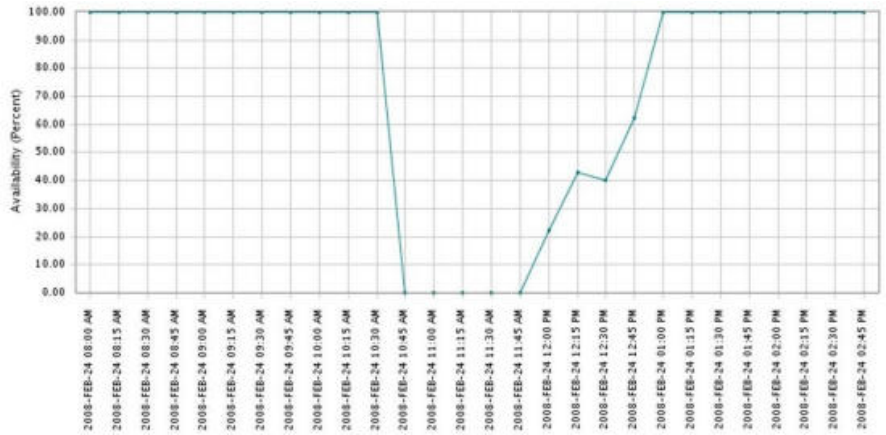
Distributed Coordinated Route Validation

Christan[2] and Aaron

Motivation

- YouTube outage due to BGP blackhole (2008)



- Other decentralized systems may suffer from similar faults – e.g. P2P, mobile ad hoc networks, data center traffic engineering

Approach

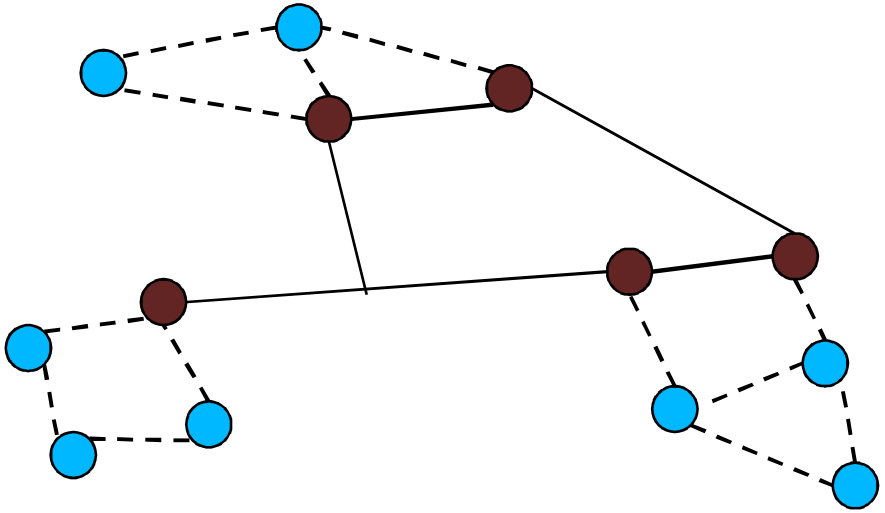
- Distributed coordinated route validation
- Each node (switch, mobile node, etc.) is responsible for monitoring part of the traffic
- Distribute observations to nodes that require the information to identify security or traffic engineering concerns
- Work has been done in this area [PODC 2007], [SIGCOMM 2010] , [ANCS 2004]

Research Challenges

- What information should be collected?
- To whom and how should the measurement data be distributed?
- How do you determine when certain behavior (e.g. malicious routes) is present?
- Balance between security and overhead (bandwidth, processing, etc)
- Can our methods be adapted to different architectures and attacks?

Mesh Network Scenario

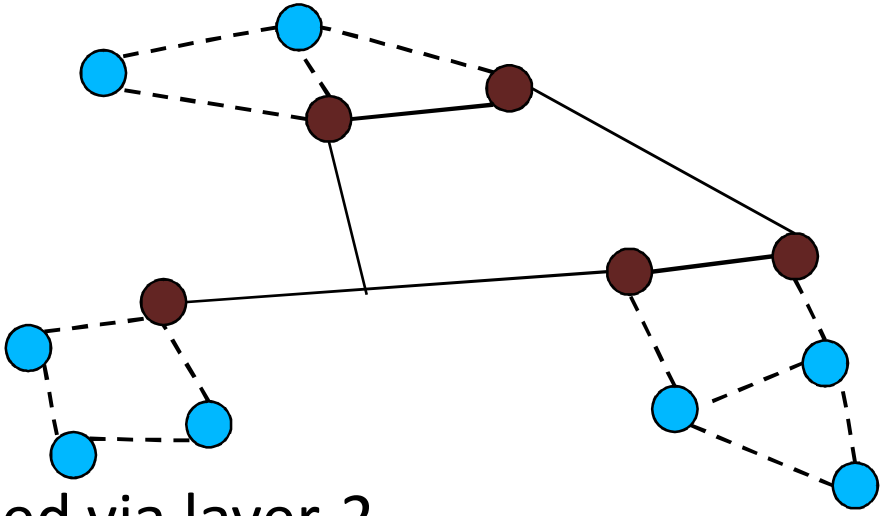
- Freifunk Network
  - Mesh nodes connected to gateway mesh node
  - Gateway mesh node connected to Internet



- Freifunk network has seen poor behavior, but it is unclear if it is a security or routing problem

Experiment Setup

- Use GENI/GLab resources to mirror real mesh
  - Wireless test beds (WinLab, Wisconsin WiMax, etc) serve as mesh networks



  - Connected via layer-2
  - Generate traffic based on past user-behavior work

Experiment

- Experiment:
  - Launch attacks based on the threat model being addressed and observe behavior or network
  - use throughput and availability between pairs of end-users as experiment metric
- Expected Results:
  - Expect significant reduction of availability
  - Conflicting routes
  - Unexpected traffic volumes
  - Look for hints that might allow us to detect the threat behavior

Architecture Independence

- Try to find metrics that are independent of the protocol and the layer (if they exist) at which routing occurs
  - “Destination” and “Route”, for example, is architecture independent: use whatever addressing exists
- Compare network behavior in other scenarios using similar attacks and the same hints

Thank you


NSF

DFG

Bundesministerium
für Bildung
und Forschung

GLab
www.german-lab.de

geni
Exploring Networks
of the Future

Related Work

[PODC 2007] Truth in advertising: lightweight verification of route integrity

[SIGCOMM 2010] How Secure are Secure Interdomain Routing Protocols?

[ACNS 2004] S-RIP: A Secure Distance Vector Routing Protocol

Challenges in Mesh Network

- Lots of confounding factors
  - Wireless limitations: bandwidth, link quality
  - Node limitations: processing, energy

Experiments & Infrastructure

- Launch an attack on mesh network using different threat models (selfish nodes, rational, irrational attackers)
- Measure impact on traffic
- Measure security metrics
- Deploy existing solutions to observe their efficiency in measuring the attack
- Use GENI/G-LAB Infrastructure (e.g. WinLab)

Threat Model

- Both types of nodes may be malicious
- Intention of malicious nodes
  - Selfish nodes: do not forward any packets, so you can use the bandwidth
  - Irrational attacks: stop others from using the network by discarding their traffic
  - Rational attacks: malicious nodes have specific goal, e.g. man-in-the-middle

Next Steps

- Build intrusion detection system that monitors the hints we identify
- Compare network behavior in other scenarios using similar attacks and the same hints
  - P2P
  - LAN – e.g. data center
  - WAN – e.g. BGP
  - Mobile ad hoc