ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 10, April 2014

A Survey on Distance Bounding Protocol for attacks and frauds in RTLS system

Srikanth S P (Assistant professor, CSE Department, MVJCE, Bangalore)
Sunita Tiwari (PG- Student, CSE Department, MVJCE, Bangalore)

Abstract*— Real time networks like Real Time Location System (RTLS), Wireless, Mobile Adhoc Network (MANet) suffer location based attacks. These attacks cannot prevent by network authentication technique like password, smart card or biometric. Location based attacks categories in distance fraud, mafia fraud, and terrorist fraud. In this paper we give a survey for physical proximity or location verification of devices, for all types of attacks and prevention technique to these attacks. Distance bounding is secure neighbor detection methods that cryptographically measure an upper bound for the physical distance between two network devices. We will emphasize on architectural view and protocols used for RTLS system and industrial Radio frequency identification (RFID). In addition, will show how distance bounding protocol use for prevention of attacks?

***Index Terms*—Distance-bounding protocol, Secure neighbor detection, RTLS**

I. INTRODUCTION

Neighbor detection is the process by which a node in a network determines the secure neighbor detection and identity of other nodes in its entire trusted network area. It is a fundamental building block of many secure neighbor detection including localization, directional antennas, RF fingerprinting, centralized system, location-based system. Time-based communications and many media access control mechanisms rely on accurate neighbor information.[1] In Real Time Location System(RTLS), neighbors are usually defined as nodes that lie within radio range of each other. In wireless communication, It is always assumed that devices are within the communication range and that communication range is location limited, which implicitly proves physical proximity. In a hostile environment, a fraudulent device can manipulate the communication range and pretended to be a neighbor. [1] As a result a device might interact with a fraudulent device. However, wireless communications are susceptible to abuse. Attackers have the freedom to perform malicious activities ranging from simple denial of service to sophisticated deception. There are various types of attacks that can arise in RTLS application such as distance attack, relay attack and terrorist attacks. Location based verification are used in many industries –like manufacturing, oil and gas, retail and healthcare. GPS-based technique is use for outdoor locating platforms. This cannot perform on indoor location tracking because we need orientation of devices like Left or Right move.

II. 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]

III. DISTANCE BOUNDING PROTOCOL

Verifying the physical location of a device using authentication protocol is an important security mechanism. Distance-bounding protocol aim to prove the proximity of two devices relative to each other. Distance-bounding protocol determines an upper bound for the physical distance between two communicating parties based on the Round-Trip-Time (RTT) of cryptographic challenge response pairs.[1] Brands and Chaum proposed a distance bounding protocol that could be used to verify a device's proximity cryptographically. This design based on a channel where the prover can reply instantaneously to each single binary digit received from the verifier. The number of challenge–response interactions is being determined by a chosen security parameter. Distance bounding protocol not only in the one-to-one proximity identification context but also as building blocks for secure location systems. After correct execution of the distance bounding protocol, the verifier knows that an entity having data is in the trusted network. Distance bounding protocol can be divided in three phase: the Commitment phase, the fast bit Exchange phase and signing phase

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 10, April 2014

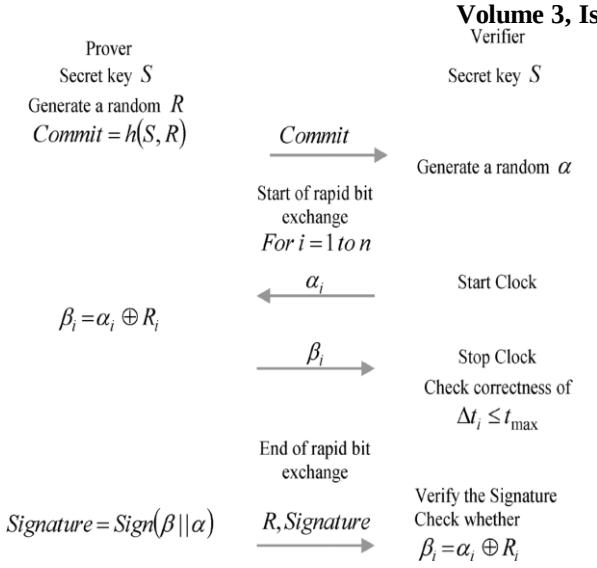

Fig-1: Distance Bounding Protocol (Brands and Chaum's protocol s)

IV. LOCATION BASED AUTHENTICATION IN RTLS

Location based authentication is used very commonly in our daily interactions in network. Location based authentication is a special procedure to prove an individual's identity and authenticity on appearance simply by detecting its presence at a distinct location. To enable location based authentication, a special combination of objects is required, RTLS are used to automatically identify and track the location of object or people in real time. Most RTLS ,Fixed reference points receive wireless signals from tags to determine their location .Example of RTLS include; finding a misplaced tool cart in a warehouse, to combined identity of multiple items placed in a single location such as on a pallet, finding medical equipment a hospital. RTLS are a form of local positioning system, and do not usually refer to GPS, mobile phone tracking. RTLS is used for indoor security [3].

