Multicast Security

F. Bergadano, D. Cavagnino, B. Crispo
Dipartimento di Informatica, Università di Torino

Plan

- Importance of Multicast
- Session Management
- Transport Protocols
- Security
  - Objectives
  - Obvious techniques
  - Problems of the obvious techniques
  - Proposed solutions

Growing interest in multicast

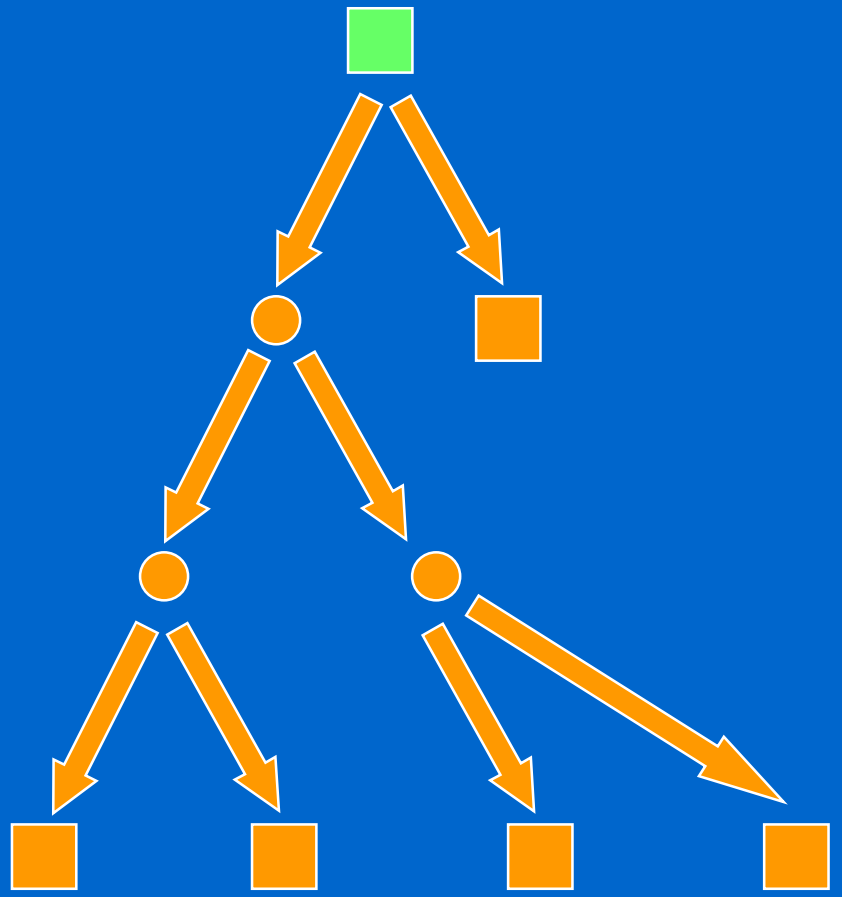
- Increase in multimedia content
- Increase in one-to-many traffic
  - web sites with very large audiences
  - ‘push’ technologies
  - streaming audio/video in web sites
- Possible widespread use of conferencing

Multicast saves resources

sender

receiver

mrouter



Multicast Sessions (‘Conferences’)

- Initiator creates session
  - obtains IP multicast address
  - advertises session characteristics (SDP/SAP)
- Senders send ‘to the group’ (IP - class D addr)
- Receivers join the group (IGMP)
- Routers manage to deliver data (PIM, DVMRP)
- Receivers may reserve QoS (RSVP)

