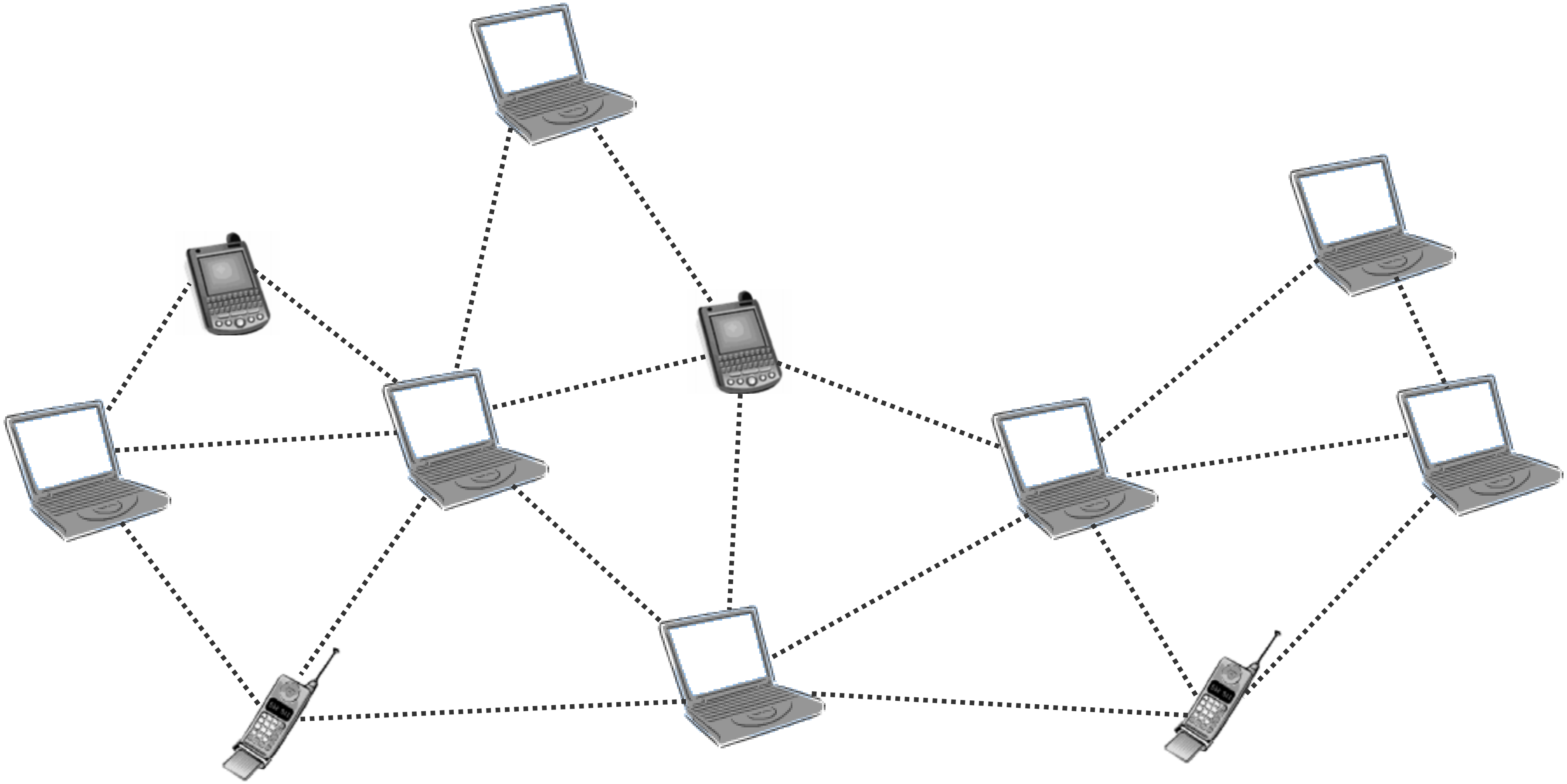
Security - is it at odds with performance?

