Journal of Information Security and Applications 42 (2018) 87–94

Contents lists available at ScienceDirect

Journal of Information Security and Applications

journal homepage: www.elsevier.com/locate/jisa

# Performing and mitigating force and terrorist fraud attacks against two RFID distance-bounding protocols

Azadeh Imani Rad[a], Mahdi R. Alagheband[b,*], Saeed Banaeian Far[b]

[a] Department of Electrical Engineering, Yadegar -e- Imam Khomeini (rah), shahr-e-rey Branch, Islamic Azad University, Tehran, Iran
[b] Department of Electrical and Computer Engineering, Science and Research Branch, Islamic Azad University, Tehran, Iran

ARTICLE INFO

*Article history:*

*Keywords:*
Distance-bounding protocols
Force attack
RFID
Terrorist fraud attack

ABSTRACT

Radio frequency identification (*RFID*) systems have been used in widespread applications to identify any object. The growth of wireless systems has caused security and privacy vulnerabilities in *RFID* systems with limited resources and low cost provers. Authentication allows that the information is transfered between only authorized people; thus, we allow different levels of access to information for different people. Distance-bounding authentication protocols are one of the most efficient methods for authentication in *RFID* systems. Distance-bounding protocols have been proposed to address attacks related to location such as distance fraud attack, Mafia fraud attack, and terrorist fraud attack. In this paper, we examine the two new proposed distance-bounding protocols *MP*, and *KA* and prove that these protocols are vulnerable against terrorist fraud attack and force attack. Finally, we improve these two schemes. Then we show that our two improved protocols are resistant against the attacks.



## 1. Introduction

Radio frequency identification (*RFID*) systems are used in various applications, such as transportation, tracking of objects and animals, electronic passports, and identification cards. Each *RFID* system has three parts: end-servers, card verifiers and provers. The prover is connected to the object that needs to be identified and the verifier has the task of collecting information related to identification. This information is then provided to the end-server [20].

*RFID* was discovered by Faraday in the mid-nineteenth century and is rooted in discoveries between 1900 and 1940, in radio and radar technologies. *RFID* is not a new technology and was first used in military applications. It was used in World War *II* for an application called Identification Friend or Foe (IFF) with the idea of gathering information about whether an aircraft is a friend or foe by detecting radio signals. *RFID* systems were used in the 70s for the security of small systems, in the 80s for data-collection systems, and in the 90s for a variety of applications, e.g., toll collection and accessing the control systems. *RFID* has also become a very popular technology in the current decade and has been used as an alternative to barcodes and optical companies. It is now widely used with great satisfaction. *RFID* is an automatic identification system of objects or people using radio waves. In the past, barcodes were used for identification, but *RFID* is used today instead of barcodes for the following reasons: *A*) there is no need for direct line of sight, and *B*) it is a possibile to identify objects uniquely, while a barcode only identifies the type of genus [21].

Providing security and maintaining privacy in *RFID* systems is very costly. *RFID* systems have limited resources and provers should be of low cost. Hence, we need an effective method to protect data in these systems. Distance-bounding protocols (DBP) have been examined as one of the most efficient methods for authentication in *RFID* systems [15,21].

In this paper we describe two DBPs (*MP* and *MP* [4,5]). We analyze them and prove that the protocols are vulnerable against both terrorist fraud and force attacks. Then, we alleviate them and analyze their alleviated protocols. We only use one more hash function and *XOR* operator for modification. So, prover and the adversary cannot cooperate together. Finally, we show the alleviated protocol have security against terrorist fraud and force attacks.

*Paper organization:* In the Section 2, we discuss the threats with which *RFID* systems are faced. After describing the works conducted on DBPs in the Section 3, we specify assessment and evaluation criteria of DBPs in the Section 4. In the Section 5, we describe and analyze two DBPs, *MP* and *KA* [4,5], in this section we show that these protocols are vulnerable to terrorist fraud attacks and force attack. Finally, in the Section 6, we compare them with their improvements to these protocols and show that our improved protocol does not suffer from the specified vulnerabilities.

* Corresponding author.
*E-mail addresses:* m.alaghband@srbiau.ac.ir (M.R. Alagheband), Saeed.banaeian@srbiau.ac.ir (S.B. Far).

https://doi.org/10.1016/j.jisa.2018.07.010
2214-2126/

## 2. RFID Threats

For the sake of simplciy, we explain *RFID* threats and model in short. There are many threats to *RFID* systems, such as distance fraud, mafia fraud and terrorist fraud [13]. These threats can be protected against by using DBPs. Note that designing the DBP resisted against all of threats is hard. Regarding to the needs of user, it can use one of the existing protocols [16,17]. In the following, we discuss these frauds:

- **Distance Fraud Attack:** This attack occurs when the prover wants to prove that its distance has been underestimated and obtain a closer distance by deceiving the verifier. However, this closer distance is not the true distance and the fraudulent prover is not in the allowed area [9,21]. To resist against distance fraud attack, can be related response and challenge together. As a result, fraudulent prover can not send response before receive the challenge.
- **Mafia Fraud Attack:** Mafia fraud attack occurs when the prover and the verifier are authenticated, but they are far from each other. The adversary wants to be between the prover and the verifier; this would cause the distance between the prover and the verifier to be underestimated. The adversary relays the connection between the prover and the verifier. This fraud may be detected by using DBPs to measure the additional delay in the round-trip time of the signal [13,21]. If two parameters including secret key and random number are applied for the response generation, DBPs can be secure against mafia attack. For example, $\mathcal{A}$ can generate $n_1$ and $n_2$ in response $h(SK\|r) = n_1\|n_2$.
- **Terrorist Fraud Attack:** In this attack, the prover cooperates with the adversary. The malicious prover is far from the verifier, But, $\mathcal{A}$ is near to it. The malicious prover provides the secret data of the protocol to the adversary, but the adversary cannot obtain the secret key ($k$) [9,13]. The protocol can be design that if malicious prover and $\mathcal{A}$ cooperate together, an adversary can not obtain the secret key.

