www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 4 Issue 5 May 2015, Page No. 12166-12170

Security in Wireless Sensor Networks using Trust Based Distance Bounding

Parvathy Menon[1], Associate Prof.Deepa S Kumar[2], Prof.M Abdul Rahiman[3]

[1]College of Engineering Munnar, Cochin University,
County Hills Munnar 685612
parvathyuvmenon99@gmail.com

[2]College of Engineering Munnar,
Research Scholar, Karpagam University, Coimbatore
deepamsk@yahoo.com

[3]Kerala Technological University,
Pro Vice Chancellor, Kerala Technological University
pvc@ktu.edu.in

Abstract: ***Determining the position of sensors is a very essential part for most WSN algorithms. When neighbor recognition fails, protocols performance and communications deteriorate. In networks affected by relay attacks the failure may be more precise. In this paper, we propose and discuss a technique that aims to circumscribe all the sensor nodes in the network using distance bounding which is a secure neighbor detection method by using secure localization. For this, we used trust based position identification for finding the position of the sensor nodes in the neighbor by applying trust based distance bounding protocol.***

Keywords: Secure Localization, Wireless Sensor Networks, Trust based position identification.

1. Introduction

Wireless sensor networks (WSNs) are predominantly used in medical, military, and environmental monitoring applications. Neighbor detection is the process by which a node in a network determines the total number and identity of other nodes in its vicinity. Recent researches in wireless technology focus towards creating the devices a lot of subtle and moveable. Then applications of wireless networks became big in several areas like military scrutiny, oceanographic studies, mine discovery etc. within the network, the devices are going to be deployed on an over sized space and therefore the knowledge collected by the sensor has to be transmitted from the supply to the sink with most accuracy and least power consumption. Since recharging of power sources of the nodes is complex, there ought to be a skillful energy reduction mechanism.

On the other hand, for successful communication of device nodes in multi hop device networks the invention of neighbor nodes is indispensable. The nodes within the network acts as routers, that transmits data packets from one neighboring node to a different. Most of the device networks encompass each static and mobile nodes. Several approaches are proposed recently for neighbor node discovery. However they're powerless to muddle through the tribulations like frequent addition of latest nodes, loss of wireless property, and augment in transmission power etc.The most essential prerequisite of a wireless network is economical routing of data from a supply to the required destination. For this every node ought to maintain the Neighborhood info domestically. Such info stipulation is maintained even in mobile networks also for tracking and alternative arrival applications because the range of pre-positioned wireless devices become larger than before, the distribution of channel became a significant concern specially for intense networks, the collision of knowledge packets cause the drop by output so there will not exist any significant network harmnization.In this scenario, the precise assessment of neighbor nodes becomes much pertinent.

It is a basic unit of many protocols including localization, routing, leader election, and group management. Localization is one of the most important facility provided by a WSN, because in most approach we are interested not only in the types of events that have taken place, but also in where the incidents have taken place. One particularly insidious threat to a wireless network is the wormhole or relay attack. In this attack, two or more attackers collaborate to record communications at the packet or bit level in one location and play them back elsewhere. Wormholes disturb communications, change routing, or incite localization errors. Neighbor based communication without any trust worthiness creates a major vulnerability in security related aspects of the network. In this type of environment, trust value plays a crucial role in all of the network tasks. So that type of networks is also called as trusted network. Constant assessment of node's performance and collection of neighbor node's opinion value about the node are used to calculate the trust relationship of this node with other nodes. By establishing a perfect trust model in the network layer, we can create secure route between source and destination without any intruders. In this paper, we used trust based position identification for finding the position of the sensor nodes in the neighbor by applying distance bounding protocols. Proposed trust based position identification equally

concentrates both in node trust and route trust. The security is provided by finding the distance between the nodes in the communication range by using distance bounding protocol to make sure that it can find the attacker which does not belong to the communication range.

2. Related Works

Wireless sensor nodes are deployed in the areas where destructive advisories attempt to spoof the position of the sensors. For example, an attacker may alter the distance estimations of a sensor to several reference points, or replay beacons from one part of the network to some distant part of the network, thus providing false localization information [1]. Therefore, a secure positioning system must have a mechanism to verify the location claim of any sensor. Some of the existing secure localization techniques are reviewed below.

