Research Article

A Secure Distance-Bounding Protocol with Mutual Authentication

Weiwei Liu ¹, Hua Guo ², and Yangguang Tian ³

¹*School of Mathematics and Statistics, North China University of Water Resources and Electric Power, Zhengzhou, China*

²*Institute of Cybersecurity and Cryptology, School of Computing and Information Technology, Beihang University, Beijing 100191, China*

³*Cyber Security Engineering Area Graduate School of Engineering, Osaka University, 2-1 Yamadaoka Suita, Osaka, Japan*

Correspondence should be addressed to Weiwei Liu; liuweiwei@ncwu.edu.cn

Received 24 December 2020; Accepted 26 April 2021; Published 1 June 2021

Academic Editor: Yinghui Zhang

Copyright © 2021 Weiwei Liu et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Distance-bounding protocol is a useful primitive in resisting distance-based attacks. Currently, most of the existing distance-bounding protocols usually do not take the reuse of nonces in designing the protocols into consideration. However, there have been some literature studies showing that nonce repetition may lead to the leakage of the shared key between protocol participants. Aikaterini et al. introduced a countermeasure that could serve as a supplementary in most distance-bounding systems allowing nonce repetition. However, their proposal only holds against passive attackers. In this paper, we introduce an active attack model and show that their countermeasure is insecure under the proposed active attack model. We also discover that all existing distance-bounding protocols with mutual authentication are vulnerable to distance-based attacks if a short nonce is applied under the proposed active model. To address this security concern, we propose a new distance-bounding protocol with mutual authentication to prevent distance-based attacks under the active adversary model. A detailed security analysis is presented for the proposed distance-bounding protocol with mutual authentication.

1. Introduction

With the rapid development of information technology like 5G, more and more people enjoy the convenience brought by various location-based services provided by service providers. Distance-based attacks enable dishonest users to cheat on their real locations and thus may cause serious economic losses to the merchants. Distance-bounding protocols play a significant role in resisting distance-based attacks since they enable one entity to decide an upper bound on the distance of the other entity contacting with him/her. Distance-bounding protocol is first proposed to preclude relay attack (mafia fraud attack) which is essentially one type of man-in-the-middle attacks by measuring the round-trip times of messages exchanged between the prover and the verifier. The relay attack could be further derived into two variants: one is a distance fraud attack, and the other is a terrorist fraud attack. The distance fraud and terrorist fraud attacks are mainly incurred by the

unreasonable design of distance-bounding protocols. Unfortunately, distance-bounding protocol, which is the only primitive that we employ to achieve both identity and distance verification, will be still used in many different security applications in the long future.

The idea of measuring round-trip time to estimate the distance between parties was first proposed by Brands and Chaum in 1993 [1]. However, due to the randomness of response bit in the rapid-bit exchange (RBE) phase, the first distance-bounding protocol achieves neither distance fraud nor terrorist fraud resistance. Furthermore, there have been many controversies about the usage of computing-expensive operations to be an exact public-key-based signature in their design. Since the most likely applications—RFID—tags are often equipped with limited computing capability, Hancke and Kuhn proposed a new distance-bounding protocol which is more compatible with RFID applications by eliminating computing-expensive operations in the slow phase [2]. They used a pseudorandom function which takes