## 3. Related work

In 1993, Brands and Chaum presented the first DBP [1]. This protocol has a final slow phase that contains signature and commitment. The final phase introduces a heavy overhead and requires an additional message to be transmitted. In 2005, Hancke and Kuhn proposed another DBP which is known as *HK* [2], and it is a milestone in this area. The challenge-and-response flows are transfered in a fast bit-exchange step without any final bit-exchange step.

There are two main families of DBPs: the *BC*-family protocols and *HK*-family protocols. Since *HK* is vulnerable to terrorist attacks, Reid et al. proposed an improved protocol in 2006 [3] however, this protocol does not provide privacy protection. In 2007, the *SP* protocol was proposed, through error correction codes and message-authentication codes to reduce the noise of the channel in the fast bit-exchange step [18]. However, the safety and the actual cost of *RFID* provers in the *SP* protocol were questioned by others. In 2008, Munilla and Peinado modified the *HK* protocol using void challenge to reduce the probability of the adversary's success; this protocol is known as *MP* [4].

Trujillo-Rusua et al. in [19] proposed a DBP, called Poulidor, based on graphs. It does not provide the best security against distance fraud or mafia fraud. This protocol uses a linear memory [19]. In 2011, Kim and Avoine proposed the *KA* protocol, which is based on a combinational scheme of random challenges and predefined challenges [5,10]. This protocol is a combination of two types of protocols, *KA*1 and *KA*2. Both protocols are resistant to mafia fraud attack. *KA*1 and *KA*2 protocols need memory bits; however, the author shows that *KA*2 needs half as much memory as *KA*1, and has increased robustness against distance fraud. In 2014, Baghernezhad et al. [7] proposed an improvement of the *JF* protocol (*BSB*), which is robust against the key-recovery attack but vulnerable to terrorist fraud. Jannati and Falahati proposed a protocol named *JF* [8] in 2012; pre-defined challenges and random challenges are used in each round. Although the authors clamed that the *JF* is robust against terrorist fraud, as distance fraud, and mafia fraud, Baghernezhad et al. showed the this protocol is vulnerable to key recovery-attack[7,9], resulting in vulnerability to mafia fraud and terrorist fraud [7]. Using key-recovery attack, the adversary's probability of success in distance fraud and terrorist fraud is maximal.

Moreover, Trujillo-Rasua et al. proposed a DBP in 2014, known as *TMA*[6]. All previous challenges in the current round of the protocol are used in forming the intended response of the verifier. It is robust against distance and mafia frauds, but it is vulnerable to terrorist fraud. In the same year, Entezari et al. presented the *EBT* protocol, which resists against mafia fraud attack and distance fraud attack [22]. Since it never directly uses a bit of key in its responses, it is also resistant to key-recovery attack. However, it is vulnerable to terrorist attack and force attack.

Two years later, Karlsson and Mitrokotsa proposed the Grouping-Proof (GP) protocol based on elliptic curves and decisional Diffie-Hellman problems [23]. It uses asymmetric encryption. This protocol is not secure against terrorist fraud attack.

**Table 1**
List of Notations.

| Parameters | Description |
|---|---|
| $\mathcal{P}$ | The Prover |
| $\mathcal{V}$ | The verifier |
| $\mathcal{A}$ | The Adversary |
| $N_V$ | The random nonce generated by verifier |
| $N_P$ | The random nonce generated by prover |
| $PRF$ | Pseudorandom Function |
| $n$ | Number of rounds in the fast phase |
| $k$ | The secret key shared between prover and verifier |
| $c_i$ | The $i$*th* challenge sent by verifier |
| $r_i$ | The $i$*th* response sent by prover |
| $\oplus$ | *XOR* operator |
| $P_{dist}$ | The $\mathcal{A}$'s provable success function |
| $\Delta T_i$ | The time difference in the $i$*th* round |
| $\Delta T_{\max}$ | Maximum allowed time difference |

## 4. Evaluation of distance-Bounding protocols

Distance-bounding protocols are evaluated with respect to various characteristics [12]. These characteristics are categorized in two groups: *security-related* and *implementation-related* [14]. According to these characteristics, the appropriate protocol can be selected. Note that the used parameters in this paper shown in Table 1.

### 4.1. Security feature

The goal of the security challenges is to reduce the probability of attacker success.

- **Resistance Against Distance Fraud:** This fraud was discussed in Section 2. The purposes of security is to prevent the attack. $\mathcal{A}$'s probability of successfully overcoming the protocol indicates the resistance or non-resistance against the fraud. One goal of creating *BC* protocols is to prevent this attack.
- **Resistance Against Mafia Fraud:** As discussed in Section 2, this attack cannot be prevented in *RFID* systems with encryption. DBPs have been created to prevent this fraud. In examining the security features of a DBP, the probability of $\mathcal{A}$'s success in the fraud is considered.