V. TYPES OF ATTACKS

A. *Distance Fraud*

A distance fraud is an attack where a dishonest and lonely prover supports to be in the neighbourhood of the verifier.[3]

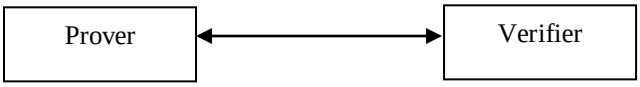

Fig-2: Distance Fraud [1]

B. *Mafia Fraud*

A mafia fraud is an attack where an adversary defeats a distance bounding protocol using a man-in-the-middle (MITM) between the reader and an honest tag located outside the neighbour.

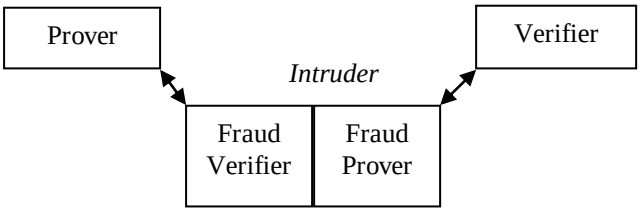

Fig-3: Mafia Fraud [2]

C. *Terrorist Fraud*

A terrorist fraud is an attack where an adversary defeats a distance bounding protocol using a man-in-the-middle (MITM) between the reader and a dishonest tag located outside of the neighbourhood, such that the latter actively helps the adversary to maximize her attack success probability, without giving to her any advantage for future attacks.

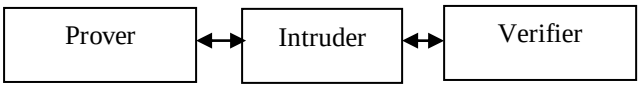

Fig-4: Terrorist Fraud [1]

VI. PREVENTION TECHNIQUE OF ATTACKS

Different methods are used for prevention of these attacks. In the distance fraud the location will not be sufficient because the verifier does not trust the prover. He wants to prevent a fraud prover claiming to be closer. Different type's location mechanisms that prevent these attacks are:

A. *Measure the signal strength*

Node can calculate distance from other node by sending it a message and see how long it takes to return. If response authenticated, fraud node can lie about being further away than it is, but not closer. Sender includes strength of transmitted message in message; Receiver compares received strength to transmitted strength to compute distance. Not secure, but can be useful when combined with other mechanisms.

B. *Measure the round trip time*

Another solutions measures the round trip time. The round trip time is the time required for exchange a packet from a specific source to a specific destination and back again. In this protocol the verifier sends out a challenge and starts a timer. After receiving the challenge, the prover does some very elementary computations to construct the response. The response is sent back to the verifier and the timer is stopped. Multiplying this time with the propagation speed of the signal gives the distance. [4] Some overcomes occur in this protocol:

1. It should be impossible for the prover to send the response before receiving the challenge.
2. The response should be dependent on the response.
3. Challenge response protocol is not enough.
4. After execution of this protocol, the verifier knows that some party is close.

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 10, April 2014

5. For example, one problem in Echo protocol, how does one can know that this entity is prover? [2]
6. The solution of these problems is propagation speed

VII. PREVENTION OF ATTACKS

We will cover three types of attack Mafia, Terrorist and Distance fraud in below section.

A. Prevention of mafia fraud

Measuring the time of flight of an electromagnetic signal in the distance bounding protocol assures that an attacker can not be further away than (s) he pretends to be. Using this principle, not only prevent distance fraud attacks but also mafia fraud attacks. It is a relay-type attack where the adversary is modelled as a fraudulent prover and verifier cooperating together, as shown in Fig.3 the fraudulent verifier interacts with the honest prover and the fraudulent prover interacts with the honest verifier. The physical distance between adversary and verifier is small. This attack enables attacker to identify himself to verifier as being prover being close to verifier, without any of prover and verifier noticing the attack. Mafia fraud attacks are particularly useful for the adversary where authentication is successful when a specific entity is close to the verifier and where the result of a successful authentication is access to a service offered by the verifier.

