ISSN: 0975-766X
CODEN: IJPTFI
Available Online through ***Research Article***
www.ijptonline.com

PROVIDING SECURITY IN REAL TIME LOCATION SYSTEM BY USING DISTANCE BOUND PROTOCOL

P.Satheesh, C.Rajagopal
U.G Student, Assistant Professor(S.G)
Department of Computer Science Engineering and Information Technology
Saveetha School of Engineering, Saveetha University, Chennai.

Received on: 25.09.2016 *Accepted on: 15.10.2016*

Abstract

This paper involves the providing security in real time location systems using distance bound. RTLS is normally embedded in mobile phones or navigational systems. Present real time location systems are based on wireless technologies such as Wi-Fi, Bluetooth, RFID and GPS. Distance bounding is most securing detection techniques that cryptographically degree an higher sure for the bodily distance between two network devices. If there is any attacks in that distance bounding , we can’t prevent by using network authentication technique like password , smart cards etc., In this paper I will explain clearly how to prevent attacks using distance bounding protocol.

Keywords: RTLS, Distance bounding protocol, GPS, Wi-Fi.

I. Introduction

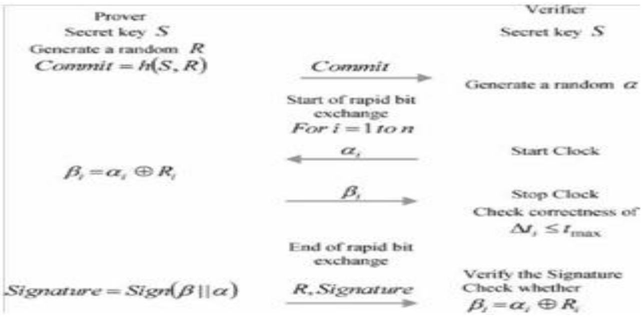
Neighbor revelation is the technique by which a center point in a framework chooses the ensured neighbor ID and character of various centers in its entire trusted framework zone. It is a key building square of various secured neighbor recognizable proof including restriction, directional radio wires, RF fingerprinting, joined structure, range based system. Time-based trades and various media access control instruments rely on upon exact neighbor information. In Real Time Location System(RTLS), neighbors are by and large portrayed as center points that exist in radio extent of each other. In remote correspondence, It is continually expected that devices are within the correspondence range and that correspondence degree is territory compelled, which absolutely exhibits physical region. In a hostile space, a false device can control the correspondence range and guaranteed to be a neighbor. in like manner a device might work together with a false contraption. Nevertheless, remote exchanges are feeble to misuse. Aggressors have the chance to perform malevolent activities going from essential difference of organization to refined craftiness. There are diverse sorts of strikes that can rise in RTLS application, for instance, detachment attack, hand-off ambush and terrorist strikes. Territory based affirmation are used as a part of various business wanders –like amassing, oil and gas, retail and social protection. GPS-based technique is use for outside discovering stages. This can't perform presentation of contraptions, for example, Left or Right move.

2. Real time Location Systems

The goal of RTLS system is to constantly know the location of the various assets that you need to track within indoor area. RTLS are a form of local positioning system, and this is not related to GPS, mobile phone tracking. RTLS are used to automatically identify and track the location of objects or people in real time. RTLS can be used in areas like Fleet tracking, Navigation, Personnel tracking, network security .There are three components to RTLS system: First, the physical infrastructure that includes the many fixed reference points. Second the active or passive RFID tags which are attached to objects or people and communicate with the physical infrastructure. Third is software layer that collects data. The physical layer of RTLS technology use radio frequency (RF) communication, infrared or ultrasound technology. RTLS usually does not include speed, direction, or spatial orientation information.

3. Distance Bounding Protocol

Checking the physical area of a gadget utilizing validation convention is an imperative security component. Separation jumping convention plan to demonstrate the vicinity of two gadgets in respect to one another. Separation bouncing convention decides an upper destined for the physical separation between two imparting parties taking into account the Round-Trip-Time (RTT) of cryptographic test reaction pairs.Brands and Chaum proposed a separation jumping convention that could be utilized to confirm a gadget's vicinity cryptographically. This outline in light of a channel where the prover can answer momentarily to every single twofold digit got from the verifier. The quantity of challenge–response associations is being controlled by a picked security parameter. Separation bouncing convention not just in the coordinated nearness distinguishing proof connection additionally as building squares for secure area frameworks. After right execution of the separation bouncing convention, the verifier realizes that a substance having information is in the trusted system. Separation bouncing convention can be partitioned in three stage: the Commitment stage, the quick piece Exchange stage and marking stage,



