Secure and Robust Localization In A Wireless Ad Hoc Environment

Satyajayant Misra, Guoliang Xue and Sarvesh Bhardwaj

***Abstract*— We study the problem of accurate localization of static or mobile nodes in a wireless ad hoc network, using the distance estimates of a group of untrusted anchors within the communication range of the nodes. Some of the anchors may be malicious and may lie independently about the distance estimate. The malicious anchors may also collude to lie about the distance estimates. In both cases, accurate node localization may be seriously undermined. We propose a scheme that performs accurate localization of the nodes in the network despite the presence of such malicious anchors. We also show how to identify most of these malicious anchors. In the case where measurements are error-free, we derive a critical threshold $\mathcal{B}$, for the number of malicious anchors that can be tolerated in the localization process without undermining accuracy. We also show how to correctly localize a node and identify all the malicious anchors in this setting. In the presence of measurement errors, we propose a convex optimization based localization scheme that can accurately localize a node, as long as the number of malicious anchors in its communication range is no more than $\mathcal{B}$. Simulation results show that our schemes are very effective. When the measurements are error prone and the number of malicious anchors is no more than $\mathcal{B}$, our scheme localizes a node with an error less than 8% and is also able to identify a significant number of the malicious anchors. Our schemes guarantee that a true anchor is not identified as malicious.**

Index Terms: Secure localization, wireless ad hoc network, convex optimization.

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 minimal requirement of infrastructure [1]. Despite significant improvements in the miniaturization and seamless deployment of the nodes making up the wireless network [12], there are still many fundamental problems that need to be addressed. The problem of node localization in the presence of malicious anchors 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 distance estimates obtained from a group of network nodes called *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. The presence of malicious anchors makes this problem significantly more complex and also introduces the need for secure localization.

In this paper, we study the problem of secure and accurate localization of a mobile/static node (MN) by itself, with the help of distance estimates, obtained from a group of untrusted anchors within its communication range. We also study how the malicious anchors can be identified. Secure localization is necessitated by the untrusted environment in which most wireless networks operate. In a significant number of works in the literature, the anchors are assumed to be trustworthy and non-tamperable. However, this is a strong assumption in an untrusted environment. In the lifetime of a network, the possibility of anchors being tampered or compromised by an adversary is fairly high. These anchors may be re-programmed by the adversary to provide false distance estimates to the nodes that are localizing themselves. Moreover multiple malicious anchors may collude, resulting in false localization of a node. This is a critical setback for the localization process as incorrect localization may have serious repercussions. The problem of secure localization has been previously studied in the literature (e.g., [8], [14], [15], [16], [25], [27]). To our best knowledge, only the work done by Li *et al.* in [16] bears close resemblance to the problem of secure and accurate localization in the presence of malicious anchors that we are studying. However, our localization scheme has better efficiency and higher accuracy. Our localization scheme is based on an Enhanced Mutual Authenticated Distance bounding (E-MAD) technique, which is an enhancement of the distance bounding (DB) techniques proposed in [3], [27].

Given an MN t and a set S_t of anchors in the communication range of t, the *bound circle* of an anchor $A_i \in S_t$, with respect to t, is the circle with A_i's position as the center and the estimate of the distance between t and A_i (denoted by r_{ti}) as the radius. We will use C_{ti} to denote this bound circle, and use D_{ti} to denote the corresponding *disk*. In the rest of this paper, any reference to the bound circle of an anchor implicitly assumes that it is with respect to an MN. When there is no measurement error and the anchors are all truthful, the location of the MN is the point in the plane where all the bound circles intersect. In this case, the malicious anchors in the network can interfere with the localization process by providing incorrect distance estimates so that all bound circles do not intersect at a single point, thus compromising the localization process. A natural question to ask is, "How many malicious anchors can the localization process tolerate?" In answering this question, we derive a *critical threshold* $\mathcal{B}$, for the number of malicious anchors that can be tolerated in the localization process of an MN without undermining accuracy. We study the problem of secure and accurate localization in two scenarios. In the first scenario, we assume that the distance estimates are error-free.

This research was supported in part by ARO grant W911NF-04-1-0385 and NSF grants CCF-0431167 and CNS-0721803. The information reported here does not reflect the position or the policy of the federal government.

Misra and Xue are with the Department of Computer Science and Engineering, Arizona State University, Tempe, AZ 85287-8809. Email: {satyajayant, xue}@asu.edu. Bhardwaj is currently a senior R&D engineer at Synopsys, Inc., Mountain View, CA, Email: sarvesh.bhardwaj@synopsys.com.

In this setting, we show how to localize the MN and identify the malicious anchors. In the second scenario, we assume that the distance estimates are error-prone. In this setting, we propose a convex optimization based localization scheme to localize the MN. When the number of malicious anchors is more than $\mathcal{B}$, no localization algorithm can guarantee accuracy of localization. Thus to better demonstrate the effectiveness of our algorithms, in the simulation studies, we assume that the number of malicious anchors in the range of the MN is at most $\mathcal{B}$. When the number of malicious anchors is at most $\mathcal{B}$, our schemes can perform accurate localization of an MN and also identify the malicious anchors. They also guarantee that there exist no false positives, that is, true anchors are never identified as malicious.

In Section II, we briefly survey related work in the area of secure localization in wireless ad hoc networks. In Section III, we present the system model. In Section IV, we discuss localization in the absence of measurement errors. In Section V, we present our mechanism for localization in the presence of measurement errors. In Section VI, we present simulation results. We conclude our paper in Section VII.

II. Related Work

Lazos and Poovendran [14] 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.* [16] 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.* [25] proposed a novel approach to secure localization based on hidden and mobile base stations. In [8], Du *et al.* proposed a general scheme to detect localization anomalies due to the presence of adversaries. In [15], Lazos *et al.* proposed a range-free localization and location verification scheme for wireless sensor networks. In [17], Liu *et al.* introduced several techniques to detect and remove compromised beacon nodes, avoid false detections, and also detect replayed beacon signals. In [27], 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. In [11], Hwang *et al.* proposed a distributed mechanism to identify malicious anchors in the network that are faking their ranging information. The work assumes that the ranging information is broadcast by the anchors in the network to be used for localization.

