

HiRLoc: High-resolution Robust Localization for Wireless Sensor Networks

Wajahat GH Mohd¹, Shelly Sharma², Avantika Saklani³ and Ashish Singhal⁴

^{1,2,3,4}Department of computer science. M-Tech Students of JB Institute of Technology, Dehradun Uttarakhand.

Abstract: In this paper the tiny nodes are deployed in target areas according to the deployment nature of target but nodes are easily targeted by attacker with physical attack of node capture. So, secure communications in some wireless sensor networks are critical because these networks are highly vulnerable to internal and external attacks. In our paper, we present an enhanced **High-Resolution Robust Localization** for security of wireless sensor networks. This combination of scheme provides the good performances and efficiency in terms of network connectivity. We propose a range-independent localization algorithm called HiRLoc that allows sensors to passively determine their location with high resolution, without increasing the number of reference points, or the complexity of the hardware of each reference point. In HiRLoc, sensors determine their location based on the intersection of the areas covered by the beacons transmitted by multiple reference points. we show that HiRLoc is robust against known attacks on WSN. Finally, our performance evaluation shows that HiRLoc leads to a significant improvement in localization accuracy compared to state-of-the-art range independent localization schemes, while requiring fewer reference points.

Index Terms: Localization, Algorithm, Design, Performance, Security.

I. Introduction:

A wireless sensor network [1], consisting of a large number of small low cost devices called sensor nodes or motes [2]. A sensor node is contained information about the battery transceiver, micro-controller and sensors. These sensor nodes are tiny resource constrain devices with the limitations of low battery power and communication range and small computation and storage capabilities. They are usually deployed in open environments where they collaboratively monitor the physical and environmental data such as temperature, pressure vibration etc., and report/relay the sensed data to other sensor nodes over a wireless network. These sensor networks consist of a large number of low-cost, low-power, and multifunctional sensor nodes that communicate through wireless media. Various WSN applications have been proposed, for example, military target tracking, environment monitoring, medical treatment, emergency rescue and smart home, and so forth. A fundamental requirement in the above applications is the location awareness of the system. Therefore, the acquisition of sensors' location becomes an important issue since sensing results without location information are mostly inapplicable. A common approach in most localization schemes is to use enough special nodes, called *locators* or *beacons*, which can obtain their locations by GPS or from infrastructure. Locations[3] of normal sensor nodes are then estimated by interacting with locators to obtain the distance or angle information. Once the location information of at least three non collinear locators are available, the relative positions of the sensors can be converted into physical positions. Energy efficiency, accuracy and security account for the major metrics in localization systems[4].

Node localization is the problem of determining the geographical location of each node in the system. Localization is one of the most fundamental and difficult problems that must be solved for WSN. Localization[2] is a function of many parameters and requirements potentially making it very complex.

The main contributions of this paper are summarized as follows.

(i) We summarize two secure localization schemes, which make use of these properties to detect and defend against the attacks.

(ii) We conduct theoretical analysis on the probability of identifying all the attacked locators, which is validated by simulations.

(iii) We analyze the effects of network parameters on the performance of our proposed schemes and compare them with other existing methods.

The remainder of this paper is organized as follows. In Section 2, we provide the related work on secure localization. Section 3 presents the proposed work for secure localization. Section 4 presents the performance evaluation and Section 5 concludes the paper and puts forward our future work.

II. Related work

➤ **ROPE(Robust Position Estimation):**

In ROPE[5], sensors initiate the localization process, by demanding localization information to be transmitted when desired. This feature allows for a highly mobile network where both locators and sensors may change positions and sensors may request new information when their position[6] becomes outdated. However, locators have to transmit individual beacons for each sensor s , in order for s to estimate its position. Hence, when the position update occurs frequently, ROPE[5] is not scalable in communication cost with the network size. To reduce the communication cost for localizing the sensors, then can modify ROPE so that locators transmit one beacon per sector for all sensors. Instead of using MACs to verify the authenticity[6] and integrity of the message, every locator associates a one-way hash chain with each of his sectors. The heads of the hash chains of all locators and the associated locators' positions and sectors are stored at each sensor. Every sensor receiving a hash, can verify the authenticity of the source, and associate it with the localization information stored. To guarantee freshness, locators need to be synchronized (via their gps clocks for example) and periodically update the localization information by transmitting the next value of each hash chain. ROPE provides both the location determination and location verification function. In location determination, each unknown node obtains its exact location by VM when it is inside at least one triangle formed by locators, and still estimates its location by center of gravity when it is not inside any triangle. The location verification mechanism[6] verifies the location claims of the unknown nodes. Since every unknown node can communicate with at least one locator, when an unknown node reports data to a locator, the locator can verify the unknown node's position by the execution of the distance bounding protocol. ROPE[5] allows sensors to estimate their own location without the assistance of a central authority, while being resistant to severe types of attacks such as the wormhole attack, node impersonation and jamming of transmissions.