SeRLoc Lazos and Poovendran propose a novel scheme for localization of nodes in WSNs in untrusted environments called SeRLoc. SeRLoc is a distributed, range-free, resource-efficient localization technique in which there is no communication requirement between nodes for location discovery[2]. SeRLoc is robust against sybil attacks, wormhole attacks and sensor compromise.

Attack Resistant Location Estimation Liu, Ning, and Du put forward two range-based robust methods to tolerate malicious attacks against beacon-based location discovery in sensor networks. The first method, attack-resistant Minimum Mean Square Estimation, filters out malicious beacon signals. This is accomplished by examining the inconsistency among location references of different beacon signals, indicated by the mean square error of estimation, and beating malicious attacks by removing such malicious data. The second method, voting-based location estimation quantizes the deployment field into a grid of cells and has each location reference 'vote' on the cells in which the node may reside. This method tolerates malicious beacon signals by adopting an iteratively refined voting scheme. Both methods survive malicious attacks even if the attacks bypass authentication [5].

Robust Statistical Methods Li, Trappe, Zhang, and Nath introduced the idea of being tolerant to attacks rather than trying to eliminate them by exploiting redundancies at various levels within wireless networks[1]. 2.4 SPINE Capkun and Hubaux device secure positioning in sensor networks (SPINE), a range-based positioning system based on verifiable multi lateration which enables secure computation and verification of the positions of mobile devices in the presence of attackers. SPINE works by bounding the distance of each sensor to at least three reference points.

3. Distance Bounding Protocols

Distance bounding involves two parties which includes a prover and a verifier. It provides the verifier with cryptographic proof which includes the maximum physical distance to the prover. The verifier depends exclusively on the information given from executing the protocol with the prover. The verifier requires a reliable and secure estimate of the distance to the prover. The security of the protocol therefore depends not only on the cryptographic mechanisms but also on the physical attributes of the communication channel that are used to measure proximity.

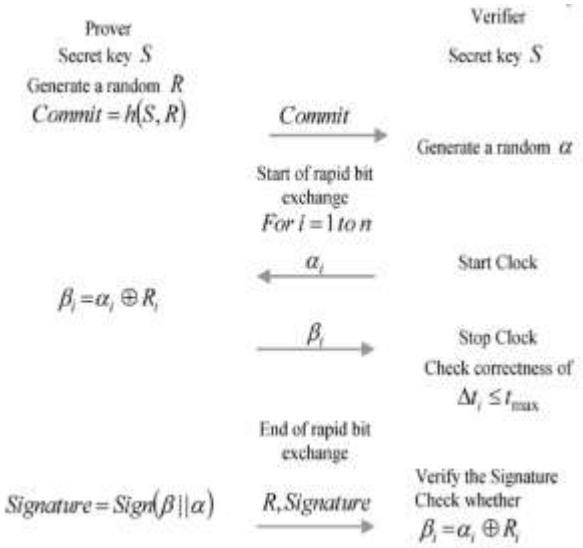

Figure 1: Distance bounding protocol(Brands and Chaums protocols) .

Distance-bounding protocols aim to prevent attackers from pretending that the prover is closer to the verifier than is actually the case. These protocols have been suggested for application in access control tokens which prevent relaying attacks .In this type of attack a local attacker relays a challenge to a distant token that returns a valid response. Distance bounding is an important aspect of many secure localization or positioning proposals where the location of nodes is inferred from their communication [2]. Such knowledge is useful for mapping the topology of the network and for geographically aware routing algorithms [3]. It has also been proposed as a protective measure for wireless networks, where relaying attacks (in this context also known as wormhole attacks) could be used to circumvent key establishment and routing protocols if an adversary tunnels messages across the network using a low latency, out-of-band channel . This pretends nodes at either end of the wormhole being closer than they actually are. Distance bounding gives a mechanism for a node to determine whether another node is a genuine neighbor which means that it should be physically located within its communication radius. Confidentiality and authentication are achieved using keys shared between neighbors. Neighboring nodes also serve as intermediaries when path keys are established between two nodes that do not share a pre-assigned key. The neighbors of a node can best detect when it is compromised and that are typically used in revocation, reputation or voting schemes. Key establishment and revocation masquerading as a neighbor forms the basis for mounting attacks on routing. We consider the secure implementation of distance-bounding protocols in ad hoc, wireless networks. We observe that typical transmission formats and modulation techniques introduce latencies, which the adversary can reduce substantially, allowing him to appear closer to the verifier than his actual position. Similarly, the symbol detection mechanism of a receiver can be optimized to provide an early indication of received bits which provides a "head start" but increases the possibility of transmission errors. It is also possible for an adversary to extract timing advantage from bit transmission by delaying to the last possible moment and then broadcasting at a significantly higher power level.

