ROSETTA: Robust And Secure Mobile Target Tracking In A Wireless Ad Hoc Environment

Satyajayant Misra[†], Sarvesh Bhardwaj[‡] and Guoliang Xue*[†]

Abstract— **In this paper, we study the problem of accurate tracking of a mobile target by a central authority, using distance estimates obtained by a group of untrusted anchors within the communication range of the target. We show how to perform accurate localization of the target in the presence of some compromised and colluding malicious anchors that lie about the position of the target. We also show how to identify most of these malicious anchors. In the case where measurements are error-free, we derive an upper bound (B) on the number of malicious anchors that may be involved in localizing the target while still not being able to undermine its accurate localization. We propose a scheme to correctly localize the target when the number of malicious anchors within its range is no more than B. It also identifies all the malicious anchors. In the presence of positive measurement errors, we propose a scheme based on convex optimization that can localize the target despite the presence of an arbitrary number of malicious anchors in its range. When the number of malicious anchors are no more than B, our scheme localizes the target with an error less than 1m and is also able to identify more than 80% of the malicious anchors. Both our schemes are simple and easy to implement.**

I. Introduction

Large scale distributed wireless networks are becoming common in both the military and civilian domains because of their relative ease of deployment and minimum requirement of infrastructure [1]. Despite significant improvements in the miniaturization and seamless deployment of the nodes making up the wireless network [2] there are still many fundamental problems that need to be addressed. The problem of node localization is one such fundamental problem.

In an infrastructureless wireless network, for cost effectiveness, not all nodes are equipped with self-localizing abilities. Most nodes localize themselves using their position estimates obtained from a group of nodes in the network called the *anchors*. The anchors are wireless nodes that are fixed and know their own positions, either by using a GPS device or from pre-programmed information. The problem of accurate localization is fairly complex due to the inherent errors in measurements resulting from barriers, such as transmission delay and interference. Given this scenario, the presence of malicious anchors makes this problem significantly more complex and also introduces the need for secure localization.

In this paper, we study a variant of the secure and accurate node localization problem, namely *robust and secure mobile target tracking*. Target tracking aims to track and localize a mobile node moving inside a network. One use of target tracking in a military setting is to to identify the positions of mobile soldiers or vehicles in any surveillance area to ascertain their safety. This is, in general, the nature of target tracking considered in this paper. In the rest of this paper, we use tracking and localization interchangeably to refer to tracking the current position of the mobile target. Secure tracking is necessitated by the untrusted environment in which most wireless networks operate. In a standard wireless network, the anchors are assumed to be trusted and non-tamperable. However, this is a strong assumption in an untrusted environment, specifically in a military setting. During the period of operation, the probability of anchors being tampered or compromised by an adversary is fairly high. These anchors may be re-programmed by the adversary to provide false information estimates about the target. Also, more than one such malicious anchors may collude to falsely localize the target away from its original position. This is a critical setback for the tracking process as incorrect tracking of a target may have serious repercussions.

The problem of target tracking has been previously studied in [3], [4]. However, to our best knowledge the problem of secure target tracking has not been studied in any detail. In this paper, we study the problem of secure and accurate tracking of a mobile target using a group of untrusted anchors within its communication range. The anchors obtain the distance estimates of the target using distance bounding techniques [5], [6]. We propose schemes that accurately track the target and also identify the malicious anchors that lie about the position of the target. We note here that we demonstrate our schemes through target localization at a given instant of time. Multiple such localizations (mechanism omitted for lack of space) at different time instances will result in tracking of the target.

Given a target t and a set S_t of anchors in the range of t, the *bound circle* of an anchor i is the circle with i's position as the center and the radius equal to the estimate of the distance between t and i. The location of the target is the point in the network where the greatest number of bound circles intersect. The presence of malicious anchors in the network can interfere in the localization process by introducing false candidate locations of the target. Hence, we derive an upper bound B on the number of false anchors in the range of the target despite which we can still robustly localize the target. In the rest of the paper, we use the terms malicious anchors and lying anchors interchangeably. In this paper, we assume that the malicious anchors only lie by enlarging the distance estimates of the target.

This research was supported in part by ARO grant W911NF-04-1-0385 and NSF grants CNS-0524736 and CCF-0431167. The information reported here does not reflect the position or the policy of the federal government.

* Author Serving as point of contact, [†] Both authors are with the Department of Computer Science and Engineering, Arizona State University, Tempe, AZ 85287-8809. [‡] is with the Department of Electrical Engineering, Arizona State University, Tempe, AZ 85287-8809. Email: {satyajayant, sarvesh.bhardwaj, xue}@asu.edu.

We study two aspects of the problem. The first is when the localization estimates are exact, hence, the position of the target can be precisely estimated as the point of intersection of all the bound circles corresponding to the truthful anchors. The second aspect studied is when the localization estimates have positive errors. In the presence of positive measurement errors, instead of a point we obtain a bound region $\mathcal{R}$ corresponding to the area of intersection of the bound circles. In this case, we propose a heuristic to track the target accurately, regardless of the number of malicious anchors in range of the target, provided that the number of truthful anchors in range of the target is at least three. We note here that the distance estimates from at least three anchors is necessary for any possible localization of the target in 2-dimensions. Our schemes also identify the malicious anchors. In the case with measurement errors, the identification of the malicious anchors is pessimistic, in the sense that some of the malicious anchors can escape identification. However, neither scheme has any false positives.

