Cluster Based Secure Location Verification System for Wireless Sensor Networks

[1] S. Velmurugan, [2] A. Senthilkumar,
Research scholar, St. Peter's University, Chennai
[3] Dr.E.Logashanmugham, Professor & Head / ECE, Sathyabama University, Chennai.

Abstract:

The location verification technique is dense in wireless sensor networks. The nodes called as verifier which is used to verify the location of sensor nodes. In this paper they have assumed that verifiers are secure, also the sensor nodes know their location, and communication range is constant and also signal strength. The sensors initially send their location and its id to all the nodes using flooding and when the verifiers gets the message there takes place collaboration between the verifiers to determine whether the location sent by the sensor node is valid or not based on the results it will decided whether the sensor is valid or malicious. If more number of verifier nodes is used then higher is the probability to detect the malicious node.

1. Introduction

1.1. Wireless Sensor Networks

A WSN can be defined as a network of devices, denoted as nodes or computers, which can sense the environment and communicate the information gathered from the monitored field (e.g., an area or volume) through wireless links. The data is forwarded, possibly via multiple hops (multiple path), to a sink (sometimes denoted as controller or monitor) that can use it locally or is connected to other networks (e.g., the Internet) through a gateway. The nodes can be stationary or moving.

They can be aware of their location or not. They can be homogeneous or not. [1]

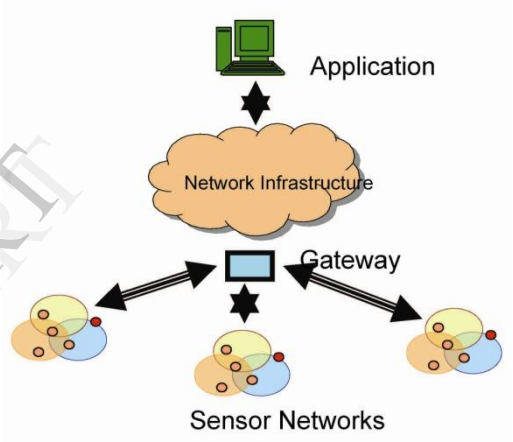

Fig. 1.1. Wireless Sensor Networks

1.2. Security issues of wireless sensor networks

In many applications security issues would be as important as energy consumption in wireless sensor networks. Since the sensors in WSN would be having small and less battery, less cost and less memory so it is very difficult to implement security protocols like public key cryptography in the resource strained sensors but we can implement it in base stations which are very powerful than sensors.[2]

Some of the issues are of security are [2]

- **Data Confidentiality:** The information exchanged between source and the destination should be kept secret not leaked to the adversary.
- **Data Authenticity:** The data should be obey authentic that is for some important decisions taken the destination should know exactly that the data originated from the validated source.
- **Data Integrity:** The data sent by the source should be exactly same as received by the destination since it should not be modified by the intruder.
- **Data Freshness:** Data communicated should be new not an old one which will be added by intruder or adversary.
- **Robustness and Survivability:** The sensor network should be robust against attacks like if there is a security attack the attack's effect should be minimized to maximum extent.

1.3. Time Synchronization

Most sensor network applications rely on some form of time synchronization. In order to conserve power, an individual sensor's radio may be turned off for periods of time. Furthermore, sensors may wish to compute the end-to-end delay of a packet as it travels between two pair-wise sensors. A more collaborative sensor network may require group synchronization for tracking applications, etc.

1.4. Authentication

When constructing the sensor network, authentication is necessary for many administrative tasks (e.g. network reprogramming or controlling sensor node duty cycle). An adversary is not just limited to modifying the data packet. It can change the whole packet stream by injecting additional packets. So the receiver needs to ensure that the data used in any decision-making process originates from the correct source. From the above, we can see that message authentication is important for many applications in sensor networks. Informally, data authentication allows a receiver to verify that the data really is sent by the claimed sender. In the case of two-party communication, data authentication can be achieved through a purely symmetric mechanism: the sender and the receiver share a secret key to compute the message authentication code (MAC) of all communicated data.

1.5. Localization

Schemes for localization in WSN have been developed in the last 20 years, mostly being motivated by military use. Localization is the process of identification of sensors by the satellites or base station to route information. Suppose if we deploy sensors in deep forest for military applications for identification for an opponent country then sensors will scattered. If the base station needs to enquire the sensors about any detections it needs to know the location where it resides if the base station does not localize then even on detection of any event the base station will be unaware hence the problem crops

up. Hence we need localization techniques.

