Enabling Secure Service in Mobile Ad-Hoc Networks

Patrick Tague
Assistant Research Professor
CyLab Mobility Research Center
Carnegie Mellon University, Silicon Valley
tague@cmu.edu
Ad-Hoc Networking

- Mobile system with no infrastructure
- Multi-hop communications and networking
- Heterogeneous system
  - Mobile mesh and sensor networks
  - Personal / ubiquitous computing
  - Networked control (cyber-physical) systems
Research Goal

Design of **practical** ad-hoc communication & networking protocols that enable or provide **secure** service
Focus on Data Delivery

**Goal:** secure data delivery using multi-hop networking

- Predictability
- Connectivity
- Reliability
- Availability
- Timeliness (QoS)
- Error-resilience

Source $s$  
Dest $d$
Loss and Failure

What causes loss and failure?
- Identifying vulnerabilities, sources of uncertainty
- Modeling attacks and attack impact

How do loss and failure affect performance?
- Inferring the causes from the losses and failures
- Science of system performance

How to design for robustness in spite of failure?
- Adapting to detected or predicted attacks and failures
- Robustness against unknown events?

Natural vs. Malicious
What types of adversarial behaviors impact data delivery?
Attack Primitives

Exploiting the Wireless Medium
- Eavesdrop, replay, jam, interfere, trace packets

Physically Attacking Devices
- Compromise, clone, move, modify (hw/sw), destroy nodes

Attacking Protocols as an Insider
- Stray from protocol, misbehave, modify/insert/drop packets
Malicious Packet Forwarding

Source $s$

100 packets

2 packets dropped

Dest $d$

98 packets

20 packets dropped

20 packets inserted

Efficient identification of inserted packets?
Distinction between causes of packet loss?
Impact of jamming on data delivery? Detection/tracking of jammers?
Efficient & Stealthy Jamming

Sender

pkt

pkt

pkt

Receiver

Effort energy

Excessive?

Targeted attack

Sufficient to corrupt packets

Harder to detect

More efficient

Wasted
Jamming Network Traffic

Collaborative jamming network; Improved efficiency & stealthiness
How to incorporate the impact of attacks into network protocols?
Task Distribution

Assignment of work/task-load over network reduces dependence on individuals
Secure service relies on the ability to continually adapt to attack scenarios.
Jamming-Aware Transport

Multi-path routing provides spatial diversity to attack

Feedback from relay nodes allows source to dynamically adapt traffic allocation over multiple fixed routing paths.

End-to-end success rate (and uncertainty) for each path can be predicted from the relayed loss rates.
Summary

- Need to understand and model increasingly practical, efficient, and stealthy attacks
- New attack/failure detection and mitigation techniques are required
- Statistical methods and adaptability improve robustness to attacks