In Section II, we briefly survey related work in the area of secure localization in wireless ad hoc networks. Section III presents the system model. Section IV discusses target tracking in the absence of measurement errors. In Section V, we present the mechanism for target tracking in the presence of measurement errors. Section VI presents the simulation results and in Section VII, we present our conclusions and scope for future work.

II. Related Work

Lazos and Poovendran [7] proposed a range independent localization algorithm to securely estimate the position of nodes in a wireless sensor network using beacons transmitted from anchors. Li *et al.* [8] identified a list of attacks that are unique to localization and proposed statistical methods to make triangulation and RF-based localization attack-tolerant. Čapkun *et al.* [6] proposed a novel approach to secure localization based on hidden and mobile base stations. In [9], Du *et al.* proposed a general scheme to detect localization anomalies caused due to the presence of adversaries. In [10], Lazos *et al.* proposed a range-independent localization and location verification scheme for wireless sensor networks. In [11], Liu *et al.* introduced many techniques to detect and remove compromised beacon nodes, avoid false detections, and also detect replayed beacon signals. In [6], Čapkun *et al.* analyzed the resistance of positioning techniques to position and distance spoofing attacks and proposed a scheme that can be used for secure positioning in wireless networks.

There have been many significant works that use optimization for localization in wireless networks. Here we identify a few that are pertinent. In [12], Bulusu *et al.* proposed distributed algorithms for localization of low power devices based on connectivity. In [13], Doherty *et al.* described a method that uses connectivity constraints and convex optimization for localization in a wireless sensor network where some of the beacon nodes know their positions. Nagpal *et al.* and Savvides *et al.* in [14] and [15], proposed localization using distributed propagation of location information and multilateration. Cheng *et al.* in [16], presented a time difference of arrival based position system for efficient location discovery in outdoor sensor networks. In [17], Savvides *et al.* derived the Cramér-Rao Lower Bound (CRLB) for network localization. They proposed that the error introduced by a localization algorithm is as important as measurement error when assessing end-to-end localization errors. In [18], Niculescu *et al.* applied the CRLB to a few of the general classes of localization problems. To the best of our knowledge no work in literature has attempted to propose a robust and secure target tracking solution as proposed by us in this paper.

III. System Model

The system model of our fixed anchors based wireless localization framework is based on the following assumptions:

1) The network consists of a set of anchors $\mathcal{S} = \{A_i, i = 1, \ldots, n\}$ that are manually placed or deployed randomly and are fixed after deployment.
2) Each anchor A_i knows its own position a_i $(a_i = (a_{ix}, a_{iy}))$.
3) All communications between the anchors and the mobile target are bidirectional.
4) The mobile target is assumed to be pseudo-static in the time instant, i.e., it is static during the tracking procedure which is of a short duration.
5) All measurements are 2-dimensional, however, the techniques apply to 3-dimensional measurements also.

A. Network Model Assumptions

1) We assume that the anchors and the mobile target are equipped with omnidirectional antennas.
2) The target and the anchors share symmetric keys for secure and authentic communication.
3) The positions of no three anchors in the network are collinear.
4) The central authority knows the positions of all the anchors in the network.
5) The anchors obtain the mobile target's distance estimate using the distance bounding (DB) protocol [6]. The nodes contain specialized hardware for such high speed DB.
6) Although the error in high speed DB is of the order of 0.08% [6], our schemes are robust enough to handle bigger errors ranging between [0, 10%] of the measured value.

B. Threat Model and Security Assumptions

In a wireless ad hoc network the adversary may be classified as, either an *outside adversary* or an *inside adversary*. An outside adversary is an entity that is not part of the network and is generally assumed to have computation ability and communication range that are orders of magnitude higher than the nodes in the network. However, these abilities are not unbounded. An outside adversary can jam or eavesdrop on communication, compromise legitimate nodes, and inject false nodes in the network. An inside adversary on the other hand, refers to a node in the network that has been compromised, in most cases by an outside adversary. The inside adversary is also a potent attacker as it forms a part of the system and, hence is privy to the shared secrets required for secure mutual and group communications.

In this paper, we address the issues of secure target tracking in the presence of colluding inside attackers and also identification of these attackers. These inside attackers are compromised anchors that lie about their distance estimates and may also collude to localize the target incorrectly, resulting in inaccurate tracking of the target. Lying anchors can compromise the location discovery process, in turn affecting neighbor discovery and routing. This may seriously malign the usefulness of the network. We do not consider the problem of the mobile target attempting to lie about its position. Some previous works, such as [6], [7] already exist in literature addressing this issue in some detail.

