A GRADIENT DESCENT BASED APPROACH TO SECURE LOCALIZATION IN MOBILE SENSOR NETWORKS

Ravi Garg, Avinash L. Varna, and Min Wu

Department of Electrical & Computer Engineering
Institute for Advanced Computer Studies
University of Maryland, College Park, MD, USA
Email: {ravig, varna, minwu}@umd.edu

ABSTRACT

Localization of constituent nodes is of fundamental importance in many wireless sensor networks (WSNs) related applications. Existing research has mainly investigated the problem of localization in static WSNs, where the localization is performed mainly at the time of the node deployment. In contrast, it is important to keep track of the current locations of the nodes by invoking the localization algorithm periodically in mobile nodes. The high computation cost associated with most existing localization algorithms makes them less practical to use in resource constrained mobile sensor networks (MSNs). Additionally, these existing techniques often fail in hostile environments where some of the nodes may be compromised by adversaries, and used to transmit misleading information aimed at preventing accurate localization of the remaining sensors. In this paper, we build on our earlier work to propose an iterative gradient descent based technique with low computational complexity to securely localize nodes in MSNs. The proposed algorithm combines iterative gradient descent with selective pruning of inconsistent measurements to achieve a high localization accuracy. Simulation results demonstrate that the proposed algorithm can find a map of relative locations of the MSN even when some nodes are compromised and transmit false information.

Index Terms— Mobile Sensor Networks, Secure Localization

1. INTRODUCTION

Many wireless sensor networks related applications require knowledge about locations of the constituent nodes. In such applications, it is desirable for the constituent nodes to be able to determine their location before they start sensing and transmitting gathered information. Many existing techniques use anchor nodes to determine the positions of other nodes in the network. These techniques often fail in hostile environments where some of the nodes may be compromised by adversaries, and used to transmit misleading information aimed at preventing accurate localization of the remaining sensors. Furthermore, sensor nodes may also have limited computational power and memory due to the low cost requirements to make it feasible to deploy sensor nodes in many commercial applications. Our previous work took these factors into consideration and proposed a computationally efficient secure localization algorithm for static WSNs to withstand malicious attacks [1].

For some applications, it is important for nodes to be equipped with mobile capabilities. For example, to achieve a broad coverage in a given area during deployment, mobile nodes can adjust their positions in order to determine the most efficient configuration [2]. Mobile nodes are also advantageous in such applications as battlefield and disaster rescue operations. Locations of the nodes change dynamically in such applications of MSNs. Therefore, we need to devise techniques to update the location estimates periodically to keep track of the nodes. Similar to static WSNs, mobile networks are also vulnerable to malicious attacks in hostile environments. Hence, it is important to design localization techniques for MSNs that are attack resilient and computationally efficient.

Several prior works have examined localization in MSNs in the absence of malicious attacks. A two-stage Monte Carlo based approach for localization was proposed in [3]. In the first stage of this method, a fixed number of candidate sample locations, satisfying the velocity constraints on a given node, are randomly drawn, and in the second stage of filtering, samples that are inconsistent with the measurements obtained from anchor nodes are filtered out. The localization accuracy of the algorithm in [3] was improved in [4] by using a box shaped region to sample particles in the prediction phase, and eliminate inconsistent particles in the filtering stage using velocity constraints. The Monte carlo algorithm was extended to incorporate security in [5] by modifying the filtering stage. Instead of identifying points that are consistent with measurements from all the anchors, the position consistent with the maximum number of measurements from anchors is determined. This approach is similar to the voting based approach in [6] to secure localization in static WSNs, and suffers from

high computational and storage requirements that may not be available for resource constrained networks.

Most of the prior works also assume the presence of anchor nodes that are used to determine the position of the mobile nodes, and cannot be applied to MSNs without anchor nodes. In contrast, we consider the case where network may not have any anchor nodes. To the best of our knowledge, this is the first work addressing the problem of localizing nodes in MSNs in the presence of malicious attacks, and without the help of anchor nodes.

