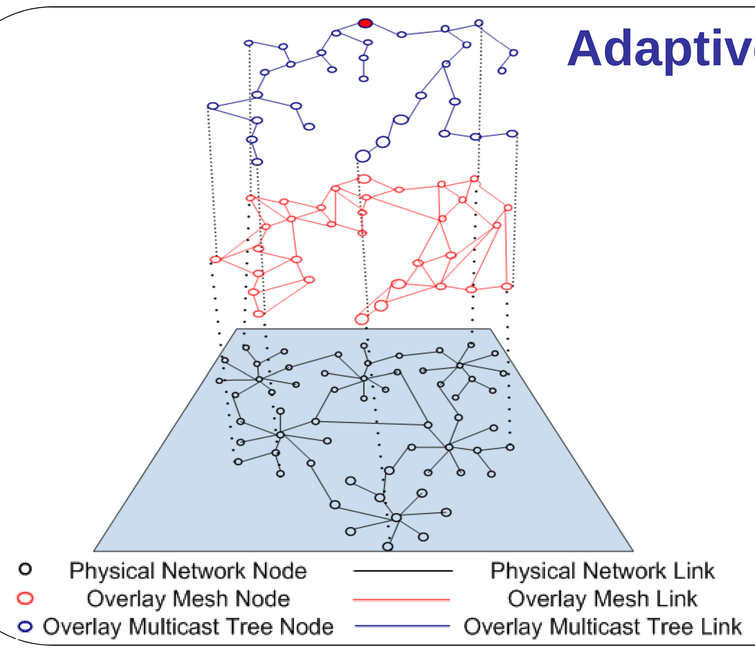
CERIAS

the center for education and research in information assurance and security

Removing the Blinders: Utilizing Data-Plane Information to Mitigate Adversaries in Unstructured Multicast Networks

David Zage, Charles Killian, and Cristina Nita-Rotaru

Department of Computer Science and CERIAS, Purdue University



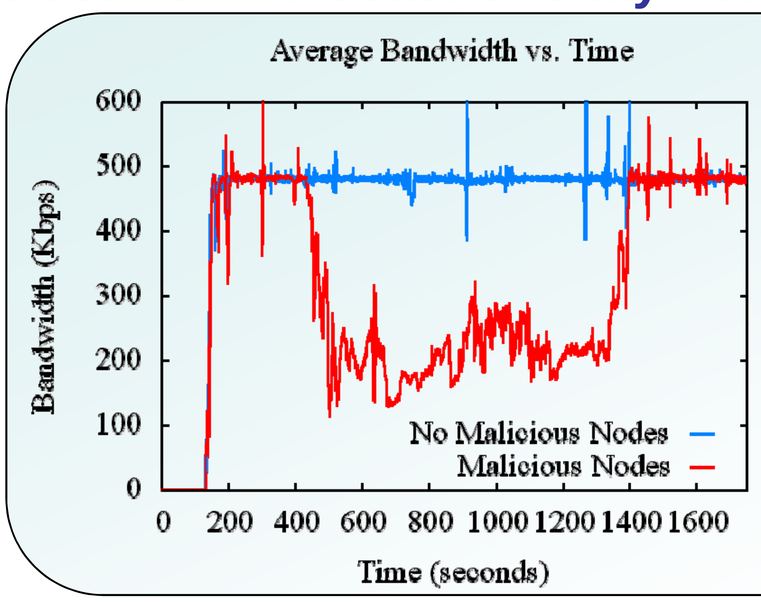
Adaptive, Unstructured Multicast Overlay Networks

- Provide increased functionality
- Use adaptivity mechanisms to dynamically optimize application metrics such as latency, jitter, bandwidth, and loss rates when selecting network paths
- Vulnerable to malicious attacks coming from outside and inside the overlay network.

Our Goal – Create adaptive unstructured multicast networks that are tolerant to malicious subversion by using information already present in the system

Insider Attacks on Unstructured Multicast Overlay Networks

- **Inside attacker capabilities:**
  - Attacker has access to all information on compromised nodes
  - **Compromised nodes can lie about the observation space**
- **Results of the attacks:**
  - Adversarial controlled path selection, increased system instability, and susceptibility to further attack.



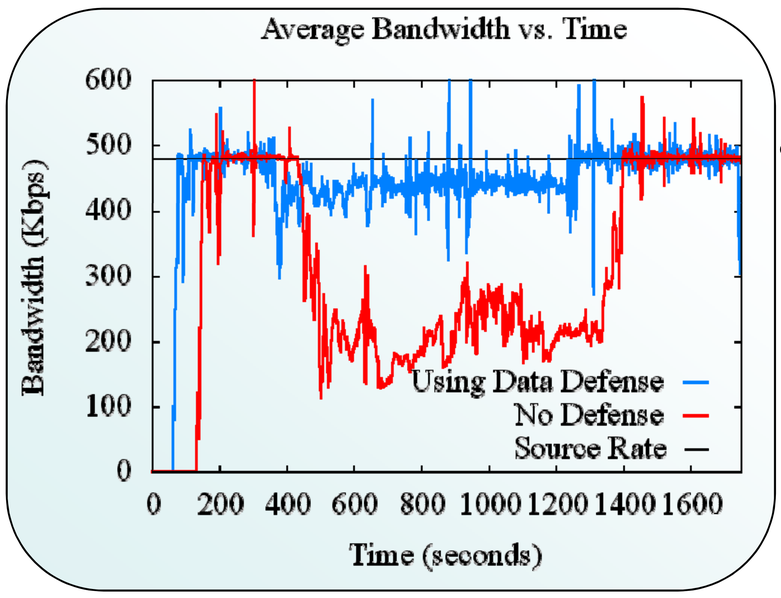
% of Malicious Nodes	# of Topology Changes
No Malicious Nodes	92
10% Malicious Nodes	393
20% Malicious Nodes	475
30% Malicious Nodes	522

Lying nodes induce topology changes and decrease the average bandwidth in ESM multicast overlay system deployments on PlanetLab.

Using Data-Plane Information to Mitigate Insider Attacks

- **Reducing erroneous adaptations**

  Utilize data-plane information already distributed in the system to construct local view of the network at each node to constrain the ability of an attacker to induce changes in the network topology.
  - Verify local view of the network against system constraints
  - Verify information based on multiple sources of input



This graph demonstrates the ability of data plane information in mitigating the effects of 30% malicious nodes in the unstructured multicast overlay lying about their metrics and dropping data.

PURDUE UNIVERSITY

CERIAS

Discovery Park e-Enterprise Center