The Problem

- provide source authentication in a multicast network
- ensure that receivers can verify that the received packets come from the registered sender
- ensure that integrity of message (packets) can be verified by receivers

Motivation

- what is multicast?
  - a single copy of packets is sent by the sender and routed to every receiver within the multicast group

- why multicast?
  - growth of the Internet has caused an explosive increase in volume of network traffic
  - using multicast, sender resources and network bandwidth can be saved considerably
  - applications include news feeds, teleconferencing, stock quotes

- why authenticate packets?
  - receivers should have the ability to verify the authenticity of the message

Cloud

sender receiver 1 receiver 2 receiver 3 malicious

multicast-enabled multicast network

Efficient Source Authentication Schemes for Multicast Communications

Jung Min Park  H. J. Siegel  Edwin K. P. Chong

Difficulties & Challenges

- in IP multicast, QoS cannot be guaranteed
  - authentication scheme should be robust against packet loss
- immunity to collusion attacks
  - scheme should be secure even against attacks from a group of registered receivers with malicious intent
- computation and communication overhead should be within reasonable limits
- authentication delay at the sender and receiver should be kept to a minimum

Our Approach (Work in Progress)

- amortize the signature over multiple packets
- apply Rabin's IDA (Information Dispersal Algorithm) to resist packet loss

Previous Work

- Gennaro and Rohatgi ('97) - stream signing
- Wong and Lam ('98) - signature tree
- Rohatgi ('99) - hybrid signature
- Canetti et al. ('99) - asymmetric MAC
- Perrig et al. ('00) - EMSS (Efficient Multi-chained Stream Signature)