Carnegie Mellon SILICON VALLEY

mobility research center

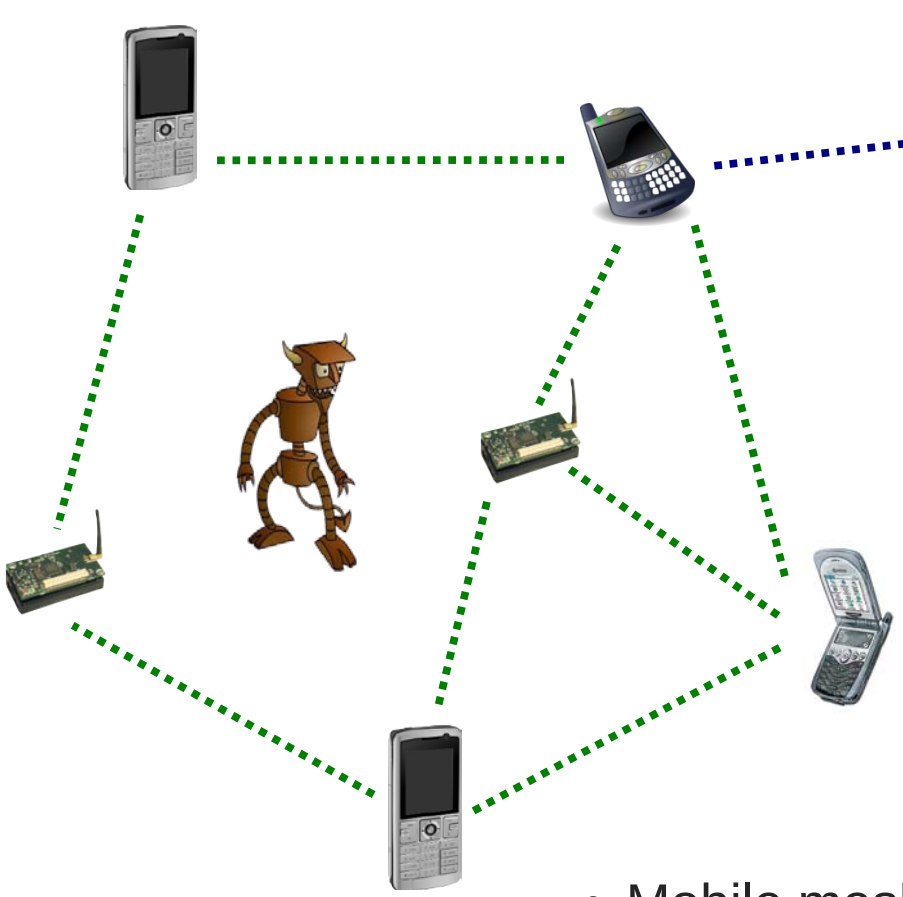
Carnegie Mellon CyLab

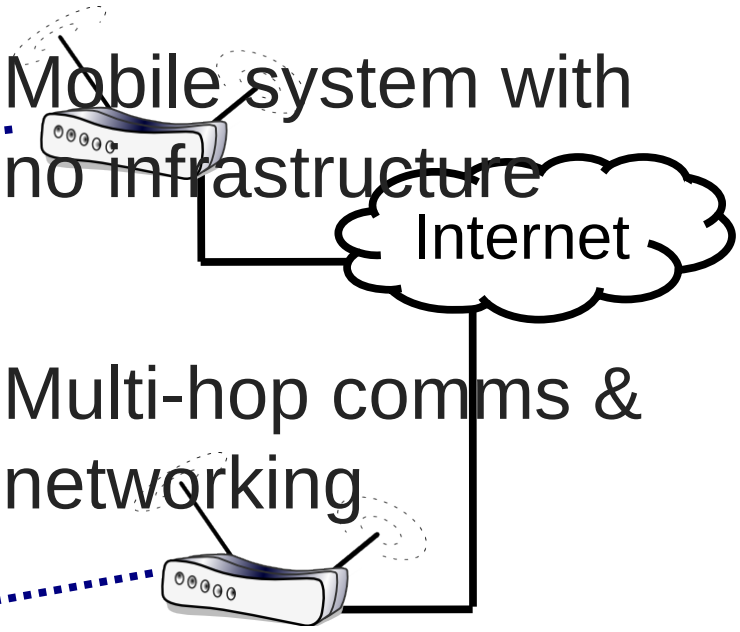
Enabling Secure Service in Mobile Ad-Hoc Networks