We assume that the communication in the target tracking process is secure and authentic. Use of high speed (DB) prevents wormhole attacks [2], which are a potent attack against localization [6]. In addition, the fact that the central authority knows the positions of the anchors, helps prevent sybil attacks [2]. The only other possible attacks are Denial of Service (DoS) attacks and distance *enlargement* or *reduction* by the malicious anchors. Protection against DoS attacks are outside the purview of this paper. However, we note that there are mechanisms in literature that address DoS attacks in wireless networks to varying degrees.

The procedure adopted in DB is useful in preventing distance reduction attacks. One such mechanism is given here. Using DB, the two parties involved in communication can estimate each other's distance. After DB, the target can send its estimate of its distance from the anchor, encrypted using a secret key that it shares with the central authority, to the anchor. The anchor in turn, sends its distance estimate of the target, its position information, and the encrypted information from the target to the central authority. The central authority can identify the lying anchor by comparing the distance estimate from the anchor with that from the target. We note here that the only way that distance reduction attacks can happen is if an anchor lies about the distance estimate obtained during DB. The above procedure can rule out distance reduction attacks. However, distance enlargement is not so easily identifiable because the anchor can enlarge the distance estimate during DB itself. This cannot be unidentified by the target. In this case, at the central authority the encrypted bound estimate from the target and that from the anchor would be the same. Our schemes address this distance enlargement attack and detect the lying anchors.

As mentioned in Section I, target localization in the presence of positive measurement errors results in a region $\mathcal{R}$. We consider only positive errors in this paper, as negative errors are generally rare. The error is often dominated by the positive terms resulting from computation overheads at the sender/receiver and also the propagation delay. In a network with malicious anchors, the boundary of the region $\mathcal{R}$ may be defined by the distance estimate of a malicious anchor. Since there is no limit on the amount by which a malicious anchor lies, therefore the area of region $\mathcal{R}$ could be considerably large, thus introducing a significant amount of uncertainty in the target's location. However, in Section IV, we show that for a more specific version of the problem, where the measurements are error-free it is possible to obtain an upper bound B, on the number of malicious anchors out of N anchors in the range of the target, whose presence does not undermine the exact localization procedure. In this situation, we provide a technique to precisely localize the target and also identify the malicious anchors. In Section V, we relax the assumption of non-zero measurement errors and propose a heuristic for target tracking. Our results indicate that when the number of malicious anchors are no more than B, our technique can still localize the target with a high accuracy (the size of $\mathcal{R}$ is small) and identify a significant number of malicious anchors. Even when the upper bound B is not satisfied the scheme has a good performance.

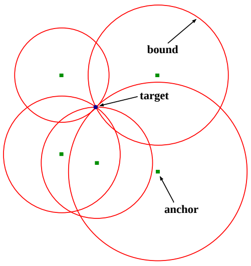


Fig. 1. Localization with multiple anchors, no measurement errors

IV. Target Tracking in the absence of Measurement Errors

If the distance bound measurements are error-free then the target is positioned on the circumference of the bound circle of an anchor in its range. In case there are more than one anchors within the communication range of the target, the position of the target is the common point of intersection of all the bound circles as shown in Figure 1. If some of the anchors, in range of the target, are lying by enlarging their corresponding distance bounds then the target will be located inside their corresponding bound circles, instead of on the circumference. Hence, it appears that if some of the anchors are lying but the majority (more than half) is truthful, then we can still correctly localize the target as the point where the majority of the circles intersect. However, in the following example, we show that even if the majority anchors are telling the truth, there is a possibility that the remaining malicious anchors can collude to obtain another point as the location of the target.

A. Motivating Example

Figure 2 shows a scenario with a target and 8 anchors in it's range labeled as $\{1, 2, \ldots, 8\}$. The truthful anchors (bound circles shown in solid) are given by the set $T = \{1, 2, 3, 4, 5\}$ and the malicious anchors (bound circles shown in dashed) are denoted by $F = \{6, 7, 8\}$. The correct position of the target is the point of intersection B of the bound circles T. The malicious anchors lie by enlarging their distance estimates, such that the point B does not lie on the circumference of their bound circles, but is contained inside them. In addition, the malicious anchors

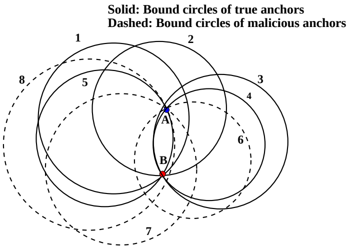

Solid: Bound circles of true anchors
Dashed: Bound circles of malicious anchors
1
2
8
5
3
4
A
6
B
7

Fig. 2. Failure of localization despite majority of the anchors being truthful

($\{6,7,8\}$) collude in an intelligent manner to intersect in another point A where two truthful anchors 4 and 5 also intersect. Hence, the number of anchors that intersect at the correct location of the target (point B) is 5 ($\{1,2,3,4,5\}$) and the number of anchors that intersect at the false location of the target (point A) is also 5 ($\{4,5,6,7,8\}$). Thus, there are two candidate locations of the target (point A and B) with the same defining characteristics, that is, majority of anchors intersect at the two locations. Under such a scenario it is impossible to uniquely localize the target.

