Distance Bounding with Delayed Responses

Sangho Lee, Jin Seok Kim, Sung Je Hong, Jong Kim

***Abstract*—Distance-bounding protocols enable the establishment of an upper bound on the distance between two communicating parties in such a way that their degree of proximity can be verified. Most of these protocols rely on multi-rounds of single-bit challenge and response. Therefore, in each round, the probability that an adversary will guess the correct response is $1/2$. This letter proposes a new method to increase the number of response states of distance-bounding protocols by injecting intentional delays to each round. Our method can reduce the probability of a correct guess from $1/2$ to $1/(2k)$ for each round, where k is the number of different delays, without significant modifications of underlying protocols. Moreover, it can be applied to passive RFID tags, because it requires no special hardware equipment.**

***Index Terms*—Distance-bounding protocol, RFID, mafia fraud attack**

I. Introduction

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. Therefore, we need an authentication protocol that can also verify the distance between communicating parties.

To solve the above problem, Brands and Chaum have proposed a distance-bounding protocol [1]. Following their preliminary study, many other distance-bounding protocols have subsequently been proposed [2]–[11]. These protocols improve on various aspects of the original protocol, resulting in attributes such as enhanced security, reduced errors, and increased noise resistance. In distance-bounding protocols, a verifier $\mathcal{V}$ seeks to authenticate a prover $\mathcal{P}$ while measuring the distance d between $\mathcal{V}$ and $\mathcal{P}$. For authentication, most of these protocols rely on multi-rounds of single-bit challenge and response, also known as a fast bit exchange phase [1]. Because the response consists of a single bit, the probability that an adversary guesses the correct response is $\frac{1}{2}$ for a single round, resulting in an overall probability of $\left(\frac{1}{2}\right)^n$ when the number of rounds is n. While exchanging the challenge and response bits, $\mathcal{V}$ checks the round-trip time (RTT) of signals to measure d. When the measured RTT is t, we can compute d as

$$d = c \cdot \frac{t - t_p}{2},$$

where c is the signal propagation speed and t_p is the processing delay at $\mathcal{P}$. To correctly measure the propagation delay $(t - t_p)$, it is necessary that the mean value of t_p is known and sufficiently small. Its variation also needs to be small enough for low measurement error. Because the value of t_p is determined by a simple, single bit operation, such requirements could be achieved.

Since the current distance-bounding protocols use multi-rounds of single-bit challenge and response, only two choices can be made in each round. Therefore, the probability that an adversary correctly guesses an appropriate response in each round cannot be lower than $\frac{1}{2}$. To overcome this limit, distance-bounding protocols with more than two states have been introduced [12], [13]. Munilla and Peinado [12] proposed the addition of a *void challenge* to realize three states. A void challenge is a challenge in which $\mathcal{V}$ intentionally sends no signal during a predetermined time interval. The objective of this void challenge is to allow $\mathcal{P}$ to identify adversary's random challenges, as the distance-bound protocol with predefined challenges does [7]. The void challenge, however, cannot be applied to passive RFID tags, because it needs time synchronization between $\mathcal{V}$ and $\mathcal{P}$ to check time intervals.

Avoine *et al.* [13] have presented a generic technique—called *MUltiState Enhancement* (MUSE)—that uses modulation to encode more than two states into a signal. MUSE can significantly reduce the probability of a correct guess to $\frac{1}{s}$, where s is the number of states. However, MUSE requires that $\mathcal{P}$ efficiently encodes and decodes signals—a capability that passive RFID tags do not usually possess. Moreover, highly encoded signals are susceptible to noise; thus, more sophisticated modulation techniques for better error correction may be required as the number of states increases.

In this letter, we propose a new method to increase the number of response states for distance bounding. Our method, *delayed response*, injects an *intentional delay* when $\mathcal{P}$ sends a response to $\mathcal{V}$. If we use k types of delays, the probability that an adversary correctly guesses both the appropriate response and the right amount of delays is $\frac{1}{2k}$. The amount of delay according to challenges is randomly determined when the challenge and response sequences are generated. Unlike the void challenge and MUSE, our method does not need time synchronization or sophisticated modulation techniques. Therefore, it can be applied to passive RFID tags.

