Multicast Security: A Taxonomy and Some Efficient Constructions

By Cannetti et al, appeared in INFOCOMM 99.

Presenter:
Ankur Gupta

Mulititcast Communication

- Examples: Internet video transmissions, news feed, stock quotes, live broadcast, on-line video games, etc.
- Challenges:

1. Security: Authentication, secrecy, anonymity, etc.
2. Efficiency: the overhead associated in providing security must be minimized: communication cost, authentication/verification time.

Multicast Issues

- Member characteristics: similar computing power or some more powerful than others?
- Membership static or dynamic? Key revocation is an issue for dynamic scenes.
- Number and type of senders? Single or multiple? Can non-members send data?
- Volume and type of traffic? Is communication in real-time?

Multicast Security Issues

- Secrecy

1. Ephemeral: Avoid easy access to non-members. Ok if non-members receive after a delay.
2. Long-term: protecting confidentiality of data for a long duration.

- Authenticity:

1. Group authenticity: each member can recognize if a message was sent by a group member.
2. Source authenticity: each member can identify the particular sender in the group.

Multicast Security Issues: Contd.

- Anonymity: keeping identity of group members secret from non-members and/or from other group members.
- Non-repudiation: ability of receivers of data to prove to 3rd parties that data was received from a particular entity. Contradicts anonymity.
- Access control: only registered and legitimate users have access to group communication. Requires authentication of users.
- Service Availability: keeping service available in presence of clogging attacks.

Performance Issues

- Latency
- Work overhead per sending
- Bandwidth overhead
- Group management activity should be minimized:

1. Member initialization
2. Member addition/deletion

General Solution Impossible!

- Impossible to find a general solution that address all the above issues.
- Identify scenes representative of practical multicast communication.

1. Single source broadcast.
2. Virtual Conference.

Single source bcast: Issues

1. Source: high-end machine, expensive computation ok at server end.
2. Recipients low-end. Efficiency at recipients is a concern.
3. Membership is dynamic and changes rapidly.
4. High volume of sign-in/sign-off possible.
5. Ephemeral secrecy generally suffices.
6. Authenticity of data critical (e.g. stock quotes).

Issues in Single source bcast

- Ephemeral secrecy: solved by having a group management center that handles access control and key management.
- How to authenticate messages?
- How to make sure that a leaving member loses the capability to decrypt?

Virtual Conferencing

- Online meeting of executives, interactive lectures and classes, multiparty video games.
- Membership usually static. No. of receivers far less than single source bcast.
- Authenticity of data and sender is critical.
- Sender and receiver of similar computation power.

Efficient Authentication Schemes

- Public key cryptography signatures is very expensive.
- Instead, we will use message authentication codes (MAC),

  MAC(k,M)= secure hash
- MACs are computationally much more efficient than digital signatures.

MAC Attacks

- Per-Message unforgeability of MAC scheme

1. Complete attack: an attacker can break any message of its choice.
2. Probabilistic attack: an attacker can forge a random message with some fixed but small probability.

Q-per message unforgeable

- A MAC scheme is q-per message unforgeable if an adversary can guess its MAC value with probability at most q.

- Assumption: we will assume there are at most w corrupted users.

Authentication scheme for single source

- Source knows l=e(w+1)log(1/q) keys, $R=hK_1,\ldots,K_li$.
- Each recipient u knows a subset of keys R_u ½ R. Every key K_i is included in R_u with probability 1/(w+1), independently for every i and u.
- Message M is authenticated by S with each key K_i using MAC and hMAC(K_1,M),…,MAC(K_l,M)i is transmitted.
- Each recipient u verifies the all MACs which were created with keys in R_u. If any of them is incorrect then rejects the message.

Performance Analysis of the scheme

- Source holds $M_S = l = e(w+1) \log(1/q)$ keys.
- Each receiver holds $M_V = e \log(1/q)$ keys.
- Communication overhead per message $C = e(w+1)\log(1/q)$ MACs.
- Running time overhead $T_S = e(w+1)\log(1/q)$ MAC computations for source and $T_V = e \log(1/q)$ per receiver.

Security of scheme

- Theorem: Assume probability of computing MAC without knowing key is q'. Then probability that a coalition of w users can falsely authenticate a message to a user is at most q+q'.

Proof: Probability that key is good (contained in user u's subset but not in any of colluders set) is:

$$g = \frac{1}{w+1}(1-\frac{1}{w+1})^w = \frac{1}{(w+1)(1+1/w)^w} > \frac{1}{e(w+1)}$$

Proof: Contd

- Therefore probability that R_u is completely covered by subsets held by colluders is $(1-g)^l < q$. If R_u is not covered completely, then there is a key K_i not known to any colluder. Therefore, its corresponding MAC can be guessed with probability at most q'. By union bound, we get guessing probability as q+q'. QED.

