Multicast Congestion Control with Distrusted Receivers

Sergey Gorinsky, Sugat Jain, and Harrick Vin

Laboratory for Advanced Systems Research
Department of Computer Sciences
The University of Texas at Austin

http://www.cs.utexas.edu/users/lasr/
The Problem

• Congestion control protocols trust receivers
  ➢ Assumption: Receivers always follow the protocol

• Trust is not a tenable assumption
  ➢ Internet is not a small close-knit community
  ➢ Receivers have incentives to misbehave
  ➢ Receivers are capable of misbehaving

• Research challenge: congestion control without the assumption of trust

• Our focus: multicast congestion control
  ➢ How can a receiver misbehave?
  ➢ What is the impact of receiver misbehavior?
Outline

• Receiver misbehavior
  ➢ Multicast versus unicast

• Threat model
  ➢ Core mechanisms in multicast congestion control
  ➢ Taxonomy of threats

• Evaluation of prominent multicast protocols

• Conclusions
Unicasted with a Misbehaving Receiver

- Unicast congestion control
  - Feedback-driven transmission adjustment
  - Misbehavior: incorrect feedback reports

- Protection against the misbehavior
  - Feedback verification
    - Sender adds a nonce to each packet
    - Feedback echoes the nonces
    - Sender checks validity of the feedback nonces

Differences between Multicast and Unicast

• Receiver multiplicity
  - Feedback is aggregated/suppressed
  - Failure to provide feedback can increase transmission
  - Receivers are anonymous

• Receiver heterogeneity
  - Session contains multiple groups
  - Group subscription is a congestion control mechanism
  - Sender has no control over group subscription

Protection against receiver misbehavior in multicast is harder
Threat Model

- What are patterns for receiver misbehavior in multicast?

- Our focus: in-band self-beneficial attacks

- Construction of the threat model: protocols $\Rightarrow$ mechanisms $\Rightarrow$ threats

Multicast congestion control

- Feedback-driven transmission adjustment
  - Feedback Generation
    - Incorrect reports
    - Failure to report
  - Feedback Aggregation
    - Forged aggregated reports
  - Feedback Suppression
    - Manipulation with feedback suppression

- Group membership regulation
  - Group subscription
    - Inflated subscription
  - Subscription synchronization
    - Prevention of other receivers from legitimate subscription
Evaluation Methodology

- Classification of existing protocols with respect to their mechanisms

<table>
<thead>
<tr>
<th>Paradigms</th>
<th>Mechanisms</th>
<th>Protocols</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Single-group</td>
<td>Feedback-free</td>
</tr>
<tr>
<td>Feedback-driven transmission</td>
<td>RMTS, SAMM, TFMCC, pgmcc</td>
<td>DSG, SIM, MLDA</td>
</tr>
<tr>
<td>adjustment</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Feedback aggregation</td>
<td>RMTS, SAMM</td>
<td>SIM</td>
</tr>
<tr>
<td>Feedback suppression</td>
<td>TFMCC, pgmcc</td>
<td>DSG, MLDA</td>
</tr>
<tr>
<td>Group membership regulation</td>
<td>WEBRC, FLID-DL, RLC, RLM</td>
<td>DSG, SIM, MLDA</td>
</tr>
<tr>
<td>Subscription synchronization</td>
<td>WEBRC, FLID-DL, RLC, RLM</td>
<td>DSG, SIM, MLDA</td>
</tr>
</tbody>
</table>

- Experiments with representative protocols for each threat
Experiments

- Simulation in NS-2
- Traffic mix
  - Multicast: M and N
  - TCP: A, B, C, and D
- Performance measures
  - Throughput
  - Loss rates
Failure to report is a passive potent attack
Forged Aggregated Reports in RMTP

Aggregation of feedback at receivers is dangerous
Manipulation with Suppression in pgmcc

Two-level control of the transmission rate opens opportunities for misbehavior
Unrestricted group access is a fundamental vulnerability of multi-group protocols.
# Classification of Vulnerabilities for Examined Protocols

<table>
<thead>
<tr>
<th>Paradigms</th>
<th>Threats</th>
<th>Vulnerable protocols</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Single-group</td>
</tr>
<tr>
<td>Feedback-driven transmission</td>
<td>Incorrect reports</td>
<td>RMTP, SAMM, TFMCC, pgmcc</td>
</tr>
<tr>
<td>adjustment</td>
<td></td>
<td>RMTP, TFMCC, pgmcc</td>
</tr>
<tr>
<td></td>
<td>Failure to report</td>
<td>RMTP</td>
</tr>
<tr>
<td></td>
<td>Forged aggregated reports</td>
<td>RMTP</td>
</tr>
<tr>
<td></td>
<td>Manipulation with suppression</td>
<td>pgmcc</td>
</tr>
<tr>
<td>Group membership regulation</td>
<td>Inflated subscription</td>
<td>WEBRC, FLID-DL, RLC, RLM</td>
</tr>
<tr>
<td></td>
<td>Prevention of other receivers from</td>
<td>RLM</td>
</tr>
<tr>
<td></td>
<td>subscription</td>
<td></td>
</tr>
</tbody>
</table>
Conclusions

• Research challenge
  ➢ Congestion control in distrusted environments

• Our focus
  ➢ Multicast congestion control with distrusted receivers

• Threat model
  ➢ Diversity of threats in multicast

• Evaluation of prominent protocols
  ➢ Vulnerabilities in all examined protocols

• Future
  ➢ Multicast congestion control protocols that are robust to receiver misbehavior