Energy-Efficient Localized Routing in Wireless Sensor Networks

S. Usha[#1], Dr. A. Tamilarasi[#2], K. Anbuthiruvarangan[*3]

[#1]*Assistant Professor, Dept. of CSE, University College of Engg., Panruti Campus, Tamilnadu, India*

[#2]*Professor & HOD, Kongu Engineering College, Perundurai,Tamilnadu, India*

[*]*PG Scholar, Dept. of CSE, Anna University, Trichy, India.*

***Abstract*— Every sensor node is essential to know their location in the sensor network, even in the presence of malicious adversaries. In that the energy conservation and scalability are critical issues in wireless sensor network. In existing algorithm combines iterative gradient descent with selective pruning of inconsistent measurements to achieve high localization and it can track the mobile nodes with small localization error when nodes are moving slowly. Localization is determining the geographical location of each node in the system.**

In Proposed algorithm called Localized Energy awareness Restricted Neighborhood , which can guarantee the energy efficiency of its localized routing in mobile sensor networks, where all nodes are moving, to estimate the relative locations of the nodes without relying on anchor nodes. Then theoretically study its critical transmission radius in distributed networks which can calculate short distance of sensor node with hop count and route for any source sensor node and destination sensor node pairs asymptotically almost surely. In propose a framework for relocating mobile sensors in a timely, efficient, and balanced manner, and at the same time, maintaining the original sensing topology as much as possible. Localized routing protocols, with the assumption of known position information, the routing decision is made at each node by using only local neighborhood information. Our main goal is to predict the energy efficient sensor node and estimated short distance consumption in Wireless Sensor Networks by carefully selecting the localization routing with secure and efficient transmission.

***Keywords*— Cloud, encrypted data, outsourced data, encrypted search**

I. 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].

Additionally, sensors should be optimally deployed to provide maximum coverage in a given area at a low communication cost. This can be achieved with the help of mobile nodes [8]. The algorithms used for such mobility assisted efficient deployment require sensors to be location aware. In robotics applications such as distributed formation and coordination, where mobile robots with limited communication range coordinate to achieve a common task, the location information of the robots is needed to ensure connectivity in the network [9]. Thus, we see that location information is important in both static and mobile sensor networks.

Node locations can be obtained by using GPS devices on the nodes. However, equipping each sensor with a GPS may not be feasible for large scale networks with small low-cost sensors. As a result, an important first step in setting up a sensor network is to accurately determine the position of each individual node through a process called *localization*. Most localization schemes rely on a set of beacon or anchor nodes with known location information to identify the positions of the remaining nodes. In these schemes, anchor nodes transmit a beacon signal which contains their own location, using which other nodes can estimate their distances from the anchors.

II. LITERATURE SURVEY

A related problem of location verification has been explored in the literature, where the focus is on developing strategies to verify that a node is indeed located at the claimed position. Methods such as verifiable multilateration, location verification using mobile base stations, and several other distance bounding protocols have been proposed to withstand attacks in secure location verification problems [4]–[5]. The problem of secure localization in WSNs in the presence of malicious adversaries has also attracted attention in the research community. A greedy approach to find the location consistent with the largest number of measurements from anchor nodes was explored in [6]. A voting-based scheme was also proposed, in which the localization area is divided into a grid and the vote count of each grid point is incremented if its

distance from an anchor node is approximately equal to the distance measurement obtained from that anchor. A similar voting approach with the help of sectored antennas and beacon nodes was proposed in [7]. From a signal processing point of view, the voting based scheme is similar in spirit to the Hough transform used for detecting objects with certain shapes in computer vision and image processing literature [10]. In the Hough transform, a voting procedure is carried out in a parameter space, from which candidate parameters for objects are determined as local maxima of accumulated votes. Similarly, in the votingbased scheme for secure localization, the location with the maximum votes is identified as the position of the node.

Aleastmedian square (LMdS) approach was proposed in [2] to solve the localization problem for scenarios where less than 50% of the nodes are malicious. This method shares similarities with the random sample consensus (RANSAC) algorithm [1], as it uses several subsets of nodes to identify candidate locations, and then chooses the solution that minimizes the median of the residues. Most of these existing methods localize the nodes with small error as long as the fraction of malicious nodes is not too large. However, the memory requirement and computational cost of running these algorithms is still high and can be difficult to meet in resource limited applications. In contrast to static sensor networks, very little work has been done on secure localization in mobile sensor networks.