B. Conditions for Exact Localization of the Target

As shown in the previous example, even if a majority of anchors in range of the target are truthful, it does not guarantee the exact localization of the target. Hence, we now derive the upper bound B on the number of malicious anchors out of N anchors in range of the target, despite whose presence exact localization of the target can be performed.

Lemma 1: Given three distinct circles A, B, and C, with different centers and radii, they have at most one point of intersection if and only if their centers are non-collinear.

Corollary 1: Given that no three anchors in the network are collinear, the bound circles corresponding to three or more anchors cannot have more than one point of intersection.

Theorem 1: Given that the number of anchors in the range of a target is N and that some of them are malicious and colluding,
a) the minimum number of truthful anchors required for exact localization of the target in the presence of colluding malicious anchors is given by $\lceil N/2 \rceil + 2$ and
b) if the number of malicious and colluding anchors is M, the number of truthful anchors needed for the correct localization of the target is at least $M+4$.

Proof: a) We have already shown in our motivating example that the presence of $\lceil N/2 \rceil + 1$ truthful anchors does not guarantee the exact localization of the target. Thus, let the number of truthful anchors in the range of the target be at least $\lceil N/2 \rceil + 2$. We know that at least three anchors are required for localization of a target. Hence, $\lceil N/2 \rceil + 2 \geq 3$. Let the target be located at point t, which will also be the common point of intersection of bound circles of all the truthful anchors. For any other point t' to be a possible candidate location for the target, another set of $\lceil N/2 \rceil + 2$ bound circles would have to intersect at t'. From corollary 1, the maximum number of truthful anchors that can intersect at t' is 2 (because they already intersect at t). In addition, if the remaining $\lfloor N/2 \rfloor - 2$ malicious anchors collude, t' can also be the point of intersection of those $\lfloor N/2 \rfloor - 2$ malicious anchors. Thus making the number of intersecting circles at t' to be $\lfloor N/2 \rfloor - 2 + 2 = \lfloor N/2 \rfloor$. Hence, any point (except t) in the network cannot have more than $\lfloor N/2 \rfloor$ anchors intersecting at its position. Thus, the target is exactly localized at the point t. Therefore, if we have a minimum of $\lceil N/2 \rceil + 2$ truthful anchors in range of the target then the target can be localized at a point (the correct location) where the bound circles of those anchors intersect. Given the minimum number of truthful anchors we obtain the maximum number of malicious anchors in the network to be $\lfloor N/2 \rfloor - 2$. This is the upper bound B on the number of malicious anchors that can exist in range of the target without hampering the correct localization of the target.

b) If the number of malicious anchors is M, then the number of truthful anchors is given by $N - M$. From part (a), sufficient conditions for the exact localization of the target are given by

$$N - M \geq \left\lceil \frac{N}{2} \right\rceil + 2 \tag{1}$$

$$M \leq \left\lfloor \frac{N}{2} \right\rfloor - 2. \tag{2}$$

From both (1) and (2), we obtain $N \geq 2M + 4$. Thus, given M malicious anchors in the range of the target, the *total* number of anchors required for exact localization of the target is $N \geq 2M + 4$. In addition, the number of truthful anchors required is at least $\lceil N/2 \rceil + 2 = M + 4$.

■

C. Identification of Malicious Anchors

Under the conditions described above for exact localization of the target, it is fairly straightforward to catch the malicious anchors once the target has been localized. For each anchor i, the distance d_i between the location of the anchor and the location of the target is computed. Since each malicious anchor lies by giving a wrong estimate of the distance between its position and the target, an anchor i will be malicious if $d_i \neq r_i$, where r_i is the radius of the bound circle of anchor i. It should be noted that *all* malicious anchors can be identified irrespective of the amount of their distance enlargements.

We now address the more general problem of target tracking in the presence of measurement errors.

V. Target tracking in the presence of Measurement Errors

Distance measurements in a wireless network are generally prone to measurement errors (mostly enlargements) due to the noisy and delay prone wireless medium. Hence, the position estimates of a target are error-ridden. Using a specialized hardware for DB, the measurement errors can be reduced to an order of 15 cms at a distance of 2 kms [6] (0.075%). However, we demonstrate using simulations that our scheme is robust enough to handle a significantly wider range of measurement errors ranging between [0, 10%] of the measured value. Due to the error in measurement, the intersection of the bound circles of the anchors is a region $\mathcal{R}$ as discussed before. That is, if C_i is the set of points inside the bound circle of anchor i, then the region $\mathcal{R} = \{x | \ x \in \mathbf{R}^2, x \in \cap_{i=1}^{N} C_i\}$, where N is the number of anchors in the range of the target. Since we make no assumption regarding the distribution of the distance estimates of the target from an anchor, all points inside the region $\mathcal{R}$ are equally likely to be the position of the target. We attempt to obtain a likely position of the target in this region. Since the sets C_i's are convex sets, their intersection region $\mathcal{R}$ is also convex. Hence, our problem is that of identifying a feasible point inside a convex region or a convex feasibility problem. Thus the problem can be written as,

$$\begin{aligned} &\min_{x} \quad 1 \\ &\text{subject to} \quad x \in \mathcal{R} = \bigcap_{i=1}^{N} C_i. \end{aligned} \tag{3}$$

