International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 2 Issue 5 ǁ May. 2014 ǁ PP.44-48

Real-Time Location Systems Security using Distance Bounding

Srikanth S P[1], Sunita Tiwari[2]
[1]*(Computer Science, MVJCE/VTU, Bangalore, India)*
[2]*(Computer Science, MVJCE/VTU, Bangalore, India)*

ABSTRACT*:* *Traditional Authentication protocols, that run between a prover and a verifier, enable the verifier to decide whether a prover is fraud or authenticate by using technique like password, smart card, but location based attacks cannot be prevent using these techniques. Networks like Real Time Location System (RTLS), Wireless, Mobile Adhoc Network (MANet) suffer location based attacks. Location based attacks categories in distance fraud, mafia fraud, and terrorist fraud. Distance bounding technique is use for secure neighbor detection in RTLS that cryptographically measure an upper bound for the physical distance between two network devices. In this paper propose architecture for physical proximity or location verification of devices, for all types of attacks and prevention technique to these location based attacks*

Keywords – *Distance bounding protocol, secure neighbor detection, RTLS*

I. INTRODUCTION

An authentication protocol is considered secure if an adversary cannot impersonate a legitimate prover. Distance-bounding is an authentication protocol prevent all three type of attacks, First is man -in -the- middle attack (MITM) or relay attacks, where an adversary forwards information between the prover and verifier such that neither honest party is aware of the attack[4]. Second, In distance attacks, a dishonest prover placed far from the verifier and Third terrorist attacks, where dishonest prover provides some limited help to the adversary, such that the adversary is able to authenticate to the honest verifier. However the prover should not forward any information that allows the adversary to authenticate without the prover's help.

For secure Neighbor detection, a node in a network determines the secure neighbor detection and identifies other nodes in its entire trusted network area. It is used various protocols for secure neighbor detection including localization, directional antennas, RF fingerprinting, centralized system, location-based system. In Real Time Location System (RTLS), neighbors are usually defined as nodes that lie within radio range of each other [3]. 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. Distance bounding protocol properties is used with RFID tags. The most common RF tags is the ISO 14443 standard, which describes two types of tags which operate at a frequency of 13.56 MHz The ISO 14443 standard describes HF (high frequency) cards[4]. These cards operate at proximity, i.e., at around 10cm. Distance-bounding protocols are not applicable for high frequency tags, but only implementable in systems with low-latency channels.

II. SCOPE OF PAPER

The scope of the paper is to detecting attacks such as man-in-the- middle attack, terrorist attack and distance fraud. If an intruder comes in secure network and impose as a trusted entity, using the distance bounding protocol we can discover fraud entity. So that the data transmitted by the prover can be receive only by authenticated verifier not by the attacker who masquerades as the same identity of original node and to eliminate the attack.

Communication involves two parties, a prover and a verifier, and provides the verifier with cryptographic proof as to the maximum physical distance to the prover. The verifier relies exclusively on information gained from executing the protocol with the prover. As the verifier requires a reliable and secure estimate of the distance to the prover, distance-bounding protocols should be integrated into the underlying communication channel. The security of the protocol therefore not only depends on the cryptographic mechanisms but also on the physical attributes of the communication channel that are used to measure proximity.

III. EXISTING SYSTEM

In conventional networks, authentication is often based upon password, secret key, and smart card or biometric. A prover convincing a verifier of some assertion is a frequently recurring element in many applications. The assertion is often the identity of the prover, but it can also be more general. Use GPS coordinates in a location verification scheme, but this method cannot be used indoor [1]. Location information does not always have to be so detailed; sometimes we are interested in the orientation. A lot of solutions can be found in the location verification scheme. There are however some drawbacks to this method. For example, it cannot be used indoor. Location information does not always have to be so detailed in the distance, the environment. Combining these pieces of information will enable to determine the exact position of the other party.

The scenario of existing system has been practically demonstrated against real-world RFID systems. The secure verification of a devices location relative to another device, so-called secure neighbor detection, is therefore crucial to the secure and reliable operation of industrial real-time location applications.

IV. PROPOSED SYSTEM

In the proposed system, attackers attacks the system and find the IP address 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.