2. PROBLEM DESCRIPTION

In this section, we describe the problem setup for secure localization in MSNs. We are interested in determining the location estimates of each node in the network, and periodically updating the estimates after a fixed amount of time. This problem can be equivalently reduced to the estimation of a relative location map that preserves the distances and neighborhood relation among the nodes. Many applications such as leader-following [7], and direction-based routing algorithms [8] require only the information about a relative location map. As relative location map preserves pairwise distances, the set of relative locations is only a rotation and translation of the absolute locations. If the absolute positions of any three nodes are known, the absolute locations of remaining nodes can be determined by estimating the rotation and translation parameters. Even in applications where the absolute locations of the nodes need to be determined, a relative location map can be used as an intermediate step in the localization process. So, instead of finding absolute locations, we estimate a relative location map of the nodes in the network.

Let us denote the location of the i^{th} node in the network at time instant t by $\mathbf{P}_i(t) = \{x_i(t), y_i(t)\}$, and let $\mathbf{S}(t) = \{\mathbf{P}_1(t), \mathbf{P}_2(t), \ldots, \mathbf{P}_N(t)\}$ be the set of positions of all the N nodes in the network. Let $d_{ij}(t) = \|\mathbf{P}_i(t) - \mathbf{P}_j(t)\|$, $j \neq i$ be the distance between nodes i and j at time t. At each time-instant, node i receives a signal containing the current location estimate of node j and a time-stamp from node j, and estimates $d_{ij}(t)$, $j = \{1, 2, \ldots, N\}$, $j \neq i$ using time of arrival or other distance estimation methods. These distance measurements may be noisy in practice, and we model the measurement errors as additive Gaussian noise, $n_{ik}(t)$, with zero mean and variance σ^2. We also assume that nodes remain stationary during transmission and processing of the time-stamp signals because the time elapsed in these operations is very small when signal is traveling at the speed of light in radio transmission or the speed of sound in ultrasound transmissions. The problem of estimating a relative location map at time instant t involves finding a set of location estimates $\hat{\mathbf{S}}(t) = \{\hat{\mathbf{P}}_1(t), \hat{\mathbf{P}}'_2(t), \ldots, \hat{\mathbf{P}}'_N(t)\}$ such that the inter-node distances $\hat{d}_{ij}(t) = \|\hat{\mathbf{P}}_i(t) - \hat{\mathbf{P}}_j(t)\|$ are approximately the same as the true inter-node distances $d_{ij}(t)$.

Multidimensional scaling (MDS) has been used to estimate such relative location maps in static WSNs [9]. This approach has high computational complexity, as it uses singular value decomposition (SVD) whose complexity is $O(N^3)$ where N is the number of nodes in the network. The solution to the MDS problem also requires the knowledge of inter-node distances between all the nodes and thus requires centralized processing. We adapt the computationally efficient gradient descent approach proposed in [1] to find a relative location map of the entire network in an iterative manner. To apply this algorithm, each node needs to know the current estimates of the position of other nodes, and its own distance from other nodes, eliminating any need for centralized processing.

Attack Model: We consider attacks where each malicious node independently falsifies the time-stamp of their signal to provide erroneous information to other nodes. We model this scenario by adding a random value u_{ik} uniformly distributed in $(0, d_{max}]$ to the distance estimate provided to the i^{th} localizing node by the kth node, if node k is malicious. A similar attack model was used in [5] to model non-coordinated attacks in MSNs. The distance estimate obtained by node i from node k at time instant t can then be written as,

$$d_{ik}^{(nc)}(t) = \begin{cases} d_{ik}(t) + u_{ik} + n_{ik}(t) & \text{if node } k \text{ is malicious,} \\ d_{ik}(t) + n_{ik}(t) & \text{otherwise,} \end{cases}$$

where $d_{ik}(t)$ is the actual distance between node i and node k, and $n_{ik}(t)$ is the Gaussian measurement noise with mean 0 and variance σ^2.