This research was supported by the MKE (The Ministry of Knowledge Economy), Korea, under the ITRC (Information Technology Research Center) support program supervised by the NIPA (National IT Industry Promotion Agency) (NIPA-2012-H0301-12-3002) and World Class University program funded by the Ministry of Education, Science and Technology through the National Research Foundation of Korea (R31-10100).

S. Lee and S. J. Hong are with the Department of Computer Science and Engineering, Pohang University of Science and Technology (POSTECH), Pohang, Republic of Korea. E-mail: {sangho2,sjhong}@postech.ac.kr

J. S. Kim is with Agency for Defense Development (ADD), Changwon, Gyungnam, 645-016, Republic of Korea. E-mail: treasure@add.re.kr

J. Kim is with the Division of IT Convergence Engineering, Pohang University of Science and Technology (POSTECH), Pohang, Republic of Korea. E-mail: jkim@postech.ac.kr

Verifier $\mathcal{V}$ — Prover $\mathcal{P}$

Picks a random $N_{\mathcal{V}}$ —$N_{\mathcal{V}}$→

←$N_{\mathcal{P}}$— Picks a random $N_{\mathcal{P}}$

$$
\begin{aligned}
H_{1,\ldots,4n} &= f(K, N_{\mathcal{V}}, N_{\mathcal{P}}) \\
d^0_{1,\ldots,n} &= H_1 || H_2 || \cdots || H_n \\
d^1_{1,\ldots,n} &= H_{n+1} || H_{n+2} || \cdots || H_{2n} \\
v^0_{1,\ldots,n} &= H_{2n+1} || H_{2n+2} || \cdots || H_{3n} \\
v^1_{1,\ldots,n} &= H_{3n+1} || H_{3n+2} || \cdots || H_{4n}
\end{aligned}
$$

Start of fast bit exchange phase

Picks $c_0 \in \{0,1\}$

Starts timer: t_0 —c_0→

Stops timer: t'_0 ←r_0— $r_0 = \bar{c}_0$

$\Delta t_0 = t'_0 - t_0$

for $i = 1$ **to** n

Picks $c_i \in \{0,1\}$

Starts timer: t_i —c_i→

If $d^{c_i}_i = 1$, $\mathcal{P}$ waits for δ

Stops timer: t'_i ←r_i— $r_i = v^{c_i}_i$

$\Delta t_i = t'_i - t_i$

end for

End of fast bit exchange phase

If $\forall i$ $r_i = v^{c_i}_i$, $\Delta t_i - d^{c_i}_i \cdot \delta \leq \mathcal{T}$, and $|\Delta t_i - \Delta t_0 - d^{c_i}_i \cdot \delta| \leq \epsilon$, **then** $\mathcal{V}$ accepts $\mathcal{P}$ **else** $\mathcal{V}$ denies $\mathcal{P}$

Fig. 1. Distance-bounding protocol with two types of delayed responses

II. Protocol with Proposed Method

In this section, we outline our method, delayed responses for distance-bounding protocol. We apply our method on Hancke and Kuhn's distance-bounding protocol [4], to take advantage of its simplicity and efficiency. However, our method can also be applied to more recent protocols [2], [3], [5]–[11] because it can increase the number of response states without significant modifications of underlying protocols.

A. Distance Bounding with Two Types of Delayed Responses

In this subsection, we propose a distance-bounding protocol that has two types of delayed responses, where an intentional delay δ may or may not be introduced into to each response (Fig. 1).

