On the Pitfalls of Using High-Throughput Multicast Metrics in Adversarial Wireless Mesh Networks

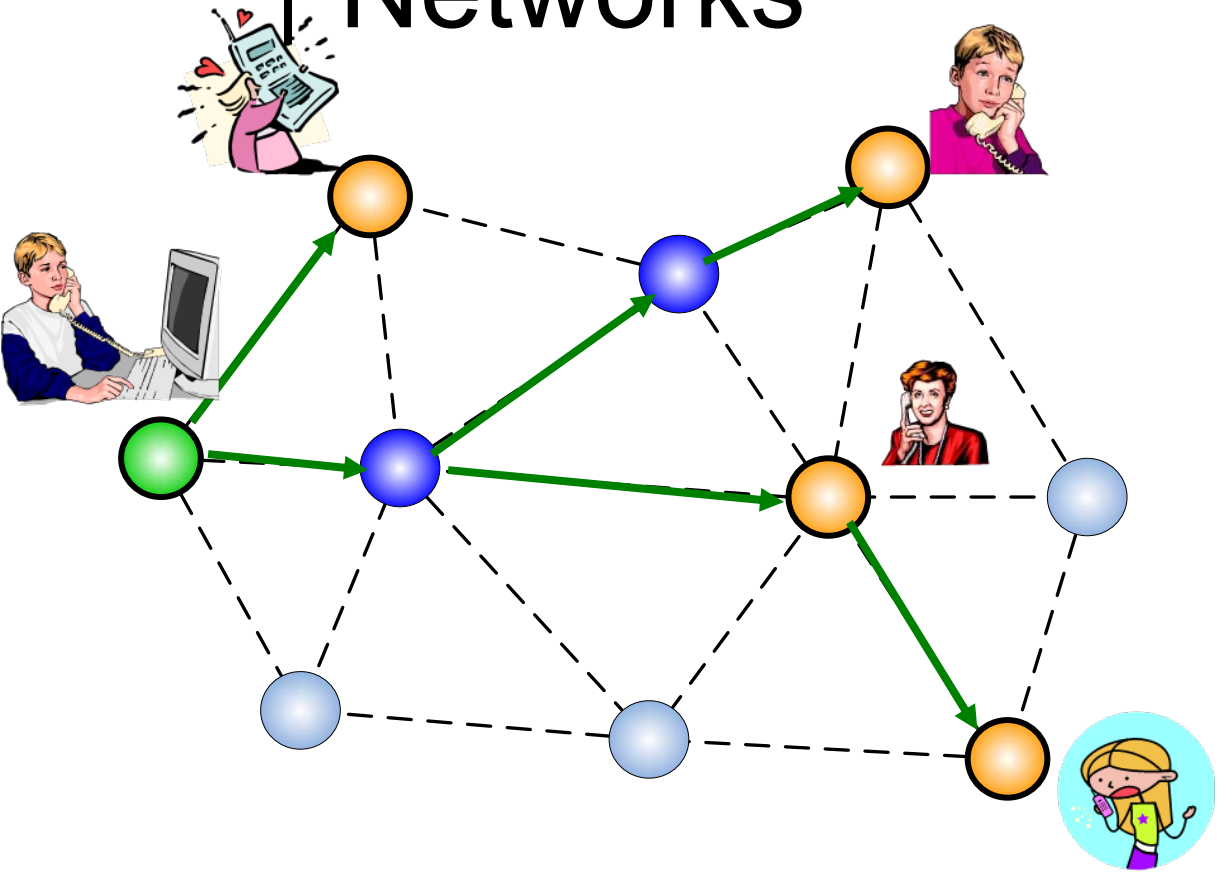
Jing Dong, Reza Curtmola, Cristina Nita-Rotaru
Department of Computer Science and CERIAS
Purdue University

