IEICE TRANS. INF. & SYST., VOL.E96–D, NO.1 JANUARY 2013

LETTER

Unilateral Distance Bounding Protocol with Bidirectional Challenges*

Myung-Ho PARK[†], **Ki-Gon NAM**[††], **Jin Seok KIM**[†], **Dae Hyun YUM**[†††a)], ***Nonmembers***, ***and*** **Pil Joong LEE**[††††], ***Member***

SUMMARY A distance bounding protocol provides an upper bound on the distance between communicating parties by measuring the round-trip time between challenges and responses. It is an effective countermeasure against mafia fraud attacks (a.k.a. relay attacks). The adversary success probability of previous distance bounding protocols without a final confirmation message such as digital signature or message authentication code is at least $\left(\frac{3}{8}\right)^n = \left(\frac{1}{2.67}\right)^n$. We propose a unilateral distance bounding protocol without a final confirmation message, which reduces the adversary success probability to $\left(\frac{5}{16}\right)^n = \left(\frac{1}{3.2}\right)^n$.

key words: *mafia fraud attack, distance bounding, authentication, security*

1. Introduction

Location information can provide a measure of trust in network applications. Users are granted some privileges or services (e.g., access to a network or purchase of goods with a smartcard payment system) when they are inside a certain area. Verifying the location of a user is therefore an important authentication mechanism.

A basic attack scenario related to location information is the distance fraud attack, where a dishonest prover tries to convince an honest verifier of a wrong statement on the physical distance between them. Usually, the dishonest prover claims to be closer than he really is and thus this problem is often called in-region verification. A more sophisticated attack scenario is the mafia fraud attack that was described by Desmedt et al. [1]. In this attack, both verifier $\mathcal{V}$ and prover $\mathcal{P}$ are honest, but a malicious adversary or intruder, which is modeled as a couple of $\{\mathcal{V}', \mathcal{P}'\}$, launches a man-in-the-middle attack between $\mathcal{V}$ and $\mathcal{P}$. The dishonest verifier $\mathcal{V}'$ interacts with the honest prover $\mathcal{P}$ and, in the meantime, the dishonest prover $\mathcal{P}'$ interacts with the honest verifier $\mathcal{V}$. Thanks to the collaboration of $\mathcal{V}'$, the fraud enables $\mathcal{P}'$ to convince $\mathcal{V}$ of an assertion related to the secret information of $\mathcal{P}$, where the typical assertion is that $\mathcal{P}$ is within a certain physical distance of $\mathcal{V}$.

In addition to the use of cryptography, which establishes the identity of the prover, a distance bounding protocol estimates the distance to the prover by measuring the signal round-trip time and multiplying it by the signal propagation speed. In order to extract the propagation time, the processing time must be as short and invariant as possible. A distance bounding protocol usually consists of multiple rounds of a single-bit challenge and rapid single-bit response (often called a fast bit exchange phase) [2]. For the case of radio signals, which travel at the speed of light, it is essentially impossible for an adversary to decrease the estimated distance.

Even though Brands and Chaum [2] introduced the first distance bounding protocol in 1993, it is only when Hancke and Kuhn [3] proposed a distance bounding protocol in 2005 that distance bounding protocols attract the attention of researchers. Hancke and Kuhn's protocol (HKP) consists of a slow phase of exchanging random nonces ($N_{\mathcal{V}}$ and $N_{\mathcal{P}}$) and a fast phase of exchanging challenge bit C_i and response bit R_i for $i = 1, 2, \ldots, n$. In the slow exchange phase, $\mathcal{V}$ and $\mathcal{P}$ compute two n-bit sequences, $v^0 = \langle v_i^0 \rangle_{i=1,\ldots,n}$ and $v^1 = \langle v_i^1 \rangle_{i=1,\ldots,n}$, using a pseudo-random function $f : \{0,1\}^* \to \{0,1\}^{2n}$. In the i-th round of the fast bit exchange phase where $1 \le i \le n$, $\mathcal{V}$ chooses a random challenge bit $C_i \in \{0,1\}$ and sends it to $\mathcal{P}$. Then, the prover $\mathcal{P}$ sends back a response bit v_i^0 (the i-th bit of v^0) if $C_i = 0$ and a response bit v_i^1 if $C_i = 1$. After the fast bit exchange phase, $\mathcal{V}$ checks the validity of the response bits R_i and the propagation time Δt_i.