3. GRADIENT DESCENT BASED APPROACH

Before describing the gradient descent based approach to secure localization in MSNs, we present a brief overview of our previous work on secure localization in static WSNs using the similar gradient descent based method [1]. The main idea behind the algorithm is to minimize a suitable cost function involving the position of the localizing node and the available measurements using an iterative gradient descent approach. The cost function is dynamically updated to remove inconsistent measurements arising from malicious nodes. The algorithm operates in two stages. In the first stage, the cost function involves data from all the anchor nodes. In the second stage, selective pruning of inconsistent measurements is performed to mitigate the effect of malicious nodes on the solution.

3.1. Gradient Descent Approach for MSNs

We extend the gradient descent algorithm proposed in [1] to be applicable for the case of MSNs, when no anchor node is present in the network. Each node i randomly initializes its estimate for the current position $\hat{\mathbf{P}}_i(0)$. At each subsequent time instant t, the i^{th} node obtains measurements $\{\hat{\mathbf{P}}_k(t-1), d_{ik}^{(nc)}(t)\}$ for $(k = 1, 2, \ldots, N; k \neq i)$ from the remaining nodes and formulates a Least Squares (LS) problem to estimate the current position of node i, $\hat{\mathbf{P}}_i(t)$, that minimizes the

following cost function:

$$f_i^{(t)}(\mathbf{P}(t)) = \sum_{k=1,\, k\neq i}^{N} \left(\|\mathbf{P}(t) - \hat{\mathbf{P}}_k(t-1)\| - d_{ik}^{(nc)}(t) \right)^2 \tag{1}$$

The negative of the derivative of each term inside the summation in Eq. (1) evaluated at current position $\hat{\mathbf{P}}_i(t-1)$ will give the gradient of each term for node i resulting due to other nodes in the network. Node i evaluates the gradient of the cost function in Eq. (1) at the estimate of its current position $\hat{\mathbf{P}}_i(t-1)$ and then updates the estimate by adding one step, $\delta(t)$, in the direction of the negative of the gradient:

$$\mathbf{g}_i'(t) = -\nabla_{\mathbf{P}} \left(f_i^{(t)}(\mathbf{P}) \right) \Big|_{\mathbf{P}=\hat{\mathbf{P}}_i(t-1)} \tag{2}$$

$$\hat{\mathbf{P}}_i(t) = \hat{\mathbf{P}}_i(t-1) + \delta(t) \times \frac{\mathbf{g}_i'(t)}{\|\mathbf{g}_i'(t)\|} \tag{3}$$

This process is repeated until the gradient becomes small enough. At this point, the algorithm converges to the LS solution of Eq. (1). The algorithm then switches to the second stage and prunes out a fraction of the terms with large magnitude of gradient in the cost function of Eq. 1. Most of these large magnitude gradient terms come from the inconsistent measurements given by the malicious nodes. As will be shown in the next section, estimates of the relative location map preserve the pairwise distances and can accurately track mobile nodes.

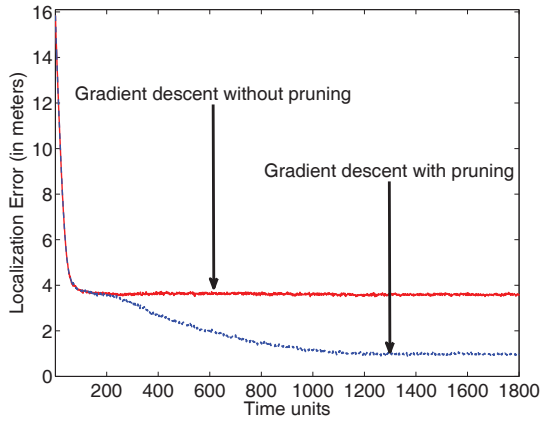
4. SIMULATION RESULTS

In this section, we demonstrate experimentally the accuracy of the proposed method for localization in MSNs under the attack model described in Sec. 2. 30 sensor nodes are randomly deployed in a 60m $\times$ 60m area. The velocity of the nodes at each instant is a random variable with x and y components, V_x and V_y, uniformly distributed on $[0, V_{max}]$. This mobility model is similar to the random way-point model used commonly for modeling mobile and ad-hoc networks [3, 10]. The measurement noise, $n_{ik}(t)$, is assumed to be additive Gaussian with mean 0 and $\sigma = 2$m. The maximum error introduced by a malicious node into the distance measurements $d_{max} = 30$m. In the selection stage of the gradient descent algorithm, we prune 50% of the force vectors.

