Volume : 4 | Issue : 4 | April 2015 • ISSN No 2277 - 8179

Research Paper

# Emerging Role of Distance Bounding Protocol with Rfid Technology in Aerospace System

Engineering

**KEYWORDS :** RFID, Mafia fraud, Distance fraud, Terrorist fraud, Distance Bounding protocol

| | |
|---|---|
| **Kavitha C** | PG Scholar,Dept.ofCSE, S.A Engineering College, Chennai |
| **Balakrishnan C** | Associate Professor, Dept.ofCSE, S.A Engineering College, Chennai |
| **Sindhuja N.R** | PG Scholar,Dept.of CSE, S.A Engineering College, Chennai |

## ABSTRACT

*RFID (Radio Frequency Identification) systems are vulnerable to replay attacks like mafia fraud, distance fraud and terrorist fraud. The distance bounding protocol is designed as a countermeasure against these attacks. These protocols ensure that the tags are in a distant area by measuring the round-trip delays during the rapid challenge response exchange. Distance Bounding protocols are cryptographic protocols which enable verifier to establish the upper bound on the physical distance to the prover. They are based on timing the delay between the sending out a challenge bit and receiving back the corresponding response bits. A timing based response followed by consecutive timing measurement provides more optimistic approach in authenticating the prover.*

## INTRODUCTION

Being resistant to both mafia and distance fraud is the primary goal of a distance bounding protocol. An important lower-bound for both frauds is $(1/2)^n$ in [6], which is the probability of an adversary who answers randomly to the n verifier's challenges during the fast phase. However, this resistance is hard to attain for lightweight DB protocols. Therefore, our aim is to design a protocol that is close to this bound for both mafia and distance frauds, without requiring costly operations and an extra final slow phase with reference to [5],[2].

Mafia fraud is an attack performed by an external attacker that physically resides closer to the verifier than the prover. The attacker aims to make one of the parties (either the prover or the verifier or both) believe that the protocol was successfully executed when, in fact, the attacker shortened the distance measurement. Distance fraud is an attack performed by a malicious prover and consists of the prover trying to shorten the distance measured by the verifier. In mafia fraud, the best protocols in terms of the distance fraud are round dependent. However, round dependency by means of predefined challenges fails to properly resist distancing fraud. Intuitively [9], [7], the higher control over the challenges the prover has, the lower the resistance to distance fraud is. For this reason, our proposal allows the verifier to have full and exclusive control over the challenges. 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 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. Terrorist fraud attack is not considered in our proposed system.

The mafia fraud is particularly powerful against the contactless technologies. The most threatening systems are Radio Frequency Identification (RFID) and Near Field Communication (NFC) because the devices answer to any solicitation without explicit agreement of their holder. The vulnerability of these technologies has already been illustrated by several practical attacks [10]. The two attacks related to mafia fraud are distance fraud and terrorist fraud. The distance fraud only involves a malicious prover, who cheats on his distance to the verifier. The terrorist fraud is an exotic variant of the mafia fraud where the prover is malicious and actively helps the adversary to succeed the attack. Measuring the physical distance between communicating parties is important for communication security. For example, we can imagine a building security system that allows a visitor to open the door to the building only when the visitor has an authorized radio frequency Identification (RFID) tag for entering the building. When authenticating the tag, the security system should also verify the upper-bound distance between the door and the tag to thwart the remote attackers who may desire to open the door from a distance between communicating parties [4]. In distance bounding protocol verifier V seeks to authenticate a prover P while measuring the distance d between V and P. For authentication, protocols rely on multi-rounds of single-bit challenge and response, known as a fast bit exchange phase. They are also light weight in the sense that they do not require an additional (time and resources consuming) slow phase to terminate the protocol. A consecutive response to the verifier provides more optimistic approach in authenticating the prover.

## SYSTEM ARCHITECTURE

By using distance bounding protocols, a device (the verifier) can securely obtain an upper bound on its distance to another device (the prover). The security of distance-bounding protocols was so far mainly evaluated by analysing their resilience to three types of attacks. In Distance Fraud attacks, dishonest provers can conspire to mislead the verifier, one prover lending the other prover its identity so that the second prover can make the first prover look closer than it is. In Mafia Fraud attacks, even if the prover is honest, an attacker tries to modify the distance that the verifier establishes by interfering with their communication.