Multiple Dynamic Sources

- Assumption: Pseudo-random one-way hash functions $\{f_k\}$
- Distinguishes between set of senders and receivers. Only a coalition of w or more receivers can falsely authenticate a message to a receiver.
- l primary keys hK_1,…, K_li where l is as in single source scheme.
- Receiver initialization: each receiver v obtains a subset R_v of primary keys where each key K_i is included with probability 1/(w+1) in R_v
- Sender Initialization: every u receives a secondary set of keys hf_{k1}(u), …, f_{kl}(u)i. Can be sent whenever a sender joins.
- Message authentication: each receiver verifies all MACs whose key its has.

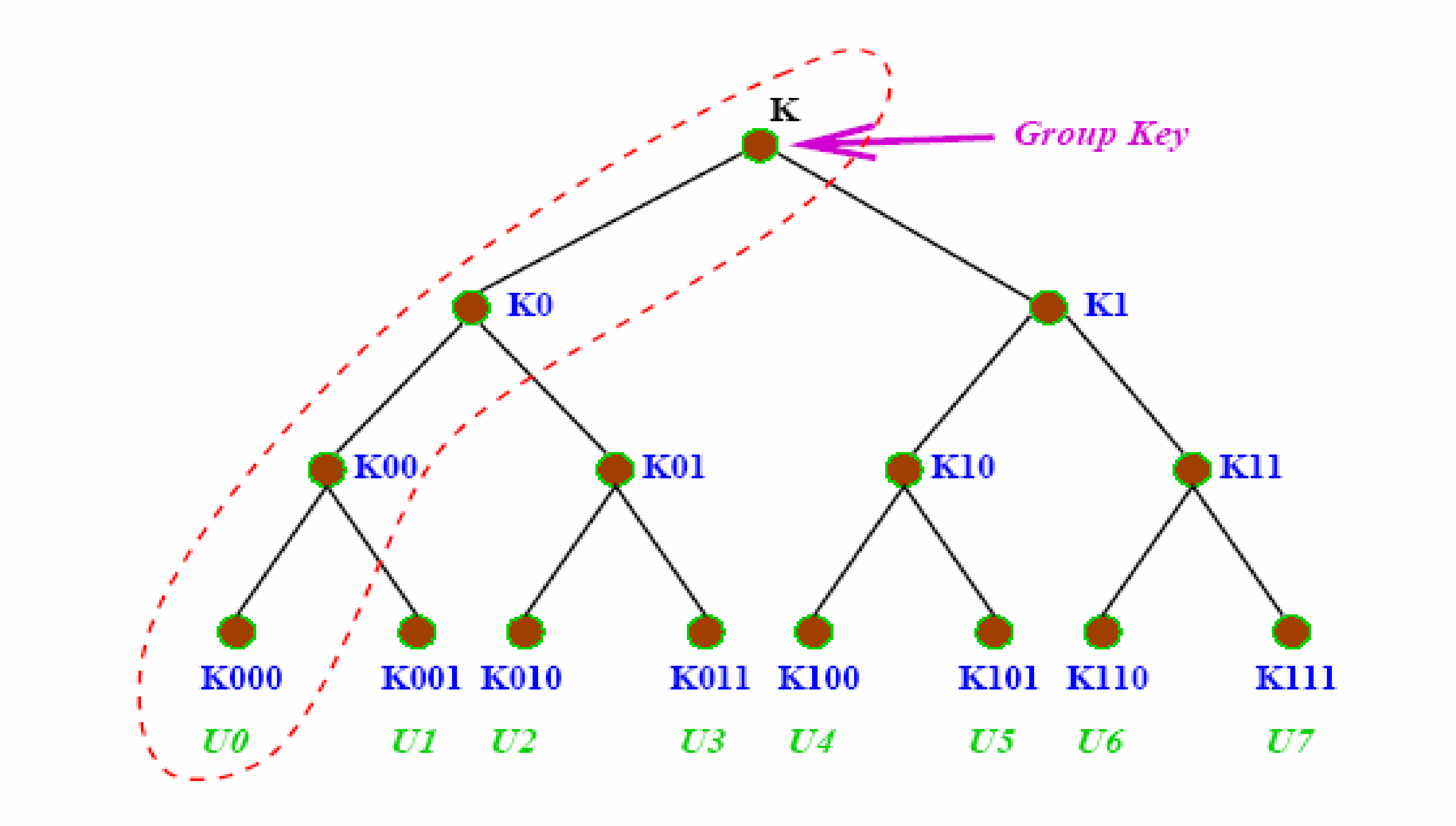
Dynamic Secrecy: User Revocation

- How to manage keys when a user leaves a group?
- We want that the old user is not able to decrypt the current communication in the group.
- Application: pay-TV applications.
- Solution: A tree based scheme will be presented now.

