Diffie-Hellman Key Distribution Extended to Group Communication

Qingfeng He
Department of Computer Science
North Carolina State University
April 02, 2003

Agenda

- Introduction
- Problem Statement
- Generic n-Party D-H Key Distribution
- Group Key Distribution Protocols
- Related Work
- Protocol Comparison
- Limitations and Future Work

Introduction

- 2-Party Diffie-Hellman Key Exchange

Alice	Bob
Pick secret S_a randomly	Pick secret S_b randomly
Compute $T_A = g^{S_a} \bmod p$	Compute $T_B = g^{S_b} \bmod p$
Send T_A to Bob	Send T_B to Bob
Compute $T_B^{S_a} \bmod p$	Compute $T_A^{S_b} \bmod p$

Shared key is reached at both parties: $g^{S_a S_b} \bmod p$

Problem Statement

- Extend 2-Party D-H to n-Party
- Motivation
- Problem of Previous Approaches
  - Protocols are too theoretical
  - Protocol security unproven

Generic n-Party D-H Key Distribution (1)

- Notation
  - n: number of participants in the protocol
  - α: exponentiation base
  - q: order of the algebraic group
  - M_i: i-th group member, i is the index
  - N_i: random exponent generated by group member M_i
  - S: subsets of $\{N_1, \ldots, N_n\}$
  - $\Pi(S)$: product of all elements in subset S
  - K_n: group key shared among n members

Generic n-Party D-H Key Distribution (2)

- Priori
  - All n participant agree on a cyclic group G, of order q and the base α
  - Each member M_i chooses a random value $N_i \in G$

Generic n-Party D-H Key Distribution (3)

- Generic Protocol:
  - Distributively revealing and computing a subset of $\{\alpha^{\Pi(S)} | S \subset \{N_1, \ldots, N_n\}\}$
  - From these subsets, member M_i computes $\alpha^{N_1 \cdots N_{i-1} N_{i+1} \cdots N_n} \bmod q$
  - Finally, M_i computes the shared key K = $\alpha^{N_1 \cdots N_n} \bmod q$

Generic n-Party D-H Key Distribution (4)

- Protocol Security Assumption
  - 2-party D-H key distribution is secure
- Proof: by induction on n

Group Key Distribution Protocol (1)

- Group Key Distribution: GDH.1
  - Upflow: M_i receives the set $\{\alpha^{N_1}, \alpha^{N_1N_2}, \ldots, \alpha^{N_1\cdots N_{i-1}}\}$ and forwards to M_{i+1} $\{\alpha^{N_1}, \alpha^{N_1N_2}, \ldots, \alpha^{N_1\cdots N_i}\}$, $i \in [1, n-1]$
  - Example: M_4 receives the set $\{\alpha^{N_1}, \alpha^{N_1N_2}, \alpha^{N_1N_2N_3}\}$ and forwards to M_5 $\{\alpha^{N_1}, \alpha^{N_1N_2}, \alpha^{N_1N_2N_3}, \alpha^{N_1N_2N_3N_4}\}$

Group Key Distribution Protocol (2)

- GDH.1 (Cont'd)
  - Downflow:
    - M_i uses the last intermediate value to compute K_n $(1<i<=n)$
    - M_i then raises all remaining values to the power of N_i and forwards the resulting set to M_{i-1}
  - Example: M_4 receives the set $\{\alpha^{N_5}, \alpha^{N_1N_5}, \alpha^{N_1N_2N_5}, \alpha^{N_1N_2N_3N_5}\}$ and forwards to M_3 $\{\alpha^{N_5N_4}, \alpha^{N_1N_5N_4}, \alpha^{N_1N_2N_5N_4}\}$

Group Key Distribution Protocol (3)

- Group Key Distribution: GDH.2
  - Upflow: M_i composes i intermediate values and one cardinal value and forwards the resulting set to M_{i+1} ($i < n$)
  - Example: M_4 receives the set $\{\alpha^{N_1N_2N_3}, \alpha^{N_1N_2}, \alpha^{N_1N_3}, \alpha^{N_2N_3}\}$ and forwards to M_5 $\{\alpha^{N_1N_2N_3N_4}, \alpha^{N_1N_2N_3}, \alpha^{N_1N_2N_4}, \alpha^{N_1N_3N_4}, \alpha^{N_2N_3N_4}\}$