two nonces and a secret key as inputs to generate a $2n$ bit sequence regarded as a response in the RBE phase. This provides certain assurance for reducing the success probability of a dishonest prover in launching distance fraud attacks. However, their construction can resist distance fraud attacks. What is more, it has been known that pre-strategy attacks will help a mafia fraud attacker obtain an extra advantage in cheating the verification distance. There are a few works trying to improve Hancke and Kuhn's distance-bounding protocols so as to reduce the success probability of potential adversaries in launching relay attacks at the RBE phase, such as [3–5]. While some variants of Hancke and Kuhn's protocol try to combat terrorist fraud attack by using a secret key as a seed for generating the response set at the slow phase based on an assumption that the (dishonest prover) adversary cannot send all the computed information to another adversary [6–8], however, the improved protocols still suffer from a new attack named key-learning attack where an adversary can recover the secret key bit by bit when repeating nonces. There are also some recent works focusing on protecting the prover's privacy from dishonest verifiers [9–11]. A recent work by Aikaterini et al. [12] makes a formal analysis about the relationship between the security of the secret key and the length of nonces used. Avoine et al. proposed another method to resist the terrorist fraud attack in which secret sharing technique [13] is employed. Capkun et al. gave rise to the first distance-bounding protocol for mutual authentication [14]; nevertheless, their protocol is based on the assumption that the prover has to be equipped with considerable computing capability. This does not scale well as RFID tag usually has limited storage and computation resource. To tackle this problem, Yum et al. proposed a new system based on Hancke and Kuhn's construction by only using a direction bit to control a user (who is involved in the protocol) to act as either a verifier or prover probabilistically [15]. Subsequently, Avoine et al. pointed out that distance-bounding protocol for mutual authentication [15] had been over-estimated and presented a generic solution for converting all previous distance-bounding protocols for unilateral authentication to mutual authentication [16].

1.1. Our Contributions. Aikaterini et al. proposed a novel research result that the security of certain distance-bounding protocols [9, 12, 17, 18] depends on the length of nonces [12]. The authors also came up with a countermeasure to reduce the success probability of an adversary in launching an impersonation attack when the repetition of nonce occurs. However, we find that their protocol is only built on the passive attacker model. Analyzing their system in the active attacker model, we find that it performs no better than the Swiss-Knife protocol under our new active attack. What is more, besides those protocols [17–20] mentioned in [12], other protocols using the secret key [6–8, 21] as a seed to generate response information could be insecure under our attack when short nonces are used. Besides, the repetition of nonce could result in other distance-based attacks to previous distance-bounding protocols. Therefore, the security

analysis should be different from the previous analysis which does not allow repetition of nonces. For instance, when short nonces are used, the distance-bounding protocols proposed in [15, 16] are suffering from distance fraud attacks. We present an enhanced protocol that can stop an adversary from launching an active attack. Security analysis of our improved protocol is also presented on a condition where repetition short nonces are used in designing the protocol.

Paper Organization. The rest of the paper is organized as follows. We present Aikaterini et al.'s protocol and a practical attack against their protocol in Section 2. A novel distance-bounding protocol is presented in Section 3. A detailed security analysis regarding the protocol is presented in Section 4, and the paper is concluded in Section 5.

2. Aikaterini et al.'s Protocol for Repetition of Nonces

2.1. Overview of Their Protocol. Aikaterini et al.'s distance-bounding protocol: theoretically, the nonces used in designing distance-bounding protocols should never repeat. Due to practical application especially RFID tags that do use short nonces, we should consider the effects that repetition of nonces brings to the security of distance-bounding protocols. A detailed analysis of this is presented in [12]. They found that if short nonces are used, some previous protocols [17–20] are suffering from a key-learning attack where a passive adversary could learn the secret key bit by bit through the sessions where nonces are repeated. They proposed a countermeasure which can reduce the success probability of getting the secret key when short nonces are used. Their protocol is illustrated in Figure 1.

Compared with protocols in [17–20], Aikaterini et al.'s protocol introduces another random number R . In the slow phase, a pseudorandom function $f(\cdot)$ is used which takes a couple of random numbers (N_v, N_p) and a constant number C as inputs to generate a $2n$ -length bit sets R^0 and R^1 . A commitment on the secret key is generated through calculating $y = k \oplus h_R(R^0, R^1)$. The main idea is that a passive adversary has to wait until a repetition of (N_v, N_p, R) occurs and then he can get some useful information about the secret key, and thus, the success probability of the adversary is reduced compared with the protocols [17–20] where the adversary only needs to wait until repetitions of (N_v, N_p) .

2.2. Active Attack on Their Protocol. In the previous research, we all assume the verifier to be honest while the prover can be dishonest. It seems normal because it is the dishonest tags trying to cheat on their real location. After the research in [12], we can find a strong excuse to assume the verifier to be malicious, since he can find an easy way to acquire the secret key of a tag and imitate the tag ever after. The active adversary we use in this report is defined as follows.