There have been many significant works that use optimization for localization in wireless networks. Here we identify a few that are pertinent. In [18], Lou and Zhang presented a distributed range-free localization scheme for mobile sensor networks. In [29], Vivekanandan and Wong proposed a range-free localization technique named Concentric Anchor Beacon (CAB). In [4], Bulusu *et al.* proposed distributed algorithms for localization of low power devices based on connectivity. In [7], 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.* [20] and Savvides *et al.* [23] proposed localization schemes using distributed propagation of location information and multilateration. Cheng *et al.* in [24], presented a time difference of arrival based position system for efficient location detection using long-range beacons. In [22], 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 [21], Niculescu *et al.* applied the CRLB to a few of the general classes of localization problems. Optimization based approaches have also been used for localization in the presence of Non-Line Of Sight (NLOS) errors [6], [5], [13], [28]. In this paper, we present a secure localization scheme that performs accurate localization and also effectively identifies a large number of malicious anchors in the network. We compare our scheme with the Least Median Square (LMS) scheme [16] and the popular Minimum Mean Square Error (MMSE) scheme [16], [23] for localization and demonstrate its effectiveness.

III. System Model

Our localization framework is based on the following assumptions. The network consists of a set of anchors $\mathcal{A} = \{A_i,\, i = 1, \ldots, n\}$ that are fixed after deployment. Each anchor A_i knows its own position (also denoted as A_i). All communications between the anchors and an MN are bidirectional. Error resilient encoding is used at the physical layer to make the wireless communication error-free. For distance estimation between an anchor A_i and an MN t, the measurement error proportion is given as ϵ_{ti}, where $\epsilon_{ti} \in [-\epsilon_{max}, \epsilon_{max}]$, ϵ_{max} being a known system parameter such that $0 \leq \epsilon_{max} < 1$. For instance, if an MN t obtains a distance estimate d'_{ti} from a true anchor A_i, given that d_{ti} is the true distance between A_i and t, then $d'_{ti} \in [d_{ti} \cdot (1 - \epsilon_{max}), d_{ti} \cdot (1 + \epsilon_{max})]$. The inequality bounding ϵ_{max} ensures that its value does not become greater than or equal to 1, resulting in a possible distance estimate that is zero or negative, which is infeasible. We note that measurement errors generally consist of processing delay and propagation delay and it is possible to obtain the worst case upper bounds for both of them using statistical analyses [9], [10], [27]. Anchor A_i may also lie to MN t about the distance estimate, with the lying proportion given by θ_{ti}. Hence if we denote the Euclidean distance between A_i and t as d_{ti}, the distance estimate with measurement errors and considering malicious anchors is

$$r_{ti} = d_{ti} \cdot (1 + \epsilon_{ti}) \cdot (1 + \theta_{ti}). \tag{1}$$

If anchor A_i is truthful, then $\theta_{ti} = 0$, otherwise $\theta_{ti} > 0$ (see discussions in Section III-B). When the measurements are error-free, we have $\epsilon_{ti} = 0$. We have *positive measurements errors* when $\epsilon_{ti} > 0$ and *negative measurements errors* when $\epsilon_{ti} < 0$. Recall that when the measurements have errors, all the bound circles C_{ti} may not intersect at a single point. In the presence of positive measurement errors, the intersection of the disks D_{ti} results in a compact convex region $\mathcal{R}_t$, which contains the MN t. In the presence of negative measurement errors, this intersection *may* be empty. In this case, our scheme enlarges the radii of all the disks by a factor of $1/(1 - \epsilon_{max})$, guaranteeing a non-empty intersection region $\mathcal{R}'_t \supseteq \mathcal{R}_t$, which contains t. As in [14], [16], [27], we assume that the MN

is pseudo-static, that is, it is static during the localization process which is of a short duration. We assume that the nodes are in the 2-dimensional Euclidean plane $\mathbb{E}^2$, where $\|x\|$ denotes the Euclidean norm of the vector/point x. However, our techniques apply to 3-dimensional space as well. We note that the distance estimates from at least three non-collinear anchors are necessary for localization of a node in 2-dimensions. We also assume that the density of the anchors in the network is uniform. In such a setting, the mobility of the MN in the network does not affect its average location accuracy.

A. Network Model and Assumptions

We assume that the anchors and the MNs are equipped with omnidirectional antennas. The MN and the anchors can generate and share symmetric keys for secure and authentic communication. The positions of no three anchors in the network are collinear. The MNs know the positions of all the anchors in the network. Given that the number of anchors in the network is not large, this requirement can be easily satisfied. The localization technique is assumed to use single-hop based communication between the anchors and the MNs. Multi-hop based communication, which is the execution of high speed distance bounding between an anchor and an MN, using multiple intermediate MNs, is prone to high errors and large distance enlargements. Hence it is inappropriate for high speed distance bounding. As a result, we study only the case where single-hop communication is used for high speed distance bounding. We assume that the anchors and the MNs use Ultra-Wide Band (UWB) radio for communication [10]. UWB radio is suitable for accurate wireless localization because of its high resolution and robustness in the presence of multipath components [10]. For localization, we use an Enhanced Mutual Authenticated Distance bounding (E-MAD) protocol, an enhancement of the technique proposed by Čapkun *et al.* [26], which uses high speed distance bounding (DB). We assume that the anchors and the MNs are capable of executing this protocol. Note that the E-MAD protocol ensures that both the anchors and the MNs can estimate their distance from each other [27], [26], as detailed in the next subsection. Although the error in high speed DB is of the order of 0.08% [27], our schemes are robust enough to handle bigger errors ranging between $[0, 10\%]$ of the measured value as will be demonstrated using the simulations results.

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 localization of an MN in the presence of inside attackers (malicious anchors) 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 MN incorrectly. 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 MN attempting to lie about its position. Previous works, such as [14], [27], already exist in the literature addressing this issue in some detail.