Let $\mathcal{V}$ denote a verifier and $\mathcal{P}$ denote a prover. They share a secret information K and a pseudorandom function $f : \{0,1\}^* \rightarrow \{0,1\}^{4n}$ for generating a uniformly random $4n$-bit sequence. At the beginning of the protocol, $\mathcal{V}$ and $\mathcal{P}$ generate and exchange random nonces $N_{\mathcal{V}}$ and $N_{\mathcal{P}}$. Using K, $N_{\mathcal{V}}$, and $N_{\mathcal{P}}$, they generate a random $4n$-bit sequence H, which they then split into four n-bit sequences d^0, d^1, v^0, and v^1.

The fast bit exchange phase of our protocol consists of $n+1$ rounds. The first round, 0-th round, is for measuring the base RTT, Δt_0. In the next n rounds, $\mathcal{V}$ and $\mathcal{P}$ exchange a challenge bit c_i and a response bit r_i as follows:

- $\mathcal{V}$ sends a random challenge bit $c_i \in \{0,1\}$.
- $\mathcal{P}$ checks $d^{c_i}_i$. If $d^{c_i}_i = 1$, $\mathcal{P}$ waits for δ. Otherwise, it proceeds to the next step.
- $\mathcal{P}$ retrieves $v^{c_i}_i$ and sends it as a response bit r_i.

On receiving the response bit r_i, $\mathcal{V}$ measures RTT $\Delta t_i = t'_i - t_i$.

After the fast bit exchange phase is finished, $\mathcal{V}$ checks the following conditions for all i ($1 \leq i \leq n$):

- $r_i = v^{c_i}_i$
- $\Delta t_i - d^{c_i}_i \cdot \delta \leq \mathcal{T}$
- $|\Delta t_i - \Delta t_0 - d^{c_i}_i \cdot \delta| \leq \epsilon$

where $\mathcal{T}$ is the upper-bound RTT, and ϵ is the expected measurement error owing to the time variations in delay generation and measurement. ϵ needs to be smaller than $\delta/2$ to verify whether $\mathcal{P}$ knows right delay values or not. If all of the above conditions are satisfied, $\mathcal{V}$ authenticates $\mathcal{P}$ and estimates the distance $\hat{d}$ between $\mathcal{V}$ and $\mathcal{P}$ as

$$\hat{d} = c \cdot \frac{\Delta t_i - d^{c_i}_i \cdot \delta - t_p}{2}.$$

Otherwise, $\mathcal{V}$ declines $\mathcal{P}$.

In the fast bit exchange phase, $\mathcal{P}$ only responds to n consecutive challenges and ignores further challenges. When $\mathcal{V}$ wants to make further tests, it needs to start from the nonce exchange phase again with different nonce values for generating new challenge-response pairs.

B. Distance Bounding with Multiple Types of Delayed Responses

A distance-bounding protocol that has two types of delayed responses can be generalized as a distance-bounding protocol that has multiple types of delayed responses. Let $k \geq 1$ denote the number of different delays. We specifically want to induce one of the k different delays $\{0, \delta, 2\delta, \ldots, (k-1)\delta\}$ for each round of the fast bit exchange. We define a pseudorandom function $f_k : \{0,1\}^* \rightarrow \{0,1\}^{2n(\lceil \log_2 k \rceil + 1)}$ for generating a uniformly random $2n(\lceil \log_2 k \rceil + 1)$-bit sequence H and split it into $2(\lceil \log_2 k \rceil + 1)$ n-bit sequences,

$$d^{0,1}, \ldots, d^{0,\lceil \log_2 k \rceil}, d^{1,1}, \ldots, d^{1,\lceil \log_2 k \rceil}, v^0, \text{and } v^1.$$

$\mathcal{V}$ and $\mathcal{P}$ can then derive the amount of delays according to each random challenge $c_i \in \{0,1\}$ as

$$\left(\sum_{j=1}^{\lceil \log_2 k \rceil} 2^{j-1} \cdot d^{c_i,j}_i \right) \cdot \delta.$$

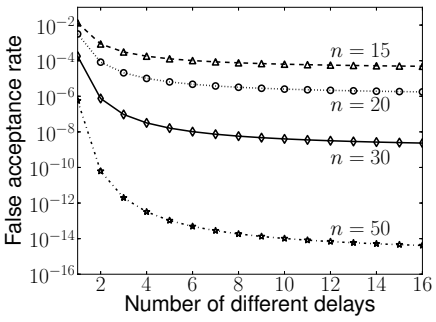

Fig. 2. False acceptance rate for the Mafia fraud according to the number of different delays. n is the number of rounds.

