Secure Group Communication over Wireless Ad Hoc Networks

by Yueh-Min Huang et al.
Presented by Navid Golpayegani

Overview

- Definitions
- Background
- Implementation
- Conclusion
- References

Definitions

- Local Area Network (LAN)
  - Group of hosts on the same physical network
- Virtual LAN (VLAN)
  - Group of hosts communicating as if located on the same LAN

Definitions

- Mobile ad hoc network (MANET)
  - System made up of wireless nodes
  - Self configuring
- Group Communication
  - Many-to-Many transmission

Definitions

- Diffie-Hellman Key exchange
  - Establish shared secret key
  - No prior knowledge of each other necessary
  - Key established over insecure channel
  - Group Diffie-Hellman

Overview

- Definitions
- Background
- Implementation
- Conclusion
- References

Background

- VLAN
  - IEEE 802.1Q
  - Frames belonging to a VLAN contain VLAND ID (VID)
  - Filtering Database (FDB) stores information of all groups
    - even unrelated

Background

- Group Diffie-Hellman
  - well known parameters
    - prime number q
    - integer $a < q$

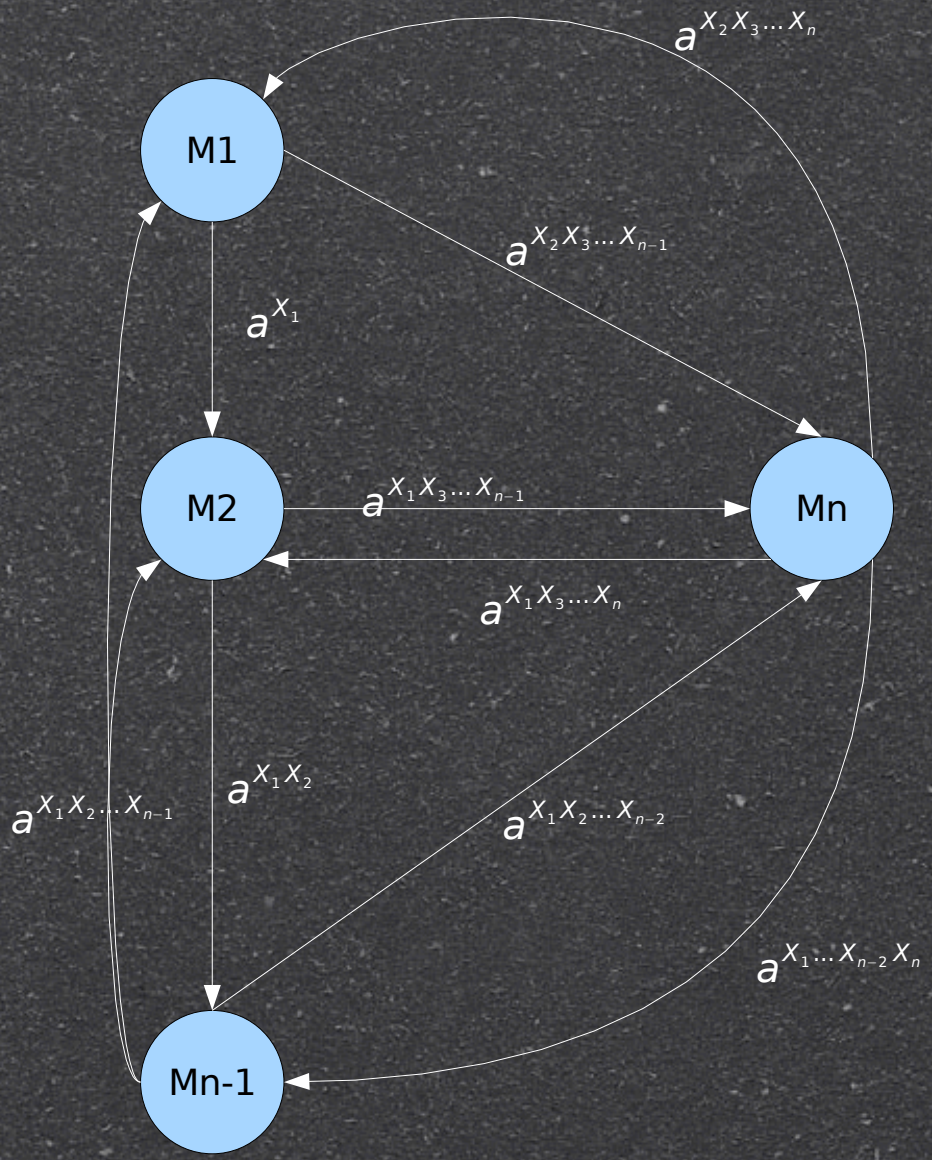
Background

- Node M_1 sends $a^{X_1} \ mod \ q$ to M_2
- Node M_2 sends $a^{X_1 X_2} \ mod \ q$ to M_3
- Node M_{n-1} broadcasts final value to all Nodes
- All nodes remove their X_i value and send $a^{\prod \{X_j | j \subset [1..n-1] \wedge j \neq i\}} \ mod \ q$ to X_n