We assume that the communication in the MN localization process is secure and authentic. Use of E-MAD, which is based on high speed DB, prevents wormhole attacks [12], which are a potent attack against localization [27]. The fact that the message exchanges in DB happen at the speed of light, the practical upper limit of the speed of radio waves, ensures that two malicious anchors cannot create a low latency link (wormhole) as it requires a speed higher than that of light. In addition, the fact that the MNs know the positions of the anchors helps prevent sybil attacks [12], because a malicious anchor that uses multiple false positions will be immediately identified by an MN. The only other possible attacks are Denial of Service (DoS) attacks and distance *enlargement* or *reduction* attacks by the malicious anchors. Protection against DoS attacks are outside the scope of this paper. However, we note that there are mechanisms in the literature that address DoS attacks in wireless networks to varying degrees [30]. Another possible attack, which is not part of our threat model is the one in which the malicious anchors can collude with some compromised MNs to incorrectly localize the other MNs. We do not study this attack scenario, although our algorithms can be modified to handle these attacks to a significant extent.

Before discussing the distance enlargement/reduction attacks, we first describe the E-MAD protocol. Fig. 1 shows the E-MAD protocol executed by two nodes u and v. Without loss of generality, we assume that u is an anchor and v is an MN. The general mechanism of this protocol is the same as that proposed by Čapkun *et al.* [26]. However, instead of using message authentication codes (MACs) for authentication, we use a one way cryptographic keyed hash function (CKHF) to encrypt the bit-commitment as shown in the initialization phase. The prover sends the bit-commitment and the corresponding key for the CKHF. The verifier opens the bit-commitment in the authentication phase, after receiving the required random number, and verifies the prover. This results in the exchange of a smaller message in the authentication phase and in addition saves two operations at each node, namely a MAC generation and the verification of the MAC of the node at the other end. Thus, E-MAD requires fewer message exchanges and less computation at the anchors and the MN in comparison to the DB technique proposed by Čapkun *et al.* [27]. We note that the algorithms used for MAC generation can be used as CKHF as well, hence our savings are not because of the use of different algorithms. The use of CKHF for sending bit-commitment allows for implicit authentication and hence the use of the explicit MAC based authentication is not necessary. This results in the savings in our scheme. The distance bounding phase helps both entities

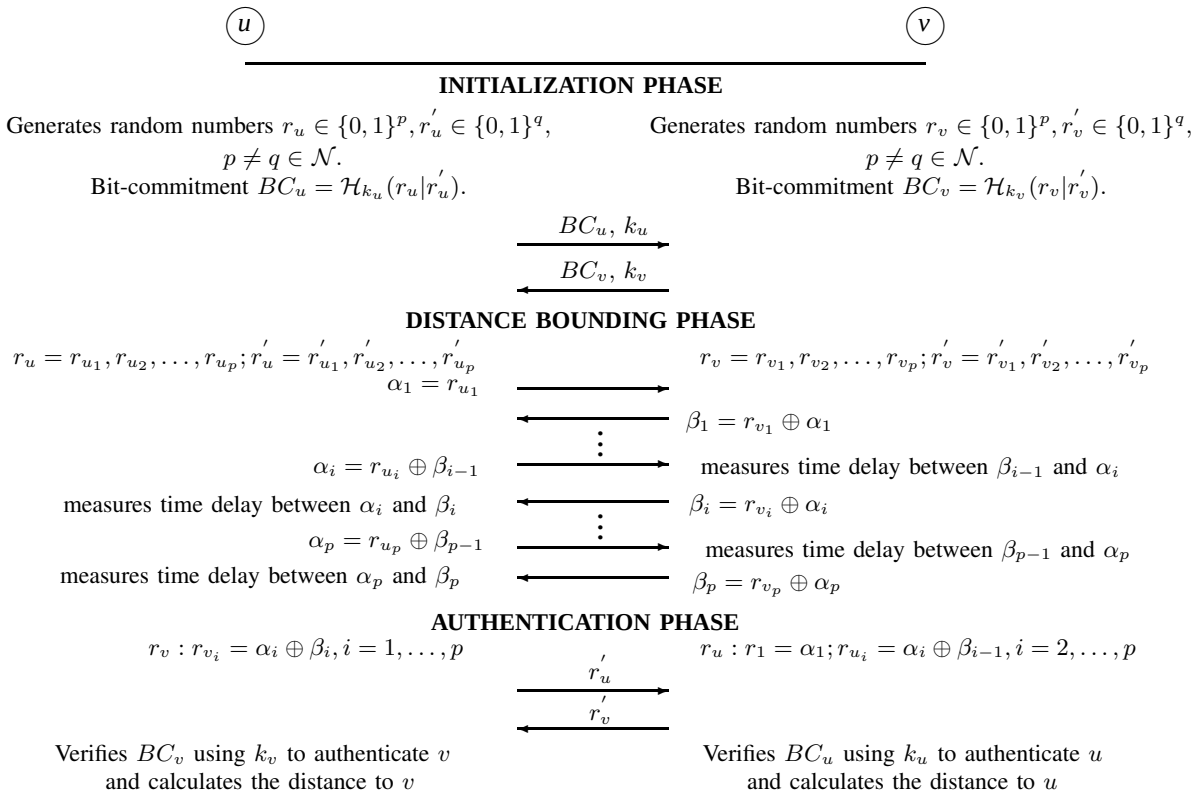


Fig. 1. Enhanced Mutually Authenticated Distance Bounding (E-MAD) using Cryptographic Keyed Hash Function (CKHF).

involved in the E-MAD protocol to calculate an upper bound on their mutual distance. To calculate the upper bound of its distance from v, u calculates the average time taken in sending a bit and receiving a reply from v. The speed of light times half of this average time gives the upper bound on the distance between u and v. Similarly, v can calculate its distance from u.

The use of the E-MAD protocol prevents distance reduction attacks. Given that the message exchange happens at the speed of light there is no way that an anchor or the MN can speed up the transmission of the exchanged bits. Hence neither the anchor nor the MN can reduce the estimate of their distance from each other. However, distance enlargement is still possible because the anchor/MN can enlarge the distance estimate during the MAD protocol by delaying message transmissions. This cannot be identified by the entity at the other end. In this paper, we assume that some of the anchors may be malicious, but all the MNs are truthful. There exist schemes in the literature that use co-operating anchors to identify malicious MNs [25], [27], [26]. Our schemes can be easily modified to do the same. For brevity we do not discuss it here. Note that due to the infeasibility of distance reduction attacks, when the malicious anchors collude to confuse the localization process of the MN, they can only do so by causing an enlargement of the distance estimates.