Definition 1. The adversary is able to eavesdrop, modify, reroute, and insert messages during the execution of a cryptographic protocol. The adversary is able to obtain the

FIGURE 1: Aikaterini et al.'s original protocol.

value of any old session key. The adversary may start any number of parallel protocols. The adversary may be a legitimate protocol participant. The adversary does not have infinite computing ability.

Active attack by $\mathcal{A}$ on their protocol:

- (1) $\mathcal{A}_2$ acts as a malicious verifier who sends a nonce N_v to an honest prover P . He records the responses N_p, R, y and makes the challenge bits $\{c_i = 0\}_{i=1}^n$ and stores the response bits $\{r_i\}_{i=1}^n$.
- (2) $\mathcal{A}_2$ keeps sending N_v to P , until a repeat nonce N_p is returned, and then in the RBE phase, $\mathcal{A}_2$ sends $\{c_i^* = 1\}_{i=1}^n$ as challenge bits and records the corresponding response bits as $\{r_i^*\}_{i=1}^n$.
- (3) $\mathcal{A}_2$ recovers the secret key k of P through calculating $k = y \oplus h_R(a, b)$, where $\{a_i = r_i, b_i = r_i^*\}_{i=1}^n$.

2.3. Theoretical Analysis of the Active Attack. We follow the analysis in [12] by allowing the nonces N be either $N = N_p$ in Swiss-Knife protocol or $N = N_v \parallel N_p$ in protocols [17–20]. It is worth noting that, under an active attack, the security depends solely on the length of nonces used while has nothing to do with the length of the key, which confirms the research in [12]. What is more, under an active attack, the adversary can fix N_v that means if N_p repeats, then N repeats. Let $N_1, \dots, N_t$ be a sequence of random numbers used in the $1, \dots, t$ session, respectively, where $\{|N_i| = d, 1 \leq i \leq t\}$. By controlling the challenge bits sent to the prover, the active adversary can recover the secret key when the first repeat of N appears. Assume the nonce space is d and let T be the event that the first repetition of N occurs, then the expected number of sessions $\mathbb{E}(T)$ could be expressed in the following equation:

$$\begin{aligned} \mathbb{E}(T) &= 2 \cdot \Pr(T = 1) + 3 \cdot \Pr(T = 2) + \dots \\ &\quad + (d + 1) \cdot \Pr(T = d + 1), \\ &= \sum_{i=2}^{d+1} i \cdot \Pr(T = i), \end{aligned} \quad (1)$$

where $\Pr(T = i)$ denotes the probability that the first repetition happens in the i th session. Because there are only d nonces, therefore the first repetition will appear in the $d + 1$ trials for sure. Let A_i be the event that there are no collisions in the previous i sessions. Let a_i be the event that the collision appears in the i session for the first time. And $\Pr(T = i)$ can be calculated in the following equation:

$$\Pr(T = i) = \Pr(a_i | A_{i-1}) \Pr(A_{i-1}). \quad (2)$$

As for A_j where $1 \leq j \leq i - 1$, it can be calculated as follows:

$$\begin{aligned} \Pr(A_j) &= \Pr(\overline{a_j} | A_{j-1}) \Pr(A_{j-1}) \\ &= (1 - \Pr(a_j | A_{j-1})) \Pr(A_{j-1}). \end{aligned} \quad (3)$$

The probability of $\Pr(a_j | A_{j-1})$ means that, in the j session, the repetition of N appears for the first time:

$$\Pr(a_j | A_{j-1}) = \frac{j-1}{d}. \quad (4)$$

According to (1)–(4), the expected number of sessions $\mathbb{E}(T)$ could be expressed in the following equation:

$$\mathbb{E}(T) = \sum_{i=2}^{d+1} i(i-1) \prod_{j=0}^{i-2} \left(1 - \frac{j}{d}\right). \quad (5)$$

Thus, the expected number of sessions when $N = 2^8, 2^{16}, 2^{24}, 2^{32}$ can be calculated as in Table 1.