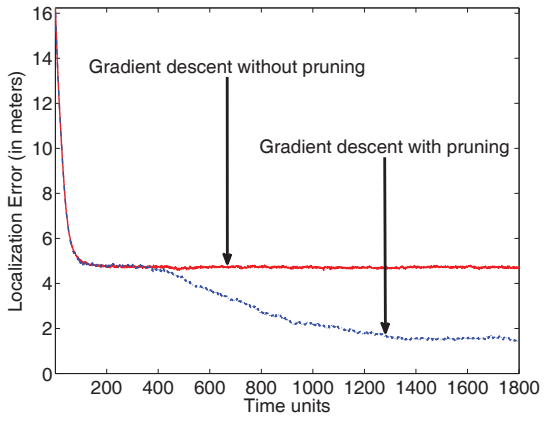
The estimation accuracy of the estimated relative location map is measured by comparing the actual inter-node distances $d_{ij}(t)$ with estimated inter-node distances $\hat{d}_{ij}(t)$, where $\hat{d}_{ij}(t) = \|\hat{\mathbf{P}}_i(t) - \hat{\mathbf{P}}_j(t)\|$. The localization error $E(t)$ is defined as the sum of the absolute difference between $d_{ij}(t)$ and corresponding $\hat{d}_{ij}$ at each time-instant for all i and j:

$$E(t) = \frac{1}{N^2} \sum_{i=1}^{N} \sum_{j=1}^{N} |d_{ij}(t) - \hat{d}_{ij}(t)| \tag{4}$$

A lower value of $E(t)$ implies that the algorithm can accurately estimate the inter-node distances and provides a relative location map that satisfies the inter-node distance constraints. The estimated relative location map can then be used to find the absolute locations of all the nodes in the network if true locations of three nodes are known.



(a) 33% of the nodes are malicious



(b) 50% of the nodes are malicious

Fig. 1. Localization error, $E(t)$, as a function of time for estimating the relative locations in MSNs.

We first evaluate the accuracy of the gradient descent algorithm for a fixed maximum velocity of the nodes $V_{max} =$ 1m/unit time. A constant step size of $\delta(t) = \frac{1}{\sqrt{2}}$ is used, which is approximately the average distance a node can move in unit time. In general, the step size can be chosen as $\frac{V_{max}}{\sqrt{2}}$. The plot of error $E(t)$ as a function of time when 33% and 50% of the nodes are malicious is shown in Fig. 1. The dashed line represents the error using the proposed gradient descent approach while the solid line represents the error when the second stage of the algorithm is not used and will be similar to the LS solution. The value of $E(t)$ is high at the initialization of the algorithm as each node initializes its position estimate randomly. The localization error decreases during subsequent time-instants as the algorithm updates the estimate of

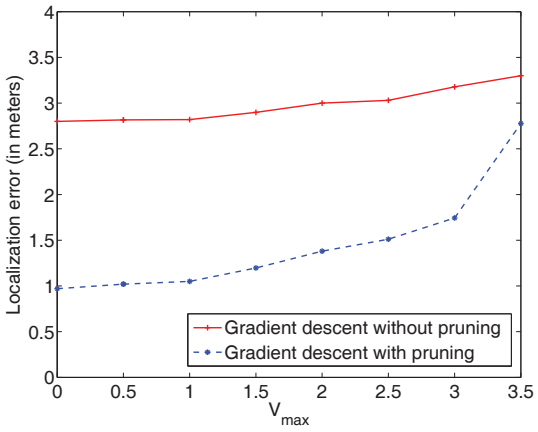


Fig. 2. Effect of velocity on the error in estimating the map of relative locations.

the position at each time-instant. Applying the second stage of the algorithm to prune out the observations due to malicious nodes further reduces the average error to less than 1m.

