Design of improved DH-DB key agreement protocol for P2P wireless networks

2007 년 5 월 4 일

연세대학교 부호 및 정보이론 연구실

박 선 영, 김 주 영, 송 홍 엽

{sy.park, jy.kim, hysong} @yonsei.ac.kr

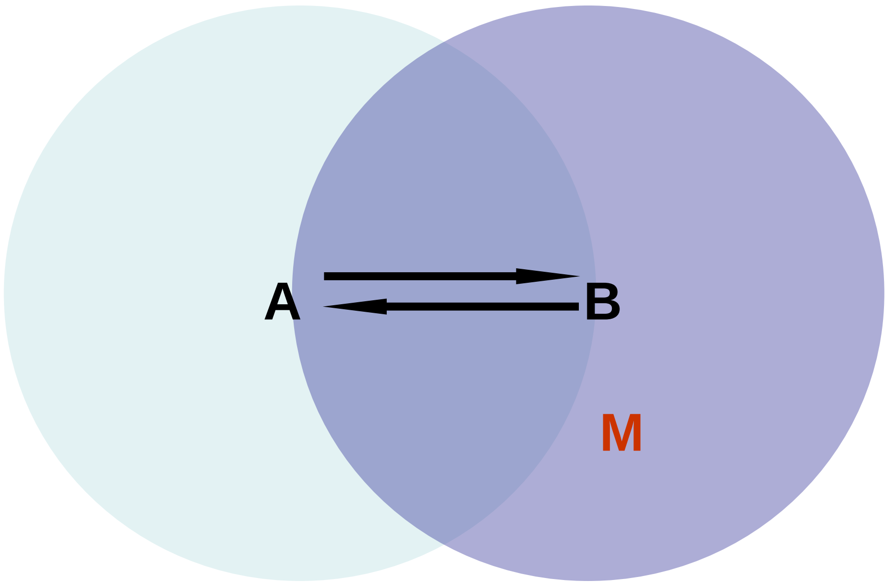
Contents

- Introduction
- Existing DH-DB protocol
- Improved DH-DB protocol
- Result and Discussion
- Conclusion
- Q & A

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

Existing DH-DB[1]



3 Phases

- Initialization
  - ✓ Generate unnecessary random string
- Distance-bounding
  - ✓ Complicated procedures for measuring the RTT
- Verification
  - ✓ Not secure in reuse of DH public parameter

- **Check integrity without involvement of users**

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

New Design Method

YONSEI UNIVERSITY

- **Commitment/opening triplet (*c*, *b*, *d*)**
  - *c:* universal hash function
  - *b*: *k*-bit output of collision-free hash function, used for measuring RTT
    - ✓ Output of hash function ensures randomness of *b.* [2]
- **Reordering of procedure**
  - Relocate visual verification between distance-bounding step and verification step
    - ✓ Ensure secure reuse of DH public parameters

[2] Mihir Bellare and Phillip Rogaway, Random Oracles are Practical: A Paradigm for Designing Efficient Protocols, ACM Conference on Computer and Communications Security 1993.

Improved DH-DB (1/2)

YONSEI UNIVERSITY

Initialization → **Distance-bounding** → **Opening**

Initialization

Alice		Bob
Given ID_A, g^{X_A}		Given ID_B, g^{X_B}
Pick $N_A \in_U \{0,1\}^k$		Pick $N_B \in_U \{0,1\}^k$
$m_A \leftarrow 0 \| ID_A \| g^{X_A} \| N_A$		$m_B \leftarrow 1 \| ID_B \| g^{X_B} \| N_B$
$(c_A, b_A, d_A) \leftarrow \text{commit}(m_A)$	c_A →	$(c_B, b_B, d_B) \leftarrow \text{commit}(m_B)$
	← c_B	

Generate commitment/opening triplet

Opening

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

Alice		Bob
	d_A →	$\hat{m}_A \leftarrow \text{open}(\hat{c}_A, \hat{b}_A, \hat{d}_A)$
		Verify 0 in $\hat{m}_A$; $i_B \leftarrow N_B \oplus \hat{N}_A$
	← d_B	
$\hat{m}_B \leftarrow \text{open}(\hat{c}_B, \hat{b}_B, \hat{d}_B)$		
Verify 1 in $\hat{m}_B$; $i_A \leftarrow N_A \oplus \hat{N}_B$	i_A →	
	← i_B	Verify $i_B = \hat{i}_A$
Verify $i_A = \hat{i}_B$		

Secure reuse of DH public parameters

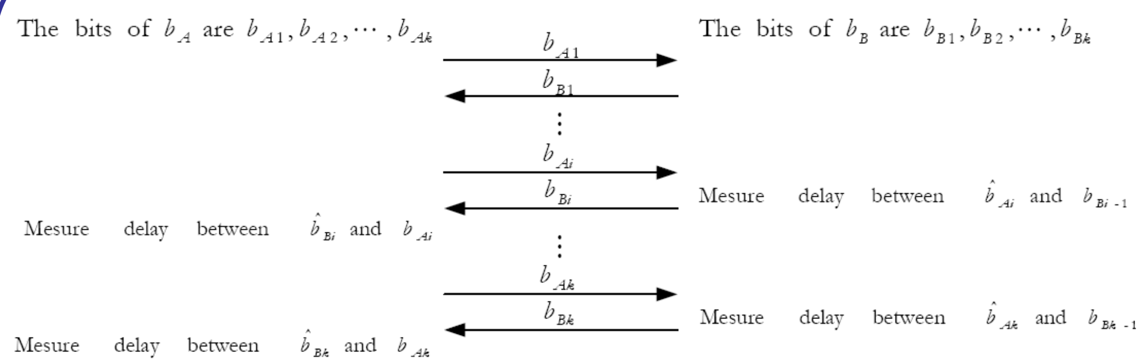
CITL

Improved DH-DB (2/2)

Initialization

Distance-bounding

Opening



Simplified distance-bounding

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	2*k*+6	2*k*+4	18	-
Proposed	2*k*+6	2*K*+2	14	(7682*(*k*/64)-64)*2 are reduced

  - If k=64,15,236 XOR operations are reduced.
- **Security**
  - The probability of MITM attack ≤$1/2^k$
  - Ensure reusability of DH public parameter

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**.

Thank you!

{sy.park, jy.kim, hysong} @yonsei.ac.kr