PURDUE UNIVERSITY

CERIAS

(DS)²

Multicast in Wireless Mesh Networks

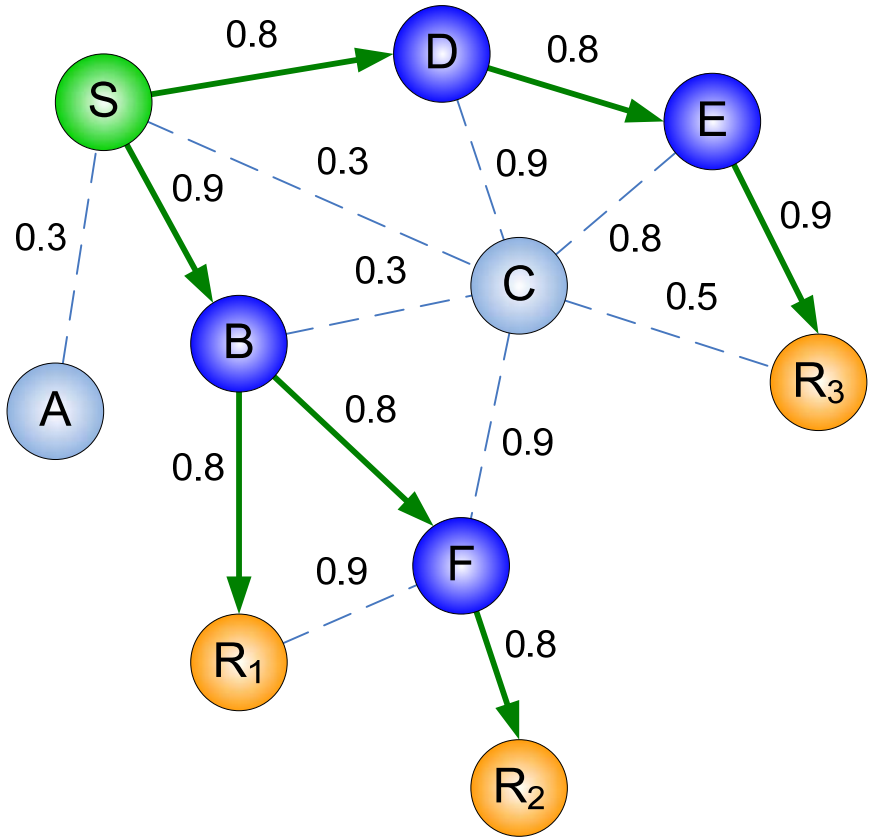


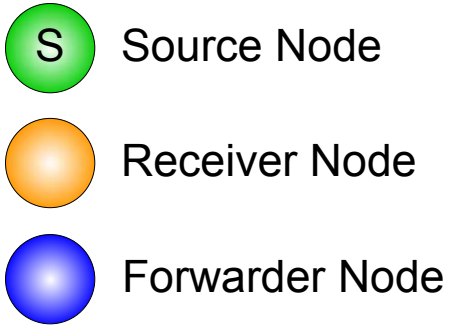
- Multimedia conferencing
- Video/audio broadcasting
- Online gaming
- Distance learning

They all need high-throughput multicast

High-Throughput Multicast

- Use *high-throughput metrics* to build high quality multicast paths





Our Contributions

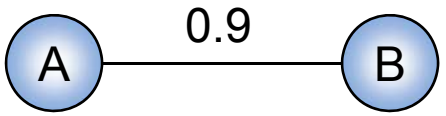
- Identify attacks against high-throughput multicast protocols
- Propose a lightweight scheme for secure and high-throughput wireless multicast
- Show experimentally:
  - The attacks are extremely damaging
  - Our defense scheme effectively mitigates the attacks and preserves the advantage of high-throughput metrics

Related Work

- Secure multicast
  - Authentication framework [Roy ’05]
  - Insider and outsider [Curtmola ’07]
- Secure unicast routing
  - Authentication framework for route discovery, e.g. SEAD, Ariadne [Hu ’02]
  - Local monitoring against packet dropping e.g. watchdog [Marti ’00]
  - End-to-end acknowledgment based e.g. ODSBR [Awerbuch ’05]

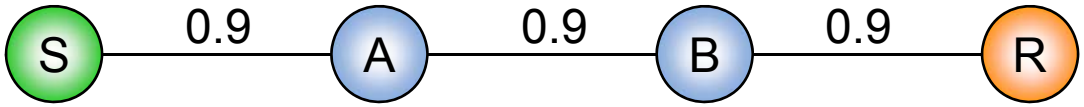
High-Throughput Metrics

- Link metric
  - Link delivery probability



- Path metric
  - Path delivery probability (SPP [Roy '06])