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 comms & 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

Timeliness (QoS)

Reliability

Availability

Error-resilience

Source *s*

Fairness

Dest *d*

Loss and Failure

What causes loss and failure?

- Identifying vulnerabilities, sources of uncertainty
- Modeling attacks and attack impact

Natural vs. Malicious

How do loss and failure affect performance?

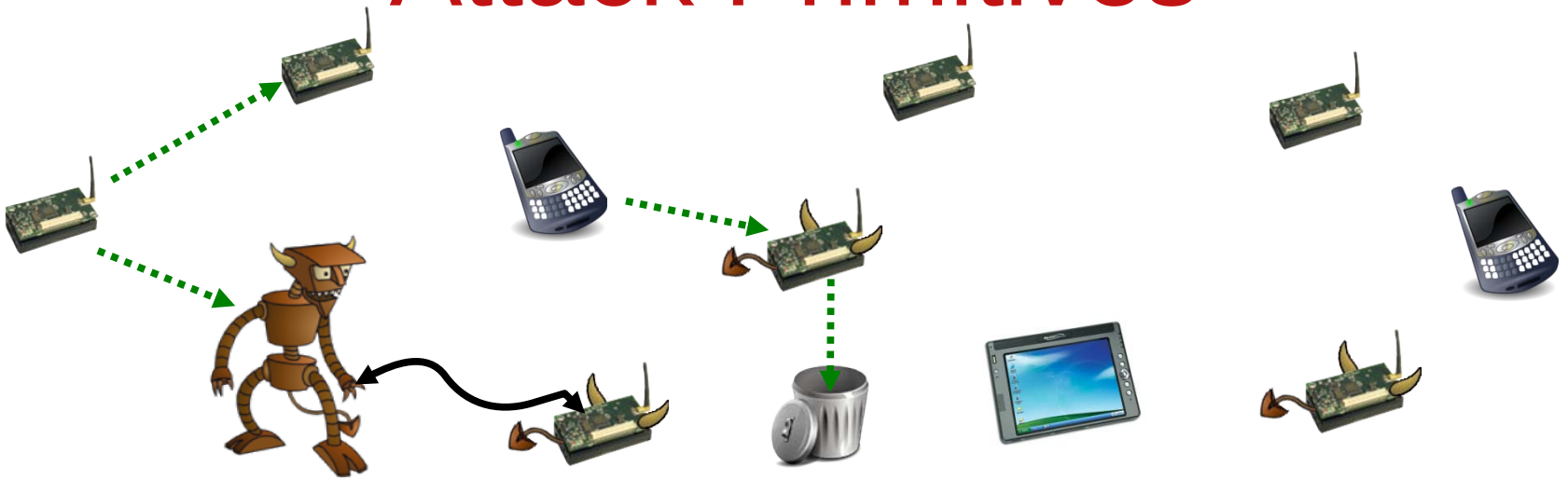
- Inferring the causes from the losses and failures
- Science of system performance

How to design for robustness in spite of failure?

- Adapting to detected or predicted attacks and failures
- Robustness against unknown events?

What types of adversarial behaviors impact data delivery?

