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

Unicast 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

S. Savage, N. Cardwell, D. Wetherall, and T. Anderson, "TCP Congestion Control with a Misbehaving Receiver", ACM CCR, October 1999

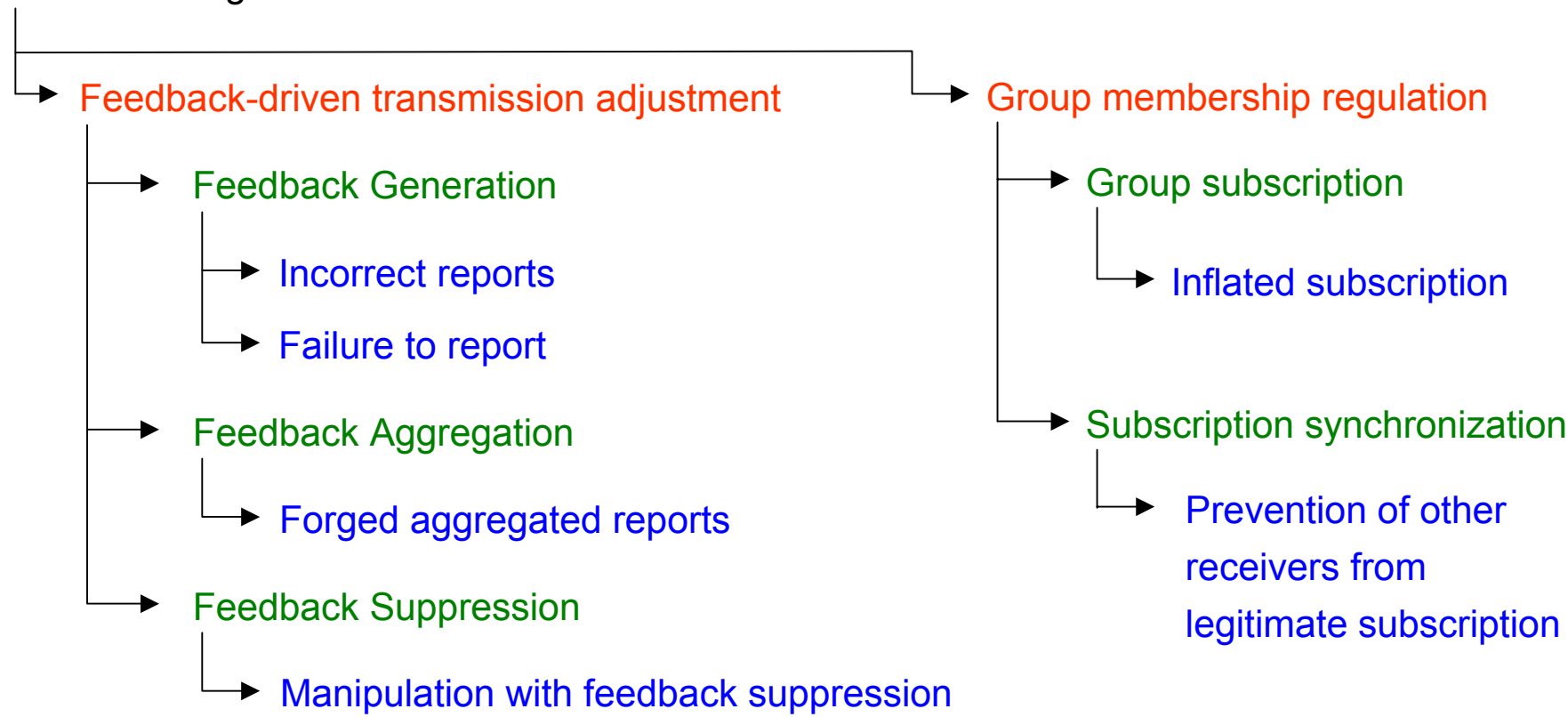
Differences between Multicast and Unicast

