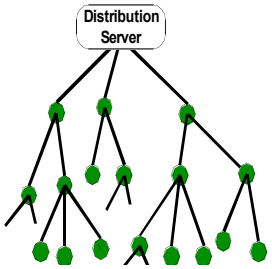
Efficient Security Mechanisms for Overlay Multicast Based Content Delivery

Sencun Zhu, Chao Yao, Donggang Liu, Sanjeev Setia, Sushil Jajodia

There are two major security problems of overlay multicast: *network access* control and *group key management*. Previous research studied these two issues separately. By exploiting the special property of overlay multicast that a node is both a group member and a router, we propose:

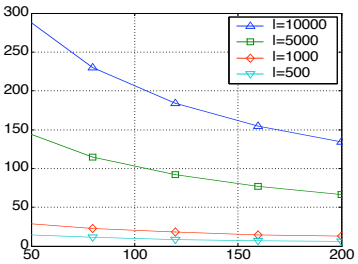
- A bandwidth-efficient scheme *CRBR* that seamlessly integrates network access control and group key management.
- A DoS-resilient key distribution scheme *k-RIP* which delivers updated keys to a large fraction of nodes with high probability even if an attacker can selectively compromise nodes in the multicast data delivery hierarchy.

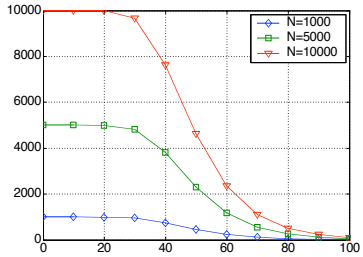
Certificate Revocation Based Group Rekeying Scheme



- System Model and Design Goal
- CRBR scheme specifications
  - Major Steps
    - Node Registration
    - Security Update Generation
    - Security Update Distribution
    - Local Recovery
  - More Details
    - Certificate Management
    - Node Joining
- Security Analysis
- Performance Evaluation:

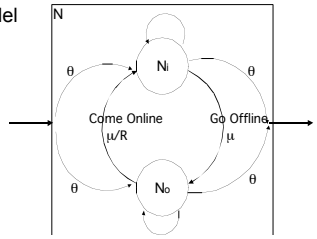
Comparisons with *LKH* and *SDR*: *Metric:* The server's bandwidth overhead



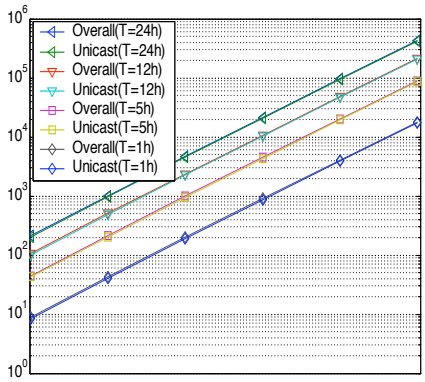


Performance Analysis

- Node Presence Dynamics
  - Exponential Distributions
  - A *Queuing* Model

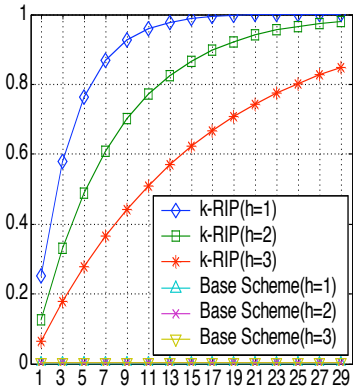


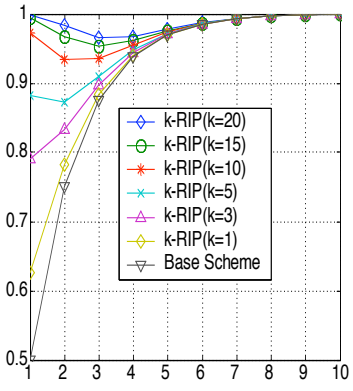
- Two scenarios: *multicasting* and *unicasting* keys
  - Key server multicasts keys to online nodes
  - Key server unicasts keys to individual nodes who missed



A k-Random Injection Scheme

- Dos Resilient k-RIP scheme for Distribution of Small-size but Critical Information
  1. Key server gets from the *Rendezvous Point (RP)* a list of *m* nodes that most recently joined the group.
  2. Key server randomly tests presence status of *m* nodes until it finds *k* online.
  3. Key server send message to *k* nodes individually.
- Comparison with the basic scheme





- Furture Work
  - Dynamic selection of *k* based on receiving status
  - Attacks Detection and Attacker Identification using Probabilistic Methods