Figure 3 shows an example scenario. The target is located at point A and it has 5 anchors ($\{1, 2, 3, 4, 5\}$) in its range. Four of the anchors ($\{1, 2, 3, 4\}$) are truthful anchors, whereas anchor 5 is a malicious anchor. The feasibility region $\mathcal{R}$ is shown in the shaded region. The solution of the convex feasibility problem could result in the point B as the estimate of the location of the target. As can be seen from the figure, the distance between point B and point A is quite large and depends on the amount by which anchor 5 lies. Thus, from the solution of the feasibility problem in (3), the maximum error between the actual location of target and its estimated location can be $\max_{x \in \mathcal{R}} \|x_t - x\|$, where x_t is the location of the target and $\| \cdot \|$ is the Euclidean norm. As shown in Figure 3, in the presence of malicious anchors, this distance can be quite large. Instead, if the location of the target is estimated using a point x_c in the *center* of region $\mathcal{R}$, then $\|x_t - x_c\| \leq \max_{x \in \mathcal{R}} \|x_t - x\|$. Thus, by estimating the location of the target as the center of the region $\mathcal{R}$, both the worst and average case errors in estimation can be minimized.

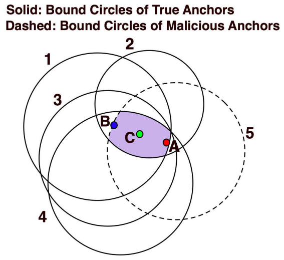

Solid: Bound Circles of True Anchors
Dashed: Bound Circles of Malicious Anchors
1
2
3
B
C
5
A
4

Fig. 3. Secure target tracking in the presence of measurement errors

The center of the region $\mathcal{R}$ can be obtained by solving the following second order cone problem (*SOCP*) [19],

$$\begin{array}{lll} \min\limits_{x,\delta} & \delta & \\ \text{subject to} & \|x - a_i\|^2 \leq \big[r_i \cdot (1 + \delta)\big]^2, & i = 1, \ldots, N \\ & \delta < 0 & \end{array} \tag{4}$$

instead of the feasibility problem in (3). The first N constraints in (4) correspond to the constraint $x \in \mathcal{R}$. The objective δ corresponds to the proportion by which the radius of each bound circle has to be reduced without making the region $\mathcal{R}$ a null set. r_i and a_i correspond to the distance bound estimate and the center, respectively, of the i-th anchor. The optimal solution x^* to the above optimization problem is the approximation of the center of the region $\mathcal{R}$.

As specified earlier, the problem of target tracking is centralized. The distance estimates are sent by the anchors to the central authority, which calculates the position of the mobile target. In our scheme, the centralized authority solves a convex optimization problem to obtain a likely position of the target. We transform the constrained optimization problem in (4) into the following unconstrained optimization problem

$$\min_{x,\delta} \quad t \cdot \delta - \sum_{i=1}^{n} \log \left[(r_i \cdot (1 + \delta))^2 - \|x - a_i\|^2 \right] - \log(-\delta) \tag{5}$$

where, t is a constant. This problem can be solved by the *barrier method* [19] using the Algorithm 1. The minimization in the centering step uses the Newton's method [19] with a tolerance $\eta = 1 \times 10^{-6}$.

Algorithm 1 Algorithm of Barrier Method

```
Given a strictly feasible $x$, $t = t^{(0)} > 0$, $\mu > 1$, tolerance $\epsilon > 0$. $\{t^{(0)} = 1.0,\ \mu = 10.0\}$
repeat
    Centering Step: Starting at $x$, compute $x^*(t)$ by minimizing the objective in (5).
    Update $x := x^*(t)$.
    Increase $t$: $t = \mu \cdot t$.
until $N/t \leq \epsilon$ $\{\epsilon = 1 \times 10^{-6}\}$
```

As the barrier method progresses, the value of δ keeps getting smaller. This results in the reduction of the bound circles, hence reducing the intersection area. After a number of iterations, when the size of the feasible region has reduced significantly, the algorithm exits and outputs a point x^* which is the center of the region. This point x^* is the estimate of the location of the target.

The barrier method presented in Algorithm 1 requires an initial starting value for x which is strictly feasible. To obtain point x we reduce the bounding circles of all the anchors by a very small amount and find the points of intersection of every possible pair of anchors. Any one of these points which lies inside all the bound circles is chosen as x.