The success probability of an adversary who launches a mafia fraud attack against HKP is $\left(\frac{3}{4}\right)^n$. This is because the adversary (acting as $\mathcal{V}'$) can query $\mathcal{P}$ in advance with some arbitrary challenge bit C_i' and obtain either v_i^0 or v_i^1 for $i = 1, \ldots, n$. In half of n rounds, the adversary's guess C_i' will be equal to the actual challenge bit C_i of $\mathcal{V}$ and thus the adversary (acting as $\mathcal{P}'$) can impersonate $\mathcal{P}$ with the success probability 1. When $C_i' \neq C_i$, the adversary randomly answers one of two possibilities (i.e., $R_i = 0$ or 1) with the success probability $\frac{1}{2}$.

A simple way to reduce the adversary success probability of HKP from $\left(\frac{3}{4}\right)^n$ to $\left(\frac{1}{2}\right)^n$ is to include a confirmation

Manuscript received March 1, 2012.

[†]The authors are with Agency for Defense Development (ADD), Changwon, Gyungnam, 645–016, Republic of Korea.

[††]The author is with the Department of Electrical Engineering, Pusan National University, Busan, 609–735, Republic of Korea.

[†††]The author is with the Department of Information and Communication Engineering, Myongji University, Yongin, Gyeonggido, 449–728, Republic of Korea.

[††††]The author is with the Department of Creative IT Excellence Engineering and the Department of Electrical Engineering, POSTECH, Pohang, Gyungbuk, 790–784, Republic of Korea.

*This research was supported by the MKE (The Ministry of Knowledge Economy), Korea, under the "IT Consilience Creative Program" support program supervised by the NIPA (National IT Industry Promotion Agency) (C1515-1121-0003).

a) E-mail: dhyum@mju.ac.kr

DOI: 10.1587/transinf.E96.D.134

message such as signature or message authentication code at the end of the protocol as in [2], which would make the protocol slower. A different approach to reduce the adversary success probability is that the prover uses some challenge bits to authenticate the verifier (i.e., to detect an illegitimate verifier). Munilla and Peinado's protocol (MPP) uses void challenges [4] and Kim and Avoine's protocol (KAP) uses mixed challenges [5]. KAP reduces the adversary success probability asymptotically to $\left(\frac{1}{2}\right)^n$ without a final confirmation message.

Recently, Yum et al. [6] introduced another technique, which we call "bidirectional challenges," to build a mutual distance bounding protocol, where a challenge bit is sent probabilistically by either the prover or the verifier. If a party does not know the correct direction of a challenge bit (i.e., who should send the challenge bit), both parties may simultaneously talk (i.e., both send challenges) or remain silent (i.e., both wait for the challenge), which helps detect an illegitimate party. The distance bounding protocol of Yum et al. [6] reduces the adversary success probability asymptotically to $\left(\frac{3}{8}\right)^n = \left(\frac{1}{2.67}\right)^n$ without a final confirmation message.

In this article, we use the bidirectional challenges to design a unilateral distance bounding protocol with adversary success probability lower than all previous protocols without a final confirmation message. Specifically, our proposed protocol reduces the adversary success probability asymptotically to $\left(\frac{5}{16}\right)^n = \left(\frac{1}{3.2}\right)^n$ without a final confirmation message.

2. Proposed Distance Bounding Protocol

We propose a unilateral distance bounding protocol with bidirectional challenges that is depicted in Fig. 1. In the slow exchange phase, the verifier $\mathcal{V}$ and the prover $\mathcal{P}$ compute four n-bit sequences, α, β, v^0, and v^1, using a pseudo-random function $g : \{0,1\}^* \rightarrow \{0,1\}^{4n}$. If $\alpha_i = 0$, the i-th round of the fast bit exchange phase is exactly the same as that of HKP; in this case, β_i is ignored. If $\alpha_i = 1$, the value of β_i determines who should send a challenge bit.