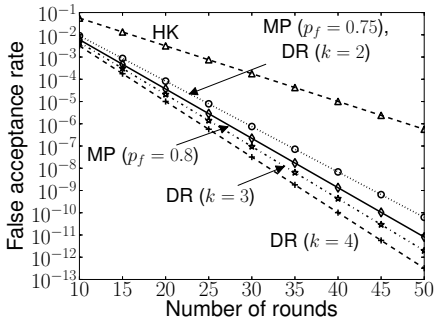

Fig. 3. False acceptance rates depending on the number of rounds

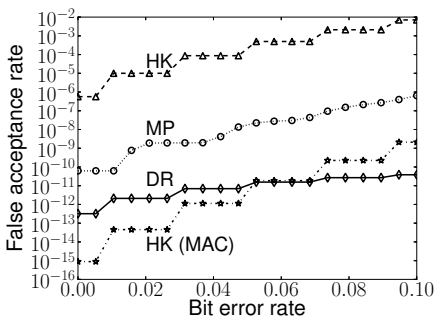

Fig. 4. False acceptance rates depending on the various bit error rates. The number of rounds is 50. MP uses $p_f = 0.75$ and DR uses $k = 4$.

III. Analysis

A. False Acceptance Rate in Noiseless Environments

We analyzed the false acceptance rate of the proposed protocol for the Mafia fraud attack, also known as a relay attack, in noiseless environments. In the Mafia fraud attack, an adversary that is located near $\mathcal{V}$ attempts to be authenticated using legitimate $\mathcal{P}$ that is located far from $\mathcal{V}$. Because $\mathcal{P}$ is far from $\mathcal{V}$, simple relays cannot fulfill the RTT requirements. Therefore, the adversary usually sends fake challenges to $\mathcal{P}$ in advance to obtain a portion of right responses. Later, the adversary can reply to $\mathcal{V}$ with right responses when $\mathcal{V}$'s challenges are the same as the fake challenges of the adversary.

Because the proposed protocol does not have techniques for detecting fake challenges, such as message authentication code (MAC), void challenges [12], or predefined challenges [7], an adversary can increase the false acceptance rate by sending fake challenges to $\mathcal{P}$ before the fast bit exchange phase is initiated. Let us assume that the adversary challenges $\mathcal{P}$ with n number of 0's. The adversary can then obtain $\lceil \log_2 k \rceil + 1$ n-bit sequences,

$$d^{0,1}, \ldots, d^{0,\lceil \log_2 k \rceil}, \text{and } v^0.$$

During the n-round fast bit exchange phase, if $\mathcal{V}$ challenges 0, the adversary can respond with an appropriate value and delays. Otherwise, the adversary has to respond with a random value and delays. Therefore, the overall false acceptance rate is

$$\left(\frac{1}{2} \cdot 1 + \frac{1}{2} \cdot \left(\frac{1}{2} \cdot \frac{1}{k}\right)\right)^n = \left(\frac{2k+1}{4k}\right)^n.$$

In addition, if we assume a more powerful prover that can support MAC for challenge and response pairs, the overall false acceptance rate becomes $\left(\frac{1}{2k}\right)^n$.

Fig. 2 shows the false acceptance rates of the proposed protocol depending on the number of different delays without MAC. As illustrated in the figure, the false acceptance rate decreases in accordance with the number of different delays and rounds. However, the reduction in the false acceptance rate resulting from the number of different delays tends to become saturated. Therefore, a large number of different delays are less meaningful.