➤ **SeRLoc(Secure Range-Independent Localization):**

The SeRLoc[7] uses trusted locators equipped with a set of higher-power sectored antennas to replace anchor nodes. The locators have longer transmission range than unknown nodes. They send anchor beacons to unknown nodes, in which contains their positions and the sectors of the antenna[8]. When a node hears multiple locators, it computes the center of gravity of the sectors corresponding to locators as its position. The SeRLoc is robust against severe WSN attacks, such as the wormhole attack, the sybil attack and compromised sensor nodes. However, SeRLoc[7] is based on the assumption that no jamming of the wireless medium is feasible. And it does not protect against attacks on locator's information, which are avoided by checking network properties[8] such as sector uniqueness and communication range. Moreover, in order to minimize the region of sector intersection to improve localization, we need to increase the number of locators and sectored antennas. (*SeRLoc*) enables sensors to determine their location based on beacon information transmitted by the locators, and present the security mechanisms that protect the location computation, in the presence of malicious adversaries. SeRLoc[7] is the range independent algorithm to find the location of the sensor nodes. In Secure Range-Independent localization algorithm sensor nodes find out their position based on the beacon information which is transmitted by the locators. SeRLoc is a distributed algorithm which is based on two-tier network architecture[8]; it allows sensor nodes to inactively find out their position without cooperating with other sensor nodes in the network. Each locator transmits different beacons at each antenna sectors, which is received by the sensor nodes within their range R . Each beacon contains the respective beacon coordinates and the sector boundary lines. Each Sensor calculates its position as the Center of Gravity (CoG)[7] of the overlapping area of the different sectors

Compared with ROPE, ROPE[5] is resistant to jamming of the communication medium, limits the maximum spoofing impact and prevents location spoofing due to the Sybil attack, with relatively low density deployment of locators. However, ROPE has higher hardware requirements, e.g., nanosecond time synchronization and instantaneous processing capacity, which is not suitable for low cost WSN.

III. PROPOSED WORK:

➤ **HiRLoc(High-Resolution Robust Localization):**

In this section we will discuss the HiRLoc scheme that allows sensors to determine their location with high accuracy even in the presence of security threats. However, we are not interested in the security threats discussed by HiRLoc. Our interest here is the localization techniques[4] proposed in HiRLoc. The algorithm considers that there are two types of nodes: locator/anchor nodes which transmit beacons with location information and normal nodes (unknown location nodes). The algorithm considers that normal nodes determine its own location by received beacon signal from locator. The beacon signal transmitted by locator node contains locator coordinates, angle of directional antenna, and locator communication range.

Locator nodes updated this information every time and retransmit it to normal nodes. Based on SeRLoc[7], in order to minimize the region of sector intersection without increasing the number of locators and sectored

antennas, the same authors propose an improved method called high-resolution range independent localization (HiRLoc), which achieves greater localization accuracy through rotatable antennas and variable transmission power, while increases computational and communication complexity[9]. It permits sensors to find out their location with high precision even if there are some security threats. HiRLoc attains passive sensor localization based on beacon information transmitted from the locators. Locator’s communication range is variable and each locator sends beacon information more than once (multiple rounds). This approach is more accurate and robust as in each round the locator may change its direction or its range or may be both. This algorithm works as; the sensor first decides the locators in which they are interested and determines the initial calculation for its location. The sensors then collect the beacon information in the multiple rounds. The locators may change its direction and range in the multiple rounds.

IV. Performance Evaluation and Simulation

After the implementation of the two algorithms HiRLoc and SeRLoc the comparison of between these algorithms is introduced in this section. The main criterion for the comparison is the localization error of each algorithm in compared to others with different network settings. The Simulator used in this experiment is Wireless Sensor Network Localization Simulator v1[9].