Tree based scheme

- Assume we have $n=2^m$ users.
- Scheme will require 2m-1 key encryptions to delete a member.
- Let u_0, u_1,…, u_{n-1} be n users. They all share a group key k with which messages are encrypted. When a user leaves, a new key k’ must be distributed.
- Users are associated with the leaves of a tree of depth m. Every node v is associated with a key k_v and each user has all keys from its leaf node to the root node.

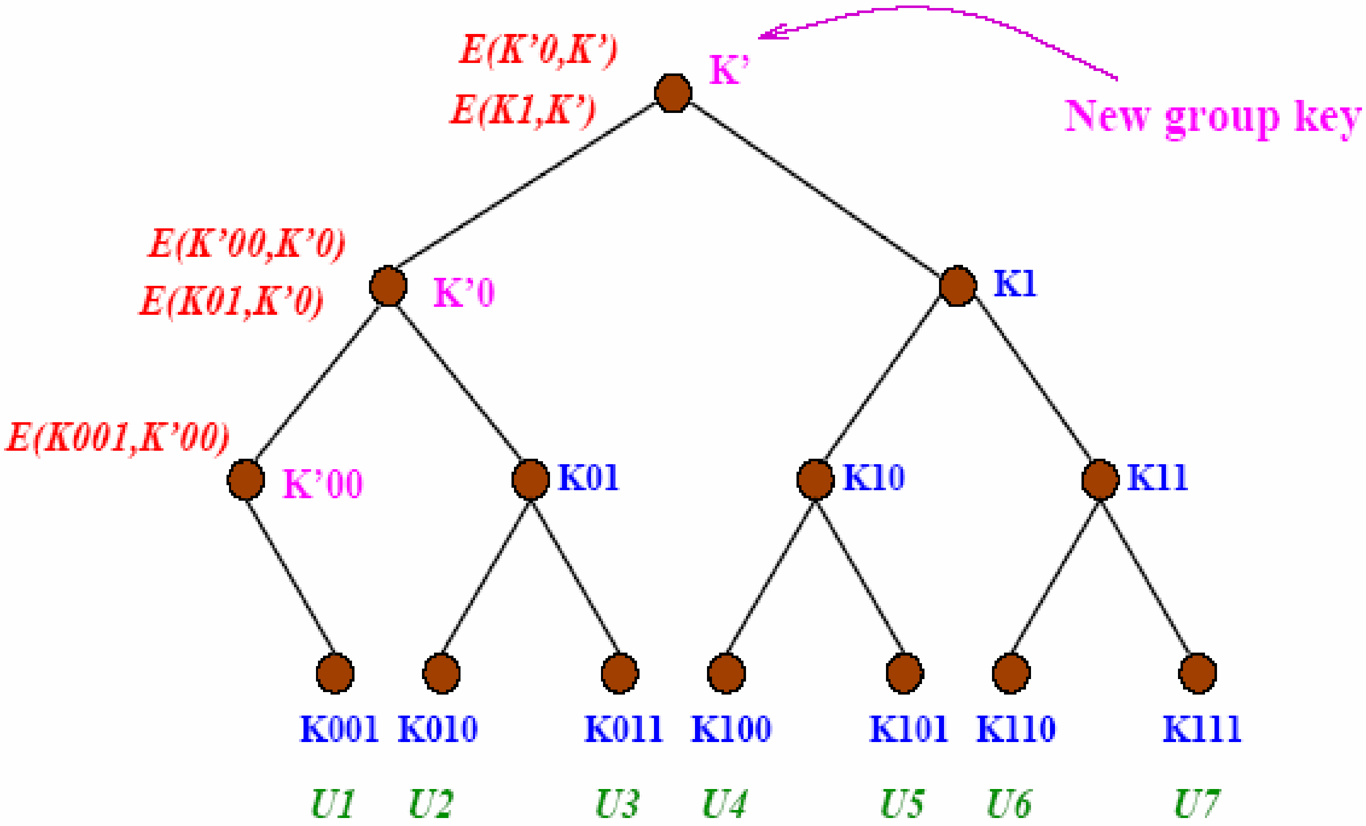
Graphic View of Initial Keys



Deleting a member

- Group controller associates a new key k'_v for every node v along the path from node u to root.
- $k'_{p(u)}$ is encrypted with $k_{s(u)}$ where p(u) is parent and s(u) sibling of u.
- All other keys $k'_{p(v)}$ is encrypted with k'_v and $k_{s(v)}$.
- All encryptions are sent to users.
- Every user is able to get every key it is intended to receive and nothing else.

