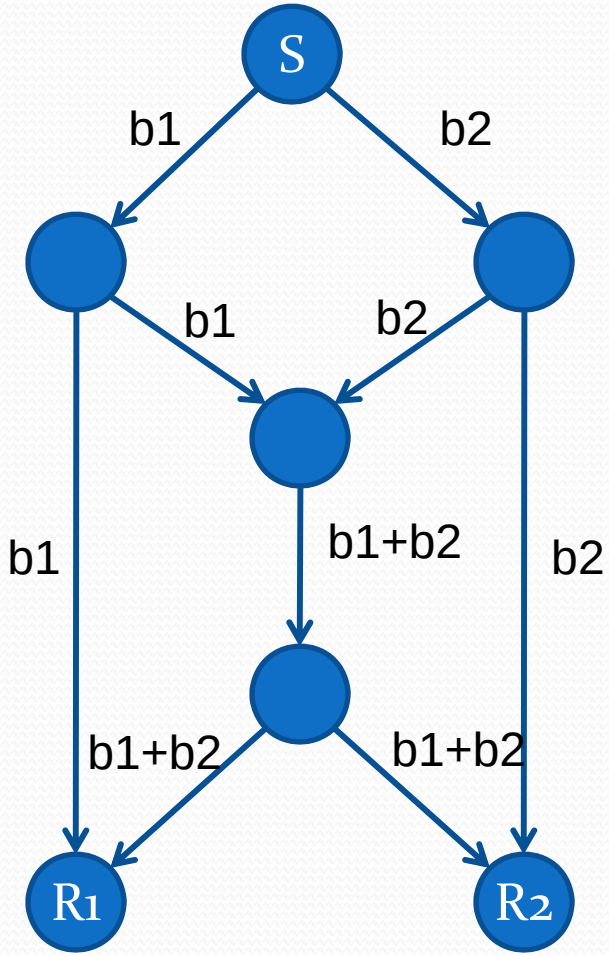
Toward Secure Network Coding in Wireless Networks: Threats and Challenges

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

Network Coding

- A new paradigm in network protocol design
- ***Intermediate nodes actively mix input packets to produce output packets***
- Applications
  - Peer-to-peer networks
  - Distributed storage
  - Wireless networks

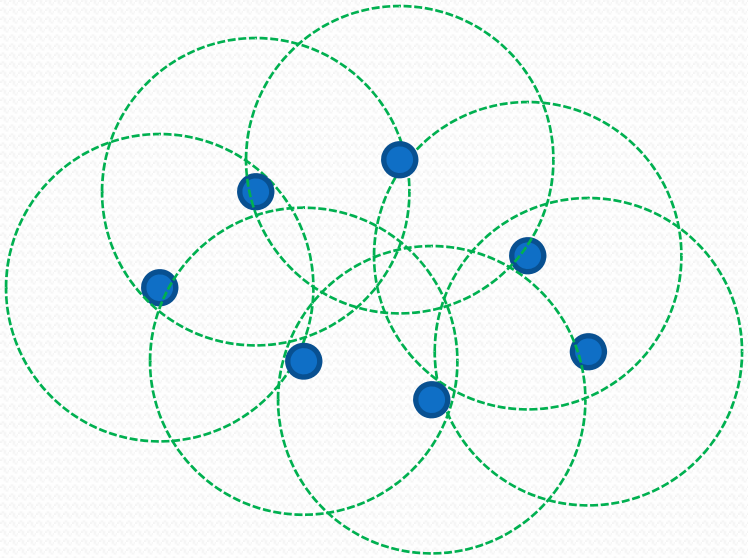


From Ahlswede, et al, 2000

Network Coding in Wireless Networks

- Fits naturally in wireless networks
- Exploits ***broadcast advantage*** and ***opportunistic listening***

- Benefits
  - Improved throughput
  - Improved energy efficiency
  - Improved reliability



Need for Security in Wireless

- Primarily performance-oriented
  - Numerous design choices and optimizations
  - No security considerations
- Wireless networks are inherently vulnerable
  - Easy eavesdropping, packet injection, jamming, spoofing
  - Easy physical access, software bugs, mis-configurations