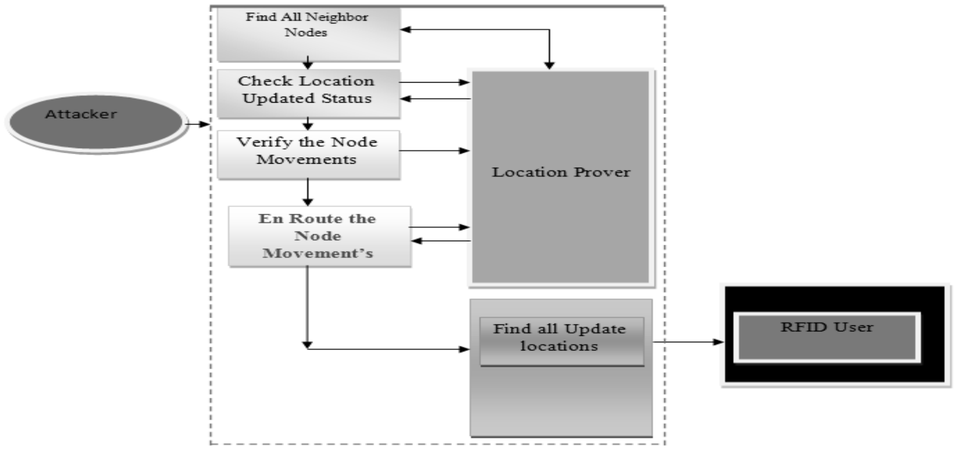
Find All Neighbor Nodes
Check Location Updated Status
Attacker
Verify the Node Movements
Location Prover
En Route the Node Movement's
Find all Update locations
RFID User

Figure-1: Architecture of Proposed System

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 neighboring nodes. When a location proof is needed at time, the prover will broadcast a location proof request to its neighboring 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. A third-party user or an application who is authorized to verify a prover's location within a specific time period. The verifier usually has close relationship with the prover, for example friends or colleagues, to be trusted enough to gain authorization.

The propagation speed of sound is much slower than that of radio waves. As a result, an attacker can intercept the ultra sound communication and forward it over a faster radio or optical communication medium to an accomplice closer to the verifier or prover, thereby reducing the time measurement and decreasing the distance estimate. Radio Frequency (RF) channels are proposed as the channel for implementing distance bounding systems [3]. A challenge-response authentication protocol is used in tight time-out constraint. As a result, characteristics like attack resistance, resource requirements and execution time varies for each protocol. The setup and verification stages can be transmitted via robust communication channels.

V. DISTANCE BOUNDING PROTOCOL

A 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]. 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. 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 [3]. 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.

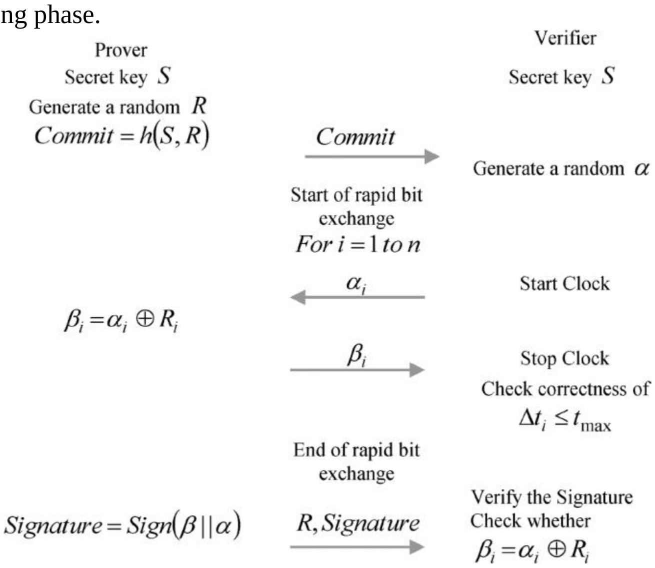

Figure-2: Distance Bounding Protocol (Brands and Chaum's protocol s)[3]

VI. ATTACKS IN DISTANCE BOUNDING

Generally Three types of attacks that are discussed under Distance-Bounding: relay attack, terrorist attack and distance attack.

A. Relay Attacks

Relay or 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 neighbor.