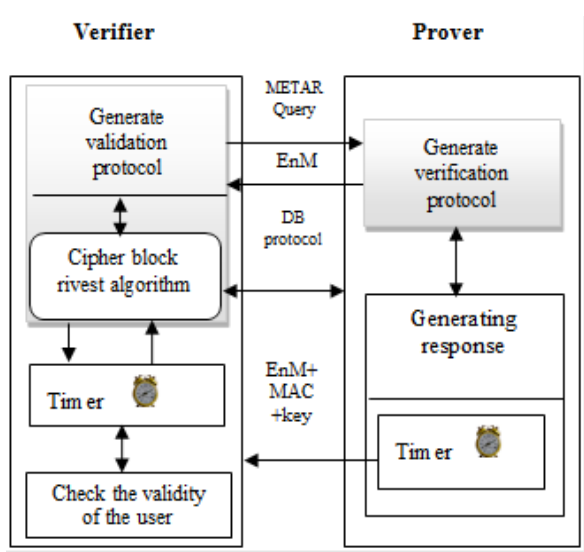


**Figure 1**: System Architecture

Volume : 4 | Issue : 4 | April 2015 • ISSN No 2277 - 8179

In Terrorist Fraud attacks, dishonest prover colludes with another attacker, to convince the verifier of a wrong distance to the prover. So far, it was assumed that distance bounding protocols that are resilient against these three attack types can be considered secure. In case of hostile attackers, the dishonest prover can pretend to be closer to or further away from the verifier than it actually is by either jumping the gun or sending a response before the request, or pretend to be further away than it is by delaying its response. The prover first commits to a nonce using a one-way function, the verifier sends a challenge consisting of another nonce, the prover responds with the exclusive-or of its and the verifier's nonce's, and then follows up with the authentication information. METAR is Meteorological elements observed at an Airport at a specific time.METAR is constructed to analyze the Weather report and cloud base height of an airplane. These details or information is passed between the verifier and prover.

The verifier uses the time elapsed between sending its nonce and receiving the prover's rapid response to compute its distance from the prover, and then verifies the authenticated response when it receives it. Through the wireless, verifier raises an authentication query to the prover side. If the prover gives an exact answer to the question means prover can able to receive the extracted information at the end.

**PROPOSED TECHNIQUE**

**Distance Bounding Protocol**

The system proposed in this paper uses the Distance Bounding protocol for secure transaction of information's in the network. Distance bounding denotes a class of protocols in which one entity (the verifier) measures an upper bound on its distance to another (untrusted) entity (the prover).Verifying the physical location of a device using an authentication protocol is an important security mechanism. Mafia fraud is a man in the middle attack against an authentication protocol where the adversary relays the exchanges between the verifier and prover, making them believe they directly communicate together.

Distance Bounding protocol aims to prove the proximity of two devices relative to each other. It determines an upper bound for the physical distance between two communicating parties based on the Round-Trip-Time (RTT) of cryptographic challenge response pairs. 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 dividing in three phase: the Commitment Phase, the Fast Bit phase and signing phase.

The first DB protocol suitable for resource-constrained devices example: RFID tags. This protocol is considered lightweight in the sense that a single computation of a hash function and a call to a Pseudo Random Number Generator (PRNG) are the most costly operations required for its execution. The simplicity and efficiency of this protocol yield to similar designs for other DB protocols which modify how answers are calculated in order to improve the security performance. The protocol first contains a slow phase in which nonce are generated and exchanged [4], [7]. From this nonce and a secret value x, the possible response used in the first phase are computed via a function f. Then the fast phase consists of n consecutive rounds. In each of these rounds, the verifier picks a challenge ci, starts a timer and sends ci to the prover. When the prover receives the challenge he computes the answer ri and sends it back to the verifier as soon as possible. Upon reception of the answer, the verifier stores as well as the round trip time. Once the n rounds are elapsed, the verifier checks the validity of the answers, i.e., the n rounds, the protocol succeeds. Initialization, execution and decision steps are presented below and a general view is provided in Fig. 2.