Performance  Security

What This Talk is About …

Study security implications of current network coding designs

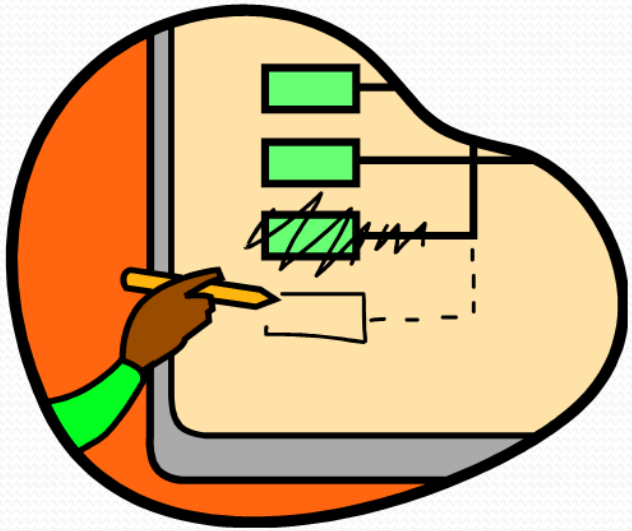
- ***Intra-flow network coding***
- ***Inter-flow network coding***

Related Work

- **Exclusively** on packet pollution attacks
  - Attacker node injects corrupted packets in the network
- Pollution Defense
  - Cryptographic [Charlies, et al; CISS 06], [Zhao, et al; ISIT 07], [Yu, et al; Infocom 08], [Krohn, et al; S&P 2004]
  - Information theoretic [Ho, et al; ISIT 04], [Jaggi, et al; Infocom 07]
  - Network error correction coding [Silva, et al; IEEE Info Theory 07], [Koetter, et al; IEEE Tran. Info Theory 08]

Outline

- System overview
  - Intra-flow network coding
  - Inter-flow network coding
- Attacker model
- Threat analysis
  - Intra-flow network coding
  - Inter-flow network coding
- Experiments
- Conclusion



Network Coding Frameworks

- Intra-Flow Network Coding
  - *Mix packets within individual flows*
  - MORE [Chachulski, et al; Sigcomm 07], [Zhang and Li; ICDCS 08], [Zhang and Li; Mobihoc 08], MIXIT [Katti, et al; Sigcomm 08]
- Inter-Flow Network Coding
  - *Mix packets across multiple flows*
  - COPE [Katti, et al; Sigcomm 06], DCAR [Le, et al; ICDCS 08], [Das, et al; NSDI 08]

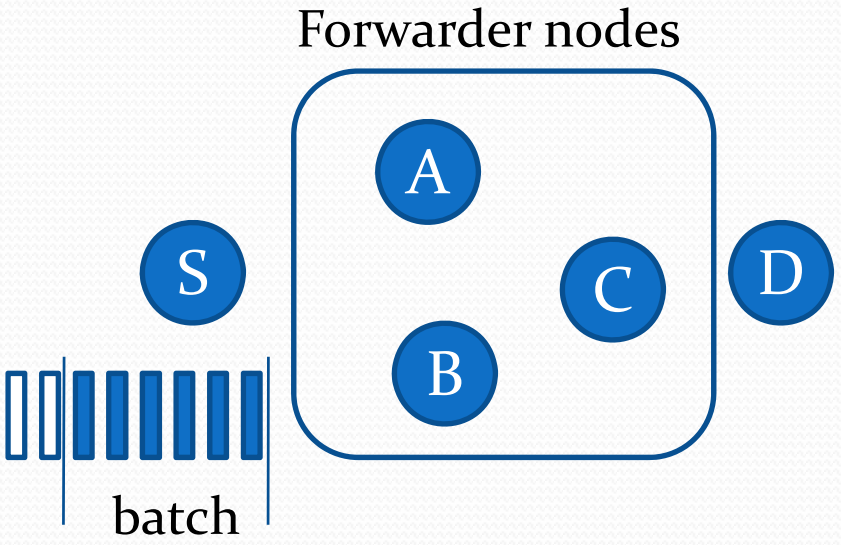
Attacker Model

- Attacker goal: denial of service attack
- Insider attacks
  - Eavesdropping, injection, modification
  - May collude
  - In-band or out-of-band wormholes
  - Flood rushing attacks
- Do not consider jamming or MAC-layer attacks

Intra-Flow Network Coding

Intra-Flow Network Coding

- Packets are sent in *batches*
- Source
  - Broadcasts coded packets
- *Forwarder* nodes
  - Buffer coded packets
  - Forward new coded packets
- Destination
  - Buffer coded packets
  - Decode packets
  - Send ACK to source



Coded packet p_c :

$p_c = c_1 p_1 + c_2 p_2 + \ldots + c_n p_n$

Components of Intra-Flow Network Coding

- Forwarding node selection and rate assignment
- Data packet forwarding
- Acknowledgment delivery