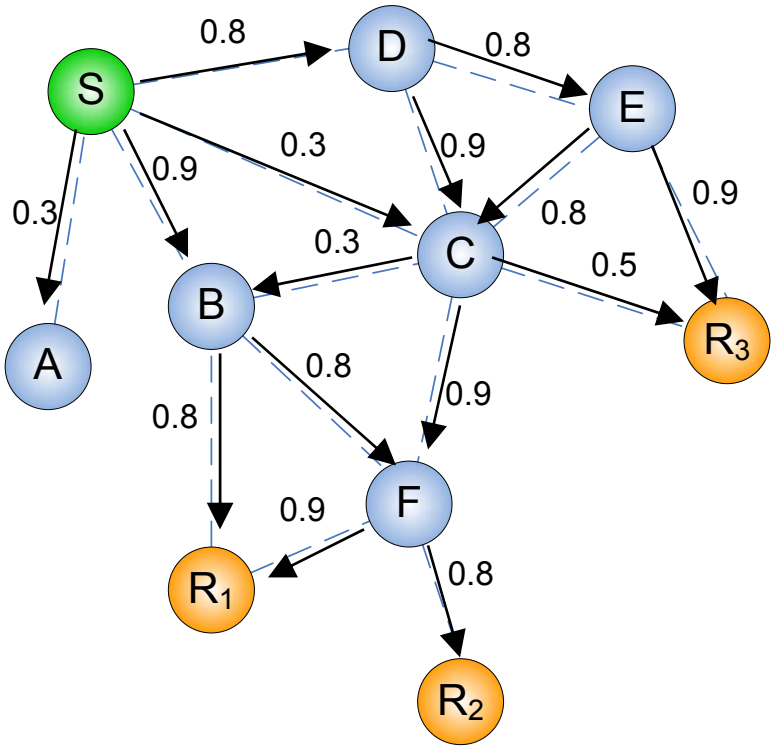
$$\mathrm{pm} = \prod m_i$$



pm(S→A→B→R) = 0.73 = 0.9*0.9*0.9

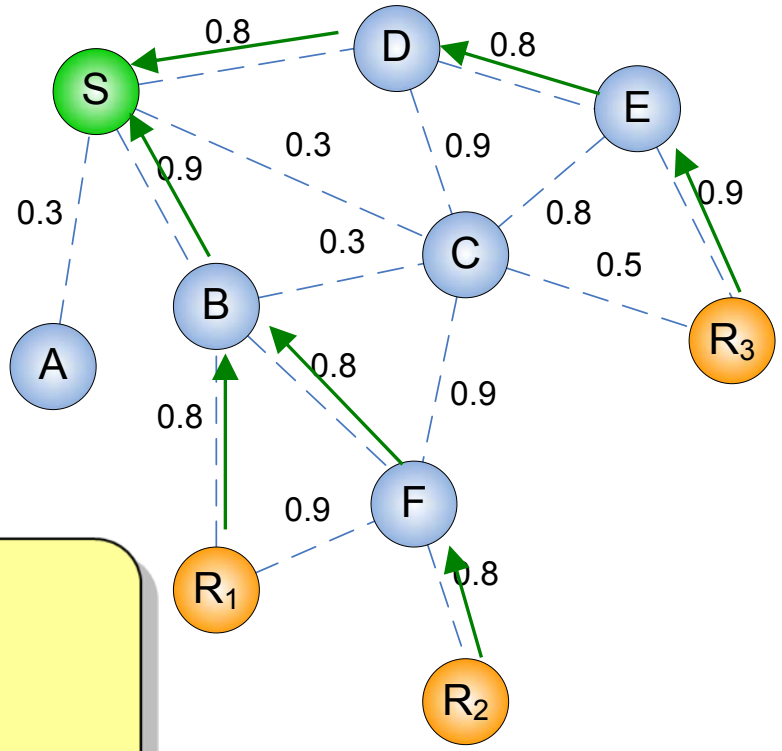
ODMRP-HT: ODMRP with High-Throughput Multicast

- Join Query flooding
  - Establishes metrics
- Join Reply
  - Selects best metric paths for data delivery



ODMRP with High-Throughput Multicast

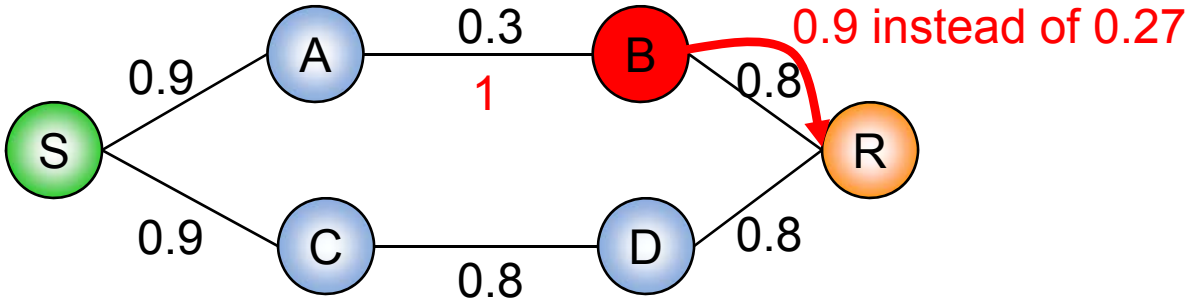
- Join Query flooding
  - Establishes metrics
- **Join Reply**
  - **Selects best metric paths for data delivery**



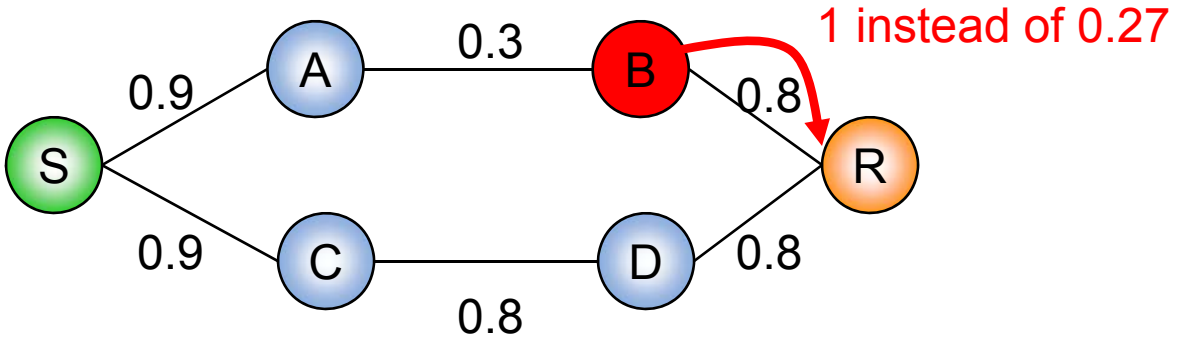
The correctness of path establishment requires the cooperation of nodes