Distance Bounding Protocol (Brands and Chaum's protocols)

5. Types of Attacks

A. Distance Fraud

A separation extortion is an assault where an exploitative and forlorn prover backings to be in the area of the verifier.[3]

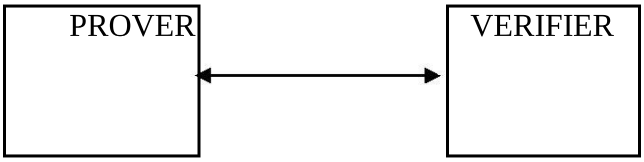


Fig.1: Distance Fraud [1].

B. Mafia Fraud

A mafia misrepresentation is an assault where a foe thrashings a separation bouncing convention utilizing a man-as a part of the-center (MITM) between the peruser and a fair tag situated outside the neighbor.

Fig.2.: Mafia Fraud.

6. Location Based Authentication in RTLS

Area based validation is utilized ordinarily as a part of our day by day cooperations in system. Area based verification is an extraordinary methodology to demonstrate an individual's character and legitimacy on appearance essentially by distinguishing its vicinity at an unmistakable area. To empower area based

C. Terrorist Fraud

A terrorist extortion is an assault where a foe annihilations a separation bouncing convention utilizing a man-as a part of the-center (MITM) between the peruser and an untrustworthy tag situated outside of the area, such that the last effectively helps the foe to expand her assault achievement likelihood, without providing for her any preference for future assaults.

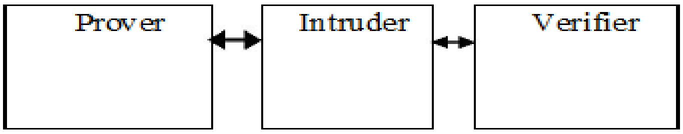


Fig.3: Terrorist Fraud [1]

7. Prevention Technique of Attacks

Distinctive strategies are utilized for counteractive action of these assaults. Out yonder extortion the area won't be adequate on the grounds that the verifier does not believe the prover. He needs to keep a misrepresentation prover guaranteeing to be closer. Diverse sort's area components that keep these assaults are:

A. Measure the signal strength

Hub can figure separation from other hub by sending it a message and perceive to what extent it takes to return. On the off chance that reaction confirmed, misrepresentation hub can lie about being further away than it is, however not closer. Sender incorporates quality of transmitted message in message; Receiver looks at got quality to transmitted quality to register separation. Not secure, but rather can be valuable when consolidated with different instrumssents.

B. Measure the round trip time

Some overcomes happen in this convention:

1. It ought to be incomprehensible for the prover to send the reaction before getting the test.
2. The reaction ought to be reliant on the reaction.
3. Challenge reaction convention is insufficient.
4. After execution of this convention, the verifier realizes that some gathering is close.
5. For illustration, one issue in Echo convention, how does one can realize that this substance is prover? [2] 6. The arrangement of these issues is proliferation speed

8. Prevention of Attacks

We will cover three sorts of assault Mafia, Terrorist and Distance extortion in beneath area.

A. Prevention of mafia fraud

Measuring the season of flight of an electromagnetic sign out yonder jumping convention guarantees that an aggressor cannot be further away than (s) he claims to be. Utilizing this rule forestall separation extortion assaults as well as mafia misrepresentation assaults. It is a transfer sort assault where the foe is demonstrated as a false prover and verifier collaborating together, as appeared in Fig.3 the fake verifier associates with the legitimate prover and the fake prover cooperates with the fair verifier. The physical separation in the middle of enemy and verifier is little. This assault empowers assailant to recognize himself to verifier as being prover being near verifier, with no of prover and verifier seeing the assault. Mafia extortion assaults are especially valuable for the foe where verification is fruitful when a particular substance is near the verifier and where the consequence of an effective confirmation is access to an administration offered by the verifier.