3. A Novel Distance-Bounding Protocol with Mutual Authentication

The primary cause of active attacks in [12] is the lack of verifier authentication. Therefore, distance-bounding protocols for mutual authentication could be a potential solution to active attacks. However, as we can see in type II attack, mutual authentication in the slow phase cannot stop an active adversary from launching an active attack because the key information the active adversary wants to gain is in the RBE phase. This means we have to implement mutual authentication in the RBE phase. Currently, there are two distance-bounding protocols achieving mutual authentication in the RBE phase [15, 16]. However, further analysis shows that if we take repetition of nonces into consideration, both protocols proposed in [15, 16] are suffering from distance fraud attacks when short nonces are used. Since all the challenge bits and response bits are generated in the slow phase, when the nonces repeat, a dishonest prover would have known the challenge bits that would be sent, and thus, he can make an advanced reply. Therefore, we design our distance-bounding protocol with mutual authentication with both fixed and random challenge messages in the RBE phase. In order to avoid confusion, the explanations of the notations used in our protocols are presented in Table 2 and our improved protocol is presented in Figure 2.

TABLE 1: Expected number of sessions with $d = 2^8, 2^{16}, 2^{24}, 2^{32}$.

The length of nonces	2^8	2^{16}	2^{24}	2^{32}
Number of sessions	20	320	5132	8.2×10^4

TABLE 2: Notations used in designing our protocol.

Notations	Explanations
k	Symmetric secret key
$f_k(\cdot)$	Pseudorandom function
R, N_p, N_v	Random numbers
$C^V, C^P, R^0, R^1, R^{0'}$	Bits
c_i	Challenge bit in the i th round
r_i	Response bit in the i th round

FIGURE 2: Our improved protocol with mutual authentication.

4. Security Analysis

In this section, we provide a detailed analysis for our proposed protocol against distance fraud, mafia fraud, and terrorist fraud attacks. We first define some notations that will be used in this section.

Let λ_i denote the adversary success probability in the i th round of the RBE phase

Let c_i and r_i be the fixed challenge bit from the prover and response bit from the verifier while c'_i and r'_i be the adversary's guessing challenge and response bits, respectively, in the i th round of the RBE phase

Let c_i^* and r_i^* be the random challenge bit from the verifier and response bit from the prover while $c_i^{*'} and $r_i^{*'}$ be the guessing challenge and response bits from an adversary in the i th round of the RBE phase$

4.1. Active Attack and Passive Attack. We first evaluate the success probability of an active adversary on our improved protocol since the adversary has no knowledge of the secret key k . When the adversary receives the fixed challenge bit c_i

from the prover P in one single round, he has to guess about the response r_i . As for the random challenge bit c_i^* , according to our active attack model, before he meets a repetition of N , he will keep sending $c_i^* = 0$ as the random challenge. Therefore, the success probability of the active adversary in one single round is $\Pr(\lambda_i) = \Pr(\lambda_i | r_i = r'_i) = 1/2$. Therefore, the success probability of the active adversary in n rounds is $(1/2)^n$.

4.2. Distance Fraud Attack. In distance fraud attack, a dishonest prover tries to make the verifier believe that he is closer than he really is by providing advanced responses. Let us consider a single round in the RBE phase. Since a dishonest prover has all the knowledge about $C^V \| C^P \| R^0 \| R^1$, he can always give a correct c_i . However, he cannot determine the challenge bit c_i^* from the verifier. When $R_i^0 = R_i^1$, he can give a success response while when $R_i^0 \neq R_i^1$ he has to choose R_i^0 or R_i^1 as an advance response. Therefore, the success probability $\Pr(\lambda_i)$ of the dishonest user in each round can be expressed as

