CAREER: Scalable, Robust and Secure Group Communication for Wireless Mesh Networks

Cristina Nita-Rotaru, Purdue University http://projects.cerias.purdue.edu/ds2/mesh.html

Problem

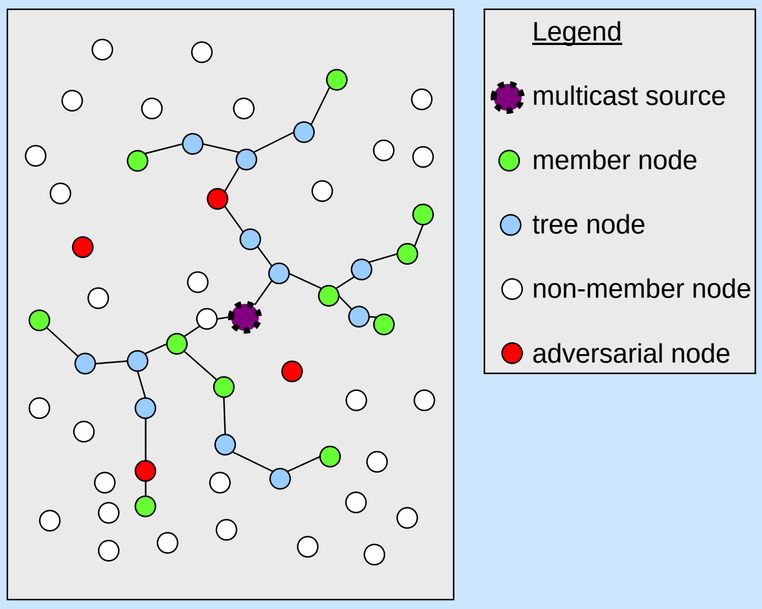
Group services in wireless mesh networks require scalable, robust and secure multicast. Multicast in multi-hop wireless networks relies on node cooperation. Malicious nodes can easily disrupt the routing protocol, data dropping, flood rushing, or wormhole attacks can be easily mounted and may cause significant damage. Solutions proposed in unicast settings are not scalable for multicast.

Approach

Our focus is to mitigate data dropping attacks (and indirectly other attacks that act as amplifiers, such as flood rushing and wormhole). We adopt a hybrid defense strategy: A proactive component ensures attacks are detected, and a reactive component ensures attackers are avoided.

Collaborative applications benefit from multicast protocols that provide support for efficient group communication.

The multicast setting in multi-hop wireless networks



Approach and Impact

New Approach

- Acknowledgement-based solutions are not scalable due to acknowledgement implosion
- Proactive component allows attack detection by periodic dissemination of data transmission rate and data rate measurement at each node
- Reactive component allows attack avoidance with a metric that captures adversarial behavior

Research Impact

- Showed that Byzantine attacks have a significant impact on authentication-only based protocols
- Achieved Byzantine-resiliency for multicast routing in multi-hop wireless networks
- Identified design principles for multicast protocols resilient to Byzantine attacks

Detecting Data Dropping Attacks

Basic Strategy

δ = upper bound for loss on a single link

S ρ_0

1 $[\rho_0, (1, \rho_1)]$

2 $[\rho_0, (1, \rho_1), (2, \rho_2)]$

3 $[\rho_0, (1, \rho_1), (2, \rho_2), (3, \rho_3)]$

4 $[\rho_0, (1, \rho_1), (2, \rho_2), (3, \rho_3), (4, \rho_4)]$

5 Node 5 reacts if $\rho_3 - \rho_5 > \delta$

$\rho_4 - \rho_5 > \delta$

Advanced Strategy

- only add rate if perceived rate decrease is $> \delta$
- additional threshold $\Delta = 2\delta$ prevents artificial rate decrease

S ρ_0

$= \delta/4$

1

$= \delta/4$

2

$= \delta/4$

3 $[\rho_0, (3, \rho_3)]$

4 $[\rho_0, (3, \rho_3), (4, \rho_4)]$

$\geq \Delta$

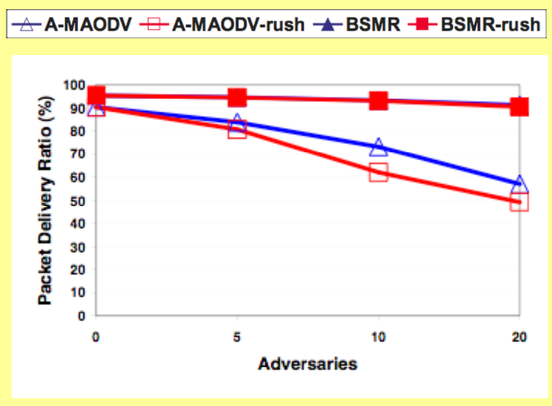
5

Experimental Results

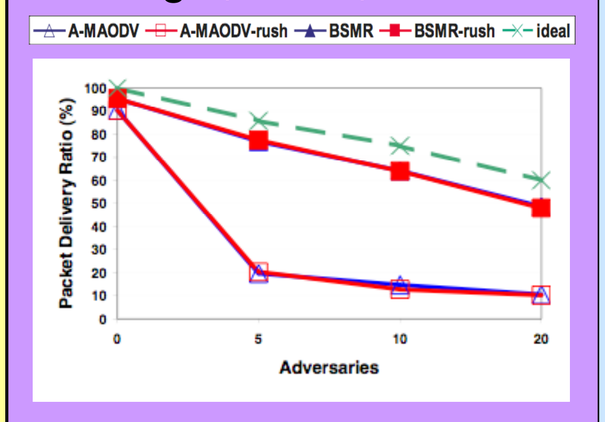
We quantify the impact of various adversarial strategies:

- adversarial positioning (random vs. strategic placement)
- adversarial group membership status (JOIN vs. NJOIN)

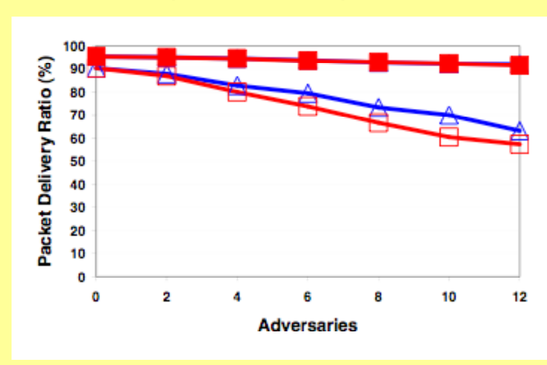
random, NJOIN, blackhole



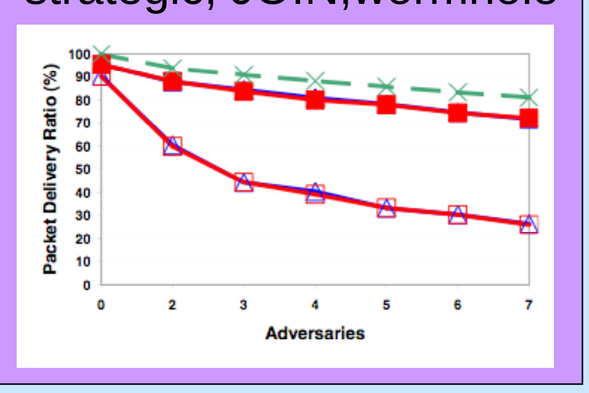
strategic, JOIN,blackhole



random, NJOIN, wormhole



strategic, JOIN,wormhole



National Science Foundation WHERE DISCOVERIES BEGIN

NSF Cyber Trust Principal Investigators Meeting
March 16-18, 2008
New Haven, CT

CERIAS PURDUE UNIVERSITY