In a network with malicious anchors, the region $\mathcal{R}_t$ could be considerably large since there is no limit on the amount by which a malicious anchor lies. This introduces a significant amount of uncertainty in the MN's location. In Section IV, we show that when the measurements are error-free, it is possible to obtain a critical threshold $\mathcal{B}$, for the number of malicious anchors out of N anchors in the range of the MN, whose presence does not undermine the exact localization process. In this situation, we show how to precisely localize the MN and also identify the malicious anchors. In Section V, we relax the assumption of non-zero measurement errors to study a more realistic problem. For this problem, we propose a scheme for accurate MN localization. Our results indicate that if the number of malicious anchors is no more than $\mathcal{B}$, our technique can still localize the MN with a high accuracy and identify a significant number of malicious anchors.

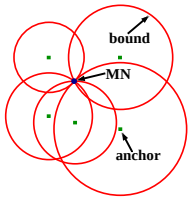
IV. Localization in the absence of Measurement Errors

If the distance estimates are error-free and the anchors are truthful, then the position of an MN t is the common point of intersection of the bound circles, provided that there are at least three non-collinear anchors within its communication range, as shown in Fig. 2(a).

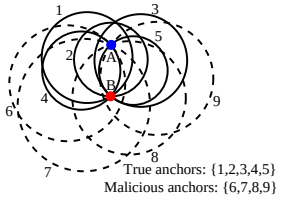
Given that the only possible attacks are distance enlargement attacks, if some of the anchors in the range of t are lying by enlarging their corresponding distance estimates, then t will be located inside their corresponding disks. Hence, it may appear that if some of the anchors are lying but the majority (more than half) is truthful, then we can still correctly localize t as the point where the majority of the bound circles intersect. However, in the following example, we show that even if the majority of anchors are truthful, there is still a possibility that the malicious anchors can collude so that the majority of the bound circles intersect at a point which is different from the true location of t.

A. Motivating Example

Figure 2(b) shows a scenario with an MN and 9 anchors in its range labeled as $\{1, 2, \ldots, 9\}$. The truthful anchors (whose bound circles are shown in solid) are given by the set $T = \{1, 2, 3, 4, 5\}$ and the malicious anchors (whose



(a) Only truthful anchors present



(b) Malicious anchors present

Fig. 2. (a) Correct localization in the absence of measurement errors and malicious anchors; (b) Incorrect localization in the presence of malicious anchors.

bound circles are shown in dashed) are given by the set $F = \{6, 7, 8, 9\}$. The correct position of the MN is the point of intersection B of the bound circles of anchors in 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 ($\{6, 7, 8, 9\}$) collude in an intelligent way to have their bound circles intersect at another point A where two truthful anchors 4 and 5 also intersect. Hence, the number of anchors that intersect at the true location of the MN (point B) is 5 ($\{1, 2, 3, 4, 5\}$) and the number of anchors that intersect at the false location of the MN (point A) is 6 ($\{4, 5, 6, 7, 8, 9\}$). This misleads the localization process, resulting in the localization of the MN at a false position A, where most of the bound circles intersect.

B. Conditions for Exact Localization

As shown in the previous example, even if the majority of the anchors in the range of the MN are truthful, it still does not guarantee exact localization of the MN. Hence, in what follows, we derive a critical threshold $\mathcal{B}$, for the number of malicious anchors out of N anchors in the communication range of an MN that can be tolerated by the localization process without undermining accuracy.

Lemma 1: Let A and B be two distinct points in the Euclidean plane $\mathbb{E}^2$. If three circles C_1, C_2, and C_3 all pass through both A and B, then the three circles are collinear. □

Corollary 1: Assume that no three anchors in the network are collinear. Then at most one point in the Euclidean plane $\mathbb{E}^2$ can have three or more bound circles passing through it. □

Theorem 1: Given that the number of anchors in the range of an MN t is N and that some of them are malicious and colluding, the minimum number of truthful anchors required for exact localization of t in the presence of colluding malicious anchors is given by $\lceil N/2 \rceil + 2$. □

Proof: By deleting anchor 9 in our motivating example, we will have a scenario where five bound circles ($\{1,2,3,4,5\}$) intersect at point B and five bound circles ($\{4,5,6,7,8\}$) intersect at point A. Therefore the presence of $\lceil N/2 \rceil + 1$ ($N = 8$) truthful anchors still does not guarantee the exact localization of an MN. Next, we shall show that the presence of at least $\lceil N/2 \rceil + 2$ truthful anchors guarantees the exact localization of the MN. Recall that t also denotes the true location of the MN t. Therefore the bound circles of all the truthful anchors intersect at point t. For any other point t' to be a possible candidate location for the MN, 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 plane cannot have more than $\lfloor N/2 \rfloor$ bound circles intersecting at it. Thus, the MN is exactly localized at point t. This proves the theorem. ■

The above theorem shows that if there are N anchors in the range of an MN, then the maximum number of malicious anchors that can be tolerated by the localization process without undermining accuracy is $\lfloor N/2 \rfloor - 2$. We call this value the *critical threshold* and denote it by $\mathcal{B}$.

C. Identification of Malicious Anchors

Under the conditions described above for exact localization of an MN t, it is easy to catch the malicious anchors once the MN has been localized. For each anchor A_i, the Euclidean distance d_{ti} is computed. Since each malicious anchor lies by giving a wrong estimate of the distance between its position and t, an anchor A_i will be malicious if $d_{ti} \neq r_{ti}$, It should be noted that *all* malicious anchors can be identified irrespective of the amount of their distance enlargements.

In the next section, we will address the problem of MN localization in the presence of measurement errors.

V. Localization in the Presence of Measurement Errors

Distance measurements in a wireless network are generally prone to errors due to the noisy and delay prone wireless medium. Hence, the distance estimates of an MN are error-ridden. Using a specialized hardware and UWB radio, the measurement errors in DB can be as low as 15 cms at a distance of 2 kms when performed outdoors (0.0075%) and 14 cms at a distance of 7 m (2.0%) when performed indoors [9], [27]. We present a localization scheme to be used in this scenario and demonstrate using simulations that our scheme is robust even when the measurement errors are as high as 10% of the true value. This shows the suitability of our scheme in more error prone and hostile environments.