Algorithm 2 Algorithm for Identifying Malicious anchors

```
GIVEN: The numeric center $x^*$ of the intersection region.
VERTICES = $\{$x| x is a vertex of $\mathcal{R}\}$
$r_R$ = 0. $\{$Defines the radius of the intersection region $\mathcal{R}\}$
for all $y \in$ VERTICES do
    if $\|y - x^*\| > r_R$ then
        $r_R$ = $\|y - x^*\|$.
    end if
end for
for all anchors $i$, $1 \leq i \leq n$ do
    $r_{i\epsilon} = r_{i\epsilon}/(1 + \epsilon_{max})$. $\{r_{i\epsilon}$ is reduced$\}$
    if $\|x^* - a_i\| \geq r_{i\epsilon}$ then
        Anchor $i$ is not malicious.
    else
        $r_{i\epsilon} = r_{i\epsilon}$ - $r_R$.
        if $\|x^* - a_i\| \geq r_{i\epsilon}$ then
            Anchor $i$ is not malicious.
        else
            Anchor $i$ is malicious, commence revocation process.
        end if
    end if
end for
```

A. Identification of malicious anchors

Let the measurement error proportion of a localization estimate for any anchor i be given by ϵ_i. Let the maximum possible measurement error, a known system parameter, be given by ϵ_{max}.

The value of the distance bound estimate with measurement error for anchor i (malicious or truthful) is given by,

$$r_{i\epsilon} = r_i \cdot (1 + \epsilon_i). \tag{6}$$

Let θ_i be the proportion by which an anchor i enlarges its distance estimate. Thus, for a truthful anchor i, $\theta_i = 0$. However, for a malicious anchor i, the value of θ_i is unknown. Thus, in general, the final radius of an anchor i can be written as,

$$r_{i\theta} = r_i \cdot (1 + \epsilon_i) \cdot (1 + \theta_i). \tag{7}$$

We note here that in case a malicious anchor lies by a small amount θ_i, such that,

$$r_{i\theta} \leq r_i \cdot \{1 + \epsilon_{max}\}, \tag{8}$$

then it is not possible to ascertain whether the enlargement is a lie or is simply a measurement error. That is, since ϵ_i is not known, it is difficult to distinguish between whether the anchor is lying or is just subject to maximum possible measurement error ϵ_{max}.

Algorithm 2 underlines the procedure to identify the malicious anchors. The vertices of region $\mathcal{R}$ in Step **2** of Algorithm 2 are obtained by finding out the points of intersection of all possible pairs of distance bound circles and choosing the points lying inside all the circles.

In order to discount the measurement errors, the radius of each anchor i is reduced by the proportion $(1 + \epsilon_{max})$. Hence, the reduced radius of i becomes,

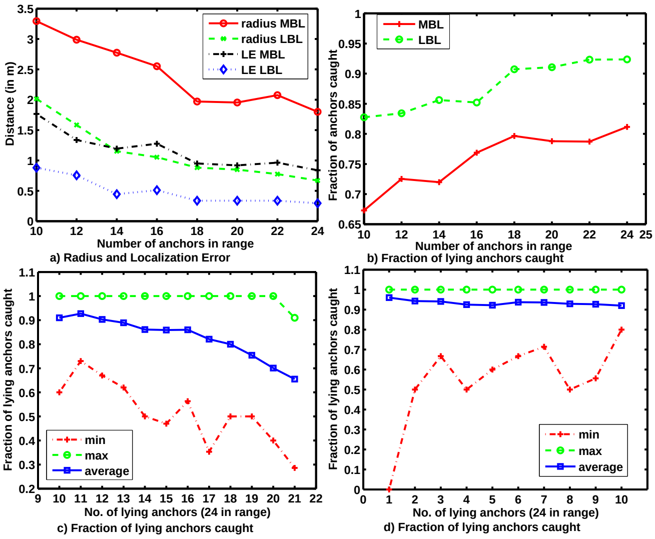
$$r'_{i\theta} = r_{i\theta}/(1 + \epsilon_{max}) = r_i \cdot (1 + \epsilon_i) \cdot (1 + \theta_i)/(1 + \epsilon_{max}). \tag{9}$$

Since $r'_{i\theta}$ is obtained by dividing each radius $r_{i\theta}$ by $(1 + \epsilon_{max})$, thus for truthful anchors $r'_{i\theta} \leq r_i$. Also, since we assume that the lie θ_i for a malicious anchor i does not satisfy equation (8), therefore $r_{i\theta}^{'} > r_i$. If we knew the distance r_i of each anchor i from the target, using the values of $r'_{i\theta}$ and r_i we could have easily identified the malicious anchors from the truthful ones. However, as we have mentioned earlier, in the presence of measurement errors, the position of the target cannot be estimated precisely, hence the r_is cannot be calculated exactly.

In our scheme, the location of the target is approximated by x^* with an uncertainty region $\mathcal{R}$ around it. In such a case, we estimate r_i as follows. Let us denote the distance between the center C_i of anchor i and x^* as $d(C_i, x^*)$. The distance r_i of the target from the anchor i is then estimated by the quantity $\hat{r}_i = d(C_i, x^*) + r_R$, where $r_R = \max\{d(x, x^*) | \; x \in \mathcal{R}\}$. That is, r_R represents the radius of $\mathcal{R}$. Steps **3** to **8** of Algorithm 2 describe how to find r_R. Since the actual location of the target is inside $\mathcal{R}$, it can be shown that $r_i \leq \hat{r}_i$. Now the actual set of truthful anchors is, $T = \{i | \; r'_{i\theta} \leq r_i\}$, and our estimated set of truthful anchors is $T' = \{i | \; r'_{i\theta} \leq \hat{r}_i\}$. Using $r_i \leq \hat{r}_i$, it is clear that $T \subseteq T'$. Hence, the set of truthful anchors estimated using our scheme contains *all* truthful anchors. In addition, it could potentially include some malicious anchors. Thus, our approach is pessimistic, in the sense that it might result in some malicious anchors being classified as truthful. However, under no circumstances is a truthful anchor classified as malicious. If the initial set of anchors was U, then the set of malicious anchors is given by $U \setminus T' = \{i | \; r'_{i\theta} > \hat{r}_i\}$. Steps **9** to **21** of Algorithm 2 identify the malicious anchors. The next section illustrates the effectiveness of our schemes through simulations.