Fig. 3 depicts the false acceptance rates of the proposed protocol without MAC (DR), Hancke and Kuhn's protocol (HK) [4], and Munilla and Peinado's protocol (MP) [12] versus on the number of rounds. The probability p_f of MP is the probability that a challenge is a full challenge (i.e., not a void challenge). MP is optimal when $p_f = 0.8$. However, obtaining such a probability is difficult; therefore, Munilla and Peinado suggested to use $p_f = 0.75$ [12]. Both DR and MP have lower false acceptance rates than that of HK. When $k = 2$, DR and MP with $p_f = 0.75$ have the same false acceptance rates. When $k \geq 3$, DR has lower false acceptance rates than that of MP with $p_f = 0.8$. Therefore, the proposed protocol has better false acceptance rates than that of HK and MP.

B. False Acceptance Rate in Noisy Environments

We also compared the false acceptance rate of the proposed protocol for the Mafia fraud attack in noisy environments with those of HK and MP (refer [12]). Let β denote the bit error rate (BER). If we allow $c = \lceil \beta n \rceil$ wrong response values owing to signal noises, the false acceptance rate of HK in noisy environments will be

$$\sum_{j=0}^{c} \binom{n}{j} \cdot \left(\frac{3}{4}\right)^{n-j} \cdot \left(\frac{1}{4}\right)^{j}.$$

The false acceptance rate of MP in noisy environments is

$$\sum_{t=0}^{n} \left(\binom{n}{t} \cdot p_f^t \cdot (1-p_f)^{n-t} \cdot \sum_{j=0}^{c_t} \binom{t}{j} \cdot \left(\frac{1}{2}\right)^t \right),$$

where t is the number of full challenges and $c_t = \lceil \beta t \rceil$.

The proposed protocol should also accept c wrong response values owing to signal noise. Our protocol, however, does not need to allow wrong response delays, because signal noise cannot affect response delays. That is, our protocol allows at most c wrong response values with right delays. Therefore, the false acceptance rate of our protocol without MAC in noisy environments is

$$\sum_{j=0}^{c} \binom{n}{j} \cdot \left(\frac{2k+1}{4k}\right)^{n-j} \cdot \left(\frac{1}{4k}\right)^{j}.$$

Fig. 4 shows the false acceptance rates of the proposed protocol without MAC, HK, MP, and HK with MAC for various BERs with the number of rounds 50. DR has lower false acceptance rates than that of HK and MP in noisy

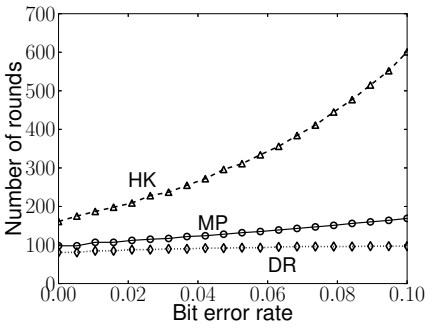

Fig. 5. The required number of rounds to achieve the false acceptance rate of 10^{-20} depending on the various bit error rates. MP uses $p_f = 0.75$ and DR uses $k = 4$.

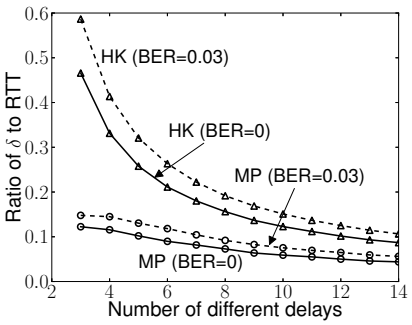

Fig. 6. Required ratio of the delay value δ to RTT according to the number of different delays for preserving the same protocol execution time. The false acceptance rate is 10^{-20}. MP uses $p_f = 0.75$.

environments. Moreover, when BER is larger than 0.05, DR has a lower false acceptance rate than that of HK with MAC. Therefore, the proposed protocol has better false acceptance rates and noise resistance than those of HK and MP.