Multicast Transport

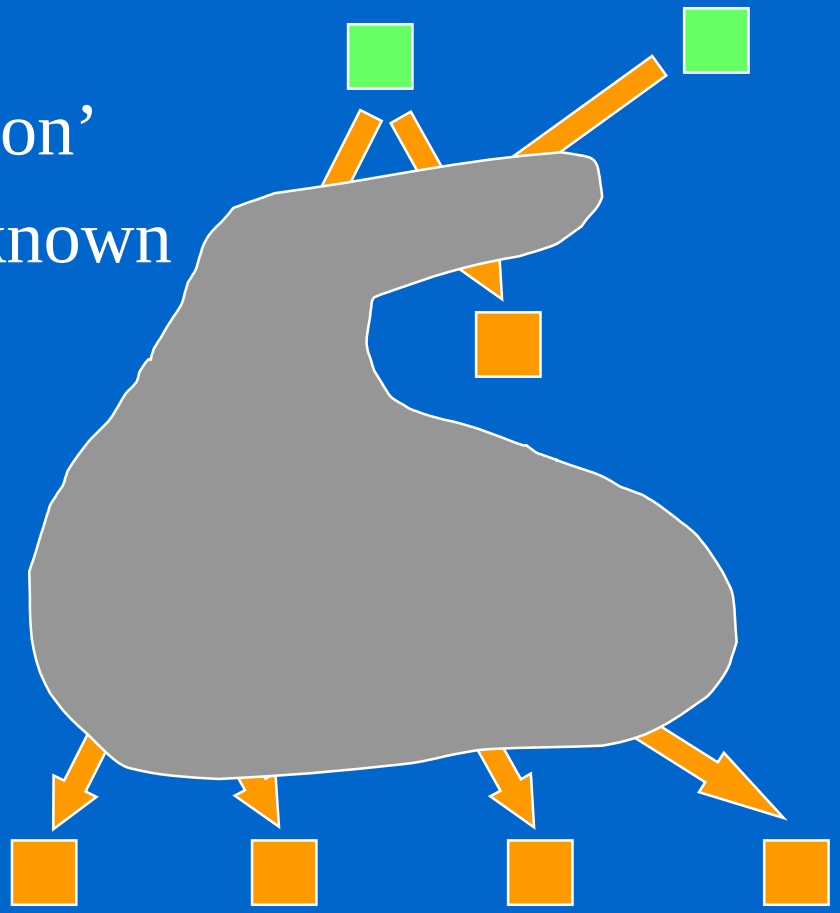
- Normally over UDP
- Timely data delivery for audio/video (RTP)
- Receivers provide management and performance information (RTCP)
- Reliable transport possible (RMTP, PGM) with flow control (no congestion control yet)

Security needed in Multicast

- Privacy (e.g. for conferencing, data distribution)
- Protecting content (e.g. subscriber broadcast)
- Authentication (e.g. for conferencing, broadcast)
- Billing/accounting (for session management, reservation or traffic)

Security difficult

- No unicast ‘connection’
- Receivers not even known
- Receivers can become senders
- Scaling problems



The ‘obvious’ solution

Standard scenario:

distribute a session key ‘somehow’ (e.g., with PK encryption) and then use it to encrypt and generate a MAC for each block of data