Background

- M_n receives each value and raises it to X_n
- New value returned to each node
- Each node raises the value to X_i
- They now all share the same secret value

Background


M1
M2
Mn
Mn-1
$a^{x_2 x_3 \ldots x_n}$
$a^{x_2 x_3 \ldots x_{n-1}}$
a^{x_1}
$a^{x_1 x_3 \ldots x_{n-1}}$
$a^{x_1 x_3 \ldots x_n}$
$a^{x_1 x_2 \ldots x_{n-1}}$
$a^{x_1 x_2}$
$a^{x_1 x_2 \ldots x_{n-2}}$
$a^{x_1 \ldots x_{n-2} x_n}$

Overview

- Definitions
- Background
- Implementation
- Conclusion
- References

Overall Design

- Centralized agent keeps track of groups
- Communication with centralized agent is assumed to be secure
- Communication done in several stages

Overall Design

- Packet includes a Virtual Subnet Identifier (VSID)
- Nodes maintain a forwarding cache table to store VSID for relaying
  - Table is populated when a cache request is received (CREQ)

Initiation Stage

- Arriving node contacts centralized agent requesting to create/join group
- Agent assigns hash function h(), security parameters q and a

Creation Stage

- Start of Group communication
- Node broadcasts VS-REQUEST packet
  - Nonce
  - ID
  - $h(Nonce_s||ID_s)$

Creation Stage

- Compute h'($Nonce_s$||ID_s) to determine if receiver is in same group
  - same groups have same h()
  - VS-REPLY packet sent pack if in same group
    - $Nonce_i$
    - ID_i
    - h($Nonce_i$||ID_i)

