

Reid et al.'s Distance Bounding Protocol and Mafia Fraud Attacks over Noisy Channels

A. Mitrokotsa, C. Dimitrakakis, P. Peris-Lopez, J. C. Hernandez-Castro

Abstract—Distance bounding protocols are an effective countermeasure against relay attacks including distance fraud, mafia fraud and terrorist fraud attacks. Reid *et al.* proposed the first symmetric key distance bounding protocol against mafia and terrorist fraud attacks [1]. However, [2] claims that this is only achieved with a $(7/8)^n$ probability of success for mafia fraud, rather than the theoretical value of $(3/4)^n$ (for n rounds) achieved by distance bounding protocols without a final signature. We prove that the mafia fraud attack success using the Reid *et al.* protocol is bounded by $(3/4)^n$ and reduces as noise increases. The proof can be of further interest as it is the first – to the best of our knowledge – detailed analysis of the effects of communication errors on the security of a distance bounding protocol.

Index Terms—Contactless smart cards, RFID, distance bounding protocols, relay attacks, mafia fraud attacks

I. INTRODUCTION

A number of secure and efficient authentication protocols for RF transponders such as contactless smart cards and RFID tags have been proposed recently. Most assume proximity between readers and transponders due to limited radio channel range. However, an intruder located between the tag T (prover) and the reader R (verifier), can trick the latter into thinking that T is in close proximity. This attack can be divided into three subcategories:

a) Distance fraud: The attacker is a fraudulent tag \bar{T} . The attack involves \bar{T} convincing the legitimate reader R of being nearer to the legitimate tag T than it really is.

b) Mafia fraud [3]: The attacker A is a pair $A = \{\bar{T}, \bar{R}\}$: \bar{T} is a fraudulent tag interacting with the legitimate reader R and \bar{R} is a fraudulent reader interacting with the legitimate tag T . Using \bar{R} , \bar{T} convinces R that the latter communicates with the legitimate tag T while in reality it communicates with the attacker A . This is achieved without the disclosure to A of the private key shared between T and R .

c) Terrorist Fraud: The attacker $A = \{T, \bar{T}\}$ is a pair of two colluding parties: a legitimate tag T and a terrorist tag \bar{T} . The attack enables \bar{T} to convince the legitimate reader R of an assertion related to the private key of T . In this attack although the legitimate tag T is dishonest and cooperates with

the terrorist tag \bar{T} , the secret key shared between the legitimate tag and reader is not revealed to the terrorist tag \bar{T} .

Distance bounding protocols were introduced in [4] to hinder distance fraud and mafia fraud attacks, by measuring the round trip delays during a rapid challenge-response exchange of n bits to infer an upper bound on the distance between the verifier and the prover. Subsequently [5] proposed a distance bounding protocol offering protection against mafia fraud only. Later, Reid *et al.* proposed a new protocol [1] with the objectives of (a) being resistant to both mafia and terrorist fraud, and (b) suitable for low-cost RFID tags. This work can be considered a reference point in the design of distance bounding protocols for constrained RF tags. Indeed, key ideas of [1] are used in recent proposals as in [6].

Contribution: We analyse the security of Reid *et al.*'s protocol (henceforth RP) against mafia fraud attack under noisy conditions. Due to power constraints and the wireless medium, RFID systems are particularly susceptible to noise, but its effect on the attacker has not been studied previously. In addition, we clarify RP's security under noise-free conditions. More specifically, [2] claims that the probability of success for a mafia fraud attack is bounded by $(7/8)^n$. However, this claim is based on an incorrect assumption about the Key Derivation Function (KDF) used in the protocol: that if the adversary can control $3/4$ bits of the input to the KDF, then he can guess the output of the KDF more easily. However, the KDF is indistinguishable from a uniform distribution unless all bits are known [1]. Nevertheless, [2] is commonly cited as evidence for the low security of RP. In this paper, we prove that the attack success probability is upper bounded by $(3/4)^n$ in noise-free conditions and refine the results of [5] by showing that it decreases polynomially as noise increases.

Notation: We consider sequences $x = x_1, \dots, x_n$ with all x_i in some alphabet \mathcal{X} and $x \in \mathcal{X}^n$. We write $\mathcal{X}^* \triangleq \bigcup_{n=0}^{\infty} \mathcal{X}^n$ for the set of all sequences. The concatenation of x with some $y \in \mathcal{X}^m$ is written as $x|y \in \mathcal{X}^{m+n}$. If $x, y \in \mathcal{X}^n$ then $x \oplus y \in \mathcal{X}^n$, where \oplus is an appropriate operator (XOR for $\mathcal{X} = \{0, 1\}$). $\mathbb{P}(A)$ denotes the probability of event A , while \triangleq implies a definition.