Reza Curtmola

Purdue University
Department of Computer Science and CERIAS

(based on joint work with Jing Dong and Cristina Nita-Rotaru)

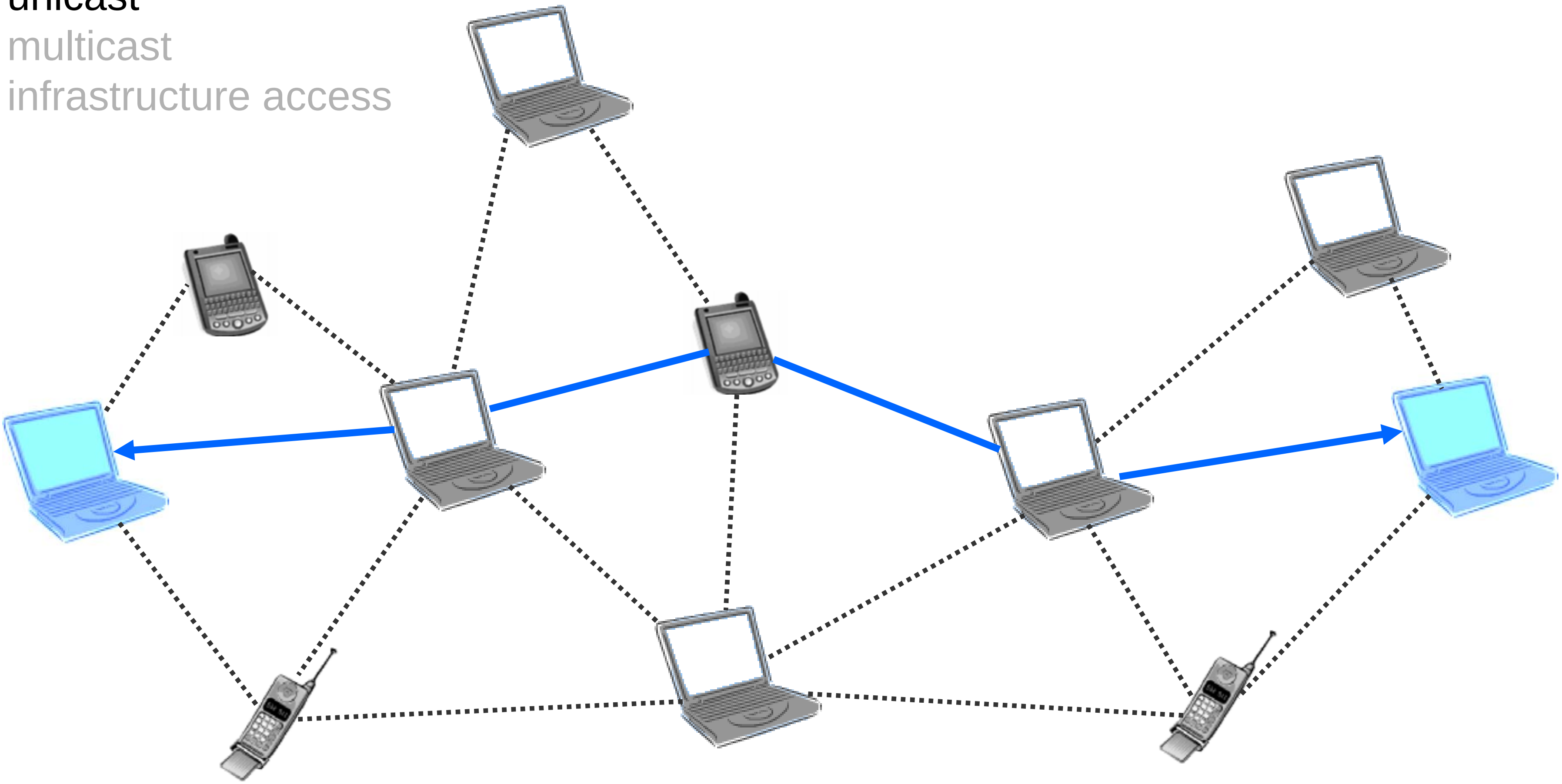
Multi-hop Wireless Networks



Multi-hop Wireless Networks

Multi-hop routing:

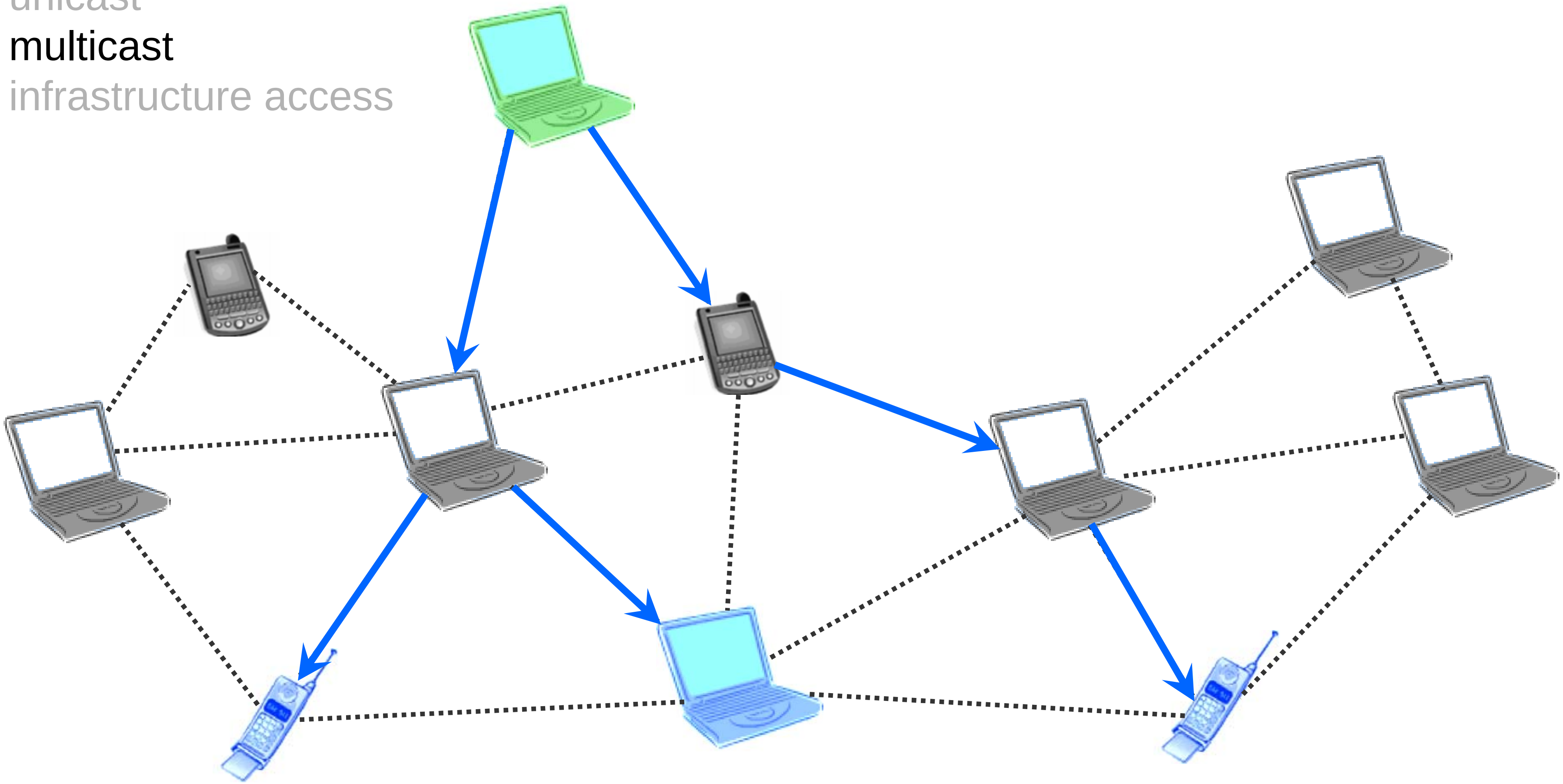
- unicast
- multicast
- infrastructure access