Attack Primitives



Exploiting the Wireless Medium

Eavesdrop, replay, jam, interfere, trace packets

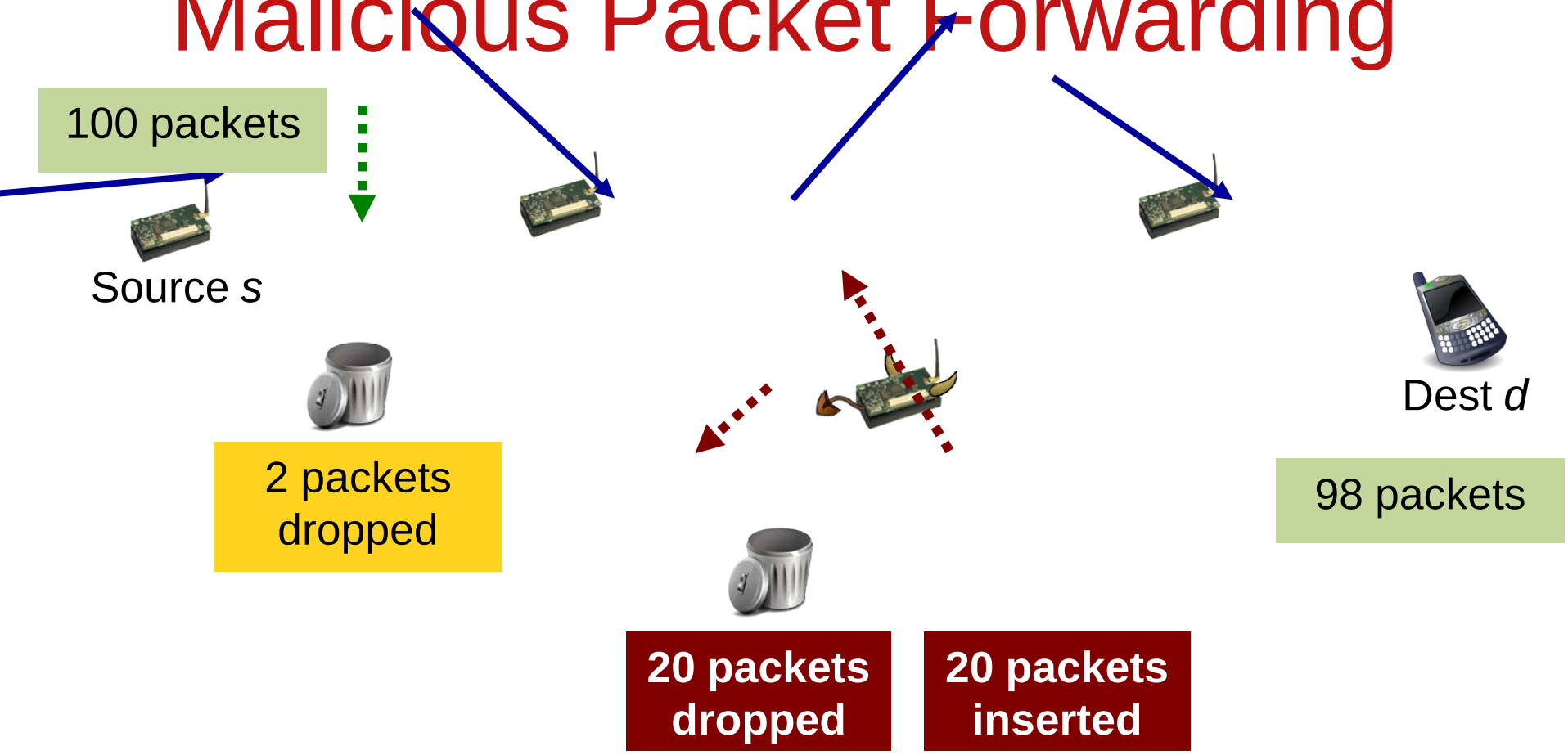
Physically Attacking Devices

Compromise, clone, move, modify (hw/sw), destroy nodes