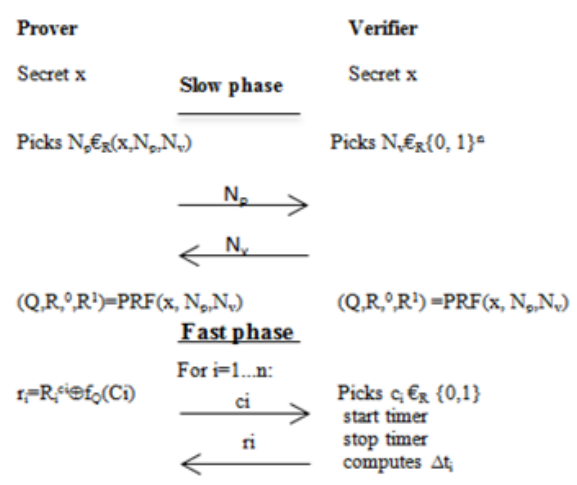


**Figure 2**: Distance Bounding Protocol

**Initialization**. The prover (P) and the verifier (V) agree on (a) a security parameter n, (b) a timing bound Δtmax, (c) a pseudo random function PRF output 3(n) bits, (d) a secret key x.

**Execution**. The protocol consists of a slow phase and a fast phase.

**Slow Phase**. P (respectively V) randomly picks a nonce NP (respectively NV) and sends it to V respectively P). Afterwards, P and V compute P RF (x, NP, NV) and divide the result into three n-bit registers Q, R0, and R1. Both P and V create the function fQ: S → {0, 1} where S is the set of all the bit-sequences of size at most n including the empty sequence. The function fQ is parameterized with the bit-sequence Q = q1 . . . qn, and it outputs 0 when the input is the empty sequence. For every non-empty bit-sequence Ci = c1 . . . ci where 1 ≤ i ≤ n, the function is defined as fQ (Ci) = Lij=1(cj∧qj).

**Fast Phase**. In each of the n rounds, V picks a random challenge ci ∈R {0, 1}, starts a timer, and sends ci to P. Upon reception of ci, P replies with ri =Rcii⊕fQ (Ci) where Ci = c1...ci. Once V receives ri, he stops the timer and computes the round-trip-time Δti.

**Decision**. If Δti< Δtmax and ri = Ri ci ⊕fQ (Ci) ∀ i ∈ {1, 2... n} then the protocol succeeds.

**Cipher Block Rivest Algorithm**

Cipher Block Rivest Algorithm is used in our proposed system for encryption process. Fast symmetric block cipher**.** Same key used for encryption and decryption algorithm. Plaintext and cipher text are fixed-length bit sequences. In cryptography, RC% is a symmetric-key block cipher notable for its simplicity. Block Ciphers plaintext is divided into blocks of fixed length and every block is encrypted one at a time. The number of rounds can range from 0 to 255, while the key can range from 0 to 2040 bits in size [7]. RC5 algorithm consists of three components: a key expansion algorithm, an encryption algorithm and a decryption algorithm. In RC5 the plaintext consist f two w-bit words and it uses an expanded key table, S [0...t-1], consisting of t=2(r+1) w bit words. The key expansion algorithm initializes S from the user's given secret key parameter K.

**Encryption**

The input block is given in two w-bit registers A and B. Assume that key-expansion has already been performed, so that array S [0...t-1] has been computed. The output is in the registers A and B. Note that each RC5 round updates both registers A and B, whereas a "round" n DES updates only half of its registers. An RC5 "half-round" (one of the assignment statements updating A or B in the body of the loop above) is thus perhaps more analogous to a DES round. Here is the encryption algorithm in pseudo code:

A=A+S [0];
B=B+S [1];
For i =1 to r do
A= ((A⊕B) <<< B) +S [2*i];
B= ((B⊕A) <<< A) +S [2*i+1];

Decryption

The decryption routine is easily derived from the encryption routine.

For i = r downto 1 do
B = ((B-S [2*i+1])>>> A) ⊕ A;
A = ((A-S [2*i] >>> B) ⊕ B; B = B-S [1];
A=A-S [0];

Key Expansion

The key expansion routine expands the user's secret key K to fill the expanded key array S, so that S resembles an array of t = 2(r+1) random binary words determined by K. The key expansion algorithm uses two "magic constants," and consists of three simple algorithmic parts.