1. Mafia fraud is useful where authentication is successful when specific entities close to the verifier.
2. The result of authentication is access to service offered by the verifier.
3. By using S. Brands and D. Chaum, distance bounding protocol prevent mafia fraud attacks.
4. It can easily be integrated into other identification protocol.

B. Prevention of Terrorist fraud

In the terrorist fraud, the adversary does not know the secret key of the prover. Now we will demonstrate how the terrorist fraud attack can be applied to the distance bounding protocol of Brands and Chaum. Roughly distance bounding protocol can be divided in three parts: the commitment phase, the fast bit exchange phase and the signing phase (commitment). There is however no strong (cryptographic) relation between these 3 phases. The verifier has no way of checking if the party that executes the commitment phase is the same as the one that executes the fast bit exchange phase or the signing phase. One is only certain of the fact that the party that executed the fast bit exchange phase is nearby the verifier and that the party that executed the signing phase knows the private key.[2] Distance bounding protocol is vulnerable to a terrorist attack. There are two extended methods to prevent terrorist fraud attack in distance bounding protocol.

Fast bit exchange using the secret key: This method uses three phases

1. Commitment phase where signals send.
2. In second phase challenge –response single bit interaction occurs.
3. And third phase, the prover uses zero knowledge prove to convince the verifier that he knows the secret key.

Using trusted hardware: In this method we stabilize relationship in signing phase and bit exchange phase using trusted hardware. In this phase attacker cannot get value from trusted hardware or cannot change the protocol direct it has to perform.[4]

VIII. RTLS SYSTEM ARCHITECTURE

Attackers attacks the system and find the IP of nodes, initial location to all the nodes and change the position of nodes by moves left and right. As our goal is not only to monitor real-time locations, but also to retrieve history location proof information when needed, a location proof server is necessary for storing the history records of the location proofs. It communicates directly with the prover nodes who submit their location proofs. As the source identities of the location proofs are stored as pseudonyms, the location proof server is entrusted in the sense that even though it is compromised and monitored by attackers, it is impossible for the attacker to reveal the real source of the location proof. The node who needs to collect location proofs from its neighbouring nodes. When a location proof is needed at time, the prover will broadcast a location proof request to its neighbouring nodes through network. If no positive response is received, the prover will generate a dummy location proof and submit it to the location proof server.

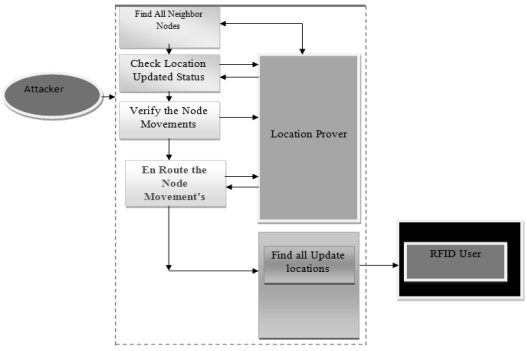

Fig-5: System Architecture

A third-party user or an application that is authorized to verify a prover's location within a specific time period. The verifier usually has close relationship with the prover, e.g., friends or colleagues, to be trusted enough to gain authorization.

IX. CONCLUSION

Physical location verification is one of the serious concerns

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 10, April 2014

in RTLS applications. Distance bounding protocols will prevent attacks by computing the distance between the prover and the verifier. We will measure round trip time to calculate the distance between trusted parties. In this paper, we have presented the basic conceptual architecture of distance bounding protocol, prevention techniques of attacks.

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 Science and Engineering, Texas A&M University in 2011 Eighth IEEE International Conference on Mobile Ad-Hoc and Sensor Systems

AUTHOR'S PROFILE

Srikanth S P is a Computer Science Engineer, presently working as an Assistant Professor in the department of Computer Science & Engineering of MVJ College of Engineering, Bangalore. He completed M.Tech from VTU Belgaum University (2004) in IT and B.E. from Mysore University (1997) in IT.

Sunita Tiwari completed B.Tech (CSE) from K.N. Modi Engg College, Ghaziabad, U.P. in 2010 and pursuing M.Tech (CSE) in MVJ College of Engineering Bangalore, Karnataka. Her research interests include Network Security, Networking..