1. Mafia misrepresentation is valuable where confirmation is effective when particular substances near the verifier.

2. The aftereffect of confirmation is access to benefit offered by the verifier

3. By utilizing S. Brands and D. Chaum, separation jumping convention counteract mafia extortion assaults.

4. It can without much of a stretch be incorporated into other recognizable proof convention.

B. Prevention of Terrorist fraud

In the terrorist extortion, the foe does not know the mystery key of the prover. Presently we will show how the terrorist extortion assault can be connected to the separation bouncing convention of Brands and Chaum. Generally separate jumping convention can be isolated in three sections: the dedication stage, the quick piece trade stage and the marking stage (responsibility). There is however no solid (cryptographic) connection between these 3 stages. The verifier has no chance to get of checking if the gathering that executes the dedication stage is the same as the one that executes the quick piece trade stage or the marking stage. One is just sure of the way that the gathering that executed the quick piece trade stage is adjacent the verifier and that the gathering that executed the marking stage knows the private key. Distance jumping convention is helpless against a terrorist assault. There are two stretched out techniques to counteract terrorist extortion assault in separation jumping convention

Fast Bit Exchange Using The Secret Key

This strategy utilizes three stages

1. Commitment stage where signals send.

2. In second stage challenge –response single piece communication happens.

3. And third stage, the prover uses zero information demonstrate to persuade the verifier that he knows the mystery key**.**

Using trusted hardware

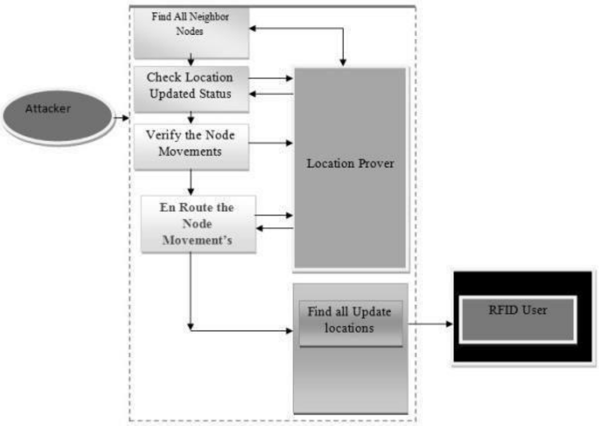
This strategy utilizes three stages

1.Commitment stage where signals send.

2. In second stage challenge –response single piece communication happens.

3. And third stage, the prover uses zero information demonstrate to persuade the verifier that he knows the mystery key.

RTLS System Architecture


Find All Neighbor Nodes
Check Location Updated Status
Attacker
Verify the Node Movements
Location Prover
En Route the Node Movement's
Find all Update locations
RFID User

Aggressors assaults the framework and discover the IP of hubs, introductory area to every one of the hubs and change the position of hubs by moves left and right. As our objective is to screen constant areas, as well as to recover history area evidence data when required, an area confirmation server is vital for putting away the history records of the area proofs. It speaks straightforwardly with the prover hubs who present their area proofs. As the source personalities of the area verifications are put away as nom de plumes, area evidence server is endowed as in despite the fact that it is traded off and observed by assailants, it is outlandish for the aggressor to uncover the genuine wellspring of the area confirmation. The hub who needs to gather area proofs from its neighboring hubs. At the point when an area confirmation is required at time, the prover will telecast an area evidence solicitation to its neighboring hubs through system. In the event that no positive reaction is gotten, the prover will create a fake area confirmation and submit it to the area evidence server.

9. Conclusion

Physical area confirmation is one of the genuine concerns in RTLS applications. Separation computing so as to jump conventions will counteract assaults the separation between the prover and the verifier. We will quantify round trek time to ascertain the separation between trusted gatherings.In this paper, we have introduced the essential applied design of separation bouncing convention, counteractive action procedures of assaults.

10. References

1. 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
2. Dave Singelee, Bart Preneel ESAT-COSIC, K.U. Leuven, Belgium.“Location Verification using Secure Distance Bounding Protocols”.

3. 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
4. R. Stoleru, H. Wu, H. Chenji, “Secure Neighbor Discovery in Mobile Ad Hoc Networks,” Department of Computer Scienceand Engineering, Texas A&M University in 2011 Eighth IEEE International Conference on Mobile Ad-Hoc and Sensor Systems
5. Vom Fachbereich Informatik der Technischen Universitat Darmstadt genehmigte "Security Aspects of Distance-Bounding Protocols" Tag der Einreichung: 20. June 2012 Tag der mundlichen Prufung: 04 July 2012
6. Samer S. Saab, Senior Member, IEEE, and Zahi S. Nakad, Member, IEEE "A Standalone RFID Indoor Positioning System UsingPassive Tags". IEEE Transactions on Industrial Electronics, VOL. 58, NO. 5, MAY 2011.