- *Definition of Magic Constants*: The key expansion algorithm uses two word-sized binary constants $P_w$ and $Q_w$. They are defined for arbitrary $_w$ as follows:

Pw = Odd ((e-2)$2^w$)

$Q_w$ = Odd ((φ-2)$2^w$)

Where e=.718281828459... (Base of natural logarithms)

ϕ=1.618033988749… (Golden ratio),

Odd(x) is the odd integer nearest to x

- *Converting the Secret Key from Bytes to Words*: The first algorithmic step of key expansion is to copy the secret key K [0… b-1] into an array L [0…c-1] of c = ⌈b/u⌉ words, where u = w/8 is the number of bytes/word. This operation is done in a natural manner, using u consecutive bytes of K to fill up each successive word in L, low-order byte to high-order byte. Any unfilled positions of L are zeroed. On "little endian" machines such as an Intel'486, the above task can be accomplished merely by zeroing the array L, and then copying the string K directly into the memory positions representing L. The following pseudo-code achieves the same effect, assuming that all bytes are "unsigned" and that array L is initially zeroed.

For i = b-1 downto 0 do

L [i/u] = (L [i/u] <<< 8) +k[i];

*[1]nitializing the Array S*: The second algorithmic step of key expansion is to initialize array S to a particular fixed (key-independent) pseudo-random bit pattern, using an arithmetic progression modulo $2^w$ determined by the "magic constants" $P_{w \text{ and } Q_{w.}}$ Since $Q_w$ is odd, the arithmetic progression has period $2^{w.}$

S [0] = $P_{w:}$
For i = 1 to t-1 do
S [i] = S [i-1] = $Q_w$;

Mixing in the secret Key: The third algorithmic step of key expansion is to mix in the user's secret key in three passes over the arrays S and L. More precisely, due to the potently different sizes of S and L, the larger array will be processed three times, and the other may be handled more times.

i= j = 0;
A = B =0;
Do 3*max (t, c) times:
A = S[i] = (S [i] + A + B) <<<3;
B = L [j] = (L [j] + A + B) <<< (A+B);
i = (i +1) mod (t);
j = (j+1) mod(c);

The key-expansion function has a certain amount of "one-wayness": it is not so easy to determine K and S.

**TECHNOLOGY USED**

The major and primary security concern of RFID is that anyone can access the RFID data because there is no line of sight problem and be able to gather data. In addition, people are cloning RFID tags and using them just as the way it was done for credit cards before. Preventing effective cloning of RFID tags is still an open and challenging problem. Criminals with RFID readers could scan crowds for high-value banknotes. And terrorists could scan digital passports to target specific nationalities.

The Interface RFID frequency identification (RFID) technology consists of small inexpensive computational device with wireless communication adequacy. In recent years, the main application of RFID technology is in inventory control and supply chain management fields. RFID tags are used to tag and track the physical goods. Within this context, RFID can be considered a replacement for barcodes. RFID technology is superior to barcodes in two aspects. First, RFID tags can store information than barcodes [3]. Unlike a barcode, the RFID tag, being a computational device, can be designed to process rather than just store data. Second, barcodes communicate through an optical channel, which require the careful positioning of the reading device with no obstacles in-between [2], [10]. RFID uses a wireless channel for communication, and can be read without line-of-sight which increases the reading efficiency. The pervasiveness of RFID technology in our everyday lives has led to concerns over these RFID tags pose any security risk. The future applications of RFID make the security of RFID networks and communications even more important than before. The ubiquity of RFID technology has made it an important component in the Internet-of-Things (IoT), a future generation Internet that seeks to mesh the physical world together with the cyber world.

The operation of the RFID tag is described below: Handshaking with the Reader (interrogator):

- The reader continuously emits RF carrier signals, and keeps observing the received RF signals for data.
- The presence of a tag ( for our discussion, we consider only passive tag) modulates the rf field, and the same is detected by the reader.
- The passive tag absorbs a small portion of the energy emitted by the reader, and starts sending modulated information when sufficient energy is acquired from the rf field generated by the reader. Note that the data modulation (modulation for 0s and 1s) is accomplished by either direct modulation or FSK or Phase modulation.

Volume : 4 | Issue : 4 | April 2015 • ISSN No 2277 - 8179

- The reader demodulates the signals received from the tag antenna, and decodes the same for further processing.