Metric Manipulation Attacks

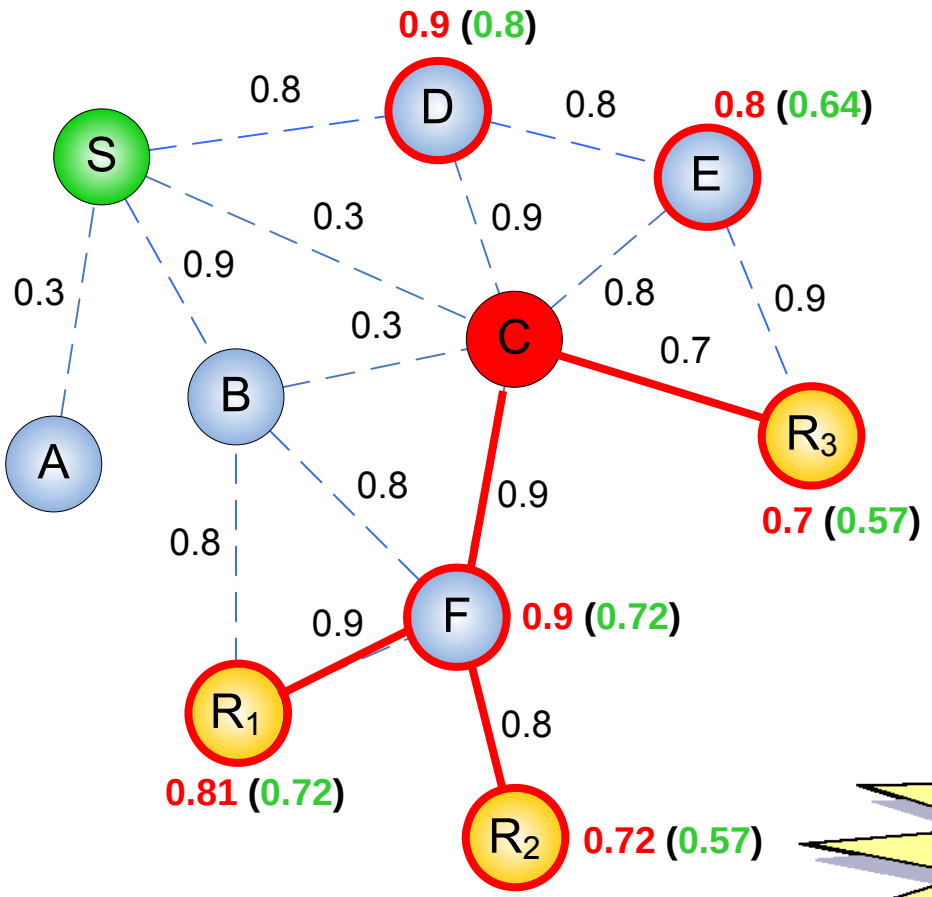
- Local Metric Manipulation
  - Attacker lies about link metric



- Global Metric Manipulation
  - Attacker lies about path metric



Impact of Metric Manipulation Attacks



- Metric poisoning
- Attacker controlled paths
  - With packet dropping, can cause significant damage
- Facilitate other attacks
  - Traffic analysis, network partition, etc

Very easy to mount!

S-ODMRP: Secure High-Throughput Multicast

- Goal: Ensure data delivery in the presence of attackers
  - Metric manipulation
  - Packet dropping
- *Do not address traffic analysis*

Security and Adversarial Model

- Security assumptions
  - Existence of public-key infrastructure
  - Secure neighbor discovery
  - Source data authentication
- Adversarial model
  - Insider or outsider attackers
  - Individual or colluding attackers