Attacking Protocols as an Insider

Stray from protocol, misbehave, modify/insert/drop packets

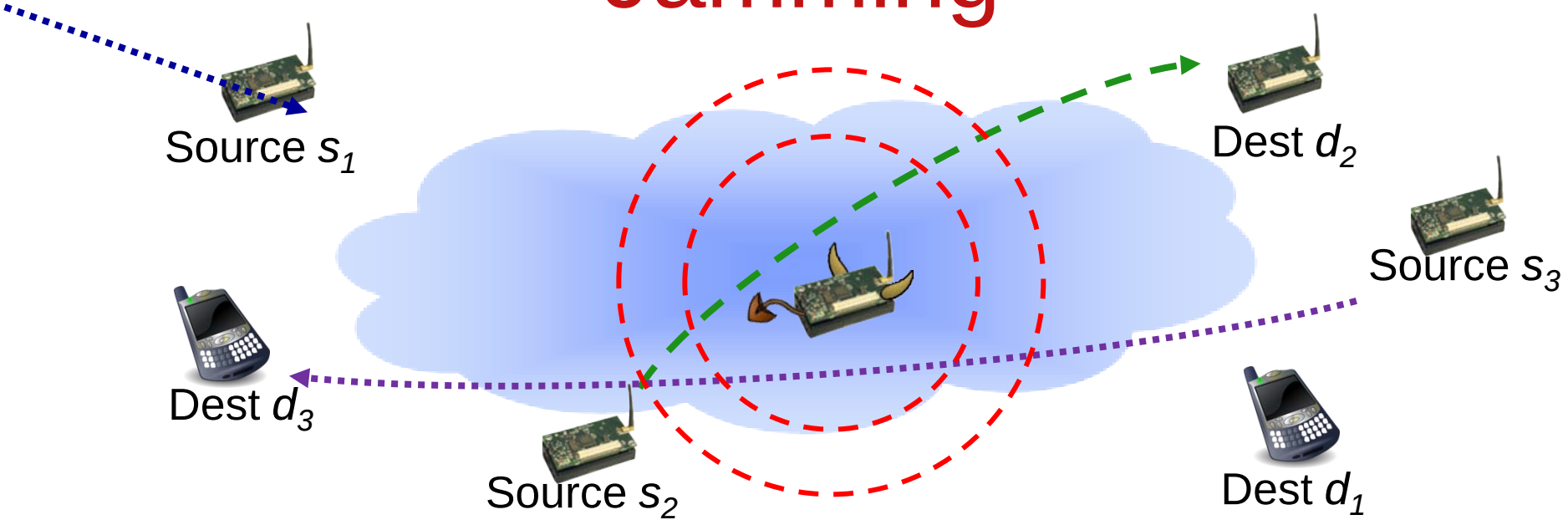
Malicious Packet Forwarding



Efficient identification of inserted packets?