VI. Simulation Results

In this section, we present the simulation results that validate our analyses. We have implemented the proposed schemes in Matlab 7.0.4. The simulation region is assumed to be a field of dimensions 100m × 100m. The position of the mobile target is chosen randomly in the network. Once the position of the target is chosen, we deploy anchors randomly around the target such that a certain number of anchors are within the communication range of the target. The communication range of the anchors and the target is chosen to be 35m. The maximum value of the measurement error is chosen to be $\epsilon_{max} = 0.1$. Hence, if r_i is the correct distance bound of anchor i then the estimated bound may lie uniformly in the range $[r_i, \, r_i \cdot (1 + \epsilon_{max})]$. The maximum value for the proportion of lie $\theta_{max} = 1.0$. So, a malicious node i with the true value of its estimated bound being $r_{i\epsilon}$ sets its bound to be a random value between $[r_{i\epsilon}, \, r_{i\epsilon} \cdot (1 + \theta_{max})]$. For the case without measurement errors, the simulations are averaged over 100 iterations for each given total anchor count in range of the target. For all the runs the number of false malicious anchors is no more than B as defined in Section IV. Our scheme localizes the target correctly in 100% of the cases and also catches the malicious anchors with a success rate of 100%. This level of accuracy is achievable as their is no margin for error for a malicious anchor. If the target does not exist on it's bound circle then the anchor is surely lying and is identified.



a) Radius and Localization Error

b) Fraction of lying anchors caught

c) Fraction of lying anchors caught

d) Fraction of lying anchors caught

Fig. 4. Simulation results in the presence of measurement errors

Figure 4 shows the results of localization in the presence of measurement errors. We illustrate two cases. First, when the number of malicious anchors are more than B. The second case, is when the number of malicious anchors are no more than B. For a given number of anchors within the range of a target we execute 20 runs for each possible configuration of number of malicious anchors for better convergence of the results. The case where the number of lying malicious anchors is no more than B is denoted as *LBL* (Less than equal to B Lying) in the graphs and the case where the number of lying malicious anchors is more than B is denoted as *MBL* (More than B Lying).

In Figure 4(a), radius MBL refers to the plot corresponding to the radius of the region (r_R), as obtained in Algorithm 2 when the number of lying anchors are more than B. The plot radius LBL corresponds to r_R when the number of lying anchors are no more than B. The value of r_R when the number of anchors lying is no more than B is lesser than r_R when the lying anchors are more than B. This is because in the former case the number of truthful anchors, which have tighter bound circles, are more. Hence, $\mathcal{R}$ which is defined by these true bound circles is smaller. The same figure also shows the amount of localization error that occurs if we approximate the position of the target by the center x^*. LE refers to localization error, LBL and MBL are the same as before. When the number of malicious anchors is no more than B, the localization error is much less, for a similar reason as before. A small $\mathcal{R}$ means that the center of the region x^* is a suitable approximation of the correct location of the target. Even in the worst case, the error in localization is less than 1m. This demonstrates the suitability of our scheme even when the measurement error is appreciable.

Figure 4(b) shows the fraction of malicious anchors caught when the number of lying anchors is no more than B; plotted as LBL, and the fraction caught when the number of lying anchors is more than B; plotted as MBL. Our scheme on an average catches more than 65% of the malicious anchors irrespective of the total number of malicious anchors in range of the target. The scheme has a very high success rate when the number of truthful anchors is more than $\lceil N/2 \rceil + 2$. From our experimental results, we have observed that when the number of anchors in range of the target is greater than or equal to 18, more than 90% of the lying anchors are caught. The better performance can be attributed to the fact that with the increase in the number of truthful anchors $\mathcal{R}$ becomes smaller, hence more lying anchors get caught.

In Figure 4(c) and 4(d), the illustrations correspond to the case where there are a total of 24 anchors in the range of the target. We illustrate the statistics of maximum, average, and minimum number of lying anchors that our scheme identifies over 50 runs for a given number of malicious anchors in range of the target. Figure 4(c) illustrates the instances where the number of malicious anchors are atleast B and Figure 4(d), the instances where the number of lying anchors are no more than B. When no more than B anchors are lying, in the best case, we are able to identify all the lying anchors. Also, in the average case, our scheme identifies more than 90% of the lying anchors. It is noteworthy that even when B or more anchors are lying, in the average case, more than 60% of the malicious anchors are caught. The success rate is lower because there are more malicious anchors, as a result $\mathcal{R}$ becomes larger and thus for anchor i $\hat{r}_i$ becomes larger. This results in less malicious anchors being caught. We note that all the lying anchors are not always identified because of the reasons outlined in Section V-A. However, the significant success rate highlighted by the simulation results reinforces the usefulness of our schemes to provide robust and secure target tracking in the untrusted wireless environment.

