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.

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

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:

<table>
<thead>
<tr>
<th>Event</th>
<th>Peak Group Size</th>
<th>Joins</th>
<th>Leaves</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rally</td>
<td>252</td>
<td>148</td>
<td>149</td>
</tr>
<tr>
<td>Competition</td>
<td>116</td>
<td>110</td>
<td>75</td>
</tr>
</tbody>
</table>

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

Application Performance
Performance for a Rekey Interval of 60 Seconds. Use of per-hop TCP to distribute keys is crucial

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.