Creation Stage

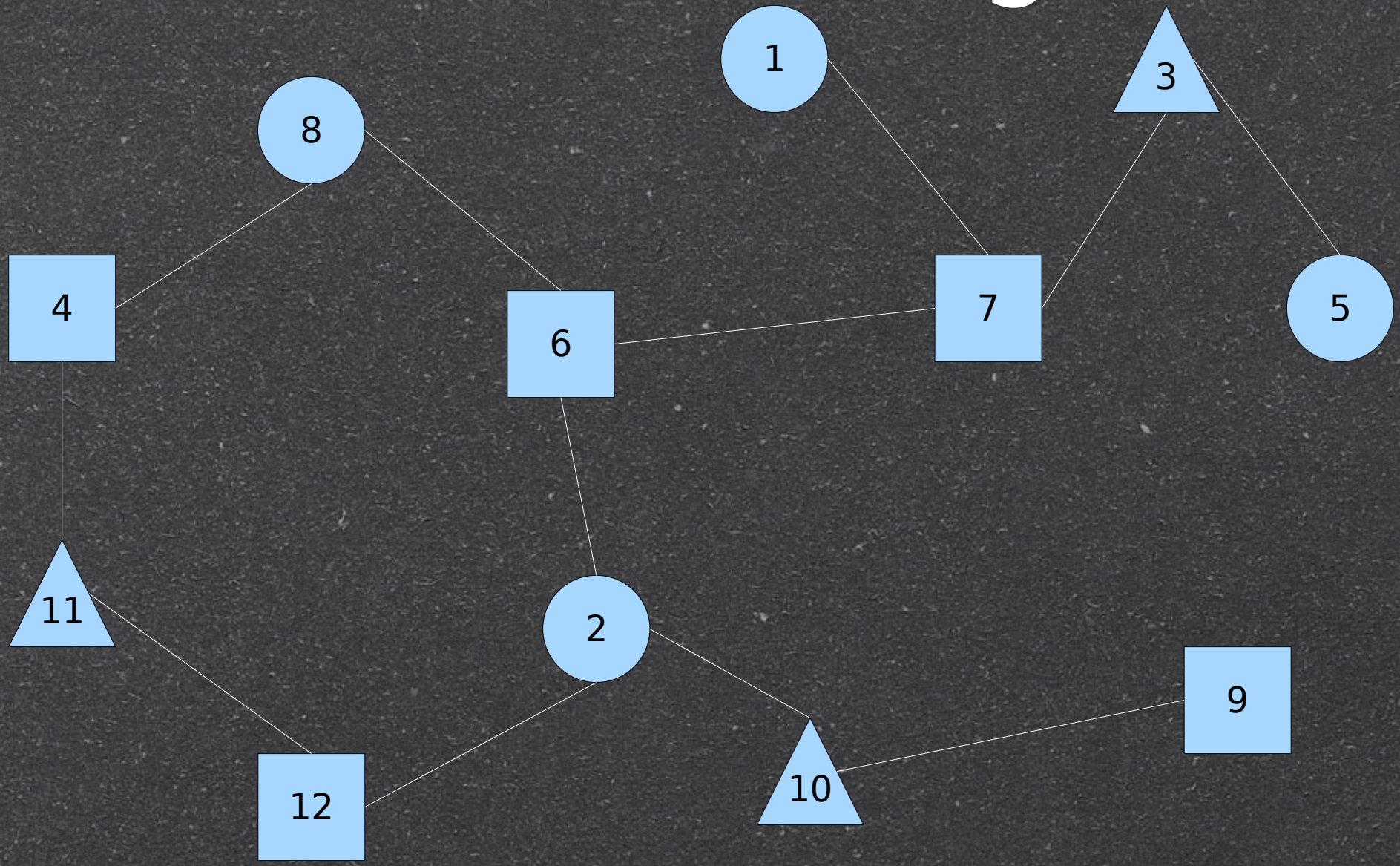
- If receiver has neighbors VS-REQUEST is relayed

Group	Existing Neighbors	Nonexisting Neighbor
Same	Reply and Relay	Reply
Different	Relay	Ignore

Creation Stage

- Initiator collects all IDs
- Creates a VSID
- Propagates subnet information to members via multicast
  - Nonce, ID, VSID, Member List, h(Nonce||ID)
- Members exchange routing information
  - Find shortest path and send CREQ

Creation Stage



Maintenance Stage

- Periodically advertise CREQ to neighbors
  - Node ID, VSID
- If no CREQ received in a while or no packets forward for VSID
  - remove from forwarding table

Transmission

- Set VSID in packet and send
  - accept packet
    - first time received
    - belong to VSID
  - relay packet
    - VSID in forwarding table
  - drop packet