- 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



Evaluation Methodology

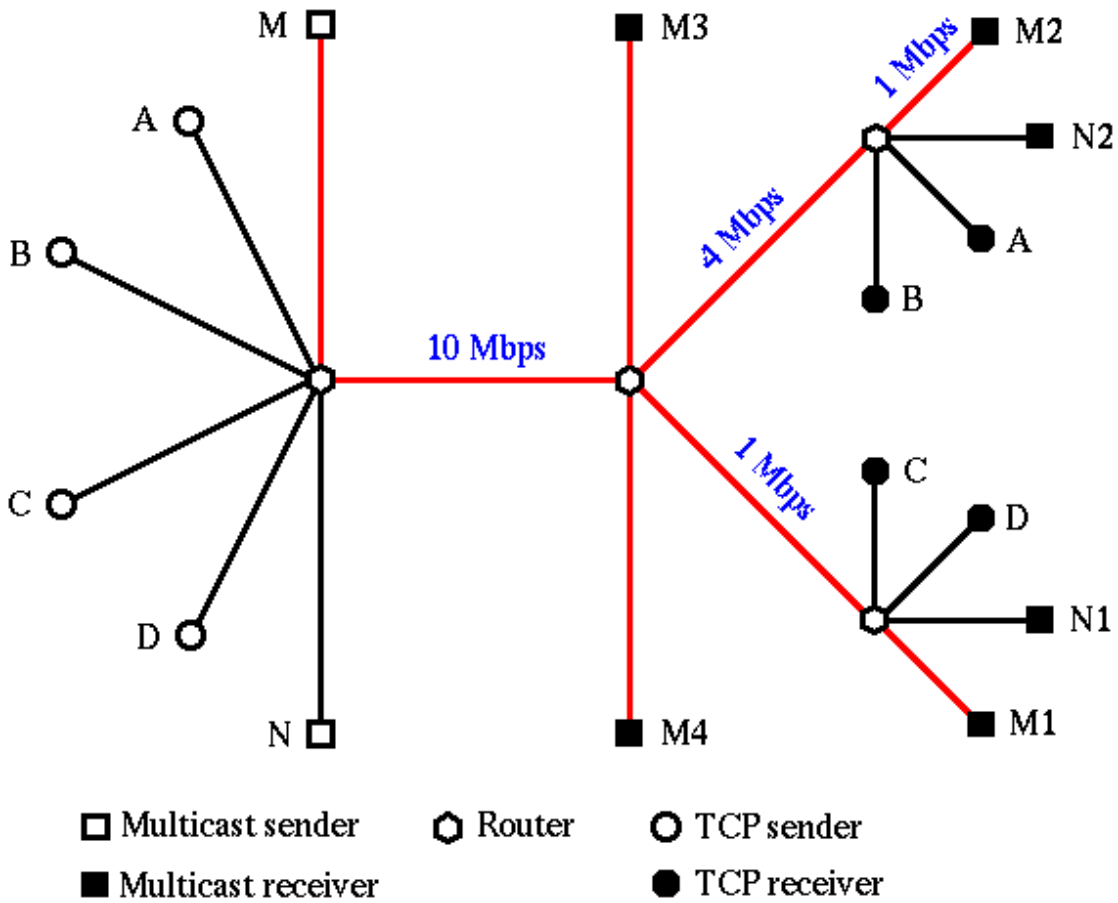
- Classification of existing protocols with respect to their mechanisms

Paradigms	Mechanisms	Protocols		
		Single-group	Feedback-free	Multi-group feedback-driven
Feedback-driven transmission adjustment	Feedback generation	RMTP, SAMM, TFMCC, pgmcc		DSG, SIM, MLDA
	Feedback aggregation	RMTP, SAMM		SIM
	Feedback suppression	TFMCC, pgmcc		DSG, MLDA
Group membership regulation	Group subscription		WEBRC, FLID-DL, RLC, RLM	DSG, SIM, MLDA
	Subscription synchronization		WEBRC, FLID-DL, RLC, RLM	DSG, SIM, MLDA