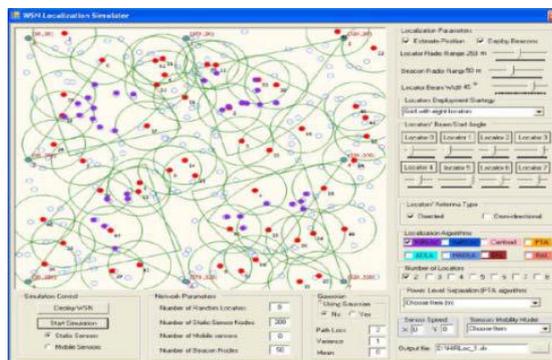


Figure 1: Simulator Snapshot

Simulation Results: The implementation is done using HiRLoc and SeRLoc; first we have implemented HiRLoc using Directional and Omni directional antennas and then SeRLoc using both antennas. The result in directional antenna is changed from that in Omni directional. we compare between all algorithms in terms of possibility of location detection and algorithm execution time. In this set of experiments[9], a large number of simulation cases are merged including different problem settings. Although HiRLoc has a very good percentage of location the nodes but its execution time is the worst. Figure 2 shows the average results of the comparison.

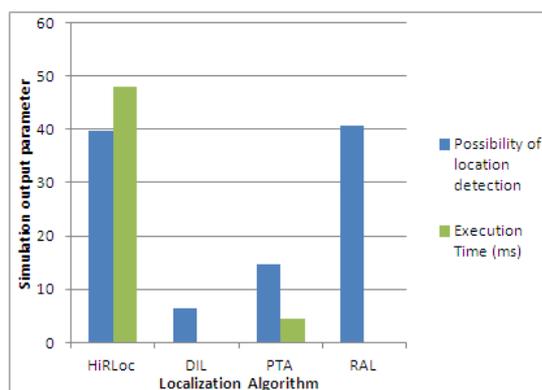
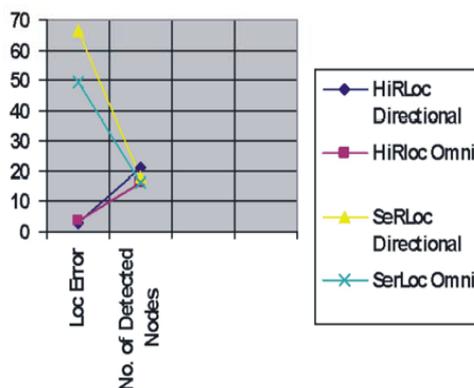


Figure 2: Comparative Chart between Simulation Output Parameter

The experimental results[9] show that among the two algorithms, High Resolution Robust Localization is the more accurate one. HiRLoc directional method is the most accurate having less localization error as shown in Figure 3



V. Conclusion And Future Work:

In this paper, we implemented two of the main localization algorithms[9] and compared among them with different problem settings. Our comparison will be helpful for WSNs designers in selecting the best localization algorithm to use. In our future work, we will study the effect of different mobility models on these algorithms.

References:

- [1] I.F. Akyildiz, and E. Cayirci, “Wireless sensor networks: A survey,” *Computer Networks*, vol. 38, no. 4, pp. 393-422, 2009.
- [2] J. Bachrach, C. Taylor. “Localization in sensor networks Handbook of Sensor Networks: Algorithms and Architectures”, Hoboken: John Wiley & Sons, 2009, pp. 277 – 310.
- [3] G. Mao, B. Fidan, B. D. Anderson. “Wireless sensor network localization techniques. *Computer Networks*”, 2010, 51(10), pp. 2529– 2553.
- [4] Adel Youssef and Moustafa Youssef. Taxonomy of Localization Schemes for Wireless Sensor Networks. In ICWN, pages 444{450, 2009.
- [5] “ROPE: robust position estimation in wireless sensor networks,” in Proceedings of the 4th International Symposium on Information Processing in Sensor Networks, April 2011, pp. 324–331.
- [6] L. Lazos and R. Poovendran, Robust Range-independent Localization for Wireless Sensor Networks, to appear In *Transactions on Sensor Networks*, available upon request.
- [7] L. Lazos and R. Poovendran, “SeRLoc: Secure range independent localization for wireless sensor networks,” in Proceedings of the 3rd ACM Workshop on Wireless Security, 2011,
- [8] L. Lazos and R. Poovendran, SeRLoc: Secure Range-Independent Localization for Wireless Sensor Networks, to appear in *Proceedings of WISE*, Philadelphia, PA, Oct. 2004, pp. 21–30.
- [9]. Naguib, A.M., XXXX. WSN-Localization-Simulator version 1.1. [http:// www.scribd.com/ doc/ 73469918/ WSN-Localization-Simulator](http://www.scribd.com/doc/73469918/WSN-Localization-Simulator).



Wajahat Gh Mohd is currently pursuing Master degree from Department of Computer science at Uttarakhand Technical University,Dhradun.He received his B-Tech. degree in Computer Science from Islamic University of Science and Technology Avantipora, Kashmir, in 2011. His current research interests are security and localization for Wireless Sensor Networks.