- If $\alpha_i = 1 \ \wedge \ \beta_i = 0$, the verifier $\mathcal{V}$ sends v_i^0 as a challenge bit (i.e., $C_i = v_i^0$). When receiving C_i, the prover $\mathcal{P}$ checks its validity. If C_i is correct, $\mathcal{P}$ sends $R_i = v_i^1$ to $\mathcal{V}$ as a response. If C_i is incorrect (i.e., $\mathcal{V}$ does not know K) or a collision is detected (i.e., $\mathcal{V}$ does not send a challenge in time), $\mathcal{P}$ sends a random response R_i and enters a protection mode. Here, the protection mode means that the prover behaves randomly for all subsequent rounds; a simple way is to replace $(\alpha, \beta, v^0, v^1)$ with random values.
- If $\alpha_i = 1 \ \wedge \ \beta_i = 1$, the prover $\mathcal{P}$ sends $C_i = v_i^0$ and the verifier $\mathcal{V}$ replies with $R_i = v_i^1$. If R_i is incorrect or a collision is detected (i.e., $\mathcal{V}$ also sends a challenge), $\mathcal{P}$ enters a protection mode.

In summary, a challenge bit is sent by the verifier $\mathcal{V}$ if $\alpha_i = 0 \ \vee \ \beta_i = 0$ (Case I) and by the prover $\mathcal{P}$ if $\alpha_i = 1 \ \wedge \ \beta_i = 1$ (Case II).

Table 1 $\Pr[\Lambda_1 | E^1_{b_1 b_2 \star b_4 b_5 \star}]$ and $\Pr[\Gamma_i | \overline{\Lambda_{i-1}}, E^i_{b_1 b_2 \star b_4 b_5 \star}]$.

α_i	β_i	α'_i	β'_i	$\Pr[\Lambda_1 \mid E^1_{b_1 b_2 \star b_4 b_5 \star}]$	$\Pr[\Gamma_i \mid \overline{\Lambda_{i-1}}, E^i_{b_1 b_2 \star b_4 b_5 \star}]$
0	-	0	-	1	1/2
0	-	1	0	1	1/2
0	-	1	1	0	0
1	0	0	-	1/2	1/2
1	0	1	0	1/2	1/2
1	0	1	1	0	0
1	1	0	-	0	0
1	1	1	0	0	0
1	1	1	1	1/2	1/2

Remark. In the proposed protocol, we assume that the prover $\mathcal{P}$ approaches the verifier $\mathcal{V}$ as close as possible; that is, the distance d between $\mathcal{P}$ and $\mathcal{V}$ is physically minimal (e.g., contact smart cards and mu-chip [7]). Theoretically, this means that the distance $d_{\mathcal{A}}$ between an adversary $\mathcal{A}$ and a user (either $\mathcal{P}$ or $\mathcal{V}$) is not shorter than d.

Theorem 1: The success probability of an adversary who launches a mafia fraud attack against the proposed distance bounding protocol is $\left(\frac{5}{16}\right)^n$ asymptotically.

Proof. Let $\mathcal{V}$ and $\mathcal{P}$ be an honest verifier and an honest prover who share a secret K. Let $\mathcal{A}$ be an adversary modeled as $\{\mathcal{V}', \mathcal{P}'\}$. After $\mathcal{V}$ and $\mathcal{P}$ exchange random nonces $(N_{\mathcal{V}}, N_{\mathcal{P}})$, the adversary $\mathcal{A}$ launches a man-in-the-middle attack that consists of two stages. In stage 1, the adversary $\mathcal{A}$ acts as a verifier $\mathcal{V}'$ running the fast bit exchange phase with an honest prover $\mathcal{P}$. In stage 2, $\mathcal{A}$ acts as a prover $\mathcal{P}'$ and runs the fast bit exchange phase with an honest verifier $\mathcal{V}$. The goal of $\mathcal{A}$ is to impersonate $\mathcal{P}$ in stage 2 by using information obtained in stage 1.