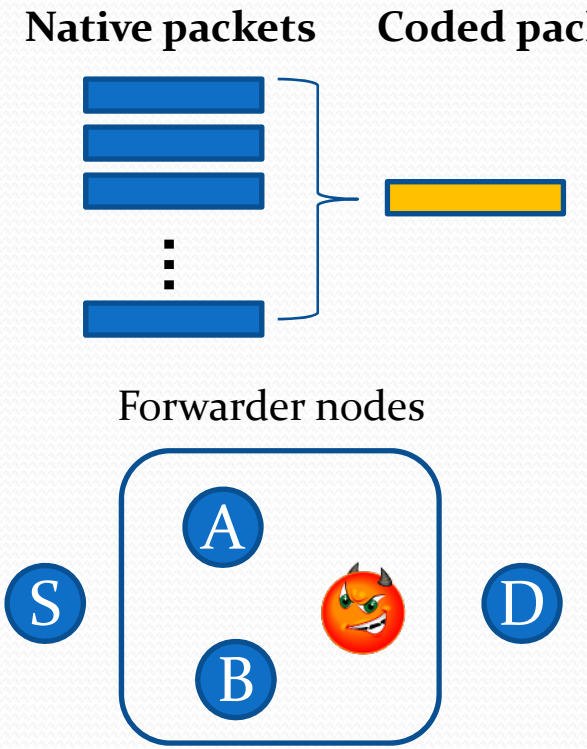
Forwarding Node Selection and Rate Assignment

- Require global knowledge
- Achieved in link state routing like approach
- Attacks
  - **Link Quality Falsification**
  - **Link Quality Modification**
  - **Wormholes**

Attacks cause incorrect forwarder node selection and rate assignment

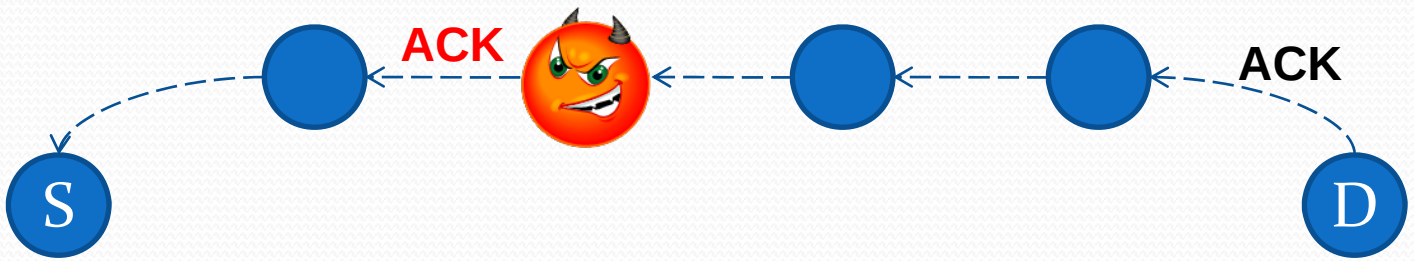
Data Packet Forwarding

- Store overheard coded packets
- Forward coded packets at pre-determined rate
- Attacks
  - **Packet Pollution**
    - Epidemic attack propagation
    - **Cannot** be defended with traditional digital signature
  - **Packet Dropping**
    - Challenging to apply monitor-based solution



Acknowledgment Delivery

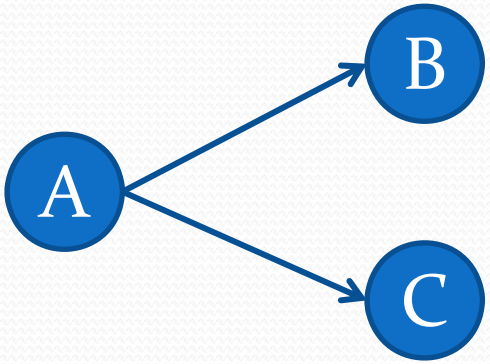
- Delivered using single path routing
- Reliability achieved via hop-by-hop acknowledgment
- Attacks
  - **ACK Injection and Modification**
  - **ACK Dropping**
  - **ACK Delay**



Inter-Flow Network Coding

Inter-Flow Network Coding

- Mix packets from multiple sources



- Combine multiple unicasts to different next hop nodes into a single broadcast
- **Decodability Condition**
  - The downstream nodes have overheard necessary packets to decode the combined packet

$P_1 \rightarrow B$
$P_2 \rightarrow C$
B overhead P_2, C overheard P_1
A broadcasts $P_1 \oplus P_2$