3.1 Types of attacks addressed by distance bounding

a. Distance Fraud

Distance fraud is a type of attack where a dishonest prover proves to be in the position of the neighborhood of the verifier[8].

b. Mafia Fraud

In mafia fraud there will be a dishonest prover and a verifier which if far apart. But there will be a third party attacker that makes it appear as in close proximity. The security services that are available cannot prevent this attack. Mafia fraud was first described by Desmedt [9], but this attack scenario has also been described as a wormhole or a relay attack [10].

c. Terrorist Fraud

In terrorist fraud there will be a third party attacker and a prover who will be dishonest. Both of them will collaborate to attack the system. The prover who is fraudulent and far away from the dishonest verifier assist an attacker who is close to the verifier. To masquerade as the prover by providing the attacker with selected cryptographic information [11].

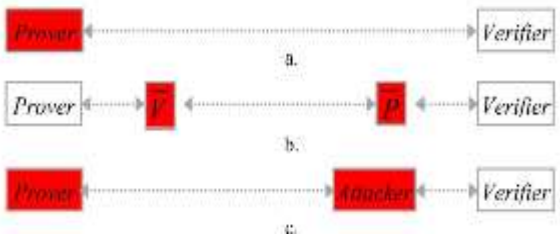

Figure 2:Main attacks that distance bounding protocols aims to prevent.(a)distance fraud(b)mafia fraud(c)terrorist fraud[3].

3.2 Advantages

The precipitation protocols, with no verification stage, without any modification, other protocol designs can also implement the threshold method, as long as the challenge bits received by the prover and the response bits sent by the prover are transmitted over an error-corrected channel during the verification stage.

The main factors influencing execution time is the transmission time, i.e., the time required to transmit data, and the processing time.

4. Proposed System

A Trust based Position Identification is performed. First phase is location estimation in which the sensor node broadcast its ID to locators which comes in sensor-to locator communication range and those locators perform distance bounding with sensor nodes. Then for every locator trust evaluation value is estimated by sensor node.

Trust based Position Identification algorithm contains two phases. First phase is location estimation in which the sensor node broadcast its ID to locators which comes in sensor-to locator communication range and those locators perform distance bounding with sensor nodes. Then for every locator of set LDBs [4], trust evaluation value is estimated by sensor node. If the trust evaluation value is greater than or equal to threshold then it is included within set LTs. If the number of locators within set LTs is greater than or equal to 3 and any 3 locators of set LTs forms an triangle around sensor, then location of sensor node is estimated through Verifiable Trilateration[4]. Otherwise localization fails. Second phase is location verification in which location claim of sensor node is verified by locator through distance bounding.

4.1 Location Identification Phase:

Step 1: The nodes s broadcasts its IDs to the locators.
Step 2:Any locator Li which might communicate bi-directionally with node s performs distance bounding with s. Distance bounding protocol verifies that node s being at a distance d sLi from Li cannot claim to be at a distance less than d sLi LDBs = {Li : ‖ Li – s ‖ ≤ rsL } … (1)
Step 3: For each locator Li that belongs to the line LDBs, sensor node s collects the trust evaluation value of locator Li as in trust model and checks whether or not the trust analysis value of the locator Li is larger than or equal to threshold value. If the trust evaluation value of locator Li is greater than or adequate to threshold then the locator is further within the set LTs.
LTs = {Li: Li ∈ LDBs, T sLi ≥ Threshold}… (2)
Step 4: Sort the set LTs of locators within the order based on trust evaluation value of locators from high to low. Step 5: If | LTs | ≥ 3 then the sensor s performs Verifiable Trilateration with the locators Li ∈ LTs . Otherwise the localization fails. Sensor s will perform Verifiable Trilateration if it is within the triangle of three locators.
Step 6: If sensor s estimates its position by Verifiable Trilateration, then it notifies all the locators Li ∈ LDBs, with the transmission of computed position encrypted by the pair wise key and terminates the algorithm.