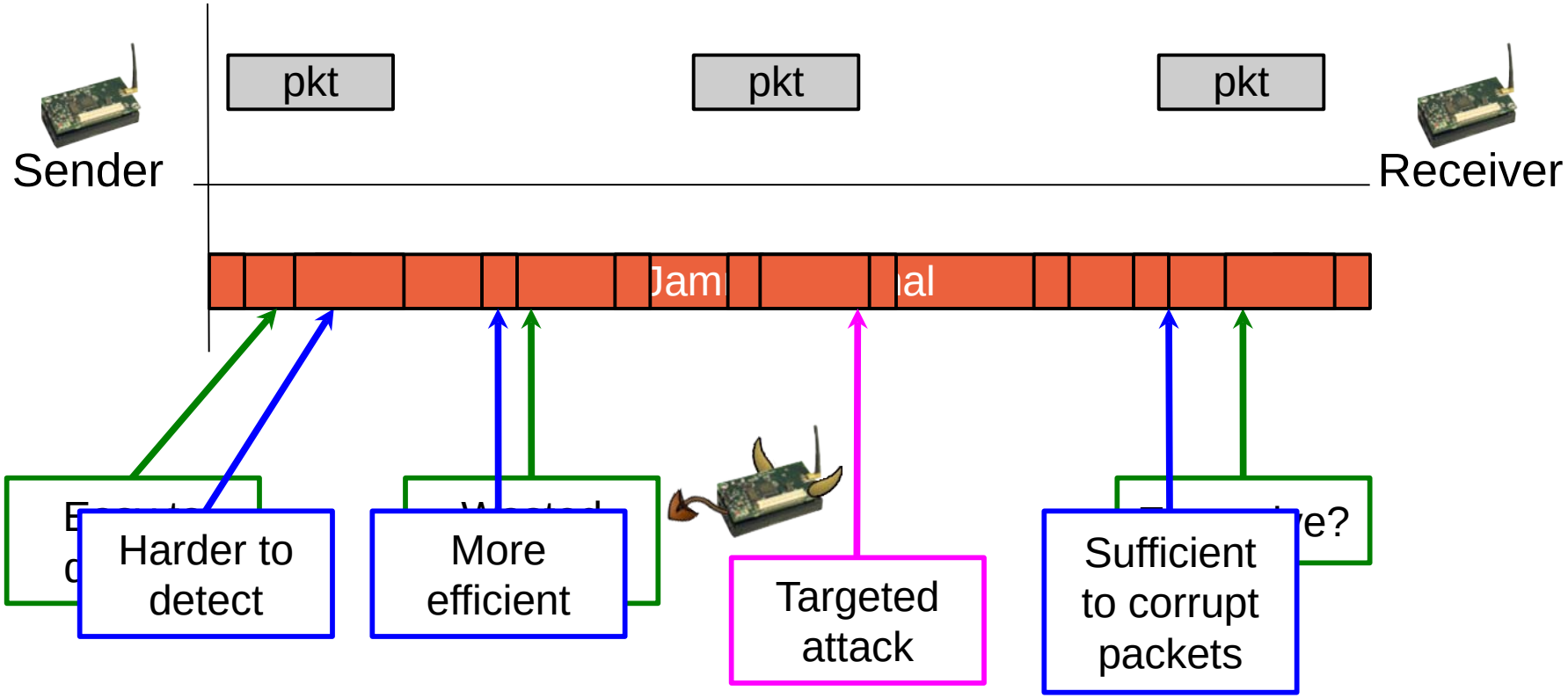
Distinction between causes of packet loss?