S-ODMRP in a Nutshell

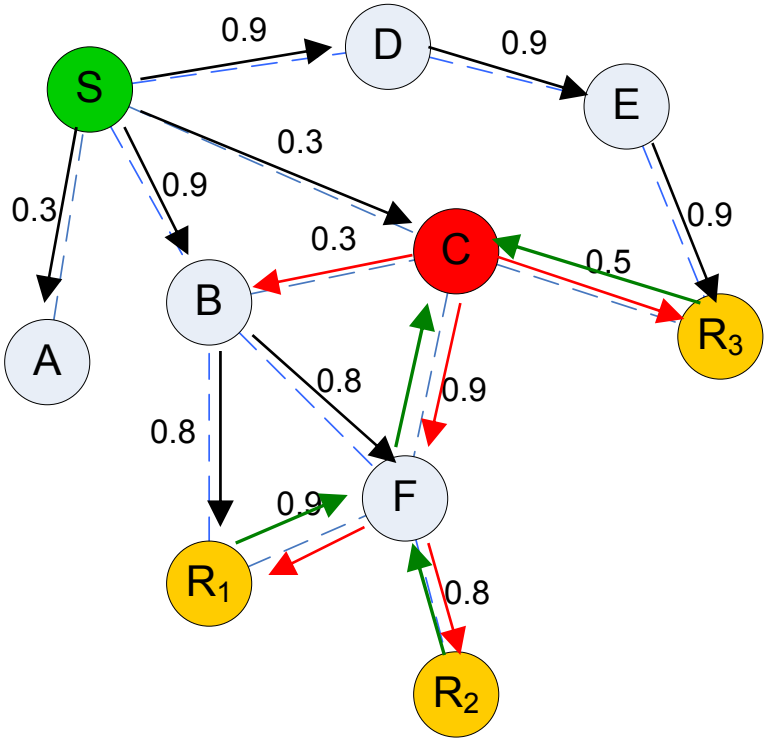
- Measurement-based attack detection
  - Derive expected PDR (ePDR)
  - Monitor perceived PDR (pPDR)
  - If ePDR-pPDR > δ, then declare attack detected
- Accusation-based attack reaction
  - Accuse suspected node for a time duration
  - Flood accusation in the network
  - Accused nodes are avoided in future path selection until the accusation expires

Challenges

- How to prevent affected honest nodes from being mistakenly accused?
- How to deal with false accusation attacks?
- How to deal with transient network variations?