Components of Inter-Flow Network Coding

- Coding opportunity discovery
- Coded packet transmission
- Routing integration

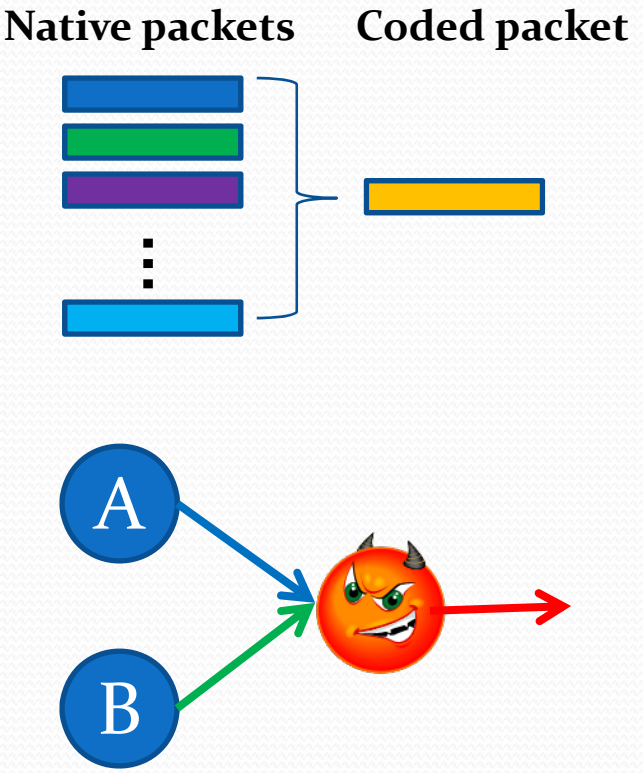
Coding Opportunity Discovery

- Localized coding [Katti, et al; Sigcomm 06]
  - Local broadcast of packet reception information
- Global coding [Le, et al; ICDCS 08]
  - Maintaining neighboring node set on packet paths
- Attacks
  - **Packet Reception Information Mis-Reporting**
  - **Link State Pollution**
  - **Neighbor Set Pollution**

Attacks cause missing coding opportunities or sending undecodable packets

Coded Packet Transmission

- Requires reliability
- Achieved via *pseudo-broadcast*
- Attacks
  - **ACK Injection and Modification**
  - **Packet Pollution**
    - Challenging to apply crypto-based solution
  - **Packet Dropping**
    - Challenging to apply monitor-based solution



Routing Integration

- Use new coding-aware routing metric
- Route computation
  - Decentralized as in on demand routing [Le, et al; ICDCS 08]
  - Centralized as in link state routing [Das, et al; NSDI 08]
- Attacks
  - **Coding Benefit Metric Manipulation**
    - Allow an attacker to attract or repel traffic
    - More challenging than other metric manipulations

Experimental Evaluations

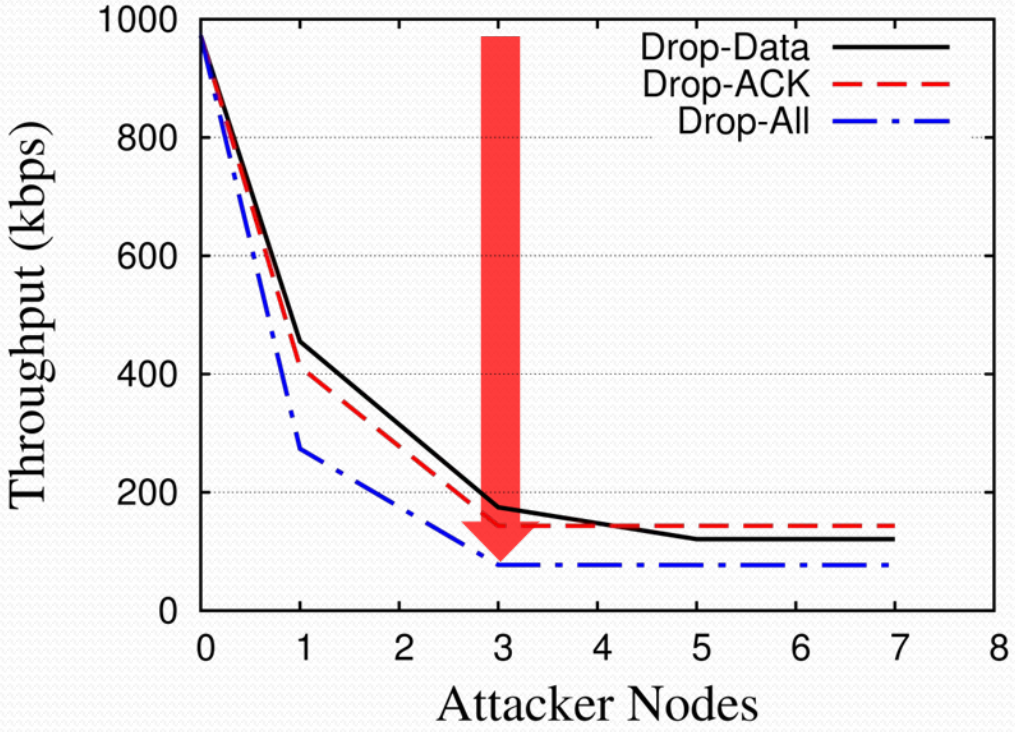
- Network coding system: MORE [Chachulski, et al; Sigcomm 07]
- Simulator: Glomosim
- Trace driven physical layer
  - MIT Roofnet trace
- 5.5Mbps raw bandwidth
- 250m range
- MORE setup
  - GF(2^8), batch size 32, packet size 1500 bytes
- Source and destination are randomly selected