Jamming

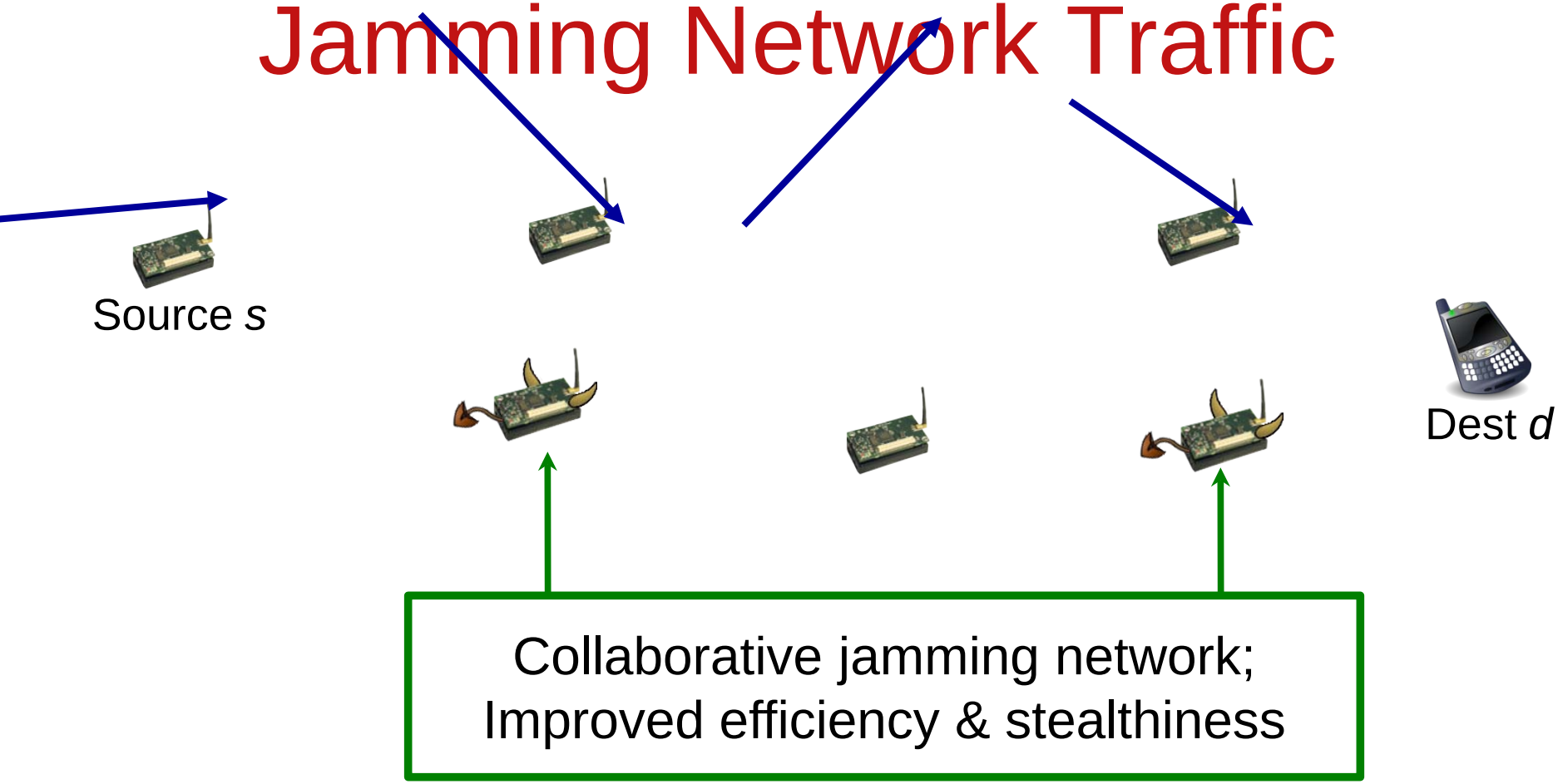


Impact of jamming on data delivery?
Detection/tracking of jammers?