S-ODMRP in Stages (1/3): Mesh Creation

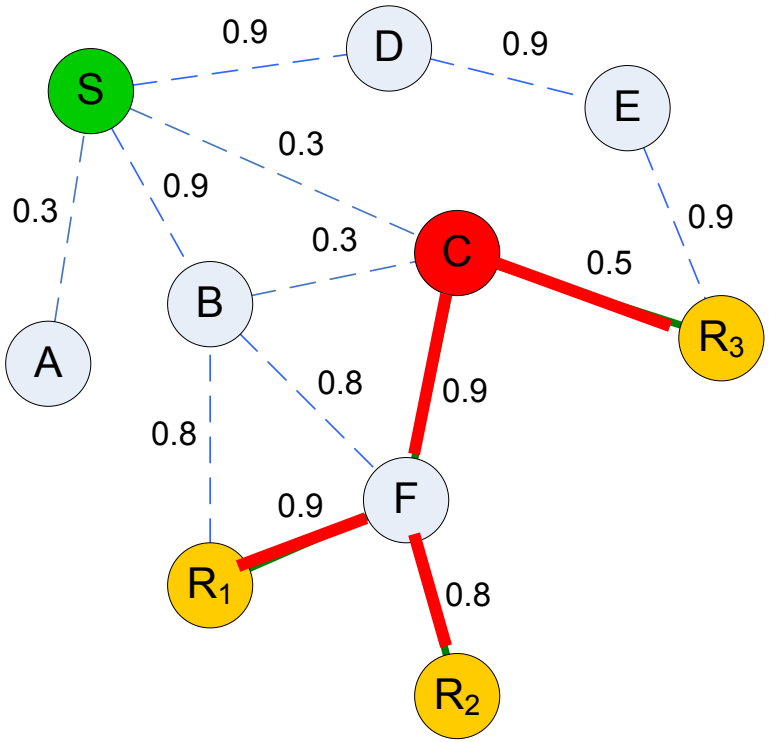
Attack: Attacker C advertises metric 1

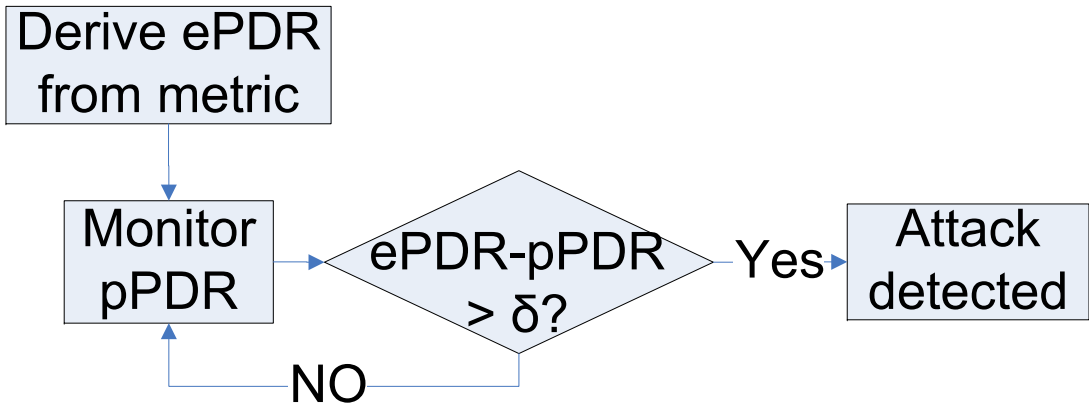


Attacker has not been detected

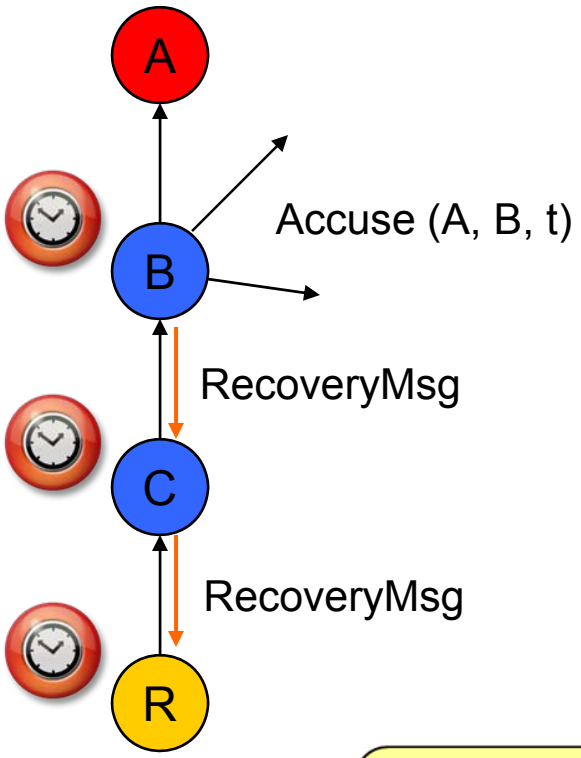
- Build data paths as usual
  - Many attacker controlled paths

S-ODMRP in Stages (2/3): Attack Detection





S-ODMRP in Stages (3/3): Attack Reaction

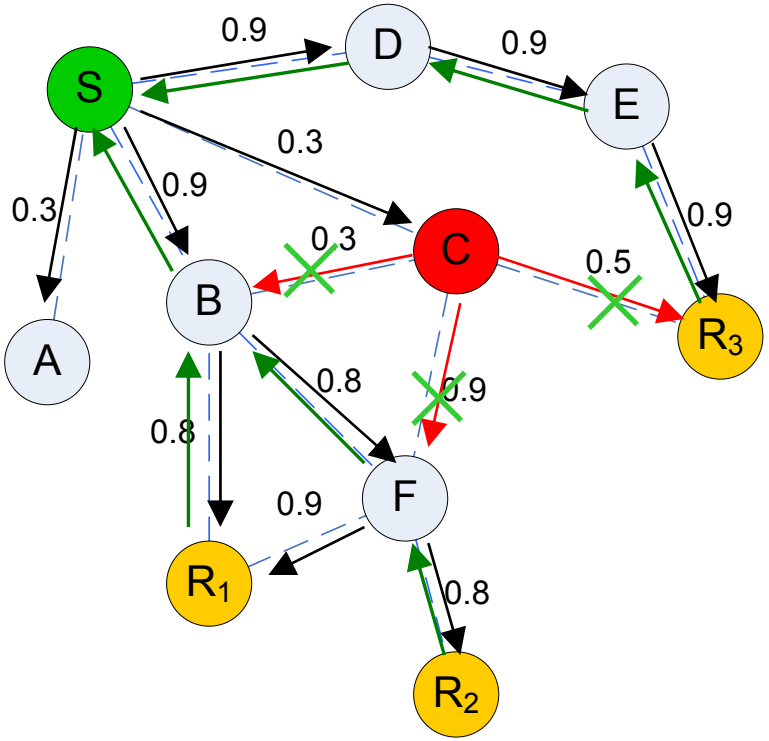


- B, C, R all start a reaction timer with timeout β(1-ePDR)
  - $ePDR_B > ePDR_C > ePDR_R$
- B times out first
  - Flood accusation message
  - Unicast RecoveryMsg downstream
- On receiving RecoveryMsg, node C
  - Cancels its reaction timer
  - Forwards RecoveryMsg downstream
- On receiving RecoveryMsg, R cancels its reaction timer

Staggered reaction timeout prevents honest nodes from being mistakenly accused

S-ODMRP: Mesh Creation – revisited

After attacker C has been detected and accused



- Build data paths
  - Attacker C is ignored

False-Accusations: Attacks and Countermeasures

- Attacker can accuse any honest node
  - Mass false accusation
  - Strategic false accusation
- Countermeasures
  - Controlled Accusation – one active accusation per node
  - Always activate the neighbor with best metric as a forwarder node, even if it is accused

Tolerating Transient Network Variations

- Transient network variations can cause false-positive accusations

- Temporary accusation
  - Accusation duration = α(ePDR-pPDR)
  - PDR discrepancy due to transient network variations is small
  - False-positive accusation duration is small

Experimental Setup

- Glomosim Simulator
- 802.11 radio, 2Mbps bandwidth, 250m range
- 100 nodes randomly placed in 1500m x 1500m area
- Group members are randomly selected
  - 20 group members, one source node
- Data rate 20 pkts/sec, 512 bytes per packet
- Attackers are randomly selected