Our localization technique uses convex optimization to estimate the position of an MN. As discussed before, in the event of negative measurement errors, the intersection region $\mathcal{R}_t$ of the disks D_{ti} may be empty. In this case, we let the MN t increase the distance estimates r_{ti} by a factor of $1/(1 - \epsilon_{max})$, resulting in the *increased distance estimate* $r'_{ti} = r_{ti}/(1 - \epsilon_{max})$. Denote the corresponding increased bound circles and disks by C'_{ti} and D'_{ti}, respectively. The

intersection of the D'_{ti} results in a non-empty region $\mathcal{R}'_t$ in which the MN is guaranteed to exist.

Since we make no assumption regarding the distribution of the distance estimates of the MN from an anchor, all points inside the region $\mathcal{R}'_t$ are likely to be the position of the MN. The worst case error in estimation would be minimized if we use the *geometric center* x_c of $\mathcal{R}'_t$ as the location of the MN, where x_c is the point such that $\max_{x\in\mathcal{R}'_t}\|x - x_c\| \leq \max_{x\in\mathcal{R}'_t}\|x - y\|$, for any $y \neq x_c$. However, the geometric center is difficult to compute. Therefore, we solve the following convex optimization problem to obtain an approximation to the geometric center.

$$\begin{aligned} \max_{x,\delta} \quad & \delta \\ \text{subject to} \quad & \|x - A_i\|^2 \leq \left[r'_{ti}\cdot(1-\delta)\right]^2, \quad i = 1,\ldots,N, \\ & x \in \mathbb{E}^2, \delta \geq 0. \end{aligned} \tag{2}$$

Essentially, we are shrinking all disks (D'_{ti}) simultaneously using a common factor $(1-\delta)$, as much as we can, provided that they still have a non-empty intersection. The first N constraints in (2) ensure that the intersection of the disks is non-empty. The objective function is to maximize δ, consequently minimizing the shrinking factor $(1-\delta)$. Clearly, this convex optimization problem has a unique optimal solution (x^*, δ^*). We call x^* the *algebraic center* of $\mathcal{R}'_t$. We transform the constrained optimization problem in (2) into the following unconstrained optimization problem,

$$\min_{x,\delta} \quad -\lambda\cdot\delta - \sum_{i=1}^{N}\log\left[(r'_{ti}\cdot(1-\delta))^2 - \|x-a_i\|^2\right] - \log(\delta), \tag{3}$$

where λ is the Lagrangian multiplier [2]. This problem can be solved efficiently using the *barrier method* [2] as presented in Algorithm 1. In Algorithm 1, the minimization in the centering step uses Newton's method [2] with a tolerance $\eta = 1\times10^{-6}$.

Algorithm 1 Illustration of Barrier Method

1: Given a strictly feasible x, $\lambda = \lambda^{(0)} > 0$, $\mu > 1$, tolerance $\epsilon > 0$. $\{\lambda^{(0)} = 1.0,\ \mu = 10.0\}$
2: **repeat**
3: *Centering Step:* Starting at x, compute $x^*(\lambda)$ by minimizing the objective in (3).
4: Update $x := x^*(\lambda)$; $\lambda = \mu\times\lambda$.
5: **until** $N/\lambda \leq \epsilon$ $\{\epsilon = 1\times10^{-6}\}$

As the barrier method progresses, the value of δ keeps increasing. This emulates the reduction of the disks D'_{ti}. After a number of iterations, when the size of $\mathcal{R}'_t$ has been reduced significantly, the algorithm stops and outputs a point x^* which is the algebraic center of $\mathcal{R}'_t$. We use the point x^* as the estimate of the location of the MN.

In this paper, we assume that the MN t has adequate resources to perform Algorithm 1 for localization. On the other hand, if it does not, then the localization may be performed by the anchors and the position information can be subsequently conveyed to the MN.

A. Identification of malicious anchors

It could happen that a malicious anchor A_i lies by enlarging its distance estimate, but

$$r_{ti} = d_{ti}\cdot(1+\epsilon_{ti})\cdot(1+\theta_{ti}) \leq d_{ti}\cdot(1+\epsilon_{max}), \tag{4}$$

either due to a small or negative value of ϵ_{ti} or due to a small value of θ_{ti}. In this case, we would consider A_i truthful because the *aggregated enlargement* of the distance estimate cannot be differentiated from the case with measurement error only. On the other hand, if A_i is a truthful anchor (i.e. $\theta_{ti} = 0$), then $r_{ti} = d_{ti}\cdot(1+\epsilon_{ti}) \leq d_{ti}\cdot(1+\epsilon_{max})$. Therefore, for our purpose, A_i is a malicious anchor if and only if $r''_{ti} > d_{ti}$. However, in the presence of measurement errors, the position of the MN cannot be computed precisely. Hence d_{ti} cannot be calculated exactly. In our scheme, we use an upper bound of d_{ti}, denoted by $\hat{d}_{ti}$, which can be computed easily. According to our analysis, if $r''_{ti} > \hat{d}_{ti}$, anchor A_i must be a malicious anchor.

Algorithm 2 Algorithm for Identifying Malicious Anchors

1: GIVEN: The algebraic center x^* of $\mathcal{R}'_t$ and
2: VERTICES := $\{x|$ x is a vertex (defined in the text) of $\mathcal{R}'_t\}$
3: V' := $\{y|$ y is the mid-point of the major arc of the bound circle constituting the boundary of $\mathcal{R}'_t\}$
4: VERTICES :=VERTICES $\cup V'$.
5: $r^* := 0$. /* Defines the radius of the intersection region $\mathcal{R}'_t$ */
6: **for all** $y \in$ VERTICES **do**
7: **if** $\|y - x^*\| > r^*$ **then**
8: $r^* := \|y - x^*\|$.
9: **end if**
10: **end for**
11: **for all** anchors A_i, $1 \leq i \leq n$ **do**
12: $r''_{ti} := r_{ti}/(1+\epsilon_{max})$. /* r_{ti} is reduced */
13: **if** $r''_{ti} > \|x^* - A_i\| + r^*$ **then**
14: Anchor A_i **is** malicious.
15: **else**
16: Anchor A_i **is not** malicious.
17: **end if**
18: **end for**