$$\begin{aligned}
 \Pr(\lambda_i) &= \Pr(\lambda_i | c_i^* = c_i^{*'}) \Pr(c_i^* = c_i^{*'}) + \Pr(\lambda_i | c_i^* \neq c_i^{*'}) \cdot \Pr(c_i^* \neq c_i^{*'}) \\
 &= \Pr(\lambda_i | c_i^* = c_i^{*'}) \Pr(c_i^* = c_i^{*'}) + \Pr(\lambda_i | R_i^{0'} = R_i^{1'}, \Pr(c_i^* \neq c_i^{*'})) + \Pr(\lambda_i | R_i^{0'} \neq R_i^{1'}) \Pr(c_i^* \neq c_i^{*'}) \\
 &\quad - \Pr(\lambda_i | c_i^* = c_i^{*'} \wedge R_i^{0'} = R_i^{1'}) \Pr(c_i^* = c_i^{*'} \wedge R_i^{0'} = R_i^{1'}) \\
 &= \frac{5}{8}.
 \end{aligned} \tag{6}$$

Therefore, the success probability of a dishonest prover in launching a distance fraud attack is $\Pr(\lambda) = (5/8)^n$.

4.3. Mafia Fraud Attack. In mafia fraud attack, both the verifier and prover are honest. An adversary tries to launch a mafia fraud attack between the verifier and prover by acting as the prover with the verifier and verifier with the prover. We say the adversary succeeds if she is successfully authenticated by either the verifier or prover. Therefore, we divide the attack into the following two situations, and the success probabilities $\Pr(\lambda^1)$ and $\Pr(\lambda^2)$ are calculated, respectively.

The adversary first acts as the prover communicating with the verifier and then acts as the verifier using the information got from the verifier and communicates with the prover

The adversary first acts as the verifier communicating with the prover and then acts as the prover using the information got from the prover and communicates with the verifier

4.3.1. Case I. In this case, the adversary possesses no knowledge about $C^V \| C^P \| R^0 \| R^1 \| R^{0'} \| R^{1'}$. Therefore, in one single round, he has to guess the values of c_i and r_i^* , and the success probability $\Pr(\lambda_i)$ in one single round can be expressed as follows: $\Pr(\lambda_i) = \Pr(\lambda_i | (c_i = c'_i) \wedge (r_i^* = r_i^{*'})) \cdot \Pr(c_i = c'_i) \wedge (r_i^* = r_i^{*'}) = 1/4$. Therefore, the success probability of the adversary under Case I in n rounds is $(1/4)^n$.

4.3.2. Case II. In this case, the adversary has to guess the response bit r_i to the prover and c_i^* that a verifier might ask later in one single round, and thus, the success probability in one single $\Pr(\lambda_i)$ round can be expressed as follows: $\Pr(\lambda_i) = \Pr((\lambda_i | (r_i = r'_i) \wedge (c_i^* = c_i^{*'})) \cdot \Pr((r_i = r'_i) \wedge (c_i^* = c_i^{*'})) + \Pr(\lambda_i | (r_i = r'_i) \wedge (c_i^* \neq c_i^{*'})) \cdot \Pr((r_i = r'_i) \wedge (c_i^* \neq c_i^{*'})) = 3/8$.

Therefore, the success probability of the adversary under Case II in n rounds is $(3/8)^n$.

4.4. Terrorist Fraud Attack. In terrorist fraud attack, a dishonest prover collaborates with an adversary trying to cheat on his real location. It is worth noticing that the dishonest

TABLE 3: Information that could be accessed by an adversary in terrorist fraud attack.

Different cases	Information
Case I	$C^P \ R^0 \ R^1 \ R^{0'} \ R^{1'}$
Case II	$C^V \ R^0 \ R^1 \ R^{0'} \ R^{1'}$
Case III	$C^V \ C^P \ R^0 \ R^1 \ R^{0'} \ R^{1'}$
Case IV	$C^V \ C^P \ R^0 \ R^1 \ R^{0'} \ R^{1'}$
Case V	$C^V \ C^P \ R^0 \ R^1 \ R^{0'} \ R^{1'}$
Case VI	$C^V \ C^P \ R^0 \ R^1 \ R^{0'} \ R^0$

TABLE 4: The success probability of the adversary under different cases.

