New DH protocol based on distance-bounding technique for peer-to-peer wireless network

22nd November, 2007

Seon-Yeong PARK, Ju-Young KIM and Hong-Yeop SONG
Yonsei University, Coding and Information Theory Lab
{sy.park, jy.kim, hysong} @yonsei.ac.kr

Some Pictures of Tor

Happy Birthday!

Contents

- **Introduction**
- **Preliminary**
  - Commitment scheme
  - MITM attack
  - DH protocol, distance-bounding protocol
- **Existing DH-DB protocol**
- **Improved DH-DB protocol**
- **Result and Discussion**
- **Conclusion**

Introduction

- **Peer-to-peer key agreement protocol**
  - Auto configuration of mobile router without shared secret
- **DH (Diffie-Hellman) protocols**
  - Vulnerability against the MITM attacks
  - Involvement of users
  - Needs of physical devices
- **Design of improved DH-DB (Distance-Bounding)**
  - Improvement of resistance to attacks
  - Optimization of protocol

DH Protocol[1]

Alice		Bob
Given ID_A, g		Given ID_B, g
Pick $\mathbf{X_A}$, and calculate $\mathbf{g^{X_A}}$		Pick $\mathbf{X_B}$, and calculate $\mathbf{g^{X_B}}$
Pick $N_A \in_U \{0,1\}^k$		Pick $N_B \in_U \{0,1\}^k$
$m_A \leftarrow 0 \| ID_A \| \mathbf{g^{X_A}} \| N_A$		$m_B \leftarrow 1 \| ID_B \| \mathbf{g^{X_B}} \| N_B$
$(L_A, K_A) \leftarrow commit(m_A)$	$\xrightarrow{L_A}$	$(L_B, K_B) \leftarrow commit(m_B)$
	$\xleftarrow{L_B}$	
	$\xrightarrow{K_A}$	
$m_B \leftarrow open(L_B, K_B)$	$\xleftarrow{K_B}$	$m_A \leftarrow open(L_A, K_A)$
Verify 1 in m_B; $i_A \leftarrow N_A \oplus N_B$	$\xrightarrow{i_A}$	Verify 0 in m_A; $i_B \leftarrow N_B \oplus N_A$
Verify $i_A = i_B$	$\xleftarrow{i_B}$	Verify $i_B = i_A$

If $i_A = i_B$, Alice and Bob accept m_B and m_A, respectively.

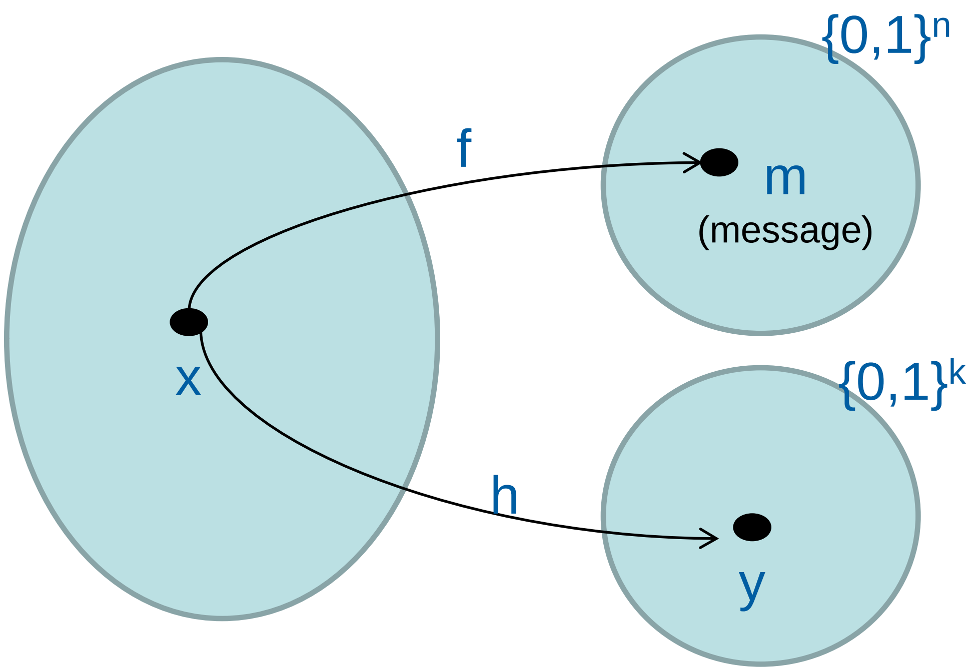
Alice	Bob
Generate $\mathbf{(g^{X_B})^{X_A}}$	Generate $\mathbf{(g^{X_A})^{X_B}}$

[1] M. Cagalj and J. -P. Hubaux, “Key agreement protocol over a radio link,”EPFL-IC-ICA, Teck. Rep. IC/2004/16, Jan. 2004.