Algorithm 2 presents our scheme to identify malicious anchors. Lines **2** through **10** compute r^*, which is the radius of the smallest circle centered at x^* that covers all points in $\mathcal{R}'_t$. Therefore, $\hat{d}_{ti} \triangleq \|A_i - x^*\| + r^*$ is an upper bound of d_{ti}. The vertices of region $\mathcal{R}'_t$ in Line **2** of Algorithm 2 are obtained by calculating the points of intersection of all possible pairs of distance bound circles C'_{ti} and choosing only the points that lie inside or on all the circles. The boundary of $\mathcal{R}'_t$ consists of major or minor arcs of some of the bound circles. For each major arc on the boundary. We also add its mid-point as the vertex. Following Lemma 2, the largest distance from x^* to a point in $\mathcal{R}'_t$ occurs at a vertex. This guarantees that $\hat{d}_{ti}$ is an upper bound of d_{ti}, because

$$d_{ti} = \|A_i - t\| \leq \|A_i - x^*\| + \|x^* - t\| \leq \|A_i - x^*\| + r^*. \tag{5}$$

Lines **11** to **18** use the condition $r''_{ti} > \hat{d}_{ti} \geq d_{ti}$ to catch some

of the malicious anchors.

Lemma 2: Let two circles C_1 and C_2 with radius r_1 and r_2 respectively, intersect at two points p and q. Let the minor arc corresponding to C_1 be $\widehat{pq}_1$ and that corresponding to C_2 be $\widehat{pq}_2$. If $\widehat{pq}_1 \geq \widehat{pq}_2$, then $r_1 \leq r_2$. Also if $r_1 \geq r_2$, then $\widehat{pq}_1 \leq \widehat{pq}_2$. □

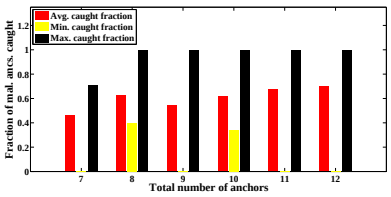
Proof: We will prove this by contradiction. Let us assume that $r_1 > r_2$, then the line C_1C_2 joining the centers of C_1 and C_2 and bisecting chord pq intersects C_2 at two points, say l and m, where m is the point on the major arc $\widehat{pq}_2$. m should be inside C_1 as $r_1 > r_2$. This implies that C_2 intersects C_1 at 4 non-collinear points (p and q being 2 of them). According to the properties of circles, only one unique circle can pass through three or more non-collinear points. Thus C_1 and C_2 are the same circle, this implies that $r_1 = r_2$, which is a contradiction. Thus we prove that $r_1 \leq r_2$. Since $\widehat{pq}_1 \geq \widehat{pq}_2$, thus $\widehat{pq}_2 \in C_1$. Using negation, $\sim (\widehat{pq}_1 \geq \widehat{pq}_2 \implies r_1 \leq r_2)$, we have, $r_1 \geq r_2 \implies \widehat{pq}_1 \leq \widehat{pq}_2$. ■

We note that Algorithm 2 does not guarantee catching all malicious anchors. Our simulation results to be presented in the next section show that our scheme is very effective. As discussed above, our scheme does not have false positives, that is, it never identifies a truthful anchor as malicious.

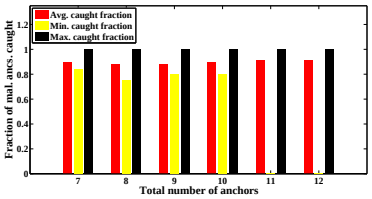
VI. Simulation Results

We have implemented the proposed schemes in Matlab 7.0.4. The simulation region was assumed to be a field of dimensions 100m × 100m. The communication range of the anchors and the MN was chosen to be 35m. The position of the MN t was chosen randomly in the field. To simulate a certain number of anchors in the range of the MN t, we randomly deployed anchors inside the range of t. The maximum value of the measurement error proportion was chosen to be $\epsilon_{max} = 0.1$. The maximum value for the proportion of lie was chosen as $\theta_{max} = 1.0$. So, a malicious anchor A_i with r_{ti} as its distance estimate (with or without measurement error) from t, set its distance estimate to be a random value in $[r_{ti},\ r_{ti} \cdot (1 + \theta_{max})]$. We also studied the effectiveness of our scheme with different values of θ. For the case without measurement errors, the results were averaged over 100 iterations for a given total number of anchors in the range of the MN. For all the runs, the number of malicious anchors is no more than $\mathcal{B}$ as defined in Section IV. Our scheme localized the MN correctly in 100% of the cases and also caught the malicious anchors with a success rate of 100%. We do not present the result here because it is guaranteed by theory as well.

For the case with error prone measurements, to demonstrate the effectiveness of our scheme we compare the error in localization in our scheme with that in the LMS scheme [16] and the MMSE technique [23]. It is well-known that the MMSE technique is prone to large errors when the anchors are lying [19]. Our simulation results, which are averaged over 50 runs, are presented in Figs. 3, 4, and 5. If the number of anchors in the range of t is given by N, the number of malicious anchors M belongs to $\{1, \ldots, \lfloor N/2 \rfloor - 2\}$. In the simulation, the number of anchors N in the range of an MN belonged to $\{7, \ldots, 12\}$. Fig. 3 shows the average, maximum, and minimum fraction of malicious anchors that were caught by our scheme over 50 runs. Fig. 3(a) shows the results when the anchors are not colluding, whereas Fig. 3(b) shows the results when the malicious anchors were colluding. To simulate collusion between the malicious anchors, the malicious anchors attempted to localize the MN 35m away from its true location. The choice of this value for the false position was motivated by the fact that the farther the false position of MN t is from its true position, the more is the resultant disruption in localization. Hence we chose a distance difference that is equal to the transmission range so as to model a large deviation from the true position due to collusion. When