Let Λ_i be the event that $\mathcal{A}$ (acting as $\mathcal{V}'$) succeeds in up to the i-th round of stage 1 (i.e., $\mathcal{A}$ succeeds in the j-th round for $1 \leq j \leq i$). Let γ_i be the event that $\mathcal{A}$ (acting as $\mathcal{P}'$) succeeds in the i-th round of stage 2. Let Γ_i be defined by $\Gamma_1 = \gamma_1$ and $\Gamma_i = \gamma_i \,|\, (\gamma_1 \wedge \cdots \wedge \gamma_{i-1})$ for $i > 1$. Denote $(\alpha'_i, \beta'_i, C'_i)$ as the adversary's guesses in stage 1 and (α_i, β_i, C_i) as the real values of $\mathcal{V}$ and $\mathcal{P}$. To describe various events, we define the following notation.

$$E^i_{b_1 b_2 b_3 b_4 b_5 b_6} \triangleq \text{Event of } (\alpha_i = b_1) \wedge (\beta_i = b_2) \wedge (C_i = b_3) \wedge (\alpha'_i = b_4) \wedge (\beta'_i = b_5) \wedge (C'_i = b_6), \text{ where } b_1, b_2, \ldots, b_6 \in \{0,1\}.$$

If b_i is irrelevant, it is replaced with a star symbol $\star$. For example, $E^i_{b_1 b_2 b_3 b_4 \star b_6}$ ignores b_5 (or β'_i).

We first compute $\Pr[\Lambda_{i-1}]$ and $\Pr[\overline{\Lambda_{i-1}}]$ as follows.

$$\Pr[\Lambda_1] = \sum_{b_1, b_2, b_4, b_5} \Pr[\Lambda_1 | E^1_{b_1 b_2 \star b_4 b_5 \star}] \Pr[E^1_{b_1 b_2 \star b_4 b_5 \star}] = 1 \cdot \left(\frac{1}{4} + \frac{1}{8}\right) + \frac{1}{2} \cdot \left(\frac{1}{8} + \frac{1}{16} + \frac{1}{16}\right) = \frac{1}{2}$$

$$\vdots$$

Verifier $\mathcal{V}$ (secret K) | **Prover $\mathcal{P}$** (secret K)

Pick a random nonce $N_{\mathcal{V}}$ —$N_{\mathcal{V}}$→

←$N_{\mathcal{P}}$— Pick a random nonce $N_{\mathcal{P}}$

$H = \langle H_i \rangle_{i=1,\ldots,4n} = g(K, N_{\mathcal{V}}, N_{\mathcal{P}})$

$\alpha = \langle \alpha_i \rangle_{i=1,\ldots,n} = H_1 \| H_2 \| \cdots \| H_n$

$\beta = \langle \beta_i \rangle_{i=1,\ldots,n} = H_{n+1} \| H_{n+2} \| \cdots \| H_{2n}$

$v^0 = \langle v_i^0 \rangle_{i=1,\ldots,n} = H_{2n+1} \| H_{2n+2} \| \cdots \| H_{3n}$

$v^1 = \langle v_i^1 \rangle_{i=1,\ldots,n} = H_{3n+1} \| H_{3n+2} \| \cdots \| H_{4n}$

Start of fast bit exchange phase
for $i = 1$ to n

Case I: $\alpha_i = 0 \ \vee \ \beta_i = 0$

Pick a random bit $s_i \in \{0, 1\}$

$$C_i = \begin{cases} s_i, & \text{if } \alpha_i = 0 \\ v_i^0, & \text{if } \alpha_i = 1 \ \wedge \ \beta_i = 0 \end{cases}$$

Start timer —C_i→

Stop timer ←R_i—

$$R_i = \begin{cases} v_i^{C_i}, & \text{if } \alpha_i = 0 \\ v_i^1, & \text{if } \alpha_i = 1 \wedge \beta_i = 0 \wedge C_i = v_i^0 \end{cases}$$

If $\alpha_i = 1 \ \wedge \ \beta_i = 0 \ \wedge \ C_i \neq v_i^0$ or a collision is detected, prover sends a random R_i and enters a protection mode.