Commitment Scheme[2]

Commitment/opening pair

- L=(y, f) is a Locked box.
- K=(x) is a Key.



Commitment procedure

1. Pick universal hash function f and x at random so that f(x)=m.
2. Compute y=h(x), where h is a collision-free hash function.
3. Send L=(y, f) to receiver.

Opening procedure

1. Send K=(x) to receiver.
2. Receiver computes f(x)=m.

[2] S. Halevi and S. micali, “Practical and Provably-Secure Commitment Schemes from Collision-Free Hashing,” *CRYPTO 96, pp. 201-215, Lecture Notes in Computer* Science, Springer-Verlag, 1996.

MITM Attack

Alice ⇄ Bob

Eve

She can collect L_A, K_A (or L_B, K_B) and get secret DH key.

She can use collected L_A, K_A (or L_B, K_B) for replay attack.

Distance-bounding Protocol[3]

- **Distance-bounding principle**

Alice	Bob
$\alpha_i \in_U \{0,1\}^k$	$\beta_i \in_U \{0,1\}^k$

Starting of rapid bit exchange

$$\xrightarrow{\alpha_i}$$

$$\xleftarrow{\beta_i}$$

End of rapid bit exchange

- Single-bit challenge and rapid single-bit response
- Upper-bound the distance between two parties based on the maximum of the delay time for responses
- Two parties communicate when they are close by.

[3] S. Brands and D. Chaum, “Distance-bounding protocols,” EUROCRYPT, Heidelberg, Germany: Springer-Verlag, vol. 765, *Lecture Notes in Computer Science,* pp. 344-359, 1993.

Environment

- **RF and sound capability[4]**
  - For accurate estimation of the distance between two parties

- **Local verification protocol[5]**
  - The measured distance appears on both device displays and the users then visually check whether there are other users/devices closer to them than the displayed distance bounds.

[4] R, Fontana, “Experimental results from an ultra wideband precision geolocation system,” *Proc. Ultra-Wideband, Short-Pulse Electromagnetics 5*, pp. 215-224, 2002.

[5] N. Sastry, U. Shankar, and D. Wagner, “Secure verification of location claims,” *Proc. ACM Workshop Wireless Security (WISe)*, pp. 1-10, 2003.

Existing DH-DB Protocol[6](1/3)

- **Initialization phase**

Alice		Bob
Given ID_A, g^{X_A}		Given ID_B, g^{X_B}
Pick $N_A, R_A \in_U \{0,1\}^k$		Pick $N_B, R_B \in_U \{0,1\}^k$
$m_A \leftarrow 0 \Vert ID_A \Vert g^{X_A} \Vert N_A$		$m_B \leftarrow 1 \Vert ID_B \Vert g^{X_B} \Vert N_B$
$(L_A, K_A) \leftarrow commit(m_A)$		$(L_B, K_B) \leftarrow commit(m_B)$
$(L'_A, K'_A) \leftarrow commit(0 \Vert R_A)$	$\xrightarrow{L_A, L'_A}$	$(L'_B, K'_B) \leftarrow commit(1 \Vert R_B)$
	$\xleftarrow{L_B, L'_B}$	
	$\xrightarrow{K_A}$	
$m_B \leftarrow open(L_B, K_B)$	$\xleftarrow{K_B}$	$m_A \leftarrow open(L_A, K_A)$
Verify 1 in m_B; $i_A \leftarrow N_A \oplus N_B$		Verify 0 in m_A; $i_B \leftarrow N_B \oplus N_A$

Eve can collect c_A, d_A (or c_B, d_B) and get secret DH key.