II. REID ET AL.'S PROTOCOL

In RP [1], the reader R and tag T , whose identifiers are $ID_R, ID_T \in \mathcal{X}^*$ respectively, share a common secret $x \in \mathcal{X}^n$. The messages exchanged are:

- 1) $R \rightarrow T$: The reader chooses a random number $y_B \in \mathcal{X}^m$ and transmits it and its identity ID_R to the tag.
- 2) $T \rightarrow R$: The tag chooses a random number $y_A \in \mathcal{X}^m$ and transmits it and its identity ID_T to the reader.

A. Mitrokotsa and P. Peris-Lopez are with the ICT Group, Technical University of Delft (a.mitrokotsa@tudelft.nl).

C. Dimitrakakis is with the Informatics Institute, University of Amsterdam (christos.dimitrakakis@gmail.com).

J. C. Hernandez-Castro is with the School of Computing, University of Portsmouth (Julio.Hernandez-Castro@port.ac.uk).

This work was supported by the Netherlands Organization for Scientific Research (NWO) under the RUBICON grant "Intrusion Detection in Ubiquitous Computing Technologies" and the ICIS project, supported by the Dutch Ministry of Economic Affairs, grant nr: BSIK03024.

It is easy to see that:

$$A = \mathbb{P}(s_i | \hat{c}_i = c'_i) = BD + C(1 - D) \quad (3)$$

In order to further simplify the derivation, we shall also define the following: $x_0 \triangleq c_i$, $x_1 \triangleq c'_i = \hat{c}_i$, $x_2 \triangleq \hat{c}'_i$, $\varepsilon_1 \triangleq \varepsilon_{RA}$, $\varepsilon_2 \triangleq \varepsilon_{AT}$.

It can now be easily seen that x_0, x_1, x_2 form a three stage Markov chain, which satisfies the assumptions of Lemma 1 (see Appendix) for $n = 2$. Applying the lemma, we obtain:

$$\begin{aligned} \mathbb{P}(x_n = x_0) &= \mathbb{P}(x_2 = x_0) = \mathbb{P}(\hat{c}'_i = c_i) = \\ &= \sum_{l=1}^2 \frac{\varepsilon_l}{k-1} \prod_{j=l+1}^2 \frac{k(1-\varepsilon_j)-1}{k-1} + \prod_{j=1}^2 \frac{k(1-\varepsilon_j)-1}{k-1} = F \end{aligned} \quad (4)$$

Similarly, we may set: $y_0 \triangleq r_i(\hat{c}'_i)$, $y_1 \triangleq \hat{r}_i = r'_i$, $y_2 \triangleq \hat{r}'_i$, $\varepsilon'_1 \triangleq \varepsilon_{TA}$, $\varepsilon'_2 \triangleq \varepsilon_{AR}$ to obtain:

$$\begin{aligned} \mathbb{P}(y_n = y_0) &= \mathbb{P}(y_2 = y_0) = \mathbb{P}(\hat{r}'_i = r_i(\hat{c}'_i) | \hat{c}_i = c'_i) = \\ &= \sum_{l=1}^2 \frac{\varepsilon'_l}{k-1} \prod_{j=l+1}^2 \frac{k(1-\varepsilon'_j)-1}{k-1} + \prod_{j=1}^2 \frac{k(1-\varepsilon'_j)-1}{k-1} = D \end{aligned} \quad (5)$$

After some calculations, we can simplify the expressions for B, C to $B = F + \theta - \theta F$ and $C = \frac{1-F}{k-1}$, since:

$$\mathbb{P}(\hat{r}'_i = r_i(c_i) | \hat{c}_i = c'_i, \hat{r}'_i \neq r_i(\hat{c}'_i), \hat{c}'_i \neq c_i) = \frac{1}{k-1}.$$

If we assume $\varepsilon_{AT} = \varepsilon_{TA} = \varepsilon_{RA} = \varepsilon_{AR} = \varepsilon$, Corollary 1 applies and equations (4) and (5) can be condensed to:

$$F = D = \frac{\varepsilon}{(k-1)} \frac{1-z^n}{1+z^n} + z^n, \quad (6)$$

where $z = \frac{k(1-\varepsilon)-1}{k-1}$ and $n = 2$.

Finally, by equation (3) and the theorem's assumption that $\theta = 1/k$ and substituting B and C we get:

$$A = \frac{F^2(k-1) + F}{k} + \frac{(1-F)^2}{k-1} \quad (7)$$

Using (6), (7) and (3) we obtain the final result, where the probability of a successful attack only depends on the noise ε , the alphabet size k and the number of rounds n . ■

For $\varepsilon = 0$, equation (6) becomes $\mathbb{P}(s_i) = \frac{2k-1}{k^2}$. Assuming $k = 2$, we obtain $\mathbb{P}(s_i) = \frac{3}{4}$ and via independence of consecutive successes, a total success probability of $(3/4)^n$ over n rounds in the rapid bit exchange. Thus, we recover Theorem 1 and the original result of [1].