Different cases	Success probability
Case II	$\Pr(\lambda) = (1/2)^n$
Case III	$\Pr(\lambda) = (3/4)^{n-1}$
Case IV	$\Pr(\lambda) = (3/4)^{n-1}$
Case V	$\Pr(\lambda) = (3/4)^n$
Case VI	$\Pr(\lambda) = (3/4)^n$

TABLE 5: Performance of existing distance-bounding protocols.

Protocols	M	T	M	NR	SA
[1]	✓	×	×	×	×
[2]	✓	×	×	×	×
[14]	✓	×	✓	×	×
[15]	✓	✓	✓	×	×
[16]	✓	✓	✓	×	×
[12]	✓	✓	✓	✓	×
Ours	✓	✓	✓	✓	✓

prover should provide as much information as possible on the condition that that information will not reveal his secret key. Therefore, we first evaluate that information in our protocol that could be given to an adversary by a dishonest prover which is presented in Table 3.

Further analysis shows that the adversary can recover C^P and then he can calculate the secret key held by the dishonest user which contradicts the definition of terrorist fraud attack. Therefore, we only need to analyze Cases II to VII, and the corresponding success probabilities are presented in Table 4.

Therefore, the success probability of the dishonest prover and adversary in launching a terrorist fraud attack is $(3/4)^{n-1}$.

4.5. Comparison with Existing Distance-Bounding Protocols.

We compare our proposed distance-bounding protocol with some popular existing protocols and the result is presented in Table 5. It can be seen from the result that our proposed protocol is the first protocol that is secure under the active adversary model as well as achieves mutual authentication. For space limitation, we use “M” to represent mafia fraud attack, “T” to represent terrorist fraud attack, “MA” to represent mutual authentication, “NR” to represent nonce

repetition, and “SA” to represent secure under active adversary model.

5. Conclusions

In this paper, we propose an active attack on the distance-bounding protocol proposed in [12] where an adversary can catch the secret key much more efficiently when short nonces are used. Theoretical analysis shows their protocol performs no better than the protocols [17–20] under our active attack. We propose an enhanced version of their protocol as a countermeasure to the active attack using the knowledge of mutual authentication. However, when previous distance bounding protocols allowing short nonces [15, 16] are applied into real-world applications, since all challenge bits in these protocols are fixed, therefore it will cause a distance fraud attack. Therefore, we set both fixed and random challenge bits in the RBE phase. Detailed security analysis is also presented which takes repetition of nonces into consideration. Through the length of the RBE phase be extended to $2n$ -length, our improved protocol shows a better result in resisting the key-learning attack as well as achieves mutual authentication.

Data Availability

The datasets used or analysed during the current study are available from the corresponding author on reasonable request.

Conflicts of Interest

The authors do not have any possible conflicts of interest.

Authors' Contributions

Weiwei Liu is mainly responsible for the design of the protocol and the corresponding security analysis. Hua Guo is in charge of the comparison between the novel protocol and the previous ones while Yangguang Tian is responsible for the paper writing and feasibility analysis.

Acknowledgments

This work was partially sponsored by the project of youth talent promotion in Henan Province under grant no. 2021HYTP011.

References

- [1] S. Brands and D. Chaum, “Distance-bounding protocols,” in *Advances in Cryptology of UROCRYPT*, pp. 344–359, Springer, Berlin, Germany, 1994.
- [2] G. P. Hancke and M. G. Kuhn, “An rfid distance bounding protocol,” in *Proceedings of the Security and Privacy for Emerging Areas in Communications Networks, 2005. SecureComm 2005. First International Conference*, pp. 67–73, Athens, Greece, September 2005.
- [3] C. Hee Kim and G. Avoine, “Rfid distance bounding protocols with mixed challenges,” *IEEE Transactions on Wireless Communications*, vol. 10, no. 5, pp. 1618–1626, 2011.