1.6. Need for security in localization

Localization involves locating the nodes for communication but the main problem associated with it is that security. If the base station determines a route to the sensor in that instant if the adversary interprets and gives another path then the information will not authentic and accurate. The adversary will give the path to its sensors then the information will not be confidential [3]. If the adversary knows the position of sensors by the results of the localization process carried at the base station then the adversary may attack all the sensors which may destabilize the network [4].

2. Literature survey

2.1. J. G. Alfaro et. al [6]

They proposed has Secure Localization of Nodes in Wireless Sensor Networks with Limited Number of Truth Tellers. According to this paper there are three algorithm been proposed for localization of nodes in a wireless sensor networks in the presence of neighboring nodes. This algorithm minimizes the number of trusted nodes to complete the process of localization. This algorithm will work efficiently if the number of liars is below a certain threshold value which will be determined. The three algorithms allow the regular nodes to identify and isolate nodes that are providing false information about their position. Moreover, their algorithms minimize the necessary number of trusted nodes required by regular sensors to complete their process of localization. They also guarantee a small exchange of data between nodes, minimizing in this manner the impact that the localization process has in terms of energy and battery life of sensors.

2.1.1. Merits and Demerits of J. G. Alfaro et. Al

They presented a set of algorithms to handle the localization process of WSN nodes in the presence of liars. The algorithms guarantee the exclusion of incorrect locations, as well as the detection and isolation of the nodes that are lying, if a given threshold of neighbors and liars is met. Otherwise, the algorithms abort the process of deriving the location, and wait to repeat the process again when such parameters can be guaranteed. The two first algorithms allow the localization process without the necessity of a trusted model between sensors. The third algorithm improves the results, but relaxing such an hypothesis, and requesting regular sensors to trust one of the nodes in their one hop neighborhood.

2.2. John A. Stankovic et. al [7]

They Proposed has an algorithm for secure walking GPS and also provide integrated localization and key distribution protocol. The major contribution of this work are (1) an extension to Walking GPS, making it secure against the three A fore

mentioned attacks; (2) an integrated localization and key distribution protocol that keeps key sets on deployed nodes very small; thereby meeting memory constraints, and ensures network communication connectivity and protection against wormhole attacks; (3) a security analysis demonstrating the correctness of our solution; and (4) a performance evaluation using parameters from a real WSN deployment, which demonstrates: a high localization accuracy, that almost all nodes are localized, the excellent scaling properties to networks of at least size 1000, the excellent performance even in the presence of realistic irregular communication ranges, and low overhead.

2.2.1. Merits and Demerits of John A. Stankovic et. al [7]

The main advantage of this algorithm is that it helps in defending the major three types of attacks (worm hole, Dolev-Yao attack, GPS denial attack) of localization and becomes complete threat and resistant to these attacks. And also in this paper they presented the design and evaluation of secure walking GPS an integral solution of secure localization and low key distribution protocol for memory constraints. This deployment of secure GPS is practically low cost and requires minimal manual interaction.

The demerit of this algorithm is that there is lot of over head is involved in the process of secure data communication between its neighbors. There is a combinatorial effort required for bootstrapping with the neighbors.

2.3. Avinash L. Varna [8],

They proposed an algorithm which is a computationally efficient algorithm to determine the location of sensors that can resist such attacks is described. The proposed algorithm combines gradient descent with a selective pruning of inconsistent measurements to achieve good localization accuracy. In this paper, we propose a new method based on gradient descent approach to solve the problem of secure localization. This method works in two stages. In stage 1, gradient is calculated using data from all the anchor nodes. In stage 2, selective pruning of inconsistent measurements is done to mitigate the effect of malicious nodes on gradient calculations. The proposed method can achieve localization accuracy comparable to existing algorithms in a computationally efficient manner. The main advantage of this gradient based approach is that it provides high secure localization process even in the presence of adverse adversary conditions.

2.4. Honglong Chen et al [9]

They proposed an algorithm for one type of attack called as worm hole attack. He designed an algorithm called as secure localization scheme against worm hole attack. The main idea of this paper is to use the properties of the network to detect and remove the worm hole and set up resistant scheme for identifying dubious nodes for secure localization.