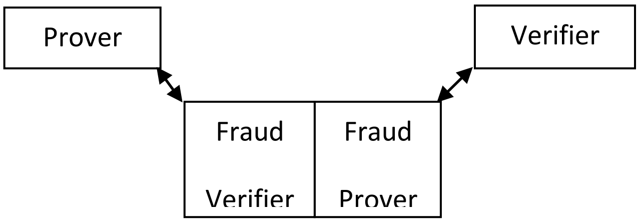

Figure-3: Relay Fraud [2]

B. Terrorist Attacks

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 neighborhood, such that the latter actively helps the adversary to maximize her attack success probability, without giving to her any advantage for future attacks.

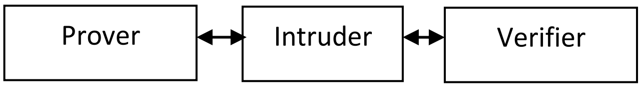

Figure-4: Terrorist Fraud [3]

C. Distance Attacks

A distance fraud is an attack where a dishonest and lonely prover supports to be in the neighborhood of the verifier network.

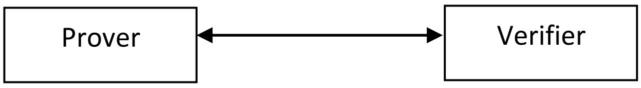

Figure-5: Distance Fraud [3]

VII. GENERALIZE SECURE NEIGHBOUR DETECTION MODEL

Following are the models for Secure Neighbor Detection

A. Directional Antenna

Directional antenna is an antenna which radiates in one or more directions allowing for increased performance on transmit and receive and reduced interference from unwanted sources. Directional antennas triangulate position using angle-of-arrival (AoA), which requires static reference nodes with antenna arrays providing fixed reference directions. These nodes must also have synchronized clocks to ensure that a transmission was made to multiple reference nodes at the same time [3].

B. Centralized Approaches

In Centralized approach we assume that there are many entities that contribute data on centralized system, from where system can check for suspicious node presence by creating and analyzing system-wide entity model [2]. This model work effectively when numbers of entities are many in numbers, not for networks like that use point-to-point RFID link or device localization using RTLS with only three reference nodes.

C. RF Fingerprinting

Radio fingerprinting is a process that identifies a physical communication channel by the unique fingerprint that characterizes its signal transmission. Each device needs to be characterized and, if nodes are mobile and subject to varying multi-path and path-loss effects, the fingerprint might need to be revised many time[4]. Thus method is prominently use in RFID devices like logistics, public transport.

VIII. PREVENTION TECHNIQUE OF ATTACKS

There are 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 [6].

IX. PREVENTION OF ATTACKS

A. Prevention of Mafia fraud

Measuring the time of flight of an electromagnetic signal in the distance bounding protocol assures that an attacker cannot be further away than (s) he pretends to be. Using this principle, not only we prevent distance fraud attacks but also mafia fraud attacks. It is a relay-type attack where the adversary is modeled as a fraudulent prover and verifier cooperating together. The fraudulent verifier interacts with the honest prover and the fraudulent prover interacts with the honest verifier.

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.

There are two extended methods to prevent terrorist fraud attack in distance bounding protocol [1].

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 [2].

X. ANALYSIS OF SECURE NEGHIBOUR DETECTION

A. Computation

In each phase calculations should be simple, otherwise they increase the round trip time. It should consider that the computation-time for each round trip is non variant.

B. Storage

RFID distance-bounding protocol must require less storage.

C. Bandwidth

Time measurements are very fragile when the parties send other messages than bits [4]. The reason is that on the one hand, fresh noise is introduced in the communication, and on the other hand, the unreliability of the transmission increases with the size of the transmitted message.

D. Reliability

Industrial applications are required to be reliable [5]. In communication environments, communication during the setup and verification stages can be transmitted via robust communication channels. However, it is likely that bit errors will occur during the exchange stage. Without sufficient error-handling the protocol will fail, and it will either require that the protocol executes again or cause the disruption of subsequent services.

XI. CONCLUSION

The security of industrial applications is important and physical location verification is one of the serious concerns in RTLS applications. Distance bounding protocol will prevent attacks by computing the distance between the prover and the verifier. We will measure round trip time to calculate the distance between two nodes for secure authentication. The analysis demonstrates the security of the protocol against a variety of attacks. Proposed system is reliable and applicable in real time system. In this paper, we have presented the basic conceptual architecture of distance bounding protocol and prevention techniques of attacks.

REFERENCES

[1] 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

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

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

[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 Using Passive Tags". IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, VOL. 58, NO. 5, MAY 2011