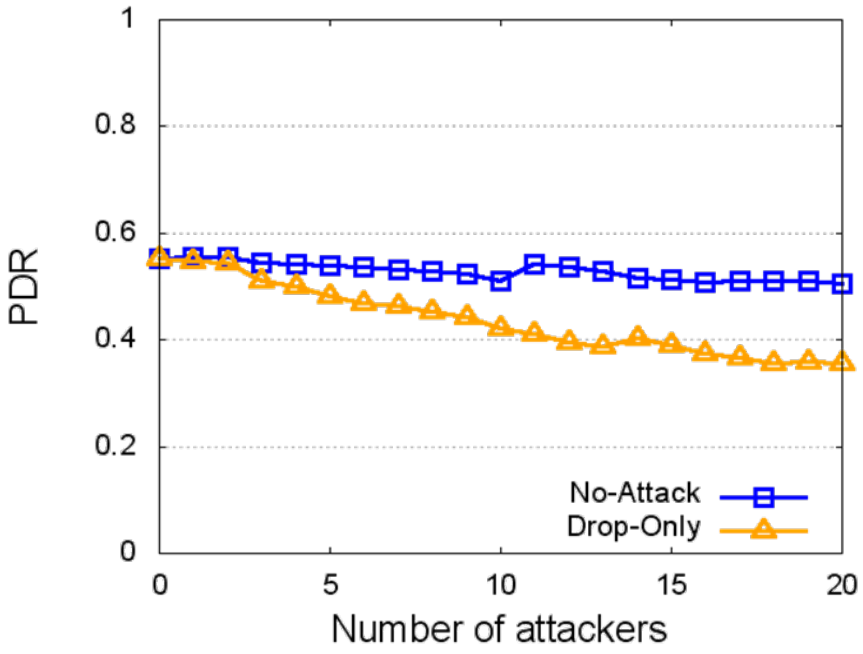
Attacker Scenarios and Metric

- Attack Scenarios
  - **No-Attack**
  - **Drop-only**
  - **LMM-Drop**: Local Metric Manipulation and dropping
  - **GMM-Drop**: Global Metric Manipulation and dropping
  - **False-Accusation**
- Metric
  - Packet delivery ratio $PDR = \frac{n_r}{n_s}$