Group Key Distribution Protocol (4)

- GDH.2 (Cont'd)
  - Downflow:
    - M_n raises every intermediate value to the power of N_n broadcasts the resulting values to all group members, in another word
    - M_n broadcasts the set $\{\alpha^{N_1 \cdots N_{i-1} N_{i+1} \cdots N_n}\}$ to M_i ($i < n$)
  - Example: M_4 receives the set $\{\alpha^{N_1N_2N_3N_5}\}$ from M_5 (Assume n=5)

Group Key Distribution Protocol (5)

- Group Key Distribution: GDH.3
  - Upflow: M_i receives the set $\{\alpha^{N_1}, \alpha^{N_1 N_2}, \ldots, \alpha^{N_1 \ldots N_{i-1}}\}$ and forwards to M_{i+1} $\{\alpha^{N_1}, \alpha^{N_1 N_2}, \ldots, \alpha^{N_1 \ldots N_i}\}$, $i \in [1, n-2]$
  - Broadcast: M_{n-1} broadcasts the set $\{\alpha^{N_1 \ldots N_{n-1}}\}$ to M_i (i != n-1)

Group Key Distribution Protocol (6)

- GDH.3 (Cont'd)
  - Response: M_i ($i < n$) factors out its own component and forwards the set $\{\alpha^{N_1 \ldots N_{i-1} N_{i+1} \ldots N_{n-1}}\}$ to M_n
  - Broadcast: M_n raises every input to the power of N_n and broadcasts the resulting set $\{\alpha^{N_1 \ldots N_{i-1} N_{i+1} \ldots N_n}\}$ to M_i ($i < n$)

Group Key Distribution Protocol (7)

- Properties Comparison

	GDH.1	GDH.2	GDH.3
Rounds	2(n-1)	n	n+1
Messages	2(n-1)	n	2n-1
Combined message size	n(n-1)	(n-1)(n/2+2)-1	3(n-1)
Exponentiations per M_i	i+1, n	i+1, n	4, 2, n
Total exponentiations	(n+3)n/2-1	(n+3)n/2-1	5n-6

Group Key Distribution Protocol (8)

- Alteration of Group Membership
  - Member addition
  - Member deletion

Group Key Distribution Protocol (9)

- Protocol Advantages
  - No synchronization
  - Small number of exponentiations
  - Minimal total number of messages (GDH.2)
  - Minimal number of rounds for asynchronous operation (GDH.2)
  - Minimal number of messages sent/received by each participant (GDH.2)
  - Security equivalent to 2-party D-H
  - Implementation simplicity

Related Work

- Ingemarsson et al. (ING)
  - Requires a synchronous startup
  - All participants must be arranged in a logical ring
- Burmester/Desmedt (BD)
  - $K_n = \alpha^{N_1N_2+N_2N_3+\ldots+N_nN_1}$
  - Cheap exponentiation operations because of relatively small exponents involved in almost all operations
  - Time (number of rounds: 2): *simultaneous* broadcasts
  - BD* (without simultaneous broadcast): 2n-1 rounds

Protocol Comparison (1)

- Comparison with GDH protocols
  - Number of rounds
    - GDH.3: n-1 simultaneous unicasts to M_n (less load compared with BD)
    - BD: n simultaneous broadcasts
  - Communication bandwidth overhead
    - GDH.2: n messages
    - BD*: least total information changed

Protocol Comparison (2)

- Comparison with GDH protocols (Cont'd)
  - Protocol efficiency (number of messages received and sent by each participant)
    - GDH.2: least overhead with respect to the communication infrastructure
  - Protocol symmetry
    - BD/BD* and ING: offer symmetric operations
    - GDH protocols: asymmetric

Protocol Comparison (3)

	ING	BD	GDH.2	GDH.3
Rounds	n-1	2	n	n+1
Messages	n(n-1)	2n	n	2n-1
Combined message size	n(n-1)	2n	(n-1)(n/2+2)-1	3(n-1)
Exponentiations per M_i	n	n+1	i+1, n	4, 2, n
Total exponentiations	n^2	n(n+1)	(n+3)n/2-1	5n-6
Divisions per M_i		1		

Limitations and Future Work

- Do not provide authentication of the participants
- Do not handle periodic re-keying
- Formal proof to support optimality/minimality claims

Thank you

- Questions?