C. Protocol Execution Time and Delay Value

The overall execution time of conventional distance-bounding protocols depends on the product of the RTT between $\mathcal{V}$ and $\mathcal{P}$ and the number of rounds of the fast bit exchange phase. Our method, however, introduces an additional delay to each round. The overall execution time of distance-bounding protocols with our method thus may be longer than that of conventional protocols. However, for the same false acceptance rate, the required number of rounds of the proposed method is smaller than that of previous protocols (Fig. 5). Therefore, if the length of overall additional delays is smaller than or equal to the product of the RTT and the reduced number of rounds, our method's execution time will be smaller than or equal to that of previous protocols. Fig. 6 shows the required ratios of the delay value δ to the RTT for preserving the same security level and protocol execution time. As the number of different delays increases the ratios decrease; and as the BER increases the ratios increase. To be comparable with MP in the protocol execution time, δ needs to be smaller than or equal to $\frac{1}{10}$ of the RTT. For instance, if the upper-bound distance between $\mathcal{V}$ and $\mathcal{P}$ is 1.5 m, then the average RTT is about 10 ns [1] and δ thus needs to be smaller than or equal to 1 ns. In Section II, we said that the expected measurement error ϵ should be smaller than a half of the delay value. Therefore, ϵ needs to be smaller than 0.5 ns in this case.

IV. Conclusion

We proposed a method, delayed responses, to enhance the security of distance-bounding protocols by increasing the number of response states. In our method, the number of response states is $2k$, where k is the number of different intentional delays. Unlike previous studies, it does not need time synchronization or modulation techniques to increase the number of states. Analysis results indicate that the false acceptance rates of our method are lower than those of previous studies in both noiseless and noisy environments.

[1] Speed of light is $299,792,458$ m/s ≈ 0.3 m/ns.

References

[1] S. Brands and D. Chaum, "Distance-bounding protocols," in *EUROCRYPT*, 1993.
[2] G. Avoine and A. Tchamkerten, "An efficient distance bounding RFID authentication protocol: balancing false-acceptance rate and memory requirement," in *ISC*, 2009.
[3] S. Drimer and S. J. Murdoch, "Keep your enemies close: Distance bounding against smartcard relay attacks," in *USENIX Security Symp.*, 2007.
[4] G. P. Hancke and M. G. Kuhn, "An RFID distance bounding protocol," in *SECURECOMM*, 2005.
[5] G. P. Hancke, K. Mayes, and K. Markantonakis, "Confidence in smart token proximity: relay attacks revisited," *Comput. Secur.*, vol. 28, no. 7, pp. 615–627, 2009.
[6] C. H. Kim, G. Avoine, F. Koeune, F.-X. Standaert, and O. Pereira, "The swiss-knife RFID distance bounding protocol," in *ICISC*, 2008.
[7] C. H. Kim and G. Avoine, "RFID distance bounding protocols with mixed challenges," *IEEE Trans. Wireless Commun.*, vol. 10, no. 5, pp. 1618–1626, 2011.
[8] C. H. Kim, "Security analysis of YKHL distance bounding protocol with adjustable false acceptance rate," *IEEE Commun. Lett.*, vol. 15, no. 10, pp. 1078–1080, 2011.
[9] J. Reid, J. M. G. Nieto, T. Tang, and B. Senadji, "Detecting relay attacks with timing-based protocols," in *ASIACCS*, 2007.
[10] D. H. Yum, J. S. Kim, S. J. Hong, and P. J. Lee, "Distance bounding protocol for mutual authentication," *IEEE Trans. Wireless Commun.*, vol. 10, no. 2, pp. 592–601, 2011.
[11] ——, "Distance bounding protocol with adjustable false acceptance rate," *IEEE Commun. Lett.*, vol. 15, no. 4, pp. 434–436, 2011.
[12] J. Munilla and A. Peinado, "Distance bounding protocols for RFID enhanced by using void-challenges and analysis in noisy channels," *Wireless Commun. Mob. Comput.*, vol. 8, no. 9, pp. 1227–1232, 2008.
[13] G. Avoine, C. Floerkemeier, and B. Martin, "RFID distance bounding multistate enhancement," in *INDOCRYPT*, 2009.