The success probability for increasing ε is shown in Fig. 2 for $k \in \{2, 4, 6, 8\}$. One may also see that a successful attack becomes less likely with increased alphabet size, or noise. A larger alphabet may result in either a longer transmission time (which is undesirable) or larger error probabilities, depending on the encoding. On the other hand, increased noise reduces the probability of successful authentication of a legitimate tag (see [5], Sec. 3.2). We may choose n, k , and a tolerance threshold [1], [5] to trade off transmission times with guarantees for false accept or reject rates. This is possible if a bound on the error is known, and the costs of transmission and false acceptance or rejection are well defined. However, we do not examine this issue here.

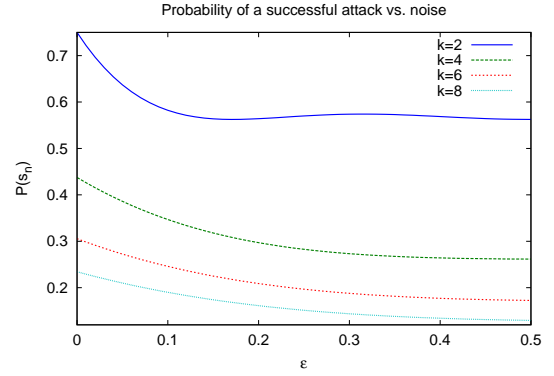


Fig. 2. Probability of Mafia Fraud attack vs. Noise for alphabet size k

IV. CONCLUSIONS

We have proved that Reid *et al.*'s protocol is secure against mafia fraud attacks. The probability that an intruder can trick the verifier into thinking that the prover is in close proximity is bounded by $(3/4)^n$ and reduces as noise increases. The result can be extended to the use of a threshold for tolerating a small number of errors [5] by plugging the expression for $\mathbb{P}(s_i)$ in the binomial cumulative distribution function. The security of this protocol can be further increased to $(1/2)^n$ by the inclusion of a signed message of the $2n$ bits sent in the rapid-bit exchange phase [4], [6]. However, such a signed message must be sent by normal communication with error correction [7], which increases authentication time.

REFERENCES

- [1] J. Reid, J. M. Gonzalez Nieto, T. Tang, and B. Senadji, "Detecting relay attacks with timing-based protocols," in *Proc. ASIACCS'07*. ACM, 2007, pp. 204–213.
- [2] S. Piramuthu, "Protocols for RFID tag/reader authentication," *Decision Support Systems*, vol. 43, no. 3, pp. 897–914, 2007.
- [3] Y. Desmedt, "Major security problems with the "unforgeable" (Feige)-Fiat-Shamir proofs of identity and how to overcome them," in *Proc. SecuriCom '88*, Mar. 1988, pp. 147–159.
- [4] S. Brands and D. Chaum, "Distance-bounding protocols," in *Proc. EUROCRYPT'93*, ser. LNCS, vol. 765, 1994, pp. 344–359.
- [5] G. Hancke and M. Kuhn, "An RFID distance bounding protocol," in *Proc. SECURECOMM'05*, Sept. 2005, pp. 67–73.
- [6] C. H. Kim, G. Avoine, F. Koeune, F.-X. Standaert, and O. Pereira, "The Swiss-knife RFID distance bounding protocol," in *Proceedings of ICISC '08*, ser. LNCS. Springer-Verlag, Dec. 2008.
- [7] C. H. Kim and G. Avoine. (2009) RFID distance bounding protocol with mixed challenges to prevent relay attacks. Cryptology ePrint Archive, Report 2009/310. [Online]. Available: <http://eprint.iacr.org/2009/310.pdf>

V. APPENDIX

Lemma 1: Assume a Markov chain x_0, x_1, \dots, x_n with $x_i \in \mathcal{X}$ and $|\mathcal{X}| = k$. The chain has the property that, for some $\{\varepsilon_i\}_{i=1}^n$ with $\varepsilon_i \in [0, 1]$: $\mathbb{P}(x_i \neq x_{i-1}) = \varepsilon_i$, for $i = 1, \dots, n$. In addition, $\mathbb{P}(x_i = x | x_i \neq x_{i-1}) = \frac{1}{k-1}$, $\forall x \neq x_{i-1}$. Then, $\mathbb{P}(x_n = c | x_0 = c)$ equals:

$$\sum_{l=1}^n \frac{\varepsilon_l}{k-1} \prod_{j=l+1}^n \frac{k(1-\varepsilon_j)-1}{k-1} + \prod_{j=1}^n \frac{k(1-\varepsilon_j)-1}{k-1}.$$

Corollary 1: If $\varepsilon_i = \varepsilon$ for all i , then for any $n \geq 1$:

$$\mathbb{P}(x_n = c | x_0 = c) = \frac{\varepsilon}{k-1} \frac{1-z^n}{1-z} + z^n, \quad z = \frac{k(1-\varepsilon)-1}{k-1}.$$