A two stage Monte Carlo based approach for localization was proposed in [2]. In the first stage, using the current estimate of the location, a fixed number of candidate sample locations that satisfy a constraint on the maximum velocity of the nodes are randomly generated. In the second stage of filtering, samples that are inconsistent with the measurements obtained from anchor nodes are filtered out, and a final estimate of location is found by averaging the remaining samples. The localization accuracy of the algorithm in [4] was improved in [9] using a box shaped region to sample particles in the prediction phase and eliminate inconsistent particles in the filtering stage. These algorithms did not consider the presence of malicious anchor nodes in the network.

The Monte Carlo algorithm was extended to incorporate security by modifying the filtering stage in [24]. Instead of identifying points that are consistent with all measurements, the position consistent with the maximum number of measurements from anchors is determined. This approach is similar to the voting-based approach [5] for secure localization in static sensor networks explained previously and suffers from the same drawback of high computational and storage requirements. Algorithms proposed in [6] use the hop count information and communication range information of sensor nodes to find a feasible region for the node position and use this information to estimate the location. These prior works assume the presence of some anchor nodes that are used to determine the position of the mobile nodes, and cannot be applied to mobile networks without anchor nodes. In this paper, we develop an iterative technique for secure localization that is applicable to both static and mobile networks.

In terms of the vector interpretation for iterative updates, the proposed algorithm has similarities to the robust localization algorithm inspired by self organizing maps proposed in [8]. The algorithm in [8] considered noise, but was not designed to withstand attacks by active adversaries, whereas we develop an algorithm for localization that can filter out malicious measurements obtained from nodes compromised by adversaries.

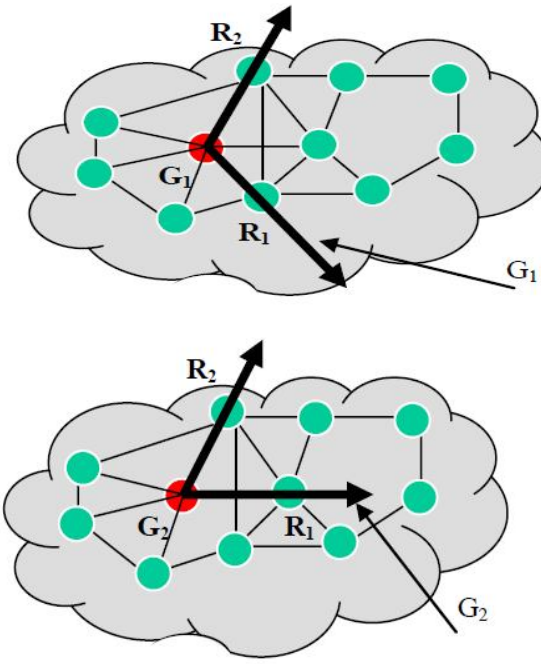
III. Protocol Overview

The proposed location discovery protocol consists of three phases: network-bootstrapping (*NB*), local position discovery (*LPD*), and global localization (*GL*). This paper is mainly dedicated to report on the *LPD* phase, describing detailed mathematical formulation and validating the accuracy of the proposed algorithm. In other words, we focus on the intra-cluster part of our localization scheme. In this section we briefly describe all phases and elaborate on the *LPD* phase in the next subsection.

The Network Bootstrapping (NB) Phase: The main tasks performed in the bootstrapping phase are: node discovery, range estimation, and cluster formation. At the end of this phase, all gateway and sensor nodes within *k*-hops, where *k* is the cluster radius defined in more details in section 3, are made aware of the presence of each other. We follow a technique similar to TinyOS beaconing [3] with a goal to build a breadth first spanning tree rooted at the gateway node such that there is at least one route from each sensor node to a gateway. Each gateway node broadcasts a node discovery message. The message contains three fields: the gateway ID, the sender ID and hop count to the gateway. All nodes receiving the message record the hop count and the sender (the gateway in the first round of broadcast) and rebroadcast the node discovery message after changing the sender's field and incrementing the hop count. If a node receives multiple node discovery messages from the same gateway, it designates as a parent the neighbor that is on the path with the minimum number of hops to this gateway.