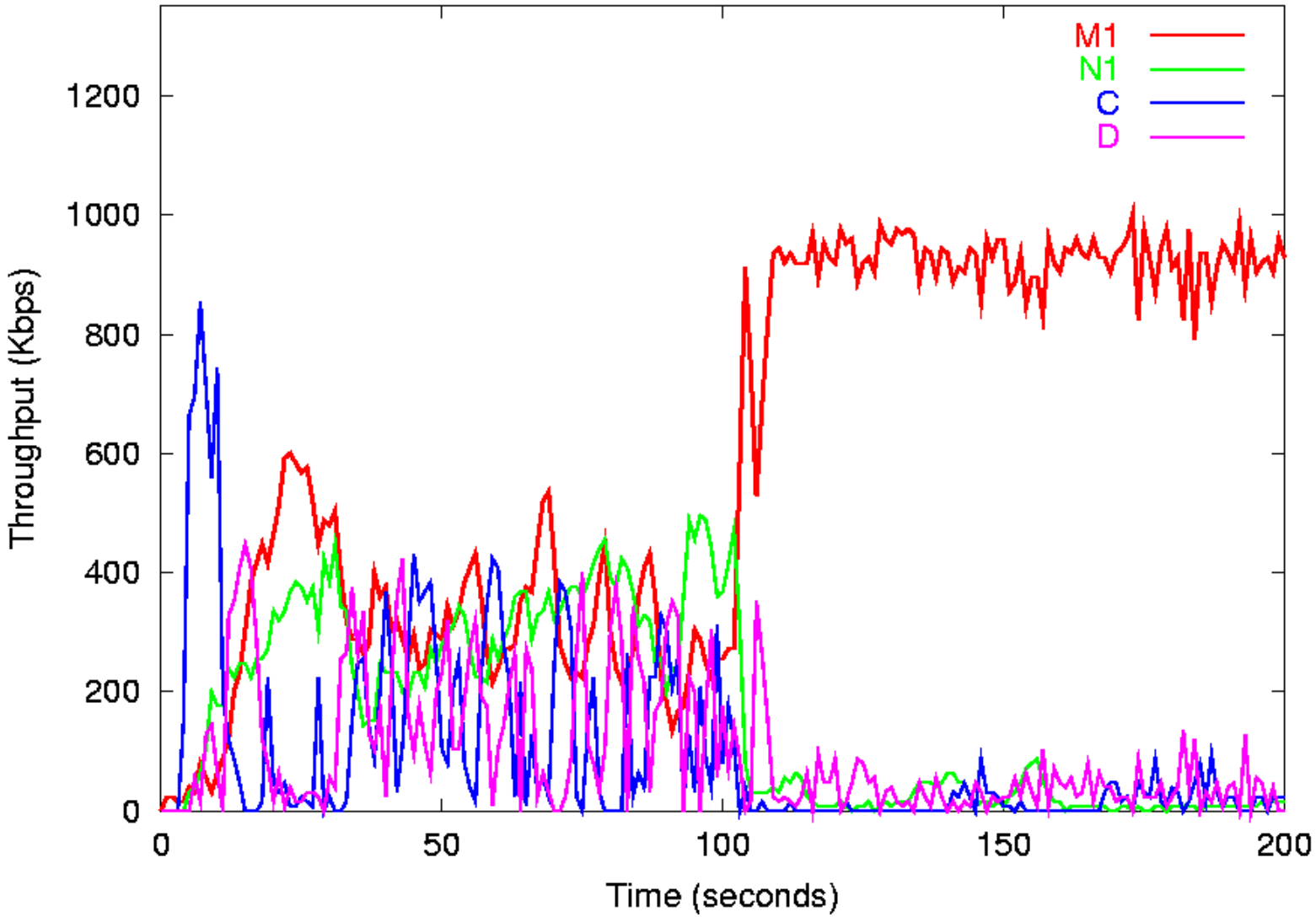
- Experiments with representative protocols for each threat

Experiments

- Simulation in NS-2
- Traffic mix
  - Multicast: M and N
  - TCP: A, B, C, and D
- Performance measures
  - Throughput
  - Loss rates