Efficient & Stealthy Jamming



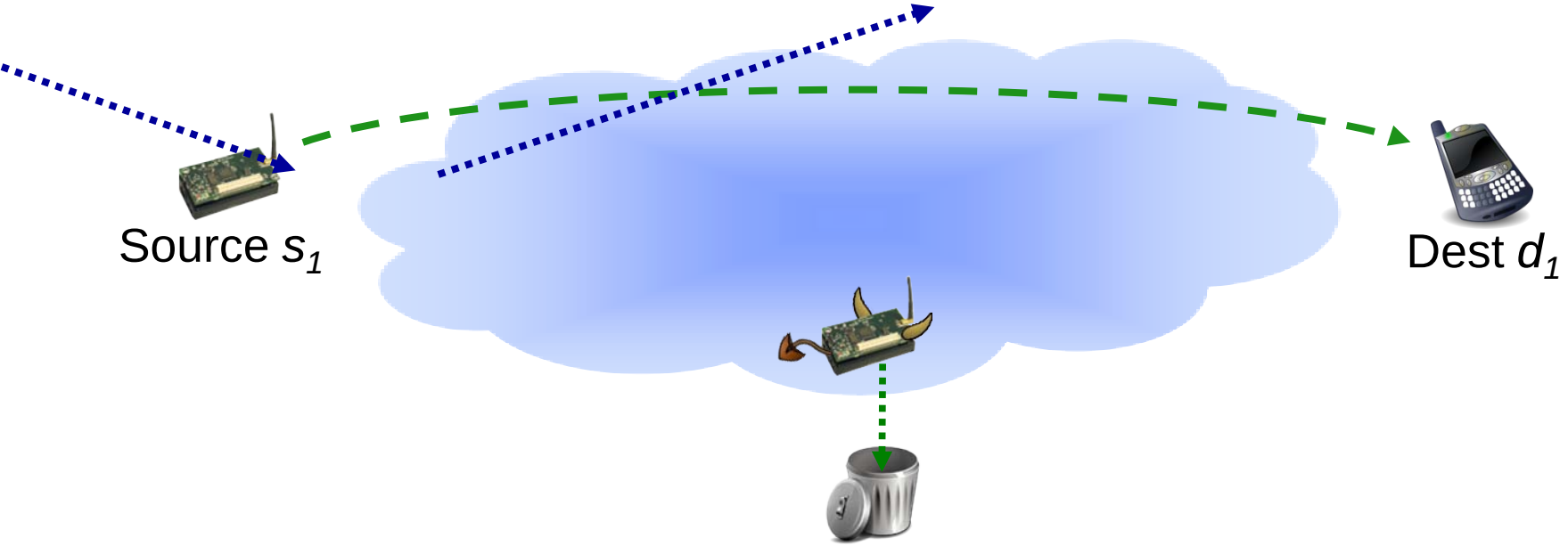
Jamming Network Traffic



How to incorporate the impact of attacks into network protocols?