4.2 Location verification phase

Whenever the node sends information along with the position to the verifier, verifier has to check the claimed position of given node. Hence, verifier conducts distance bounding with s. So, the sensor cannot declare to be at a distance that is less than the particular one.

5. Security Analysis

5.1 Attacker model

It is assumed that attacker can imitate the location estimated by the sensors. However, the attacker does not restrict sensors from estimating the position. If the localization of sensor node fails, it is believed that it is under attack. Also it is assumed that attacker is capable of jamming the signals of network entities. However, jamming signals from all the entities results in failure of localization of the sensor node.

5.2 Wormhole attack

In wormhole attack an attacker receives packet at one point in the network, “tunnels” them to alternative point in the network. Then the locators sends information about its location as reply, the attacker collects this information and tunnels this to another point in the network and replies them. It is assumed that a set of locators replied to the sensor s is under attack and s performs Verifiable Trilateration with the three locators Li Lj Lk ∈ LTs such that s lies within Δ Li Lj Lk. If the attacker jams

the signal from one locator, assume Li and replies as Li after some time, then s still resides within Δ Li Lj Lk. Suppose the distance from sensor node s to Li is enlarged then any one of the other then the locators need to reduce the distance. This is not possible due to distance bounding protocol. Hence, the spoofing of position of s by attacker is not possible. localization fails if the attacker jams the signals from all the locators of set LTs .

5.3 Compromised node attack

A network entity is said to be compromised if attacker gains authority of all the information related to the entity. Suppose if the attacker compromise the locators then it can jam the signals of those locator which results in failure of localization if significant locators are compromised. However, if the attacker adds bogus location information to the compromised locators, then trust model helps in detecting it and those untrustworthy locators are not included in it.

6. Results

The proposed system is implemented using NS2.NS2 is mainly used for the simulation purpose. For this we are using ns allinone 2.35.Here 50 nodes are considered to form the system. The nodes are configured. The nodes will find the neighbors within its transmission range.Then the nodes which do not belong in the transmission range are found out and are excluded.

Performance analysis of the proposed method using the proposed system can be clearly understood using the graphs shown below.