Attack Setup

- Attacker nodes are selected at random among all forwarding nodes

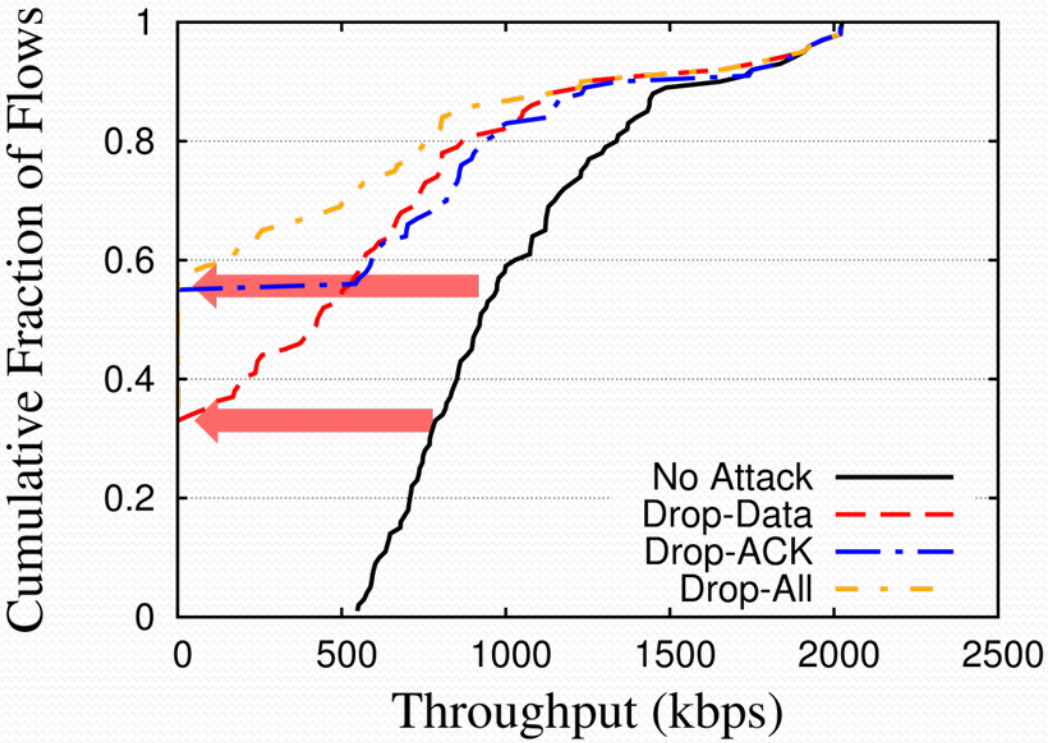
- Scenarios
  - **Drop-Data**: only data packets are dropped
  - **Drop-ACK**: only ACK packets are dropped
  - **Drop-All**: both data and ACK are dropped

Impact on Multiple Attackers



Packet dropping attacks are very damaging

Impact of Single Attacker



Even a single attacker can cause a large impact

Conclusion

- We reveal a wide range of vulnerabilities in existing network coding systems
  - Pollution is only tip of an iceberg
- Coding introduces new attacks, and makes existing attacks more challenging to defend
- Open Question

Can we design a secure network coding system that still preserves the performance gains?

Questions?

Jing Dong (dongj@cs.purdue.edu)