Multi-hop Wireless Networks

Multi-hop routing:

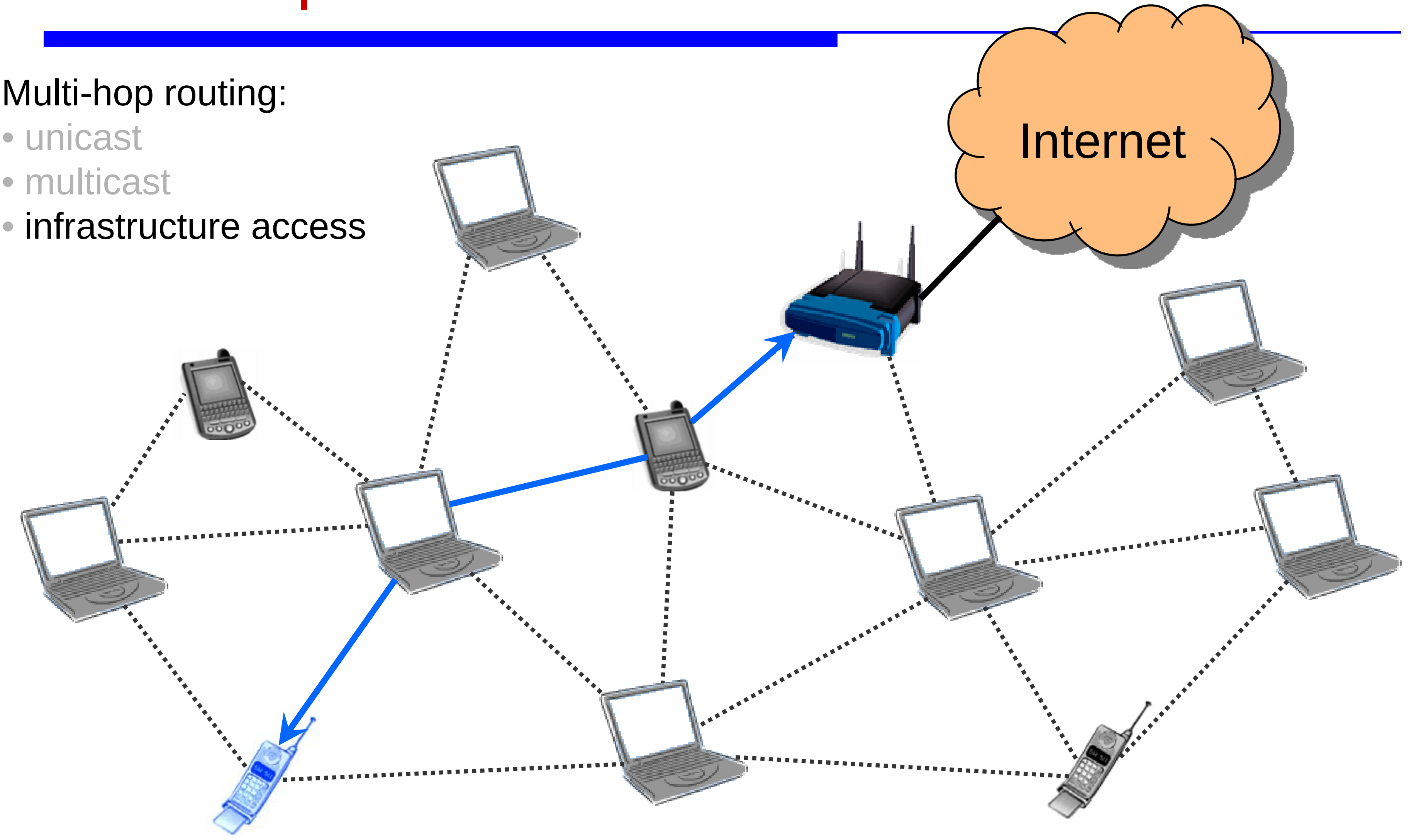
- unicast
- multicast
- infrastructure access