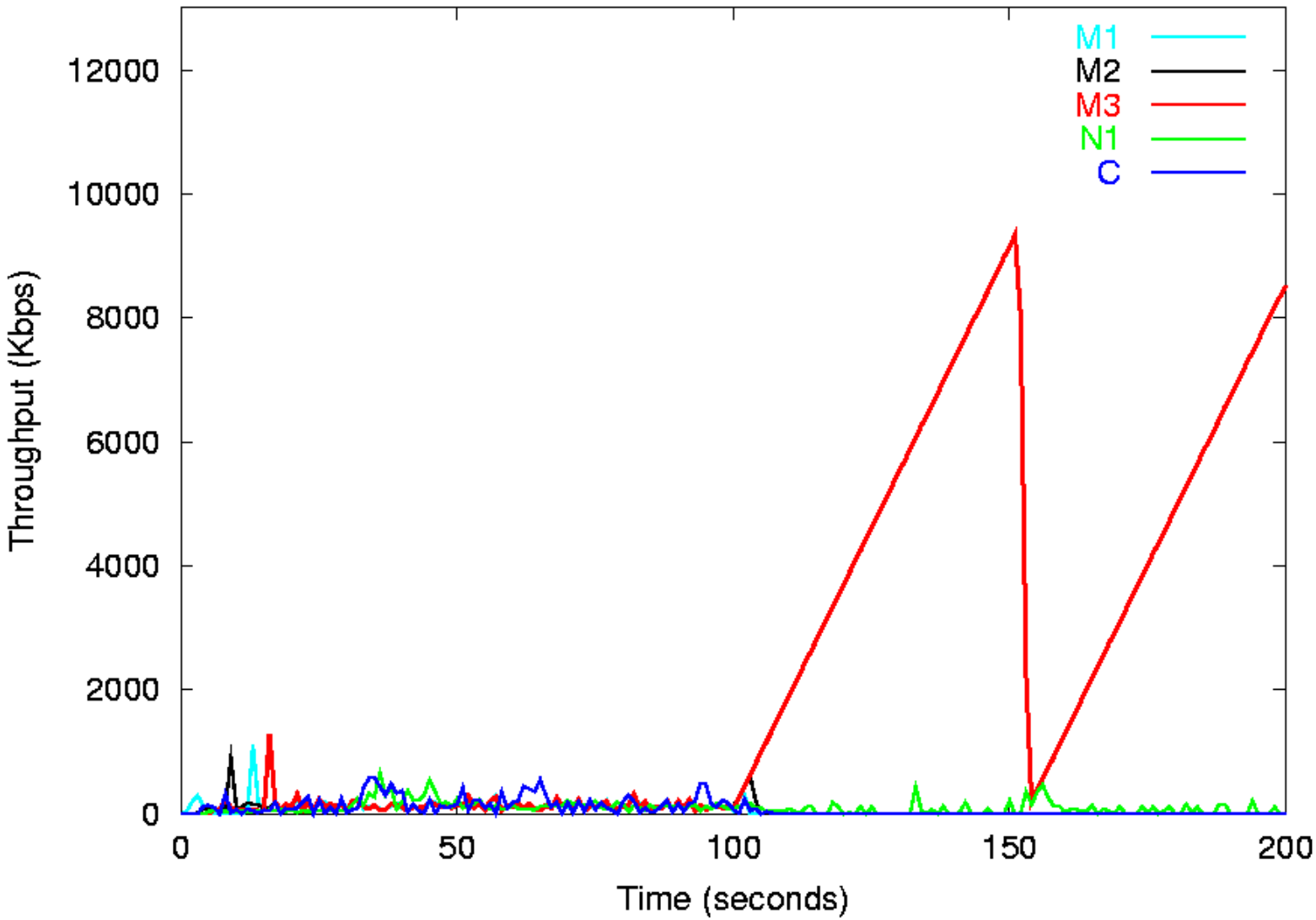


Failure to Report in TFMCC