They proposed a novel secure localization scheme which is divided into three phases: wormhole attack detection, neighboring locator's differentiation and secure localization

2.4.1. Merits and Demerits of Honglong Chen et al [9]

The main merit of this algorithm is that it works well under general system model like military applications where the nodes will be scattered, no direct path will be present which will make the situation worse that it is highly difficult to detect the worm hole but this algorithm works for wireless ad hoc and also other hostile environments.

The main demerit of this algorithm is that it is very difficult to tackle if multiple worm hole attacks the network it will be complicated and difficult to obtain secure localization.

2.5. Wen Tao Zhu et al [10]

They proposed an innovative solution for secure node localization using two light weighted modules which can also be integrated. First, they harness simple geometric triangular rules and an efficient voting technique to enable the attack detection module, which identifies and filters out malicious location references. They then developed a secure localization module that computes and clusters certain reference points, and the position of the concerned regular node is estimated with the centroid of the most valuable reference points identified. The integrated solution also makes the network highly resistant to malicious attacks.

In this paper, they addressed the problem of secure sensor localization, in the presence of both benign and compromised beacons, with a novel modular solution. The proposal features two lightweight modules, which are for dedicated functionalities respectively but can also be closely integrated. Accordingly, their technical contributions are twofold. First, based on the geometric triangle inequality, they developed a lightweight attack detection module employing certain voting mechanism. Due to its simplicity in attack detection and mitigation, it is a kind of defense preferable for low-cost sensors. Second, they developed a standalone secure localization module that can intrinsically tolerate some malfunctioning beacons. By voting and clustering certain reference points, it can provide practical and efficient location discovery.

Extensive simulations show that when employed in tandem with the attack detection module, the secure localization module can provide a dependable and robust position estimation service even in highly challenging conditions. Due to the modular design, the developed solution is flexible and extensible in nature, which facilitates future improvement. Moreover, our proposal does not depend on special device assumptions (like extra wireless hardware or precise time synchronization) that are inapplicable to

the current generation of WSN, nor is it based on sensor nodes with special knowledge.

2.6. Mattia Monga et al [11]

They proposed an algorithm for secure node localization based on two player strategy or game theory. In this paper they look at the problem of assessing security of node localization. In particular, they analyze the scenario in which Verifiable Multilateration is used to localize nodes and malicious nodes try to masquerade as non-malicious. They resort to non-cooperative game theory and we model this scenario as a two-player game. They analyze the optimal players' strategy and they show that the Verifiable Multilateration is indeed a proper mechanism able to reduce the profitability of fake positions. Their analysis demonstrates that, when the verifiers play a pure strategy, the malicious node can always masquerade as unknown with a probability of one and the induced deception could be not negligible. Instead, when the verifiers play mixed strategies, the malicious node can masquerade as unknown with a very low probability and the expected deception is virtually negligible.

The assessment of the trustworthiness of wireless sensor node localization information is a fundamental challenge in order to provide further trust to applications and data. Verifiable Multilateration is a secure localization algorithm that defines two tests for evaluating node behavior as malicious, robust or as a ultimate choice as unknown. In case of unknown nodes, VM does not have enough information for evaluating the trustworthiness of the node. This lack of information may be exploited by a malicious user. In this paper they modeled VM has as a strategic non-cooperative game, on order to study the overall equilibrium properties of the system. They considered a verifier player against a malicious node and they analyzed the behavior in case of the adoption of both pure strategies and mixed ones. The conducted analysis demonstrates that, when the verifiers play a pure strategy, the malicious node can always masquerade as unknown with a probability of one and the induced deception could be not negligible. Instead, when the verifiers play mixed strategies, the malicious node can masquerade as unknown with a very low probability and the expected deception is virtually negligible.

3. The advantages of our newly proposed solution are as follows

- Since we are using clustering, the overhead of flooding location verification message to entire network is reduced. Also the number of anchors is restricted to the number of clusters.
- Since the anchors are authenticated by the sink, they are trusted.
- Use of GPS receivers is avoided by using range based techniques for localization like RSSI, AOA etc.

- Use of MAC in the location information increases the integrity.
- The verification exchange between the anchors is reliable since they use energy efficient shortest paths.

4. Problem Identification:

1. One of the main problems is flooding since only the verifiers need the sensor location but sending sensor location to randomly to all the unwanted nodes will create some unwanted traffic in the network.
2. They have assumed verifiers are secure which will be impractical assumption in real world scenario because if any malicious node compromises the verifier then all the adversary nodes will get access into WSN and get the whole network into its control.
3. The network is assumed reliable but the wireless networks are more prone to dropping packets which will make it unreliable.
4. The location and the number of verifiers are not mentioned exactly.