Multi-hop Wireless Networks

Multi-hop routing:

- unicast
- multicast
- infrastructure access



Multi-hop Wireless Networks

- Advantages:
  - Increased coverage at low cost
  - Increased reliability
  - Increased flexibility => management and maintenance cost savings

Deployment of Wireless Mesh Networks

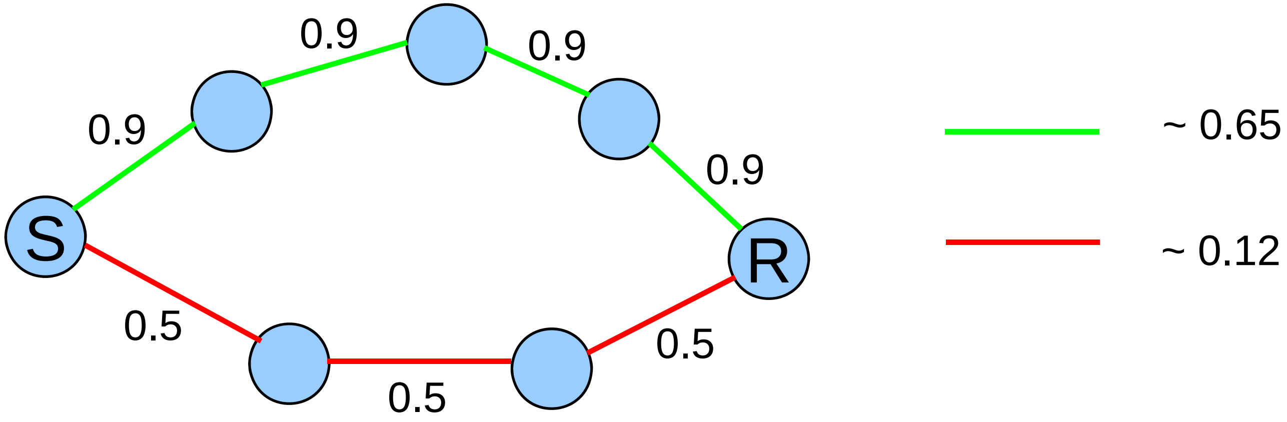
- Municipal public WiFi networks
  - March 2007: installed in 81 cities, under development in 164 cities
  - Public services (automatic meter reading, real-time access to security cameras, monitoring of public transportation systems etc.)
  - High-speed Internet access
- Developing countries, rural networks
- Isolated areas, rugged terrain
- Temporary venues (construction sites, outdoor concerts)
- Warehouses
- Military
- Vehicular networks

Challenges

- In municipal public WiFi networks:
  - How to prioritize and balance loads?
  - How to monitor ongoing availability?
  - Security
    - Need to balance the need for open access (guest) and preventing users from downloading illegal content
    - Security at network layer