Recall that each sensor node is capable of estimating the distance to neighboring nodes that are within its transmission range using Time of Arrival (TOA) technology [1] or Radio Signal Strength (RSS) [2]. In this paper, we assume that the TOA method is used to estimate the distances between nodes. After building the spanning tree, each sesnor node reports its distance estimates to the gateway. All distance reports received or generated by a node are forwarded to its parent until they reach the gateway node. It should be noted that some nodes may receive node discovery messages from more than one gateway, we will refer to those nodes as *boundary nodes*. Boundary nodes are essential for the global localization phase as we will discuss later. A boundary node should store the gateway ID and the ID of the neighbor sensor (parent) on the path with least number of hops to this gateway, for all the

gateways it hears from. Boundary nodes will be affiliated with more than one cluster for the purpose of localization.



IV. Algorithm & Architecture

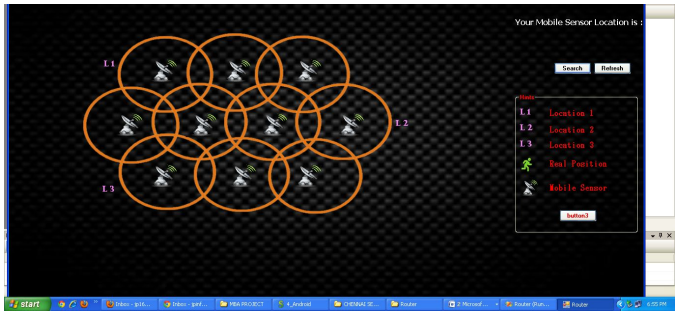
In this paper, we present an efficient anchor-free protocol for localization in wireless sensor networks. Each node discovers its neighbors that are within its transmission range and estimates their ranges. Our algorithm fuses local range measurements in order to form a network wide unified coordinate systems while minimizing the overhead incurred at the deployed sensors. Scalability is achieved through grouping sensors into clusters. Simulation results show that the proposed protocol achieves precise localization of sensors and maintains consistent error margins. In addition, we capture the effect of error accumulation of the node's range estimates and network's size and connectivity on the overall accuracy of the unified coordinate system. Results show that the proposed algorithm utilizes fewer computational resources and achieves an accuracy better than /or comparable to that of existing schemes. The proposed secure localization algorithm can also be used in mobile sensor networks, where all nodes are moving, to estimate the relative locations of the nodes without relying on anchor nodes. There has been a growing interest in the applications of wireless sensor networks in unattended environments. In such applications, sensor nodes are usually deployed randomly in an area of interest. Knowledge of accurate node location is essential in such network setups in order to correlate the gathered data to the origin of the sensed phenomena and assure the relevance of the reported information.

Algorithm as follows:

pick a location randomly;
estimate relative location of nodes
measure critical transmission radius
for every second
calculate the hop counts from source
end for
check probability gradient;
if(greater than threshold value)
revoke hop node;
else
allow subject to perform action;
end if;
end;

V. Discussion

The following screen shows the implementation of our proposed work. We have implemented and tested with a system configuration on Intel Dual Core processor, Windows XP and Using Visual Studio 2008, C#.net. The details of each module for this system are as follows:



VI. Conclusions

We are currently working out and validating the detailed clustering and global localization algorithms. In the future, we aim to analyze the error accumulation and how to limit it. There are two types of error accumulation: intra-cluster error accumulation during the *LPD* phase as *k* increases; and inter-cluster error accumulation during the *GL* phase. In this paper we have focused on the first type of errors. We intend to extend the scope to cover inter-cluster error accumulation. As another extension, we also plan to consider the case of homogeneous network where all nodes are equal (i.e. there are no gateway nodes). In this case, a clustering algorithm is needed in order to select a set of cluster heads, which cover the entire network such that each sensor node belongs to at least one cluster.

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 × 60m when up to 50% of the nodes are malicious, and nodes are moving with a maximum velocity of 3 meters per second.

VII. REFERENCES

[1] A. Baggio and K. Langendoen, "Monte-Carlo localization for mobile wireless sensor networks," in *Proc. Conf. Mobile Ad-Hoc Sens. Netw. (MSN)*, HongKong, 2006.

[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, "Attackresistant 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.