

SECURE LOCALIZATION IN WIRELESS SENSOR NETWORKS

Tanveer Zia and Albert Zomaya
School of Information Technologies
University of Sydney
{tanzia, zomaya}@it.usyd.edu.au

ABSTRACT

Wireless sensor networks have very promising future to many applications. Ensuring that sensor nodes locations are verified and are protected from malicious attacks will enable sensor networks deployment in mission critical applications. Due to the deployment nature, sensor nodes are highly vulnerable to localization attacks where an adversary can capture the nodes, changes its location or replaces it with a malicious node. In this paper we study this problem and present a secure localization scheme where nodes can securely locate themselves and send a message about their location to the neighboring nodes, eventually that message reaches the cluster leader and then to a secure base station. To find the location of nodes, we take advantage of triangulation method and protect the message transmission with a secure triple key management scheme.

KEYWORDS

Sensor networks Localization; secure locations; secure key management

1. Introduction

Wireless sensor networks are consisting of large number of tiny sensors and actuators with limited energy, computations and transmission power [3, 4]. Sensor nodes are randomly deployed in an environment where they are prone to physical interaction and most likely left unattended after deployment. Although nodes have many limitations but they report to a single destination called base station which is believed to be a powerful computer safely located with large computation resources.

We consider a hierarchical topology of sensor networks where sensor nodes form a parent child relationship in clusters when deployed [1, 2]. In this topology, nodes broadcast their IDs and listen to the neighbors, add the neighbors IDs in its routing table and count the number of neighbors it could listen to. Hence these connected neighbors become a cluster. Each cluster elects a sensor node as a leader. All inter-cluster communication is routed through cluster leaders. Cluster leaders also serve as fusion nodes to aggregate packets and send them to the base station. A cluster leader receives highest number of messages, this role changes after reaching an energy threshold, hence giving opportunity to all nodes becoming

a cluster leader when nodes move around in a dynamic environment. Coverage of cluster depends on the signal strength of the cluster leader. Cluster leader and its neighbor nodes form a parent-child relationship in a tree-based network topology. In this multi hop cluster model, data is collected by the sensor nodes, aggregated by the cluster leader and forwarded to the next level of cluster leader, eventually reaching the base station. Due to the deployment nature, nodes are highly vulnerable to localization attacks from compromised networks and malicious nodes. In this paper we argue that using four triangulation methods and a secure set of keys, impact of localization attacks can be reduced or eliminated in optimum scenarios. This paper discusses two main concepts in our secure localization process (i) determining the node location, and (ii) securing the node location. The remainder of this paper is organized as follows: Section 2 summarizes previous work done on secure localization in wireless sensor networks. Section 3 lists the threat models we are addressing. Section 4 discusses our node location mechanism based on triangulation method. In section 5 we describe our triple-key management scheme [11] to secure the localization mechanism. Section 6 evaluates the proposed localization mechanism, and finally Section 7 concludes our paper.

2. Related Work

Lazos and Poovendran [9] have proposed a secure localization technique based on the use of directional antennas. Referring to some applications where sensor nodes to be disguised having directional antennas is not feasible. Capkun and Hubaux [5] use explicit RF distance bounding in order to obtain a verifiable location in the presence of attackers. This scheme assumes the known position of certain nodes "landmarks". Landmarks are placed across the network in an organized manner which we think would be an issue in applications such as battlefield where nodes are deployed by dropping from aircrafts, determining landmarks position may not be practical then. Anjum et al [10] present a secure localisation algorithm based on transmission of nonces at different power levels from anchor nodes. This raises an issue of a node which has exhausted its power.

3. Threat Models

In order to determine the secure location we consider following threats [7] to sensor networks:

Selective Forwarding – An adversary selectively forwards the packets. A malicious node act like a black hole and refuses to forward every packet it receives.

Impersonation Attacks – Malicious nodes impersonate to be a cluster leader and lures nodes to a wrong position

Sinkhole attacks – Attracting traffic to a specific node, e.g. to prepare selective forwarding

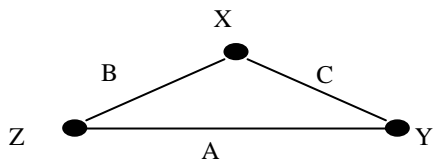
Sybil attacks – A single node presents multiple identities, and allows reducing the effectiveness of fault tolerant schemes such as distributed storage and multipath etc.

Wormhole attacks – Tunneling of messages over alternative low-latency links to confuse the routing protocol, creating sinkholes etc.

Physical displacement of nodes – An attacker physically moves a node from its original location to another location.