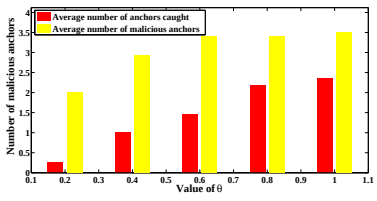
(a) The non-colluding case



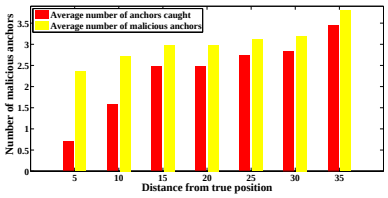
(b) The colluding case

Fig. 3. Fraction of malicious anchors caught by our scheme

the anchors were not colluding, on an average our scheme was able to identify at least 45% of the malicious anchors. When the malicious anchors were colluding, on an average more than 85% of them were caught. This is because when the malicious anchors colluded, they attempted to localize the MN 35m away from t. This resulted in a large enlargement of their bound circles, hence making them more susceptible to getting caught. To study the effect due to the amount of malicious anchors are lying, we study the result corresponding to varying values of θ_{max} (in the non-colluding case) and the distance between the false position and t (in the colluding case). These results are presented in Fig. 4. In this setting, the value of N was 12 and that of M was 4. For each data point on the X-axis, the bar on the right represents the average number of malicious anchors in the range of t and the bar on the left represents the average number of malicious anchors caught. Fig. 4(a) illustrates the case where the malicious anchors are not colluding. The lying proportion θ was assigned values between 0.2 and 1.0 with a step size of 0.2. Fig. 4(b) illustrates the case where the malicious anchors are colluding to localize t at a false position. The distance between t and and the false position was assigned values ranging from 5m to 35m in steps of size 5m. We observe that with the increase in the value of θ_{max} in the non-colluding case or the increase in the distance in the colluding case, the number of malicious anchors in the range of t increases. This is due to the increase in the magnitude of their lying potential (θ_{max} or the distance). Thus



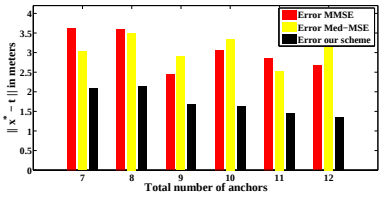
(a) The non-colluding case



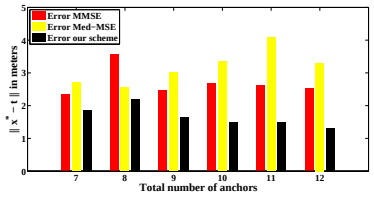
(b) The colluding case

Fig. 4. Graph showing the number of malicious anchors caught with a change in the amount by which they lie.

the number of malicious anchors that do not satisfy Equation (4) and are designated as malicious also increases. We observe that with an increase in the malicious anchors lying potential, more number of these anchors were caught. In addition, with a higher value of θ_{max} or the distance between the false position and t, the percentage of malicious anchors caught by our scheme also increases.



(a) The non-colluding case



(b) The colluding case

Fig. 5. Comparison of localization error in MMSE, LMS, and our scheme.

Fig. 5 shows the comparison of our scheme with other schemes, namely LMS (denoted as Med-MSE) and modified MSE (denoted as MMSE). Fig. 5(a) presents the result when the malicious anchors are lying without collusion. Fig. 5(b) presents the result when the malicious anchors are colluding. With the use of only the estimates obtained from anchors that have been identified by our scheme to be true, the modified MMSE scheme results in an average estimation error that is comparable with that obtained when using the LMS scheme, which is more computation intensive [16], [19]. However, the error obtained by our scheme is always less than that from the other two techniques. With an increase in the number of anchors, the use of our scheme results in a decrease in the value of localization error. This is expected, because the number of true anchors increases with the increase in the number of anchors, resulting in a reduction in the size of $\mathcal{R}'_t$. Consequently, reducing the error in the use of our scheme and refining the estimate. However, the basic least squares technique on which the LMS and MMSE schemes are based can not guarantee such a refinement. Our scheme is also better than the LMS/MMSE schemes in another aspect. It ensures that the MN being localized is certain to exist inside $\mathcal{R}'_t$, obtained in Algorithm 1. The LMS and the modified MMSE schemes cannot provide any such guarantees.

When the anchors are colluding, with the use of the LMS scheme the estimation errors first increase with increase in the number of anchors because the number of malicious anchors also increase, and then decrease as the number of true anchors become large. The modified MMSE scheme gives better results than the LMS scheme as the malicious anchors are removed from the estimation process. This demonstrates that even the modified MMSE scheme, which is much simpler than the computation intensive LMS scheme, can perform much better localization if the malicious anchors are effectively removed from the localization process. Our scheme provides even better results than the modified MMSE scheme, with the localization error value being less than half of the others in most cases. The maximum value of the average estimation error was less than 2.5m when N was 8, which is less than 8%. The simulation results underline the efficacy of our scheme for improving localization accuracy in the presence of malicious anchors.

VII. Conclusions and Future Work

In this paper, we have proposed a robust and secure schemes for MN localization in the presence of malicious anchors. We proved a critical threshold for the number of malicious anchors that can be tolerated by the localization process without undermining the accuracy of MN localization in an error-free environment. Our schemes perform robust localization when there are no measurement errors and also when both positive and negative measurement errors exist. Simulation results demonstrated the effectiveness of our schemes in localizing the MN and also identifying the malicious anchors.

Acknowledgment

We thank the Associate Editor and the anonymous reviewers whose comments on an earlier version of this paper have helped to significantly improve the presentation of this paper.

References

[1] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. Wireless sensor networks: A survey. *Computer Networks*, 38(4):393–422, 2002.

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

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

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

[5] Y-T. Chan, Y. Hang, and H. Ching. Exact and approximate maximum likelihood localization algorithms. *IEEE Transactions on Vehicular Technology*, 55(1):10–16, January 2006.

[6] Y.-T. Chan, W.-Y. Tsui, H.-C. So, and P. Ching. Time of arrival based localization under NLOS conditions. *IEEE Transactions on Vehicular Technology (TVT)*, 55(1):17–24, 2006.

[7] L. Doherty, K. Pister, and L Ghaoui. Convex position estimation in wireless sensor networks. In *Proceedings of the IEEE INFOCOM*, pages 22–26, 2001.

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

[9] R. Fontana. Experimental results from an ultra wideband precision geolocation system. In *Ultra-Wideband, Short-Pulse Electromagnetics 5*, pages 215–223. Springer US, 2002.

[10] S. Gezici, T. Zhi, G. Giannakis, H. Kobayashi, A. Molisch, H. Poor, and Z. Sahinoglu. Localization via ultra-wideband radios: a look at positioning aspects for future sensor networks. *IEEE Signal Processing Magazine*, 22(4):70–84, 2005.

[11] J. Hwang, Tian He, and Y. Kim. Detecting phantom nodes in wireless sensor networks. In *INFOCOM*, pages 2391–2395, 2007.