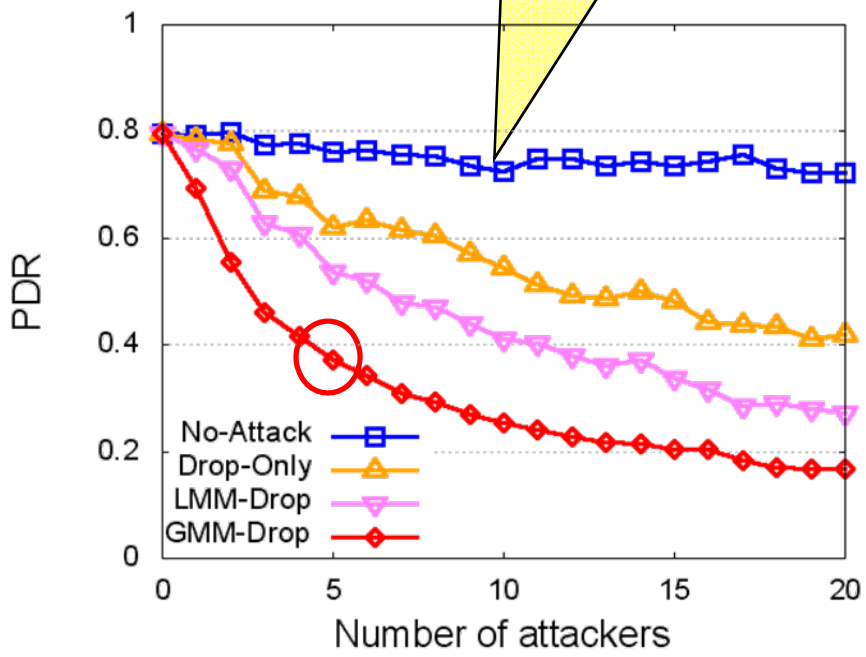
Attack Impact

High-throughput metric improves performance

Attack on ODMRP



Attacks on ODMRP-HT

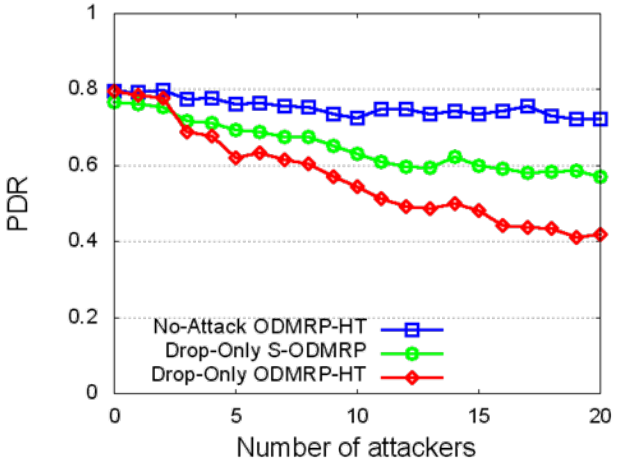


Mesh is resilient to attacks

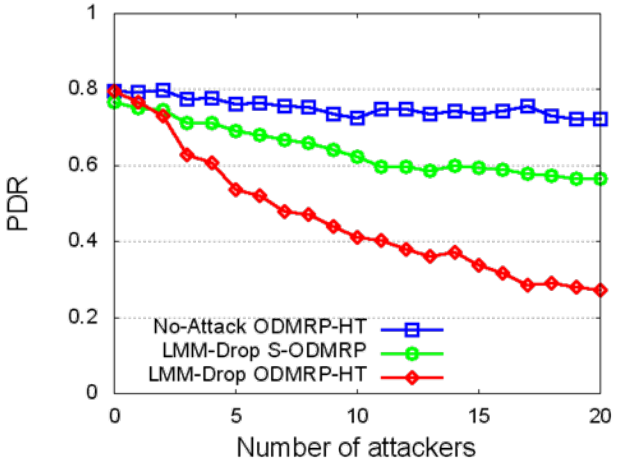
High-throughput metrics are a double-edged sword

Effectiveness of S-ODMRP

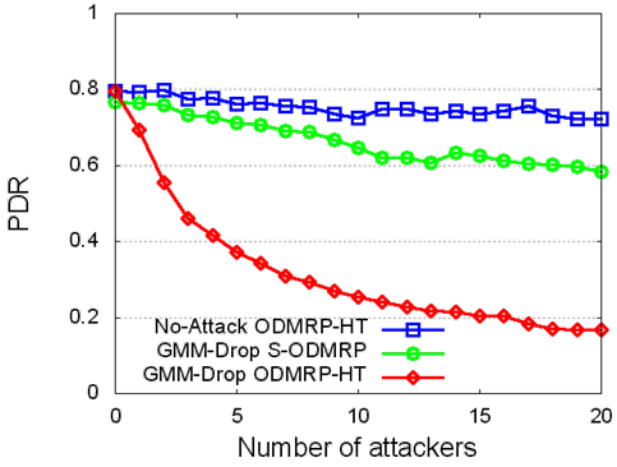
Drop-Only



LMM-Drop

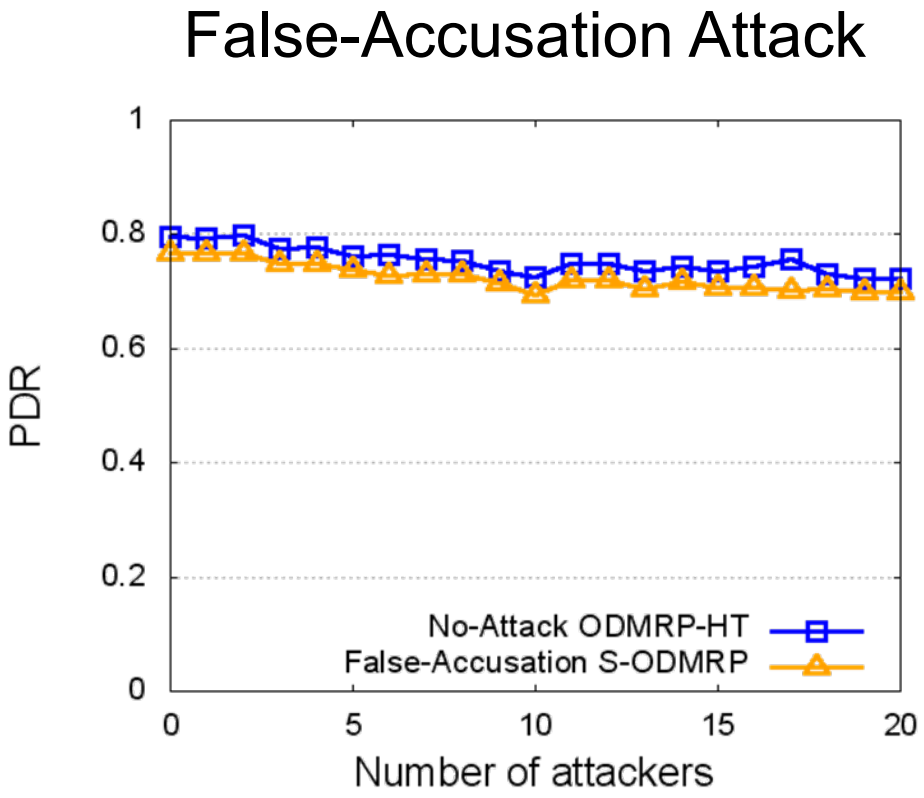


GMM-Drop



Our defense successfully mitigates all three types of attacks

Resiliency to Attack



S-ODMRP is resilient to False-Accusation attacks

Conclusion

- High-throughput multicast is an important service for wireless mesh networks
- Aggressive path selection is a double-edged sword
  - It improves performance
  - But it introduces severe security vulnerability
- We proposed an effective and lightweight scheme for achieving secure high-throughput wireless multicast

Thank You!

Questions?

Contact: dongj@cs.purdue.edu