4. Determining the Node Location

A basic feature of a location system is the ability to determine the location of a node and verify its distance from the neighboring nodes [8]. In our secure Localization mechanism each node determines its position by calculating its distance from its neighbours using four methods in Triangulation: Lateration, attenuation, propagation and angulations. Figure 1 below describes the triangulation process to determine the node location. Each node determines its position by calculating its distance from its neighbours. Node location in triangulation is calculated by using trigonometry laws of sines and cosines as follows:



Sines Laws
$$\frac{\sin A}{X} = \frac{\sin B}{Y} = \frac{\sin C}{Z}$$

Cosines Laws
$$A^2 = B^2 + C^2 - 2BC \cos(X)$$

$$B^2 = A^2 + C^2 - 2AC \cos(Y)$$

$$C^2 = A^2 + B^2 - 2AB \cos(Z)$$

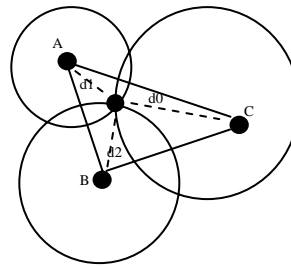


Figure 1 (a) Triangulation Lateration: Each node determines its position by calculating its distance (d) from its neighbours.

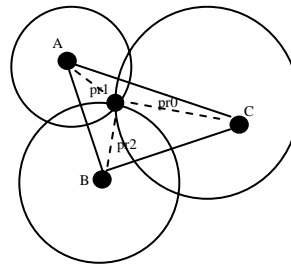


Figure 1 (b) Triangulation Attenuation: Decrease in signal strength (pr) as distance between two node increases.

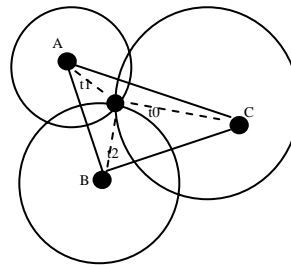


Figure 1 (c) Triangulation Propagation: Node A sends a message to node B, node B calculates the time difference $t_2 - t_1$, from the time difference node B knows its position.

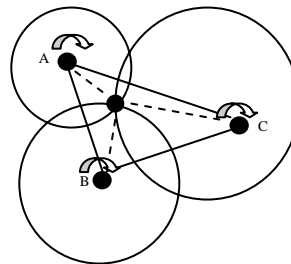


Figure 1 (d) Triangulation Angulations: uses angles to determine the distance between nodes using directional antennas.

4.1 Lateration

We assume that when the nodes are deployed they know their location through an atomic multilateration [6] process. In this process node estimates its location if it is in the range of three other nodes. When a base station sends beacon to form the network topology, nodes reply with their position in the network. Each node determines its position by calculating its distance from its neighbours.

4.2 Attenuation

In attenuation triangulation model, signal strength decreases as distance between two nodes increases. We assume a dense network where nodes are deployed in close distances. In a hierarchical clustered model parent nodes are aware of their child nodes locations.

4.3 Propagation

Node A sends a message to node B, node B calculates the time difference t_2-t_1 between two nodes.

4.4 Angulations

Angulations use angles to determine the distance between nodes using directional antennas. In 2D position two angles and one distance measurement is used, while in 3D position two angles, one length and one azimuth measurement is used.

5. Securing the Node Location

Nodes change its position if they move in a dynamic network or if an adversary has compromised the node. In the event of compromise a node is considered as a malicious node. The localization process described here is protected by a secure triple-key management scheme [11] which consists of three keys: two pre-deployed keys in all nodes and one in-network generated cluster key for a cluster to address the hierarchical nature of sensor network.

K_n (network key) – Generated by the base station, pre-deployed in each sensor node, and shared by the entire sensor network. Nodes use this key to encrypt the data and pass onto next hop.

K_s (sensor key) – Generated by the base station, pre-deployed in each sensor node, and shared by the entire sensor network. Base station uses this key to decrypt and process the data and cluster leader uses this key to decrypt the data and send to base station.

K_c (cluster key) – Generated by the cluster leader, and shared by the nodes in that particular cluster. Nodes from a cluster use this key to decrypt the data and forward to the cluster leader.

Base station broadcasts a beacon message to the sensor network; this message is encrypted by the K_n . If the receiving node is a cluster leader it decrypts the message using K_s and encrypts it again with its K_n and forwards it to the nodes in its cluster. Nodes in the cluster use its K_c to decrypt the message, adds its location and reply back to the cluster leader with its location encrypted with K_n . Cluster leader receives the locations from all nodes in the cluster and encrypts it with K_n and sends it to the base station. Base station uses its K_s to decrypt the message and becomes aware of the nodes location in the entire network. The process of base station to cluster leader and nodes and vice versa is described in the following steps:

Step 1: To establish the secure communication, base station builds a packet which contains:

ID_{BS}, K_n, TS, MAC, S (message)

Step 2: Cluster leader builds a packet containing following information:

ID_{CL}, K_n, TS, MAC, S (message)

Step 3: Nodes to cluster leader packet consists of:

ID_{sn}, k_n, TS, MAC, S (message)

Step 4: Cluster leader aggregates the messages received from the nodes in its cluster and forwards it to the base station using the packet: ID_{CL}, K_n, TS, MAC, S (Aggr message). Figure 2 below illustrates the key calculation process among the nodes, cluster leaders and the base station.