Case II: $\alpha_i = 1 \ \wedge \ \beta_i = 1$

←C_i— $C_i = v_i^0$

$R_i = v_i^1$ —R_i→ If $R_i \neq v_i^1$ or a collision is detected, prover enters a protection mode.

end for
End of fast bit exchange phase

Check R_i and Δt_i for Case I and C_i and collision for Case II.

Fig. 1 Unilateral distance bounding protocol with bidirectional challenges.

$$\Pr[\Lambda_{i-1}] = \left(\frac{1}{2}\right)^{i-1}$$

$$\Pr[\overline{\Lambda_{i-1}}] = 1 - \Pr[\Lambda_{i-1}] = 1 - \left(\frac{1}{2}\right)^{i-1}$$

where $\Pr[\Lambda_1 | E^1_{b_1 b_2 \star b_4 b_5 \star}]$ is given in Table 1.

The conditional probabilities $\Pr[\Gamma_i | \overline{\Lambda_{i-1}}]$ and $\Pr[\Gamma_i | \Lambda_{i-1}]$ can be computed as follows.

$$\begin{aligned} &\Pr[\Gamma_i | \overline{\Lambda_{i-1}}] \\ &= \sum_{b_1,b_2,b_4,b_5} \Pr[\Gamma_i | \overline{\Lambda_{i-1}}, E^i_{b_1 b_2 \star b_4 b_5 \star}] \Pr[E^i_{b_1 b_2 \star b_4 b_5 \star}] \\ &= \frac{1}{2} \cdot \left(\frac{1}{4} + \frac{1}{8} + \frac{1}{8} + \frac{1}{16} + \frac{1}{16} \right) = \frac{5}{16} \end{aligned}$$

$$\begin{aligned} &\Pr[\Gamma_i | \Lambda_{i-1}] \\ &= \sum_{b_1,\ldots,b_6} \Pr[\Gamma_i | \Lambda_{i-1}, E^i_{b_1 b_2 b_3 b_4 b_5 b_6}] \Pr[E^i_{b_1 b_2 b_3 b_4 b_5 b_6}] \\ &= 1 \cdot \left(\frac{2}{16} + \frac{6}{32} + \frac{2}{64} \right) + \frac{1}{2} \cdot \left(\frac{6}{16} + \frac{8}{32} + \frac{2}{64} \right) = \frac{43}{64} \end{aligned}$$

where the probabilities $\Pr[\Gamma_i | \overline{\Lambda_{i-1}}, E^i_{b_1 b_2 \star b_4 b_5 \star}]$ and $\Pr[\Gamma_i | \Lambda_{i-1}, E^i_{b_1 b_2 b_3 b_4 b_5 b_6}]$ are summarized in Table 1 and Table 2.

The probability $\Pr[\Gamma_i]$ is obtained from $\Pr[\Gamma_i | \overline{\Lambda_{i-1}}]$ and $\Pr[\Gamma_i | \Lambda_{i-1}]$.

$$\begin{aligned} \Pr[\Gamma_i] &= \Pr[\Gamma_i | \Lambda_{i-1}] \Pr[\Lambda_{i-1}] + \Pr[\Gamma_i | \overline{\Lambda_{i-1}}] \Pr[\overline{\Lambda_{i-1}}] \\ &= \frac{43}{64} \cdot \left(\frac{1}{2}\right)^{i-1} + \frac{5}{16} \cdot \left(1 - \left(\frac{1}{2}\right)^{i-1}\right) \\ &= \frac{5}{16} + \frac{23}{64} \left(\frac{1}{2}\right)^{i-1}. \end{aligned}$$

Table 2 $\Pr[\Gamma_i|\Lambda_{i-1}, E^i_{b_1b_2b_3b_4b_5b_6}]$.