[12] 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*, 1(2–3):293–315, September 2003.

[13] W. Kim, J. Lee, and G.-I. Jee. The interior point method for an optimal treatment of bias in trilateration location. *IEEE Transactions on Vehicular Technology (TVT)*, 55(4):1291–1301, 2006.

[14] L. Lazos and R. Poovendran. HiRLoc: High-resolution robust localization for wireless sensor networks. *IEEE Journal on Selected Areas of Communications*, 24(2):233–246, February 2006.

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

[16] 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)*, pages 91–98, 2005.

[17] 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)*, pages 609–619, 2005.

[18] J. Lou and Q. Zhang. Relative distance based localization for mobile sensor networks. In *GLOBECOM*, 2007.

[19] S. Misra, G. Xue, and A. Shrivastava. Robust localization in wireless sensor networks through the revocation of malicious anchors. In *Proceeding of the IEEE International Conference on Communications (ICC)*, 2007.

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

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

[22] 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*, pages 317–332, 2003.

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

[24] A. Thaeler, M. Ding, and X. Cheng. iTPS: an improved location discovery scheme for sensor networks with long-range beacons. *J. Parallel Distrib. Comput.*, 65(2):98–106, 2005.

[25] S. Čapkun, M. Čagalj, and M. Srivastava. Securing localization with hidden and mobile base stations. In *Proceedings of the IEEE International Conference on Conference Communication (INFOCOM)*, 2006.

[26] S. Čapkun, L. Buttyán, and J. Hubaux. Sector: secure tracking of node encounters in multi-hop wireless networks. In *Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks*, pages 21–32, New York, NY, USA, 2003.

[27] S. Čapkun and J. Hubaux. Secure positioning in wireless networks. *IEEE Journal on Selected Areas of Communications*, 24(2):221–232, February 2006.

[28] S. Venkatesh and R. Buehrer. Nlos mitigation using linear programming in Ultra-wideband location-aware networks. *IEEE Transactions on Vehicular Technology*, 56(5):3128–3198, 2007.

[29] V. Vivekanadan and V. Wong. Concentric anchor-beacons CAB localization for wireless sensor networks. *IEEE Transactions on Vehicular Technology*, 9:3972–3977, June 2006.

[30] A. Wood and J. Stankovic. Denial of service in sensor networks. *IEEE Computer*, 35(10):54–62, 2002.

Satyajayant Misra received his integrated M.Sc. (Tech) Information Systems and M.Sc.(Hons) Physics in June 2003 from the Birla Institute of Technology and Sciences (BITS), Pilani. He is currently a Ph.D. candidate in the Department of Computer Science and Engineering at Arizona State University. His research interests include identifying security, privacy, reliability, and survivability issues in wireless sensors and ad hoc networks and formulating efficient solutions to handle them. He has published papers in journals such as IEEE Communications Surveys and Tutorials and Computer Networks and conferences such as, IEEE Infocom, IEEE MILCOM, and IEEE ICC. He has also served on the technical program committees of GLOBECOM'2007 and ChinaCom'2008.

Guoliang (Larry) Xue (SM'99/ACM'93) received the BS degree (1981) in mathematics and the MS degree (1984) in operations research from Qufu Teachers University, Qufu, China, and the PhD degree (1991) in computer science from the University of Minnesota, Minneapolis, USA. He is a Full Professor in the Department of Computer Science and Engineering at Arizona State University. He has held previous positions at Qufu Teachers University (Lecturer, 1984-1987), the Army High Performance Computing Research Center (Postdoctoral Research Fellow, 1991-1993), the University of Vermont (Assistant Professor, 1993-1999; Associate Professor, 1999-2001).

Dr. Xue's research interests include efficient algorithms for optimization problems in networking, with applications to survivability, security, privacy, and energy efficiency issues in networks ranging from WDM optical networks to wireless ad hoc and sensor networks. He has published over 150 papers in these areas, including many papers in journals such as IEEE Transactions on Circuits and Systems, IEEE Transactions on Communications, IEEE Transactions on Computers, IEEE Transactions on Vehicular Technology, IEEE/ACM Transactions on Networking, SIAM Journal on Computing, SIAM Journal on Discrete Mathematics, SIAM Journal on Optimization, and conferences such as ACM MobiHoc, ACM/SIAM SODA, and IEEE Infocom. His research has been continuously supported by federal agencies including NSF and ARO.

Xue received the *Graduate School Doctoral Dissertation Fellowship* from the University of Minnesota in 1990, a *Third Prize from the Ministry of Education of P.R. China* in 1991, an *NSF Research Initiation Award* in 1994, and an *NSF-ITR Award* in 2003. He is an Editor of Computer Networks (COMNET), an Editor of IEEE Network, and the Journal of Global Optimization. He has served on the executive/program committees of many IEEE conferences, including Infocom, Secon, Icc, Globecom and QShine. He served as a TPC co-chair of *IEEE IPCCC* in 2003, a TPC co-chair of *IEEE HPSR* in 2004, the General Chair of *IEEE IPCCC* in 2005, a TPC co-chair of *IEEE Globecom'2006 Symposium on Wireless Ad Hoc and Sensor Networks*, a TPC co-chair of *IEEE ICC'2007 Symposium on Wireless Ad Hoc and Sensor Networks*, and a TPC co-chair of *QShine* in 2007. He also serves on many NSF grant panels and is a reviewer for ARO.

Sarvesh Bhardwaj received his B.Tech. in Electrical Engineering from the Indian Institute of Technology, Delhi in 2000, M.S. in Electrical and Computer Engineering from the University of Arizona, Tucson in 2003, and Ph.D. in Electrical Engineering from the Arizona State University, Tempe, AZ in 2006.

He is currently a Senior R&D Engineer with Synopsys, Inc., Mountain View, CA. He was a postdoctoral Research Associate in the School of Computing and Informatics at the Arizona State University, Tempe, AZ during Spring 2007. He also held the position of Staff Engineer with Stratosphere Solutions from January-July 2007. He was with MindTree Consulting, Bangalore as a VLSI Design Engineer from June-December 2000. His research interests include Statistical Analysis and Optimization of integrated circuits in the presence of process variations, logic synthesis, and Design for Manufacturability.