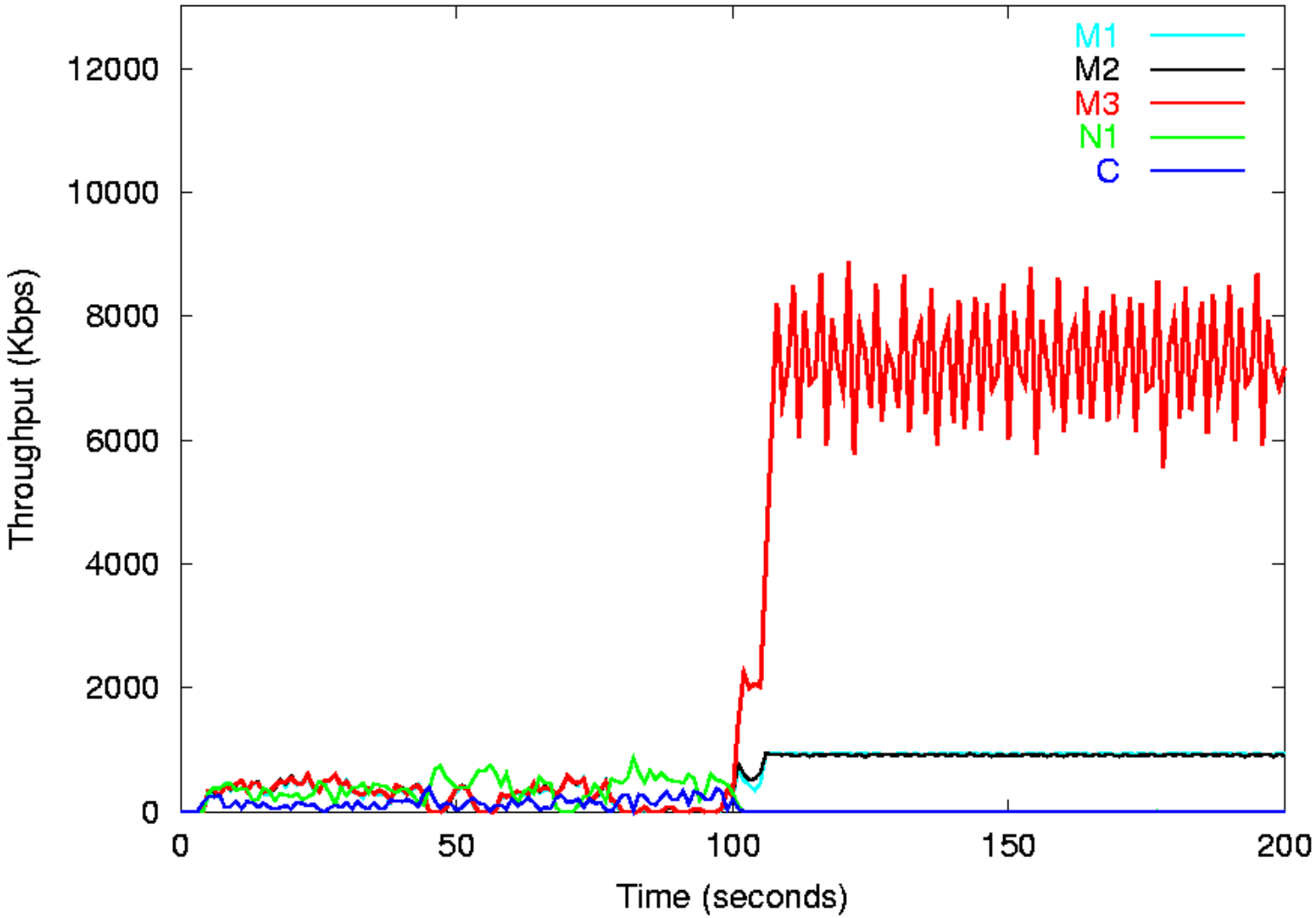
Failure to report is a passive potent attack