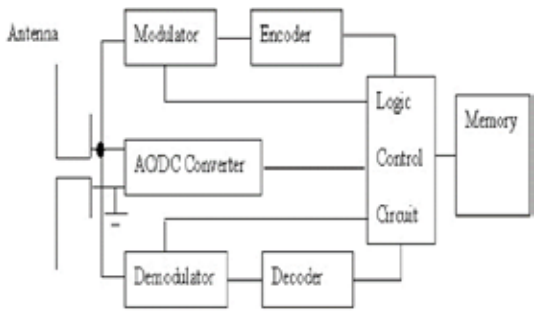


**Figure 3**: The Block Diagram of RFID TAG

**RFID Building Blocks:**

- Tags: A tag is the data carrier and normally contains the ID number, and unique EPC code programmed into the Tag.
- Tag Antenna: The tag antenna is connected to the chip in tag. It could be wire or printed using conductive ink.
- Reader Antenna: It is a coil included in plastic or similar case, and normally measures 12 -18 inches square
- Reader: A reader captures the data provided by the tag within the detectable area of the Reader.

**TOWARD SECURE IDENTIFICATION**

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 [7], [11]. He wants to prevent a fraud proverclaiming to be closer. Different types of mechanism that prevent these attacks are:

- *Signal strength Measurement:* 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 compute distance.

- *Total Round Trip Time:*Another solutions measure the round trip time. The round trip time is the time required for exchange a packet from 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 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.

- *Consecutive Time Measurement:* Timing based input information followed by consecutive timing measurement provides more optimistic approach in authenticating the user. The verifier uses the time elapsed between sending its nonce and receiving the prover's rapid response to compute its distance from the prover, and then verifies the authenticated response when it receives it. Our proposed system provides a proof breaks down concept if the prover is dishonest.

**CONCLUSION**

The consecutive based distance bounding protocol has been introduced in this paper which provides the optimistic approach to identify the relay attack. This protocol thwarts both mafia and distance frauds with less computation memory. For computer-intensive systems, our consecutive timed response provides significantly better throughput for a broad variety of scenarios, including the mafia fraud, distance fraud and terrorist fraud attack. The encryption and decryption can use more than one different algorithm on each round of the resistance, which provides more confidential services in the system.

## REFERENCE

[1] Ronalndo Trujillo-Rasua, Benjamin Martin, and GildasAvoine, "Disrance-bounding facing both mafia and distance frauds", IEEE Transactions on Wireless Communications, vol 9, May 2014. | [2] Sangho Lee, Jin SeokKim, Sung Je Hong, and Jong Kim, "Distance Bounding with Delayed Responses", IEEE Communications Letters, vol. 16, September 2012. | [3] Kapil Singh, "Security in RFID Networks and Protocols", International Journal of Information and Computation Technology, vol.3, pp.425-432, 2013. | [4] Srikanth S P, SunithaTiwari, "A Survey on Distance Bounding Protocol for attacks and frauds in RTLS system", International journal of Engineering and Innovative technology (IJEIT), vol.3, April 2014. | [5] Claus P. Schnorr, "Efficient signature generation by smart cards", Journal of Cryptology, vol.4, no.3, pp. 161-174, 1991. | [6] Capkun, Srdjan and EI Defrawy, Karim and Tsudik, Gene. "GDB: Group Distance Bounding Protocols", arXiv.org, 2010. | [7] G. Avoine, C. Lauradoux, B. Martin, "How secret-sharing can defeat terrorist fraud", The 4th ACM Conference on Wireless Network Security, WiSec'11, pp.145-156. | [8] G. Avoine "RFID, Distance Bounding Multiple Enhancement", progress in cryptography, pp.290-307. | [9] J. Munilla, A. Painado, "Distance Bounding Protocol for RFID enhanced by using void challenges and analysis in noise channels", compute 8(2008) 1227-1232. | [10] J. Kelsey, B. Schneier, and D. Wagner, "Protocol interactions and the chosen protocol attack", 5th International Workshop on Security Protocols, volume 1361 of LNCS, pages 91{104. Springer, 1997. | [11] A. Mitrokotsa, C. Dimitrakakis, P. Peris-Lopez, and J. C. Hernandez-Castro, "Reid et al.'s Distance Bounding Protocol and Mafia Fraud Attacks over Noisy Channels, IEEE Communications Letters, Vol.14, No. 2, February 2010. |