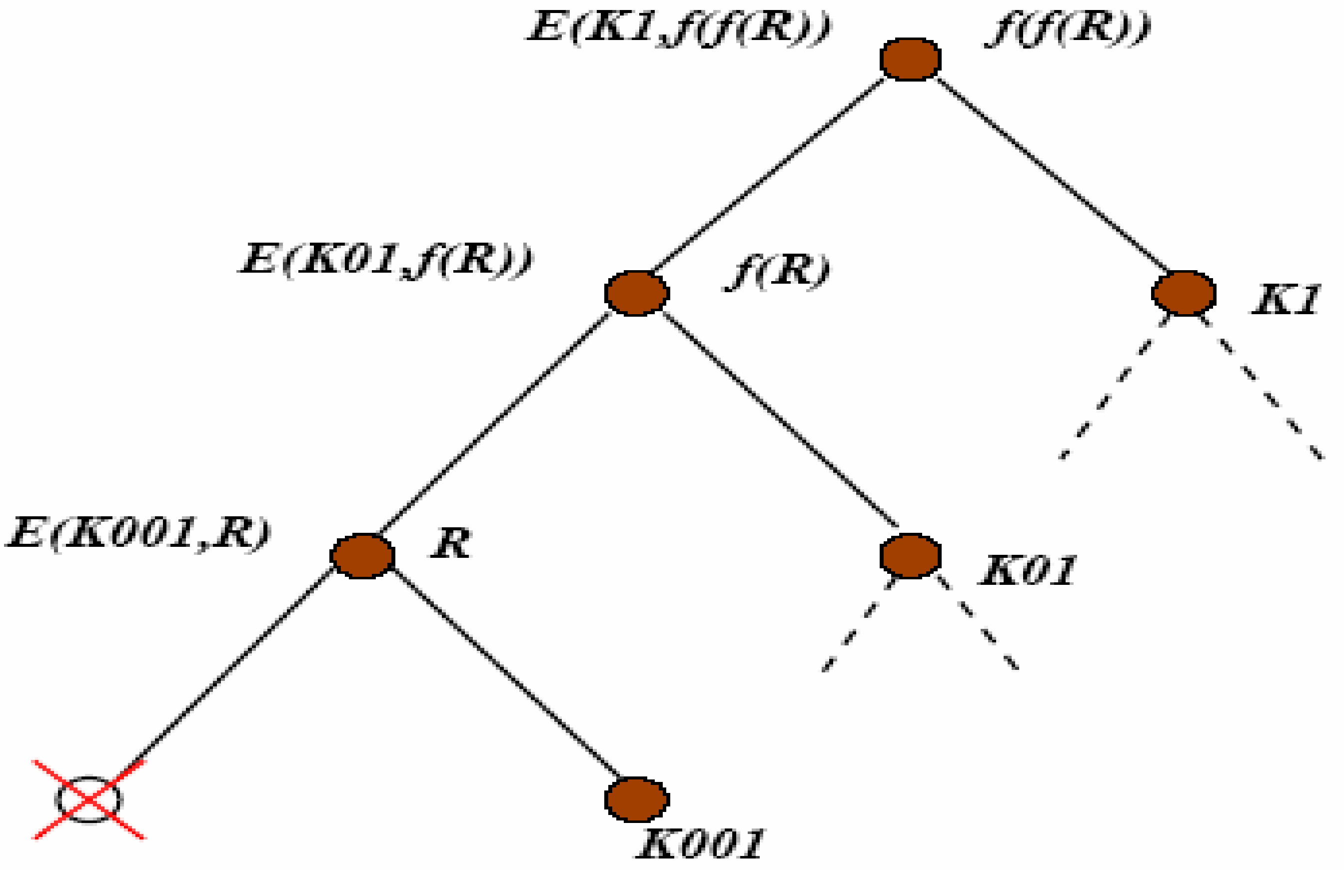
Graphical View for Deletion



Improved Scheme

- Reducing communication overhead from 2m to m.
- Assume a PRG that doubles its input $G(x)=L(x)R(x)$ where $|x|=|L(x)|=|R(x)|$
- Associate a value $r_v=R^{d(u)-d(v)-1}(r)$ where $R^0= r$ (a random value) and $d(v)$=depth of node v.
- Key $k'_v=L(r_v)=L(R^{d(u)-d(v)-1}(r))$
- Each $r_{p(v)}$ is encrypted with $k_{s(v)}$ and sent to all users.

Graphical view of improved scheme



Conclusions

- Secrecy in multicast communication comes in many flavors: group vs source authentication, long-term vs ephemeral secrecy, anonymity vs non-repudiation etc.
- Benchmarks: a) single source and large no. of recipients b) virtual conferencing: modest no. of senders and receivers.
- Authentication based on MAC codes.
- Key revocation using tree based approach.

Thank You!