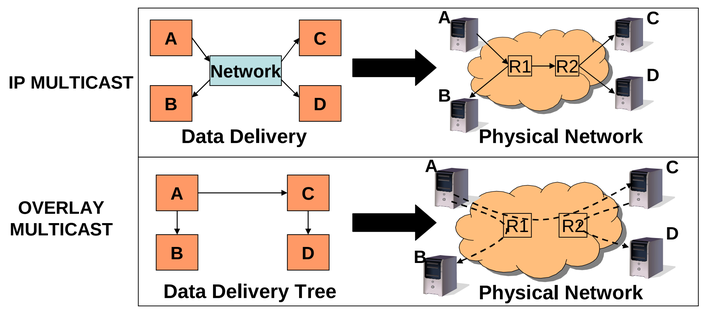
Enabling Confidentiality of Data Delivery in an Overlay Broadcasting System

Ruben Torres, Xin Sun, Aaron Walters, Cristina Nita-Rotaru, Sanjay Rao
Purdue University

Overlay Multicast

In a Multicast Group: Source (A) and members (B,C,D)



IP Multicast, the network infrastructure delivers data.

Overlay Multicast, members form a tree to deliver data.

Incorporating Confidentiality in Overlay Multicast Systems

In IP Multicast:

- Network infrastructure manage the multicast
- Routers efficiently distribute keys in the multicast group

In Overlay Multicast:

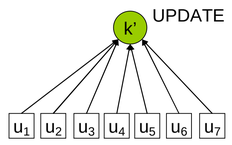
- Nodes forward keys to other nodes
- Keys can get lost easily if nodes:
  - Don't forward the keys
  - Fail
  - Leave the group
- Reliable key distribution is required

Main Goal: Evaluate the performance of key management and distribution techniques in an overlay system using Planetlab

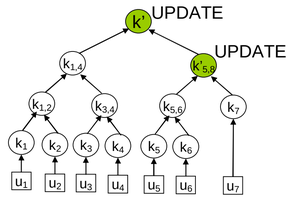
Key Management Schemes

- In data broadcasting, we need efficient encryption, achieved by symmetric cryptography algorithms.
- This requires all participants to share a *group key*
- We employ the LKH protocol to reduce the number of encryptions needed when changing the *group key*
- Keys are changed periodically at the *rekey event*

In a group of 8 (N = 8) users, u8 leaves. The Group key changes.



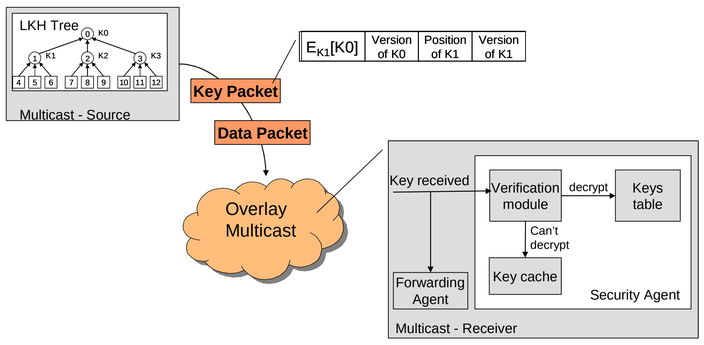
Key-Star: O(N) encryptions to change k



LKH: O(log N) encryptions to change k

Implementing Key Management in an Overlay Multicast System

Keys changes at the LKH tree. At the next rekey event the source distributes key packets using the data delivery structure (a tree).

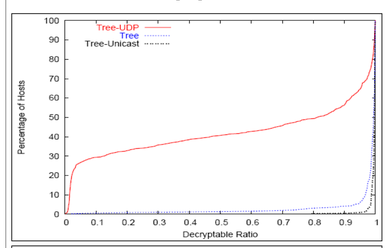


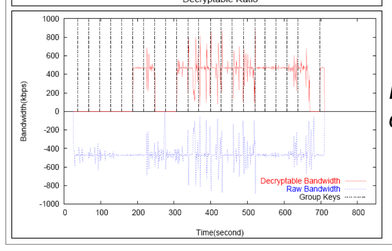
Evaluation Methodology

- Metrics:
  - Decryptable Ratio: Fraction of bandwidth received that can be decrypted.
  - Computation Overhead at the Source: Average Encryptions per second
  - Communication Overhead at the Source: Average bandwidth of all control messages sent and receive.
- Traces: 20 minutes segments from real operational broadcasts used in our evaluation. Characteristics of some of them:

Event	*Peak Group Size*	*Joins*	*Leaves*
Rally	252	148	149
Competition	116	110	75

Application Performance



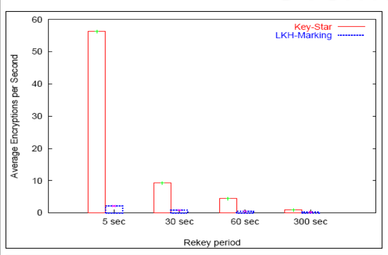


Performance for a Rekey Interval of 60 Seconds.

Use of *per-hop TCP* to distribute keys is crucial

Impact of Loss of Key Packets on User Performance

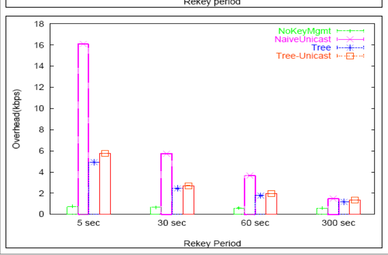
Overhead



Computation Overhead

-LKH performs better than *Key-Star* for small rekey intervals.

-For larger rekey intervals, the number of encryptions increase by group dynamics

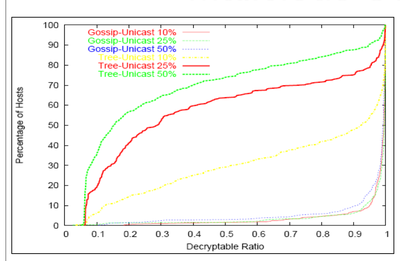


Communication Overhead

- Overhead decreases when the rekey interval increases

-*Tree* performs better than *NaiveUnicast* for small rekey intervals

Malicious Scenarios



-Per-hop reliability is not enough in some scenarios

-More resilient distribution schemes can be used instead of Tree (e.g. Gossip)

Final Remarks

- It is feasible to enable confidentiality in Overlay Multicast Systems while achieving good performance at low overheads.
- It is critical to use TCP to ensure per hop reliability.