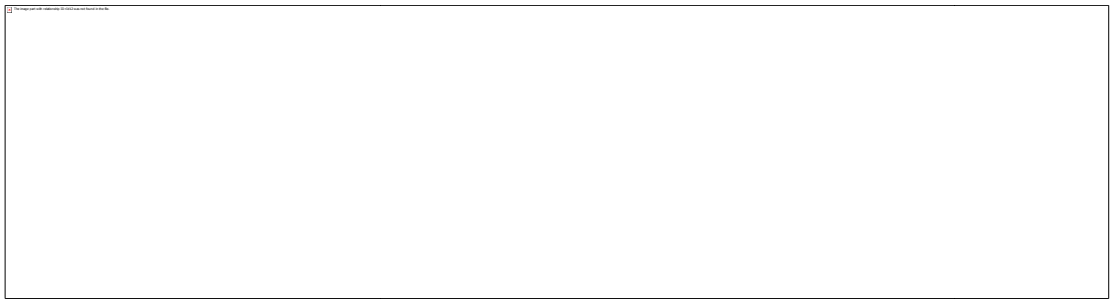
The simulation area consists of a 500 m two dimensional terrain. The optimal number and placement of beacon nodes is important. But as optimal beacon placement is not the main focus of this paper, we assume a small but reasonable beacon node population of 43 beacon nodes (approximately 1 beacon for every 10 m 10 m), which is scattered uniformly over the 500 m 500 m area. The position of the target node is also uniformly selected and there is no node mobility (beacon or target). Currently, the maximum radio ranges of the nodes are selected such that every beacon node is available for localization (250 m). In this set of simulations, we assume an independent distance estimation error selected from some fixed distribution. In order to verify the accuracy and efficiency of the proposed algorithms for different distributions of the distance estimation error, we simulate the algorithms for both uniformly and normally distributed distance estimation errors.

5. POLYNOMIAL TIME ALGORITHM

In this section, we discuss the simulation results for the Polynomial-Time algorithm.

5.1. Experiments with Uniform Measurement Error

In the first set of simulations, we evaluate the Polynomial- Time algorithm for the case when the distance estimation error is uniformly distributed between ½__; __. We observe the performance of the algorithm for increasing values of _, as the number k of malicious nodes increases from 0 up to some maximum tolerable value. As the total number of available beacons is fixed (n ¼ 43), the maximum number of malicious beacons that the algorithm can tolerate is 43_3 2 ¼ 20 (from Theorem 4.2). The algorithm is executed for each value of _ from 0 to 5 m in steps of 1 m and for each value of k from 0 to 20 (kmax ¼ 20). We then plot the average localization error e as an average of the error in localization of the target over 100 runs of the algorithm (see Fig. 3).The reason is that in this case, the continuous region is just a single point in the intersection of at least kmax þ 3 rings. Also it can be seen that e increases as k increases. This is consistent with the intuition that more number of malicious beacon nodes should decrease localization precision. For lower values of k, i.e., k < kmax, more honest rings are available for localization, resulting in a smaller sized continuous region, and thus, a more accurate localization. As the number of malicious nodes increases, the number of honest rings diminishes, and thus, the quality of localization decreases.



5.2. Experiments with Normal Measurement Error

Once again, to ensure that the evaluation results are not restricted to only uniformly distributed errors, the simulations for Heuristic 1 are repeated with a normally distributed distance estimation error. All other experiment parameters are unchanged. The distance measurement error follows a normal distribution with mean 0 and standard deviation _ 2 . As before, the distribution is modified such that the probability density outside ½__;þ__ becomes 0. Fig. 4c plots the average localization error e for each pair of ðk; _Þ when the measurement error follows a normal distribution. Fig. 4d plots the corresponding simulation time. We can observe that the curves are analogous to those in Figs. 4a and 4b, respectively, except that the localization error e increases much more slowly with k.

6. CONCLUSION AND FUTUREWORK

In this paper, we have addressed the problem of secure distance-based localization in the presence of cheating beacon nodes. By means of a sound mathematical analysis, we have derived the conditions for secure and robust distance-based localization in the presence of cheating beacons. Specifically, we have outlined the necessary and sufficient conditions for achieving a bounded localization error, and defined a nonempty class of algorithms that can achieve such a bounded error. We have also proposed three novel distance-based localization algorithms, specifically a polynomial-time algorithm and two heuristic-based algorithms that belong to this class of bounded error distance-based localization algorithms. We have verified the localization accuracy and execution efficiency of these algorithms using measurements from simulation experiments. Experimental results show that all the algorithms performed consistently for different distributions of the distance measurement error. We have also extended the existing localization framework to include more practical models for the distance measurement error and have verified the performance of the algorithms under such scenarios. The error model for radio signals currently used in the analysis can be further improved to characterize errors in specific hardware technologies and environments. The path loss parameters in the current distance estimation error model can be adjusted depending on network-specific factors including obstructions, interference due to noise, and multipath fading. Well-known statistical models such as Rayleigh or Rician distributions [33] or published signal measurement data sets for specific wireless systems can be used for this purpose. Distance estimation error models for other technologies such as acoustic and UWB can also be used to further analyze the proposed secure localization framework. Although the analytical results and bounds presented here are very general and have been verified for simple error models, it would be worthwhile to observe how these results (both theoretical and empirical) would extend to specific wireless environments and systems. This will be undertaken as future research on this topic.

REFERENCES

[1] J. Hightower and G. Borriello, “Location Systems for Ubiquitous Computing,” Computer, vol. 34, no. 8, pp. 57-66, Aug. 2001.

[2] D. Niculescu and B. Nath, “DV Based Positioning in Ad Hoc Networks,” J. Telecomm. Systems, vol. 22, pp. 267-280, 2003.

[3] R. Stoleru and J.A. Stankovic, "Probability Grid: A Location Estimation Scheme for Wireless Sensor Networks," Proc. First IEEE Conf. Sensor and Ad Hoc Comm. and Networks (SECON '04), 2004.
[4] M.W. Carter, H.H. Jin, M.A. Saunders, and Y. Ye, "SpaseLoc: An Adaptive Subproblem Algorithm for Scalable Wireless Sensor Network Localization," SIAM J. Optimization, 2006.
[5] J. Liu, Y. Zhang, and F. Zhao, "Robust Distributed Node Localization with Error Management," Proc. ACM MobiHoc, 2006.
[6] G. Mao, B.D.O. Anderson, and B. Fidan, "Path Loss Exponent Estimation for Wireless Sensor Network Localization," Computer Networks, vol. 51, pp. 2467-2483, 2007.
[7] R. Moses, D. Krishnamurthy, and R. Patterson, "A Self- Localization Method for Wireless Sensor Networks," Eurasip J. Applied Signal Processing, special issue on sensor networks, vol. 2003, pp. 348-358, 2003.