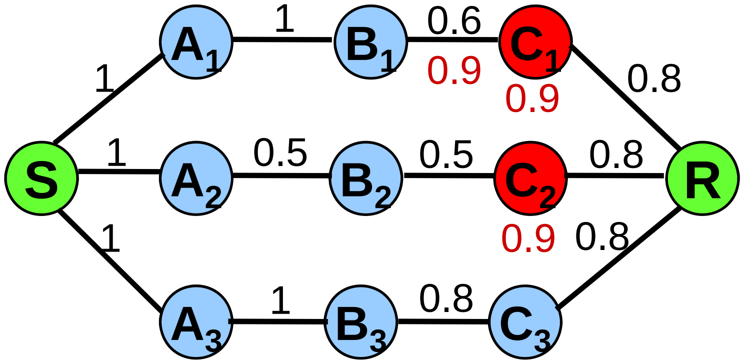
High-throughput Metrics for Routing

- Traditionally, routing protocols use hop-count metric
  - Not optimal for applications that seek to maximize throughput
- Select paths based on *link-quality* metrics (*high-throughput* metrics)



Security Challenges

- Implicit assumption: all nodes behave correctly during metric computation and propagation
- In adversarial networks, this assumption leads to unexpected consequences: *metric manipulation attacks*

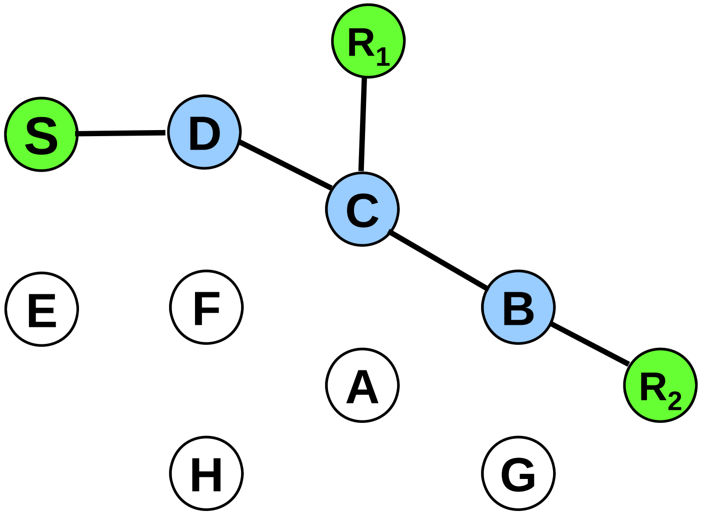


More Undesirable Effects

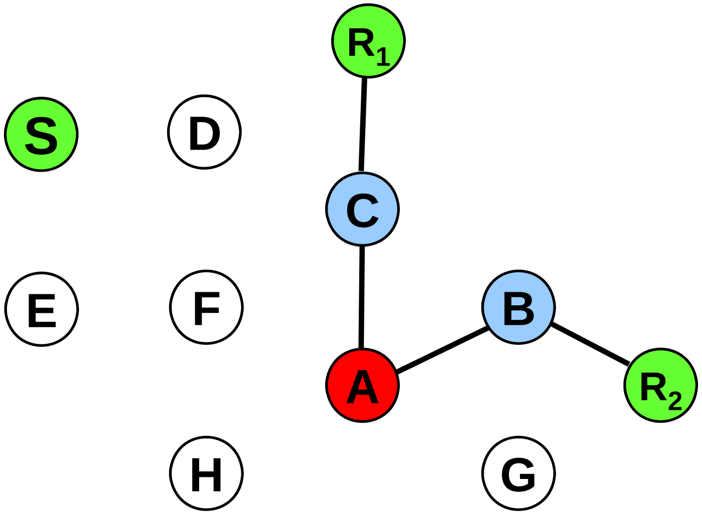
- Epidemic nature of the metric manipulation attack:

  metric poisoning effect

Benign case



Attack case



Aggressive path selection is a double-edged sword

Our Solution

- Measurement-based attack detection
- Accusation-based attack reaction

- With careful protocol design, it is possible to achieve both high-throughput and attack resiliency, while maintaining a low protocol overhead

- More details in:

  [IEEE SECON 2008]

  "On the Pittfalls of Using High-Throughput Multicast Metrics in Adversarial Wireless Mesh Networks"

  Dong, Curtmola, Nita-Rotaru