Existing DH-DB Protocol[6](2/3)

- **Distance-bounding phase**

Alice		Bob
The bits of R_A are $R_{A1},\ldots,R_{Ak}$		The bits of R_B are $R_{B1},\ldots,R_{Bk}$
The bits of i_A are $i_{A1},\ldots,i_{Ak}$		The bits of i_B are $i_{B1},\ldots,i_{Bk}$
$\alpha_1 \leftarrow R_{A1} \oplus i_{A1}$	$\xrightarrow{\alpha_1}$	
	$\xleftarrow{\beta_1}$	$\beta_1 \leftarrow R_{B1} \oplus i_{B1} \oplus \alpha_1$
	$\vdots$	
$\alpha_i \leftarrow R_{Ai} \oplus i_{Ai} \oplus \beta_{i-1}$	$\xrightarrow{\alpha_i}$	Measure delay between β_{i-1} and α_i
	$\xleftarrow{\beta_i}$	$\beta_i \leftarrow R_{Bi} \oplus i_{Bi} \oplus \alpha_i$
Measure delay between α_i and β_i		
	$\vdots$	
$\alpha_k \leftarrow R_{Ak} \oplus i_{Ak} \oplus \beta_{k-1}$	$\xrightarrow{\alpha_k}$	Measure delay between β_{k-1} and α_k
	$\xleftarrow{\beta_k}$	$\beta_k \leftarrow R_{Bk} \oplus i_{Bk} \oplus \alpha_k$
Measure delay between α_k and β_k		

Existing DH-DB Protocol[6](3/3)

- **Verification phase**

Alice		Bob
	$\xrightarrow{K'_A}$	$0\|\|R_A \leftarrow open\ (L'_A, K'_A)$
$1\|\|R_B \leftarrow open\ (L'_B, K'_B)$	$\xleftarrow{K'_B}$	
$i_{Bi} \leftarrow \alpha_i \oplus \beta_i \oplus R_{Bi}\ (i = 1,\dots,k)$		$i_{A1} \leftarrow \alpha_1 \oplus R_{A1}$
Verify $i_A = i_B$		$i_{Ai} \leftarrow \alpha_i \oplus \beta_{i-1} \oplus R_{Ai}\ (i = 2,\dots,k)$
		Verify $i_B = i_A$

Why here?

Alice and Bob visually verify that
there are no other users/devices in their integrity region.

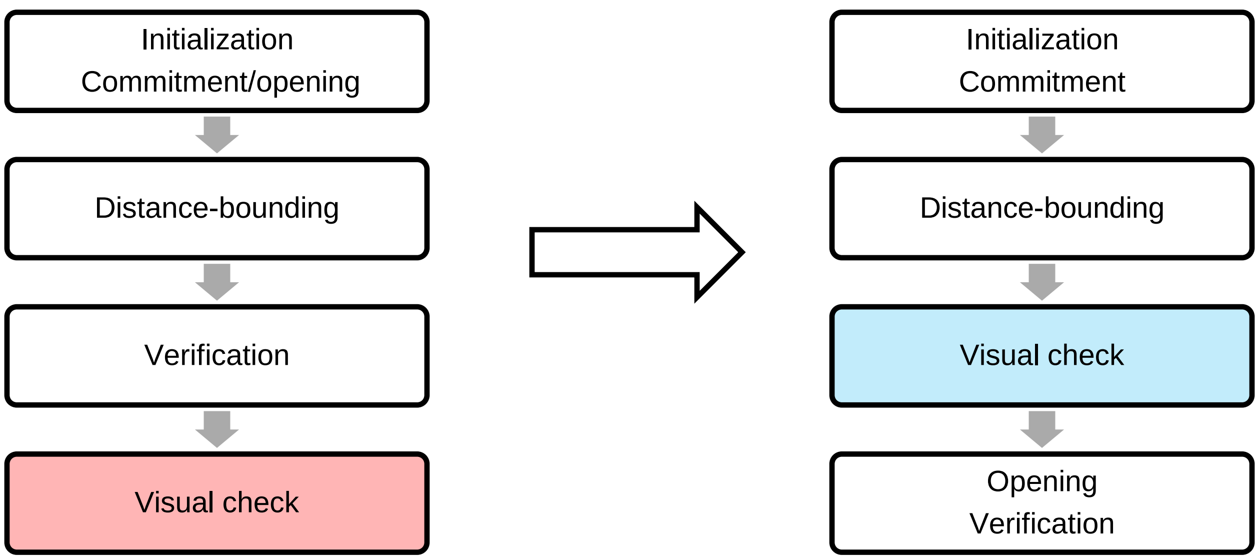
[6] M. Cagalj, S. Capkun, and J. -P. Hubaux, "Key agreement in peer-to-peer wireless networks," *Proceedings of the IEEE,* Volume 94, Issue 2, Feb. 2006.