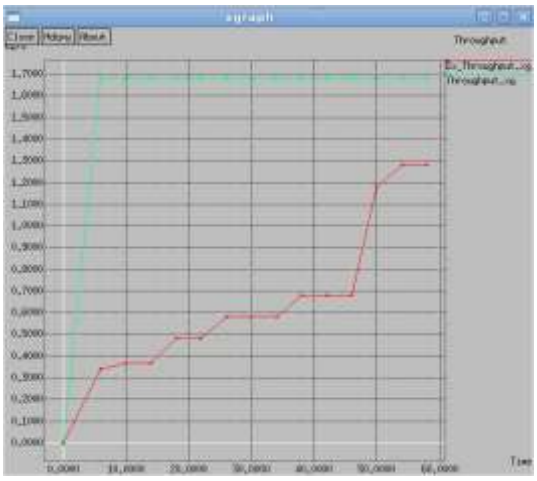

Figure 3 Throughput

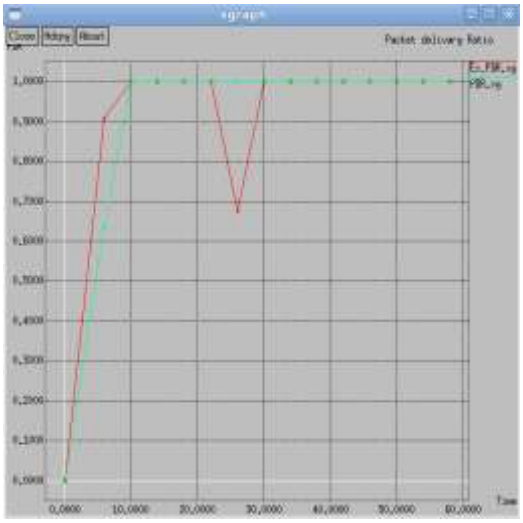

Figure 4 Packet delivery ratio

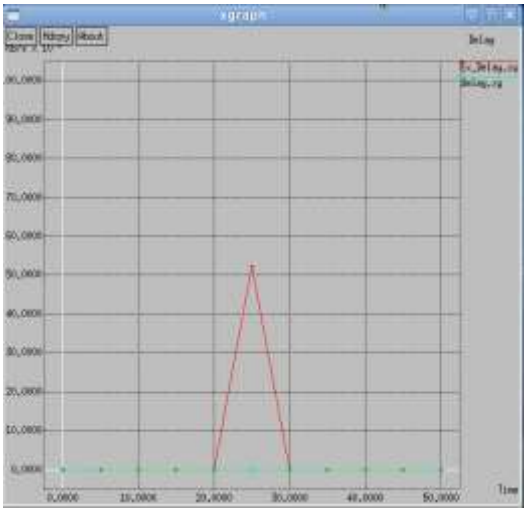

Figure 5 Delay

7. Conclusion

Verifying the physical proximity or location of a device is becoming an important security requirement. Distance-bounding provides cryptographic assurance as to the upper bound for the physical distance between two communicating parties, without requiring additional device characterization or information from third parties. As a result, this method is adaptable to provide SND[7] services in a variety of communication architectures. The proposed system used trust based position identification to find the untrustworthy nodes. It uses the distance bounding protocol to find the distance between the neighbouring nodes. The proposed method helps in finding the most trustworthy nodes and thus forwarding the packets only through the nodes which are trustworthy and thus avoiding the attacker node.

References

[1] S. Brands and D. Chaum, Distance-bounding protocols, In Workshop on the theory and application of cryptographic techniques on Advances in cryptology, pp. 344-359. SpringerVerlag New York, Inc., 1994.

[2] L. Lazos and R. Poovendran, SeRLoc: Secure Range-Independent Localization for Wireless Sensor Networks, in Proceedings of WISE, Philadelphia, PA, Oct. 2004, pp. 21–30.

[3] Adnan Abu-Mahfouz, Member, IEEE, and Gerhard P. Hancke, Senior Member, IEEE "Distance Bounding: A Practical Security Solution for Real-Time Location Systems". IEEE transactions on industrial informatics, vol. 9, no. 1, February 2013.

[4] N. Priyantha, A. Chakraborthy and H. Balakrishnan, The Cricket Location-Support System, In Proceedings of MOBICOM, Boston, MA, USA, Aug. 2000, pp. 32-43.

[5] D. Stinson, Cryptograhpy: Theory and Practice, 2nd edition, CRC Press, Boca Raton, FL, 2002.

[6] R.J. Fontana, E. Richley, and J. Barney, Commercialization of an F Precision Asset Location System. In Proceedings of IEEE Conference on Ultra Wideband Systems and Technologies, Nov. 2003.

[7] Dave Singelee, Bart Preneel ESAT-COSIC, K.U. Leuven, Belgium. "Location Verification using Secure Distance Bounding Protocols".

[8] Chong Hee Kim and Gildas Avoine " RFID distance bounding protocol with mixed challenges to prevent relay attacks" Universities Catholique de Louvain Louvain-la-Neuve, B-1348, Belgium.

[9] Y. Desmedt, C. Goutier, and S. Bengio, "Special uses and abuses of the fiat-shamir passport protocol," in *Advances in Cryptology—CRYPTO'87*, C. Pomerance, Ed. Berlin, Germany: Springer, 1988, pp. 21–39.

[10] G.P.Hancke, K.E.Mayes,andK.Markantonakis,"Confidence In smart token proximity: Relay attack revisited,"*Computing Security*, vol.28, pp. 615–627, 2009.

[11] Y. Desmedt, "Major security problems with the unforgeable" (feige)Fiat_Shamir proofs of identity and how to overcome them," in *Proc.6th Worldwide Congress Comput. Commun. Security Protection*, 1988,pp. 147–159.