- [4] S. Lee, J. Kim, and S. Hong, "Distance bounding with delayed responses," 2012.
- [5] J. Munilla and A. Peinado, "Distance bounding protocols for rfid enhanced by using void-challenges and analysis in noisy channels," *Wireless Communications and Mobile Computing*, vol. 8, no. 9, pp. 1227–1232, 2008.
- [6] C. Hee Kim, G. Avoine, F. Koeune, and O. Pereira, "The swiss-knife rfid distance bounding protocol," in *Proceedings of the 11th International Conference on Information Security and Cryptology*, pp. 98–115, Seoul, South Korea, December 2008.
- [7] A. Yang, Y. Zhuang, and D. S. Wong, "An efficient single-slow-phase mutually authenticated rfid distance bounding protocol with tag privacy," in *Information and Communications Security* Springer, Berlin, Germany, 2012.
- [8] Y. Zhuang, A. Yang, D. S. Wong, G. Yang, and Q. Xie, "A highly efficient rfid distance bounding protocol without real-time prf evaluation," in *Network And System Security of Lecture Notes In Computer Science*, J. Lopez, X. Huang, and R. Sandhu, Eds., Springer, Berlin, Germany, 2013.
- [9] N.-S. Jho and T.-Y. Youn, "Dynamic membership management in anonymous and deniable distance bounding," *Sustainability*, vol. 12, no. 24, Article ID 10330, 2020.
- [10] P. Elena, A. Yang, H. Qiao, G. Hancke, and A. Mitrokotsa, "Distance bounding meets human based authentication," *Future Generation Computer Systems*, vol. 80, pp. 627–639, 2018.
- [11] A. Gildas, M. Jorge, and A. Peinado, "Enleadtwodots security of distance-bounding: a survey," *ACM Computing Surveys*, vol. 51, pp. 1–33, 2018.
- [12] A. Mitrokotsa, P. Peris-Lopez, C. Dimitrakakis, and S. Vaudenay, "On selecting the nonce length in distance-bounding protocols," *The Computer Journal*, vol. 19, no. 2, 2013.
- [13] G. Avoine, C. Lauradoux, and B. Martin, "How secret-sharing can defeat terrorist fraud," in *Proceedings of the WiSec 2021: Conference on Security and Privacy in Wireless and Mobile Networks*, pp. 145–156, Abu Dhabi, Dubai, June 2011.
- [14] S. Čapkun, L. Buttyán, and J.-P. Hubaux, "Sector: secure tracking of node encounters in multi-hop wireless networks," in *Proceedings of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks*, pp. 21–32, Fairfax, VI, USA, January 2003.
- [15] S. Jin, J. Sung, and P. J. Lee, "Distance bounding protocol for mutual authentication," *IEEE Transactions on*, vol. 10, no. 2, pp. 592–601, 2011.
- [16] G. Avoine and C. H. Hee Kim, "Mutual distance bounding protocols," *IEEE Transactions on Mobile Computing*, vol. 12, no. 5, pp. 830–839, 2013.
- [17] G. Kapoor, W. Zhou, and S. Piramuthu, "Distance bounding protocol for multiple rfid tag authentication," in *Proceedings of the Embedded and Ubiquitous Computing, 2008. EUC'08. IEEE/IFIP International Conference*, pp. 115–120, Vancouver, Canada, December 2008.
- [18] C. Hee Kim, G. Avoine, F. Koeune, and O. Pereira, "The swiss-knife rfid distance bounding protocol," in *Proceedings of the Information Security and Cryptology-ICISC 2008*, pp. 98–115, Seoul, South Korea, June 2009.
- [19] J. Reid, J. M. Gonzalez Nieto, T. Tang, and B. Senadji, "Detecting relay attacks with timing-based protocols," in *Proceedings of the 2nd ACM Symposium on Information, Computer and Communications Security*, pp. 204–213, Singapore, April 2007.
- [20] Y.-J. Tu and S. Piramuthu, "Rfid distance bounding protocols," in *Proceedings of the First International EURASIP Workshop on RFID Technology*, Vienna, Austria, September 2007.
- [21] P. Peris-Lopez, J. C. Hernandez-Castro, C. Dimitrakakis, A. Mitrokotsa, and M. E. Juan, "Shedding light on rfid distance bounding protocols and terrorist fraud attacks," 2009, <https://arxiv.org/abs/0906.4618>.