Problems of the ‘obvious’ solution

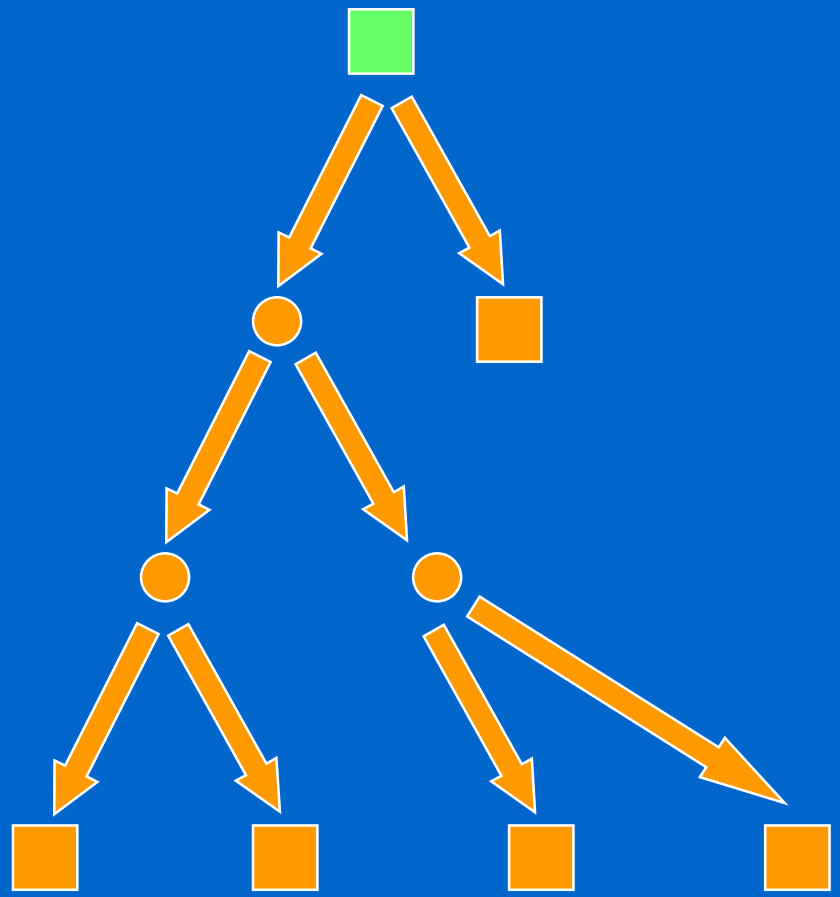
Problem 1:

key management

Problem 2:

individual

authentication



(Symmetric) Key management

- Key distribution
- Key refresh
- Group membership revocation

Key Distribution

Again, there are ‘obvious’ ways to do it:

a Key Distribution Center (KDC) unicasts session keys to each group member, encrypted with her PK or with a shared key

but:

Scaling problem, PKI or shared keys needed

Key Distribution

GKMP [RFC 2093,2094] a symmetric variation of this obvious scheme:

A group controller GC (a per-group KDC) generates session keys, sends them to each group member GM, encrypted with K(GC,GM)

but still:

Scaling problem, long-term shared keys needed

Key Distribution

SMKD [RFC 1949] a scalable variant:

The GC generates session keys, delegates private distribution of keys to routers

but:

Routers trusted, PKI or shared keys needed

best implemented with CBT routing

Key Distribution

[Mittra, ACM SIGCOMM 97] also scalable, further simplifies member revocation:

The GC shares keys with GIs (group intermediaries) , GIs share different keys with individual group members

but:

GIs trusted, re-encryption delay

Key refresh and membership revocation

- Redistribution
- Redistribution in subgroup [Mittra, ACM SIGCOMM 97]
- Broadcast Encryption [Fiat and Naor, Crypto 1992]

Individual authentication

- Many MACs
  - authentication data long
  - key management very complex
- Digital Signatures
  - inefficient for multicast end applications
  - inefficient if considered by routers

Individual authentication existing solutions

- Online/offline signatures [Even, Goldreich, Micali, Crypto 1989]
- One-time signatures [Gennaro & Rohatgi, Crypto 1997]
- Many MACs, but not as many as there are users [Canetti et al., 1998]

Individual authentication needed for billing/accounting

- RSVP [RFC 2205]
- RSVP over IPSEC [RFC 2207]
- RSVP authentication [Baker-Lindell 1999]
- SAPv2 authentication/encryption
- Flow authentication for maching usage to reservations (against ‘theft of service’) and announcements (against ‘session stealing’)

Protection of Content

- Encryption
- Broadcast Encryption [Fiat and Naor, Crypto 1992]
- Watermarking
- Chameleon [Anderson, Manifavas, 1997]
- Watercasting [Brown, Perkins, Crowcroft, 1999]
- work at GMD: multicast corrupted data, unicast FECs

Conclusions

- Security needed for multicast
- Security difficult in multicast

  - good research topic
  - need for prototype implementations
  - exploitation possible with selected applications and for billing/accounting

Multicast Security Research at the University of Torino

- MBONE applications setting
  (SDR + VIC + VAT/RAT + WB/WBD + NTE)
- Means for efficient individual authentication & more
- Project for 2 years (1999-2000)
- Prototype expected soon

http://security.unito.it/multicast