Analysis of Existing DH-DB

- **Verification phase**
  - Vulnerable to the MITM attack
  - Insecure in reuse of DH public parameter
- **Distance-bounding phase**
  - Complicated procedures to hide verification string
- **Initialization phase**
  - Generate unnecessary random string for distance-bounding

New Design (Improved)

- **Commitment/opening triplet (f, y, x)**
  - f is an index of universal hash function
  - x is a random string such that f(x)=m where m is a message
  - y is a k-bit output of the collision-free hash function h(x), used for measuring RTT
- **Reordering of procedure**



Security

- **Resistance against the MITH attack**
  - Eve cannot open m without x.
  - h is a one-way hash function: Eve cannot find x easily even though she knows y, where $h(x)=y$.

We can use **y** for measuring RTT without any loss in security!

- **Secure reusability of DH public parameter**
  - The protocol is broken if Eve exists in integrity region before Alice and Bob exchange x_A and x_B.

Improved DH-DB (1/3)

- **Initialization phase**

Alice		Bob
Given ID_A, g^{X_A}		Given ID_B, g^{X_B}
Pick $N_A \in_U \{0,1\}^k$		Pick $N_B \in_U \{0,1\}^k$
$m_A \leftarrow 0 \| ID_A \| g^{X_A} \| N_A$		$m_B \leftarrow 1 \| ID_B \| g^{X_B} \| N_B$
$\boxed{(f_A, y_A, x_A) \leftarrow commit(m_A)}$		$\boxed{(f_B, y_B, x_B) \leftarrow commit(m_B)}$
	$\xrightarrow{f_A}$	
	$\xleftarrow{f_B}$	

  - Generate commitment/opening triplet

Improved DH-DB (2/3)

- **Distance-bounding phase**

Alice		Bob
The bits of y_A are $y_{A1},\ldots,y_{Ak}$		The bits of y_B are $y_{B1},\ldots,y_{Bk}$
	$\xrightarrow{y_{A1}}$	
	$\xleftarrow{y_{B1}}$	
	⋮	Simplified distance-bounding
	$\xrightarrow{y_{Ai}}$	Measure delay between y_{Bi-1} and y_{Ai}
Measure delay between y_{Ai} and y_{Bi}	$\xleftarrow{y_{Bi}}$	
	⋮	
	$\xrightarrow{y_{Ak}}$	Measure delay between y_{Bk-1} and y_{Ak}
Measure delay between y_{Ak} and y_{Bk}	$\xleftarrow{y_{Bk}}$	

Improved DH-DB (3/3)

Opening phase

Alice		Bob
Alice and Bob visually verify that there are no other users/devices in their integrity region.		
	$\xrightarrow{x_A}$	$m_A \leftarrow open(f_A, y_A, x_A)$
$m_B \leftarrow open(f_B, y_B, x_B)$	$\xleftarrow{x_B}$	Verify 0 in m_A; $i_B \leftarrow N_B \oplus N_A$
Verify 1 in m_B; $i_A \leftarrow N_A \oplus N_B$	$\xrightarrow{i_A}$	Verify $i_B = i_A$
Verify $i_A = i_B$	$\xleftarrow{i_B}$	

- Secure reuse of DH public parameter

Structure of Protocol (Summary)

Initialization and commitment	• Pick DH exponent • Commit messages (Send a locked box)
Distance-bounding	• Upper-bound the distance and make integrity region
Visual check	• Check the existence of attacker in the integrity region
Opening and verification	• Open messages(Unlock the box) • Check verification string for integrity

Analysis of Performance

- **Assumption**
  - Same universal and collision-free hash function
  - Only consider XOR operation
  - 3-DES random generator
- **Result**

	Message (success)	Message (fail)	Parameters	XOR Operation
Existing	2k+6	2k+4	18	-
Proposed	2k+6	2k+2	14	Reduce (7682*(k/64)-64)*2 operations

- When k=64, the number of reduced XOR operation is 15,236.

Conclusion

- **Contribution**
  - Provide improved DH-DB to the fundamental problem of key agreement over a radio link
  - Appropriate for devices which have **limited power, limited memory, and limited computational power**.