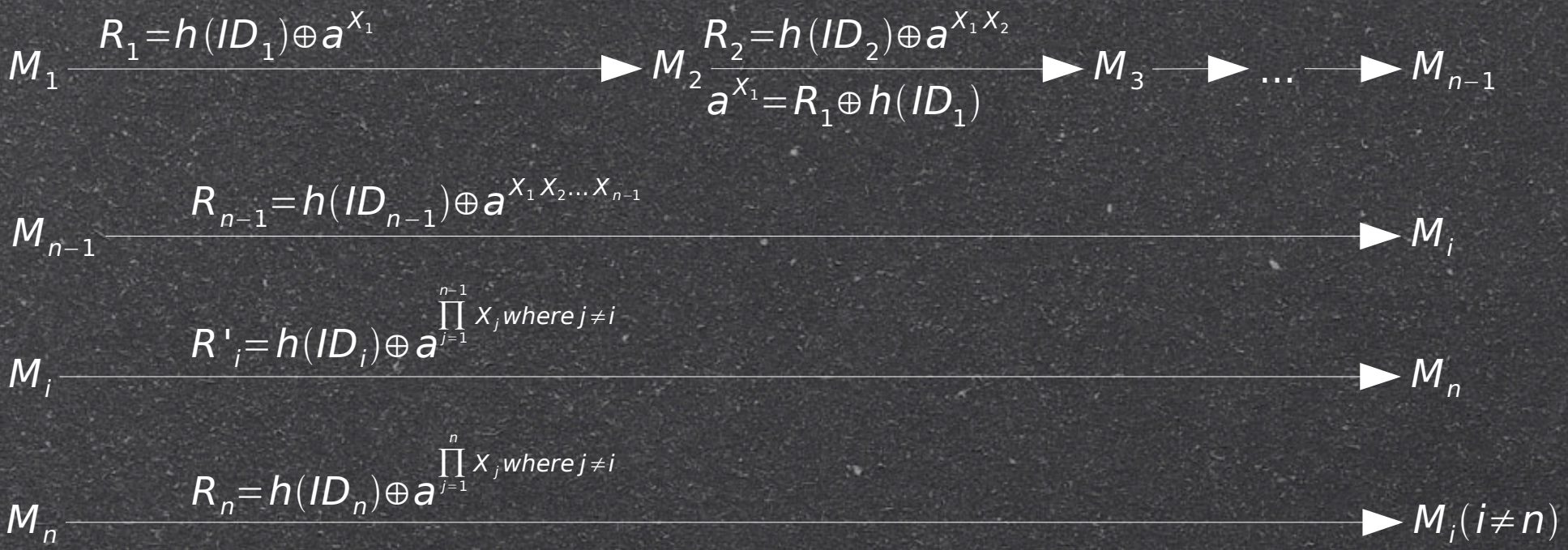
Group Key Agreement

- Each node generates X_i and $Y_i = a^{X_i}$
- Transmit $h(ID_i) \oplus Y_i$ to i+1
- i+1 retrieves a^{X_i} and transmits $a^{X_i X_{i+1}}$
- Node n-1 performs same operation and sends result to all nodes except n

Group Key Agreement

- All nodes factor out their X_i
- Send value to node n
- Node n adds its own X_n and returns value to i
- Node i adds X_i back
- All nodes now have same secret value

Group Key Agreement



Group Key Agreement

- New members send VS-JOIN
  - Nonce, ID, h(Nonce||ID)
- Existing member sends VS-REFRESH
  - Nonce, ID, VSID, member list, h(Nonce||ID)
  - New Key agreement

Group Key Agreement

- Leaving members send VS-QUIT
  - Nonce, ID, h(Nonce||ID)
  - Multicast
  - Members drop ID from member list
  - Restart Key Agreement

Overview

- Definitions
- Background
- Implementation
- Conclusion
- References

Conclusion

- Exponent computation
  - 5n-6
- Message exchange
  - 3(n-4) unicasts
  - 1 multicast

Conclusion

- No experimental analysis
- Inefficient with large number of nodes and frequent leave/join
- Some claims without explanation
  - Shortest path from routing info
- XOR similar to one time pad
  - Only secure if used once

References

- “Constructing Secure Group Communication over Wireless Ad Hoc Networks based on a Virtual Subnet Model”
- “One-Time-Pads”, http://www.schneier.com/crypto-gram-0210.html#7, Bruce Schneier