VII. Conclusions and future work

In this paper, we have proposed two robust and secure schemes for target tracking. We have also proved a necessary bound on the number of false anchors whose presence does not undermine the accuracy of target localization in an error-free environment. Our first scheme handles localization when there are no measurement errors, whereas the second scheme handles the case with measurement errors. Simulation results show the effectiveness of our schemes in localizing the target and also identifying the malicious anchors. In future, we shall attempt to provide a stricter performance bound on our second scheme.

References

[1] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “Wireless sensor networks: A survey,” *Computer Networks*, vol. 38, no. 4, pp. 393–422, 2002.

[2] C. Karlof and D. Wagner, “Secure routing in wireless sensor networks: Attacks and countermeasures,” *Elsevier's Ad Hoc Networks Journal, Special Issue on Sensor Network Applications and Protocols*, vol. 1, no. 2–3, pp. 293–315, September 2003.

[3] S. Pattem, S. Poduri, and B. Krishnamachari, “Energy-quality tradeoffs for target tracking in wireless sensor networks.” in *Proceeding of Information Processing in Sensor Networks (IPSN)*, 2003, pp. 32–46.

[4] W.-P. Chen, J. C. Hou, and L. Sha, “Dynamic clustering for acoustic target tracking in wireless sensor networks,” *IEEE Transactions on Mobile Computing*, vol. 03, no. 3, pp. 258–271, 2004.

[5] S. Brands and D. Chaum, “Distance bounding protocols,” in *Advances in Cryptology - Eurocrypt 93, ser. Lecture Notes in Computer Science, LNCS 765*, 1994, pp. 344–359.

[6] S. Čapkun and J. Hubaux, “Secure positioning in wireless networks,” *IEEE Journal on Selected Areas of Communications*, vol. 24, no. 2, pp. 221–232, February 2006.

[7] L. Lazos and R. Poovendran, “HiRLoc: High-resolution robust localization for wireless sensor networks,” *IEEE Journal on Selected Areas of Communications*, vol. 24, no. 2, pp. 233–246, February 2006.

[8] Z. Li, W. Trappe, Y. Zhang, and B. Nath, “Robust statistical methods for securing wireless localization in sensor networks,” in *Proceedings of Information Processing in Sensor Networks (IPSN)*, 2005, pp. 91–98.

[9] W. Du, L. Fang, and P. Ning, “LAD: Location anomaly detection for wireless sensor networks,” in *Proceedings of the 19th IEEE International Parallel and Distributed Processing Symposium (IPDPS)*, 2005.

[10] L. Lazos, R. Poovendran, and S. Čapkun, “ROPE: Robust position estimation in wireless sensor networks,” in *Proceedings of Information Processing in Sensor Networks (IPSN)*, 2005, pp. 324–331.

[11] D. Liu, P. Ning, and W. Du, “Detecting malicious beacon nodes for secure location discovery in wireless sensor networks,” in *Proceedings of the 25th IEEE International Conference on Distributed Computing Systems (ICDCS)*, 2005, pp. 609–619.

[12] N. Bulusu, N. Heidemann, and D. Estrin, “GPS-less low cost outdoor localization for very small devices,” *IEEE Personal Communication Magazine*, vol. 7, no. 5, pp. 28–34, 2000.

[13] L. Doherty, K. Pister, and L. Ghaoui, “Convex position estimation in wireless sensor networks,” in *Proceedings of the IEEE INFOCOM*, 2001, pp. 22–26.

[14] R. Nagpal, H. Shrobe, and J. Bachrach, “Organizing a global coordinate system from local information on ad hoc sensor network,” in *Proceeding of IPSN*, 2003, pp. 333–348.

[15] A. Savvides, C. Hans, and M. Srivastava, “Dynamic fine-grained localization in ad-hoc networks of sensors,” in *Proceeding of ACM MobiCom*, 2001, pp. 166–179.

[16] X. Cheng, A. Thaeler, G. Xue, and D. Chen, “TPS: A time-based positioning scheme for outdoor wireless sensor networks,” in *Proceeding of Joint Conference of the IEEE Computer and Communications Societies (INFOCOM '04)*, vol. 4, 2004, pp. 2685–2696.

[17] A. Savvides, W. Garber, S. Adlakha, R. Moses, and M. Srivastava, “Error characteristics of multihop node localization in ad hoc sensor networks,” in *Proceeding of IPSN*, 2003, pp. 317–332.

[18] D. Niculescu and B. Nath, “Error characteristics of ad hoc positioning systems (APS),” in *Proceeding of ACM MobiHoc*, 2004.

[19] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge University Press, 2004.