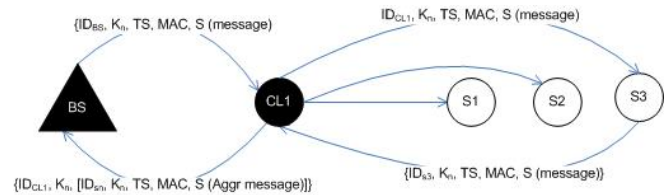


Figure 2: Key calculation using the secure triple-keys.

Notations

ID_{BS} : Base station ID

K_n : Network Key

K_s : Sensor Key

K_c : Cluster Key

ID_{CL} : Cluster leader ID

ID_{sn} : Sensor node ID

TS: An encrypted time stamp for beacon authentication

S: Seed value randomly generated by the base station

Aggr message: Aggregated message by a cluster leader

MAC: Message authentication code for message m , generated using key k

BS: Base station – a node assumed to be very powerful with extra ordinary computation resources

6. Evaluation

Our aim to provide a secure localization scheme is to prevent sensor nodes from adversarial attacks. In the presence of secure triple keys, an adversary can not produce any localization message as the neighboring nodes will reject the message from an unknown source. A malicious node injected in the network will not be able to communicate with the legitimate nodes due to the absence of secure keys. In a typical sensor communication we assume a maximum packet size of 44 bytes: IDs (3 bytes), Secure Triple-Keys (3 bytes), Time Stamp (1 byte), Seed value (1 byte), data (0..31 bytes) and MAC (4 bytes).

This adds an overhead of 3 bytes for the secure-triple keys which we think is worth ensuring that the network is protected from adversarial attacks. Preliminary results show that the packet delay due to the overhead is

marginal. Given the ongoing developments in enhancing nodes program memory and processing power our secure localization scheme would be feasible in determining the secure location of sensor nodes.

7. Conclusion

We have presented a secure Localization scheme in sensor networks to verify the node distance from the neighboring nodes in protection of our secure triple key management scheme. We have exploited the four triangulation methods: Lateration, attenuation, propagation and angulations to determine the node location through distance, signal strength, time difference and position of angles. Our analysis and evaluation shows that the fractional overhead due to our secure key triple management scheme does not compromise the performance of sensor networks instead it mitigates the security threats that would be otherwise a big concern due to malicious node presence in the sensor networks.

References

- [1] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-Efficient Communication Protocol for Wireless Microsensor Networks," IEEE Proceedings of the 33rd Hawaii International Conference on System Sciences, Jan. 2000, pp. 1–10.
- [2] M. Tubaishat, J Yin, B. Panja, S. madria, "A Secure Hierarchical Model for Sensor Networks", ACM SIGMOD, Volume 33 , Issue 1 March 2004, ACM Press, NY
- [3] I. Khalil, S. Baghi, and C. Rotaru, "DICAS: Detection, Diagnosis and Isolation of Control Attacks in Sensor Networks", IEEE Securecomm 2005, 5-9 September 2005, Athens Greece.
- [4] C.Y. Chong, and S.P. Kumar, "Sensor Networks: Evolution, Opportunities, and Challenges", IEEE 2003
- [5] S. Capkun and JP Hubaux, "Secure Positioning of Wireless Devices with Application to Sensor Networks", In the proceedings of IEEE INFOCOM 2005, Miami, FL, USA
- [6] A. Savvides, C.C. Han, and M.B. Strivastava, "Dynamic Fine-Grained Localization in Ad-Hoc Networks of Sensor", In the proceedings of ACM SIGCOM, July 2001, Rome, Italy
- [7] C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", University of California at Berkeley, USA 2003
- [8] N. Sastry, U. Shankar, D. Wagner, "Secure Verification of Location Claims", proceedings of the 2003 ACM workshop on Wireless Security, 2003. pp. 1-10.
- [9] L. Lazos and R. Poovendran, "SeRLoc: Secure range-Independent Localization for Wireless Sensor Networks", In the proceedings of ACM WiSe'04, October 1, 2004, Philadelphia, Pennsylvania, USA.
- [10] F. Anjum, S. Pandey, and P. Agrawal, "Secure Localization in Sensor Networks using Transmission Range Variation", In the proceedings of IEEE MASS 2005 Workshop, November 7-11, 2005, Washington DC, USA.
- [11] T. A. Zia, and A. Y. Zomaya, "A Secure Triple-Key Management Scheme for Wireless Sensor Networks", In the proceedings of the IEEE INFOCOM 2006 Students Workshop, April 23-24, 2006, Barcelona, Spain