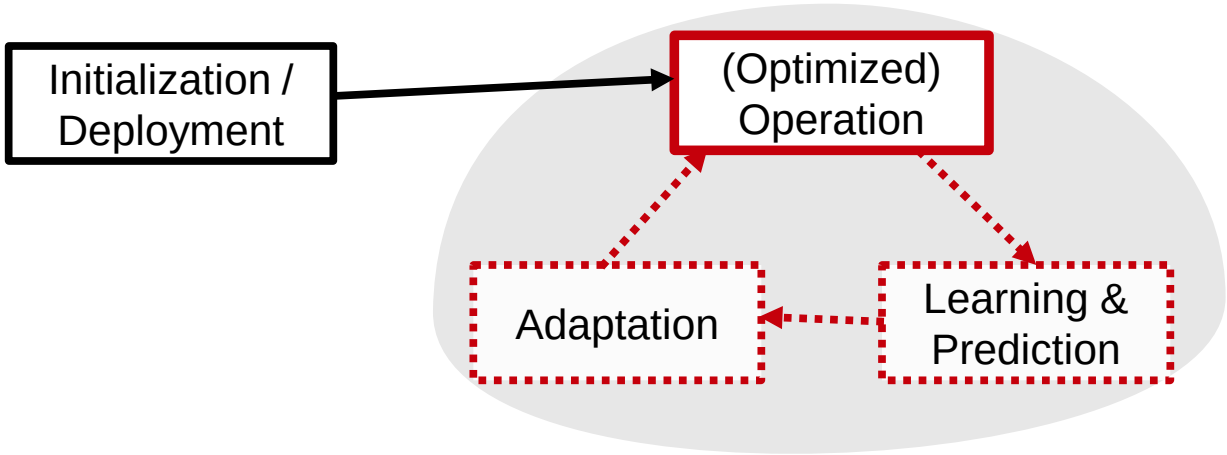
Task Distribution

Assignment of work/task-load over network reduces dependence on individuals



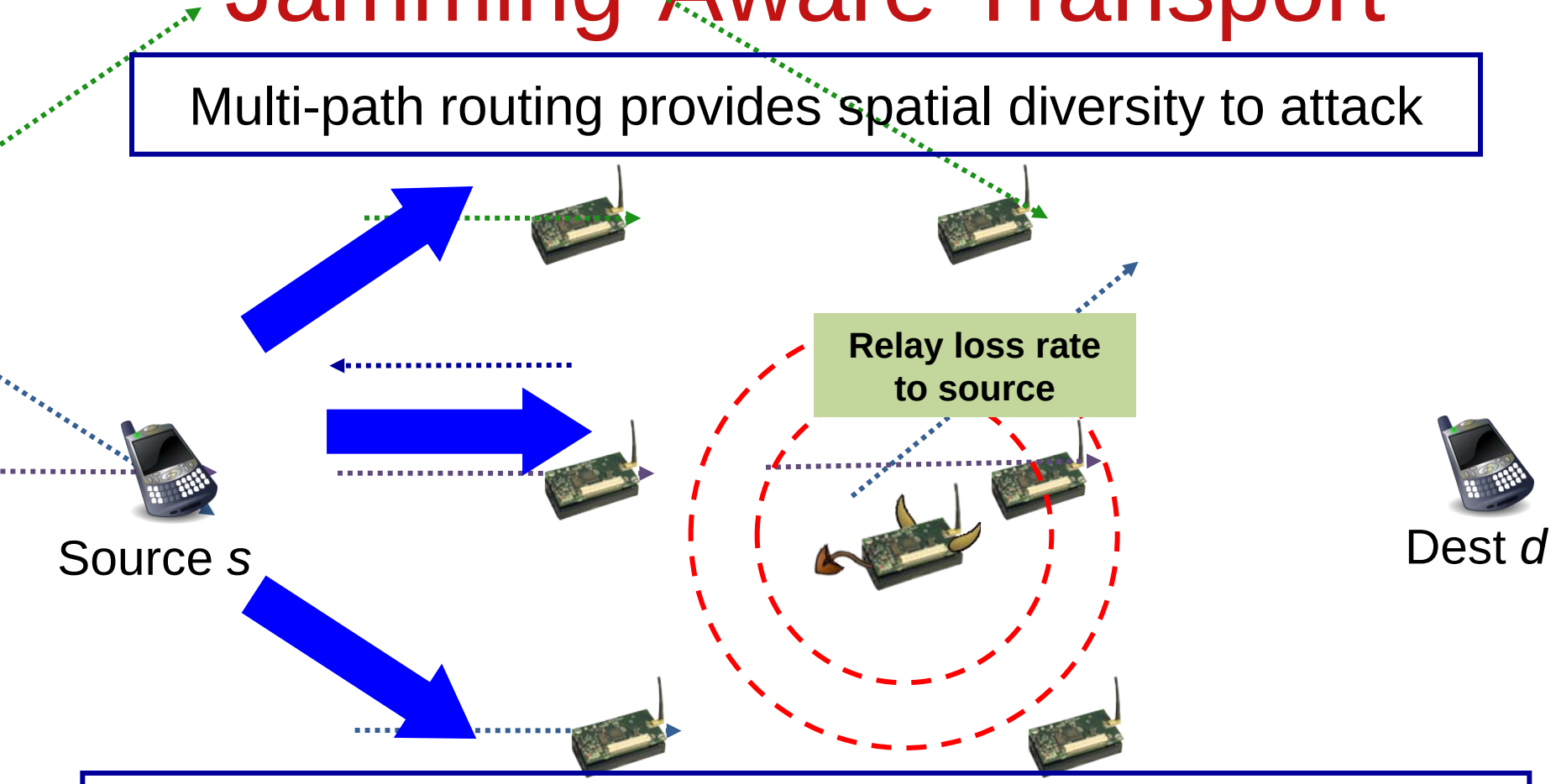
Adaptability

Secure service relies on the ability to continually adapt to attack scenarios



Jamming-Aware Transport

Multi-path routing provides spatial diversity to attack



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

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

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