5. Conclusion

In this proposal we use anchors for localization and location verification. Initially we form clusters in the network. In each of the cluster, we choose an anchor node (with GPS facility) and rest all as regular sensor nodes. These anchors will be monitored with the help of sink or base station. Reliable paths will be established between each anchors based on their residual energy. There is a pair wise shared key between the sink and each anchor node so that the anchor nodes can be securely authenticated by the sink. For the interaction between sensor and anchor we use public/private key pairs for encryption and decryption. For location verification, the sensor will send its id, location and timestamp.

This information is protected with Message Authentication Code (MAC) using SHA-1 or MD5. Using the private key, it will encrypt the MAC and the encrypted information is sent to the anchor, in hop-by-hop manner. If any intermediate node receives this encrypted information, it will add its own MAC value and re-encrypt with its private key.

Finally, when the anchor receives the encrypted information from all the sensor nodes, it will decrypt and verify the MAC of all the nodes, ensuring integrity. Then it verified the location information sent by the sensor node by checking the actual hop distance and Euclidean distances.

The verification results are now exchanged between each anchor nodes through the reliable paths and collaborative verification is performed to classify the sensor as Trusted or UN trusted. If it is trusted sensor, the location information will be sent to the base station, securely using the shared key.

6. References

[1] CHIARA BURATTI, ANDREA CONTI, DAVIDE DARDARI AND ROBERTO VERDONE, "AN OVERVIEW ONWIRELESS SENSOR NETWORKS TECHNOLOGY AND EVOLUTION", 2009

[2] MAYANK SARAOGI, "SECURITY IN WIRELESS SENSOR NETWORKS", UNIVERSITY OF TENNESSEE, KNOXVILLE

[3] ZORAN S. BOJKOVIC, BOJAN M. BAKMAZ, AND MIODRAG R. BAKMAZ, "SECURITY ISSUES IN WIRELESS SENSOR NETWORKS", INTERNATIONAL JOURNAL OF COMMUNICATIONS ISSUE1, VOLUME 2, 2008

[4] JIANQING MA¤, SHIYONG ZHANG, AND XIAOWEN TONG, "SECURE LOCALIZATION FOR WIRELESS SENSOR AND ACTOR NETWORK", 2007

[5] AZZEDINE BOUKERCHE, UNIVERSITY OF OTTAWA, "SECURE LOCALIZATION ALGORITHMS FOR WIRELESS SENSOR NETWORKS", IEEE COMMUNICATIONS MAGAZINE • APRIL 2008

[6] J. G. ALFARO, M. BARBEAU, AND E. KRANAKIS, "SECURE LOCALIZATION OF NODES INWIRELESS SENSOR NETWORKS WITH LIMITED NUMBER OF TRUTH TELLERS", 2009

[7] QI MI, JOHN A. STANKOVIC, RADU STOLERU, "SECURE WALKING GPS: A SECURE LOCALIZATION AND KEY DISTRIBUTION SCHEME FOR WIRELESS SENSOR NETWORKS", *WISEC'10,* MARCH 22–24, 2010, HOBOKEN, NEW JERSEY, USA.

[8] RAVI GARG, AVINASH L. VARNA, AND MIN WU, "GRADIENT DESCENT APPROACH FOR SECURE LOCALIZATION IN RESOURCE CONSTRAINED WIRELESS SENSOR NETWORKS", UNIVERSITY OF MARYLAND, COLLEGE PARK, MD, USA.

[9] HONGLONG CHEN, WEI LOU, AND ZHI WANGY, "SECURE LOCALIZATION AGAINST WORMHOLE ATTACKS USING CONFLICTING SETS", 2010

[10] WEN TAO ZHU, YANG XIANG, JIANYING ZHOU, ROBERT H. DENG, FENG BAO, "SECURE LOCALIZATION WITH ATTACK DETECTION IN WIRELESS SENSOR NETWORKS", PUBLISHED ONLINE: 19 APRIL 2011 © SPRINGER-VERLAG 2011

[11] NICOLA GATTI, MATTIA MONGA, SABRINA SICARI, "LOCALIZATION SECURITY IN WIRELESS SENSOR NETWORKS AS A NON-COOPERATIVE GAME", 2010