We also examine the effect of the node velocity on the localization accuracy. We fix the value of d_{max} to $20m$ and determine the localization error after convergence for different maximum velocities V_{max}. Fig. 2 compares the localization accuracy of the gradient descent algorithm with and without pruning as a function of the velocity. The step size of the gradient descent algorithm is chosen to be $\frac{V_{max}}{\sqrt{2}}$ as described previously. The point corresponding to $V_{max} = 0$ denotes the special case of determining relative location map in the static network in the absence of any anchor node. A small finite step size is used to update the estimates at each iteration for the case of $V_{max} = 0$. From this figure, we also observe that as long as the velocity is small, the error in estimating the map of relative locations is small. As the node velocity increases, the localization error also increases. The increment in localization error is more in the gradient descent approach with pruning as opposed to without pruning. At high velocities, each node can move quite far from its previous position and the gradient descent approach may not be able to track the node position accurately. Applying multiple iterations in each time unit can alleviate this problem at the expense of higher computational complexity.

5. CONCLUSION

In this paper, we extended our earlier work to propose a computationally efficient algorithm based on an iterative gradient descent approach to securely estimate a relative location map of the nodes in mobile sensor networks in the presence of malicious adversaries. The proposed algorithm combined iterative gradient descent with selective pruning of inconsistent measurements to achieve a high localization accuracy. The proposed algorithm was shown to be attack resilient to malicious adversaries injecting false information under the described attack model. The average localization error in the relative location map was less than 1.5m for a deployment region of size 60m $\times$ 60m when up to 50% of the nodes are malicious, and nodes are moving with a maximum velocity of 3 meters per second.

6. REFERENCES

[1] R. Garg, A. Varna, and M. Wu, "Gradient descent approach for secure localization in resource constrained wireless sensor networks," in *IEEE Intl. Conf. on Acoustics Speech and Signal Processing (ICASSP)*, Mar. 2010, pp. 1854 –1857.

[2] Y. Mao and M. Wu, "Coordinated sensor deployment for improving secure communications and sensing coverage," in *ACM Workshop on Security of Ad-hoc and Sensor Networks*, 2005, pp. 117–128.

[3] L. Hu and D. Evans, "Localization for mobile sensor networks," in *Proceedings of the 10th ACM Annual Intl. Conf. on Mobile Computing and Networking (MobiCom)*, 2004, pp. 45–57.

[4] A. Baggio and K. Langendoen, "Monte-carlo localization for mobile wireless sensor networks," in *Conf. on Mobile Ad-hoc and Sensor Networks (MSN)*, 2006.

[5] Y. Zeng, J. Cao, J. Hong, S. Zhang, and L. Xie, "SecMCL: A secure monte carlo localization algorithm for mobile sensor networks," in *IEEE 6th Intl. Conf. on Mobile Adhoc and Sensor Systems (MASS)*, Oct. 2009.

[6] D. Liu, P. Ning, A. Liu, C. Wang, and K. Du, "Attack-resistant location estimation in wireless sensor networks," *ACM Transactions on Information and System Security*, vol. 11, no. 4, pp. 1–39, 2008.

[7] N. Michael, M.M. Zavlanos, V. Kumar, and G.J. Pappas, "Distributed multi-robot task assignment and formation control," in *IEEE Intl. Conf. on Robotics and Automation*, May 2008, pp. 128 –133.

[8] M. Mauve, A. Widmer, and H. Hartenstein, "A survey on position-based routing in mobile ad hoc networks," *IEEE Network*, vol. 15, no. 6, pp. 30 –39, Nov. 2001.

[9] S. Yi, R. Wheeler, Y. Zhang, and M. Fromherz, "Localization from mere connectivity," *Proceedings of ACM Intl. Symp. on Mobile Ad-hoc Networking & Computing*, pp. 201–212, 2003.

[10] T. Camp, J. Boleng, and V. Davies, "A survey of mobility models for ad hoc network research," *Wireless Communications & Mobile Computing (WCMC): Special Issue On Mobile Ad Hoc Networking: Research, Trends And Applications*, vol. 2, pp. 483–502, 2002.