α_i	β_i	C_i	α'_i	β'_i	C'_i	$\Pr[\Gamma_i\|\Lambda_{i-1}, E^i_{b_1b_2b_3b_4b_5b_6}]$
0	-	0	0	-	0	1
0	-	0	0	-	1	1/2
0	-	0	1	0	0	1
0	-	0	1	0	1	1/2
0	-	0	1	1	-	1/2
0	-	1	0	-	0	1/2
0	-	1	0	-	1	1
0	-	1	1	0	0	1/2
0	-	1	1	0	1	1
0	-	1	1	1	-	1/2
1	0	0	0	-	0	1
1	0	0	0	-	1	1/2
1	0	0	1	0	0	1
1	0	0	1	0	1	1/2
1	0	0	1	1	-	1/2
1	0	1	0	-	0	1/2
1	0	1	0	-	1	1
1	0	1	1	0	0	1/2
1	0	1	1	0	1	1
1	0	1	1	1	-	1/2
1	1	0	0	-	-	1/2
1	1	0	1	0	-	1/2
1	1	0	1	1	-	1
1	1	1	0	-	-	1/2
1	1	1	1	0	-	1/2
1	1	1	1	1	-	1

Finally, the adversary success probability can be computed as follows.

$$\begin{aligned}\Pr\left[\bigwedge_{i=1}^{n}\gamma_i\right] &= \Pr[\gamma_1]\Pr[\gamma_2|\gamma_1]\cdots\Pr\left[\gamma_n|\bigwedge_{i=1}^{n-1}\gamma_i\right] \\ &= \prod_{i=1}^{n}\Pr[\Gamma_i] \\ &= \prod_{i=1}^{n}\left(\frac{5}{16}+\frac{23}{64}\left(\frac{1}{2}\right)^{i-1}\right)\end{aligned}$$

which is in the order of $\left(\frac{5}{16}\right)^n$ as n increases. One can verify that $\Pr[\bigwedge_{i=1}^{n}\Gamma_i] < 5.74\left(\frac{5}{16}\right)^n$ holds for all practical purposes (e.g., $n \leq 100$) with numerical computing softwares (e.g., MATLAB). □

3. Conclusion

We propose unilateral distance bounding protocol using bidirectional challenges. In the proposed protocol, either the prover or the verifier probabilistically send a challenge. The adversary success probability is asymptotically to $\left(\frac{5}{16}\right)^n$ without a final confirmation message, which is lower than that of previous protocols without a final confirmation message.

References

[1] Y. Desmedt, C. Goutier, and S. Bengio, "Special uses and abuses of the Fiat-Shamir passport protocol," CRYPTO, Lect. Notes Comput. Sci., vol.293, pp.21–39, Springer, 1987.

[2] S. Brands and D. Chaum, "Distance-bounding protocols," EUROCRYPT, Lect. Notes Comput. Sci., vol.765, pp.344–359, Springer, 1993.

[3] G.P. Hancke and M.G. Kuhn, "An RFID distance bounding protocol," 1st Int. Conf. Security Privacy Emerging Areas Commun. Netw. (SECURECOMM), pp.67–73, IEEE Computer Society, 2005.

[4] J. Munilla and A. Peinado, "Distance bounding protocols for RFID enhanced by using void-challenges and analysis in noisy channels," Wireless Commun. Mobile Computing, vol.8, no.9, pp.1227–1232, 2008.

[5] C.H. Kim and G. Avoine, "RFID distance bounding protocol with mixed challenges to prevent relay attacks," 8th Int. Conf. Crytology Netw. Security (CANS), Lect. Notes Comput. Sci., vol.5888, pp.119–133, Springer, 2009.

[6] 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.

[7] RFID Jouranl, "Hitachi unveils smallest RFID chip." http://www.rfidjournal.com/article/view/337.