Forged Aggregated Reports in RMTP



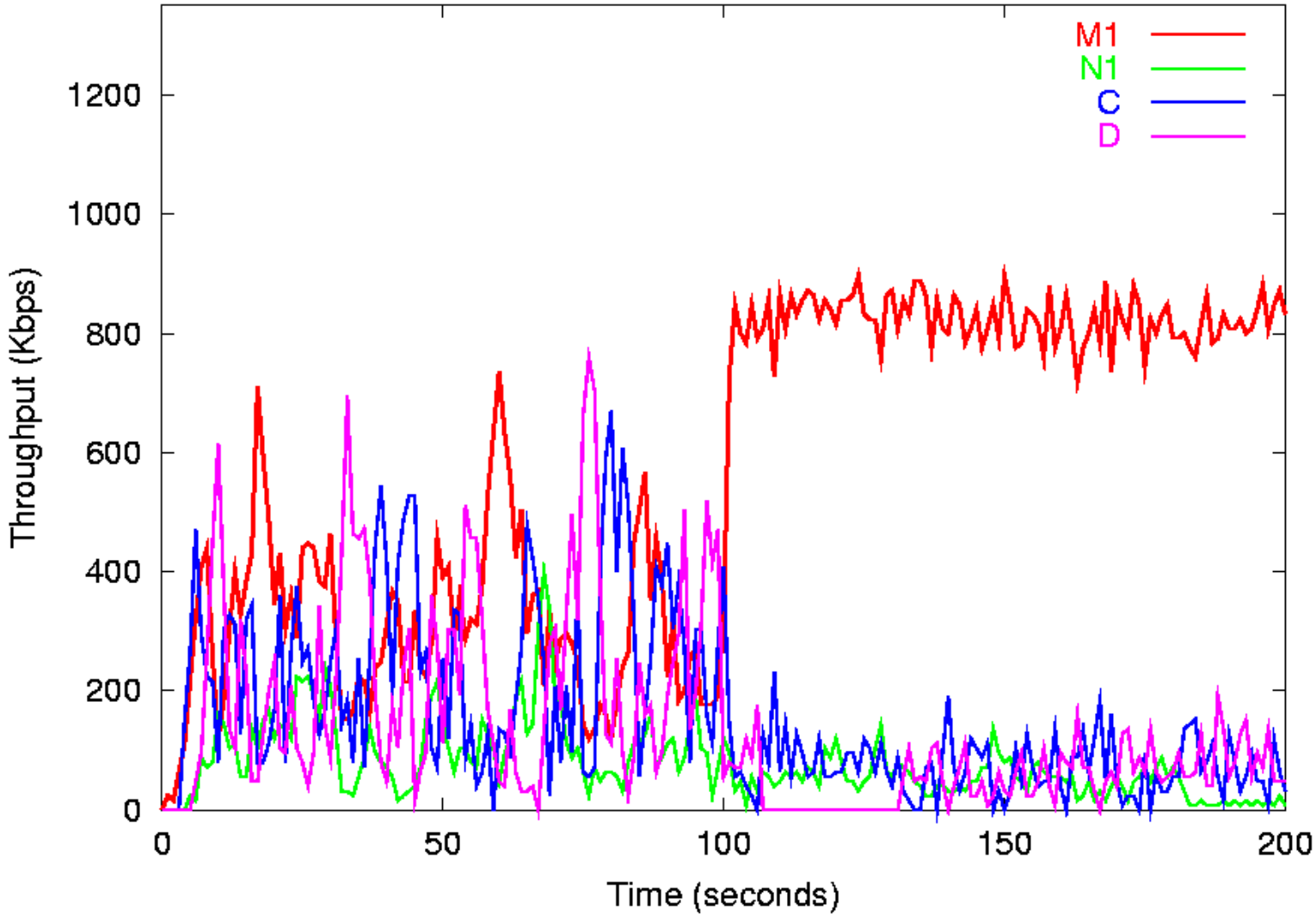
Aggregation of feedback at receivers is dangerous

Manipulation with Suppression in pgmcc



Two-level control of the transmission rate opens opportunities for misbehavior

Inflated Subscription in FLID-DL



Unrestricted group access is a fundamental vulnerability of multi-group protocols

Classification of Vulnerabilities for Examined Protocols

Paradigms	Threats	Vulnerable protocols		
		Single-group	Feedback-free	Multi-group feedback-driven
Feedback-driven transmission adjustment	Incorrect reports	RMTP, SAMM, TFMCC, pgmcc		DSG, SIM, MLDA
	Failure to report	RMTP, TFMCC, pgmcc		DSG, SIM, MLDA
	Forged aggregated reports	RMTP		
	Manipulation with suppression	pgmcc		
Group membership regulation	Inflated subscription		WEBRC, FLID-DL, RLC, RLM	DSG, SIM, MLDA
	Prevention of other receivers from subscription		RLM	

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