Wireless Network Security

Spring 2016

Patrick Tague

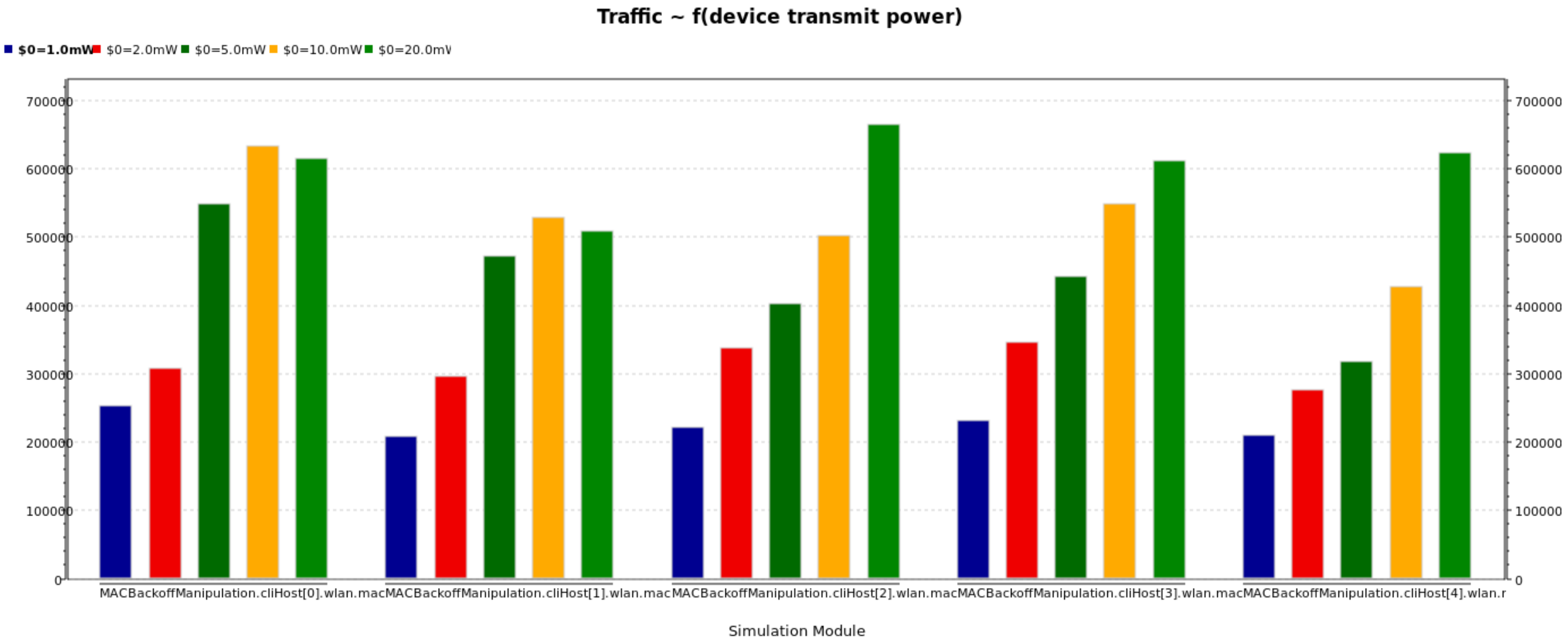
Class #10 – OMNET++ Tutorial II;
Network Layer Threats;
Identity Mgmt.

©2016 Patrick Tague

Class #10

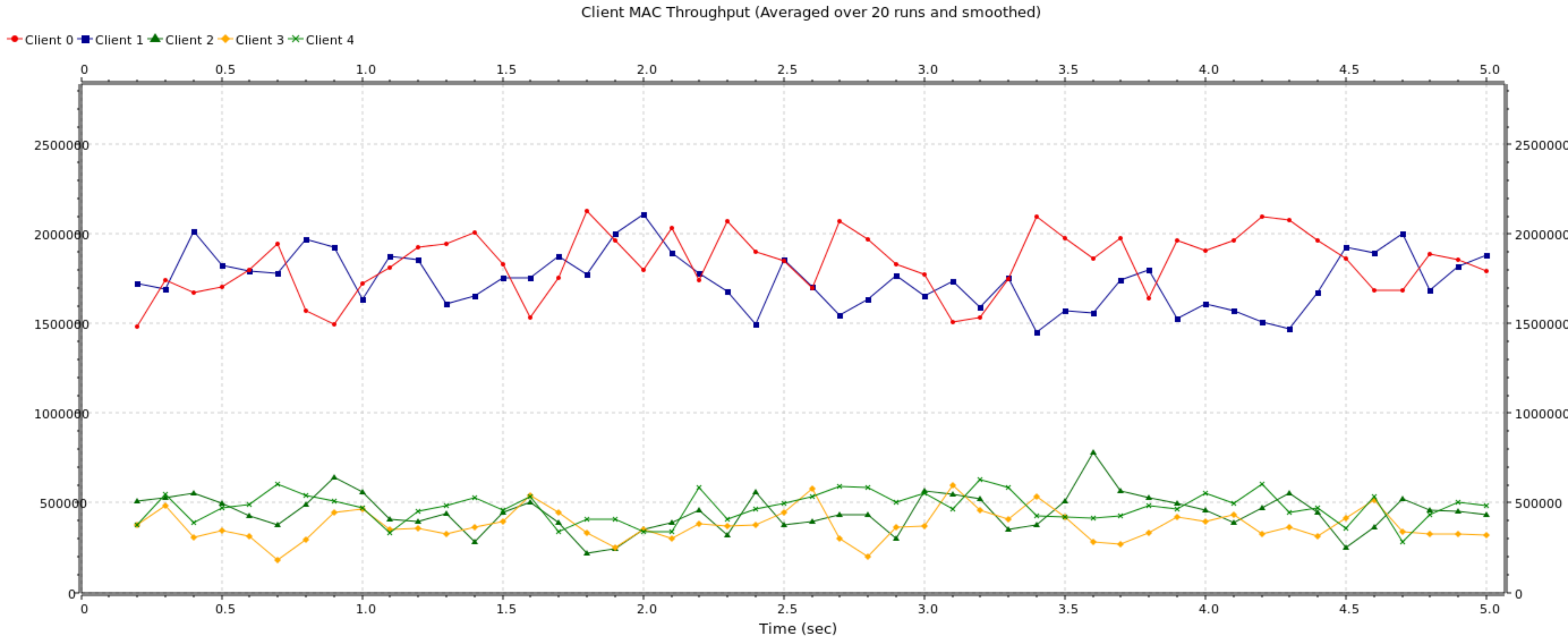
- OMNET++ Tutorial II
  - Variable simulation parameters
  - Multiple runs
  - Analysis using datasets
- Summary of wireless network layer threats
- Specific threats related to identity (depending on how long we spend on OMNET)

Variable Parameters



- **.radio.transmitterPower = ${1.0mW, 2.0mW, 5.0mW, 10.0mW, 20.0mW}

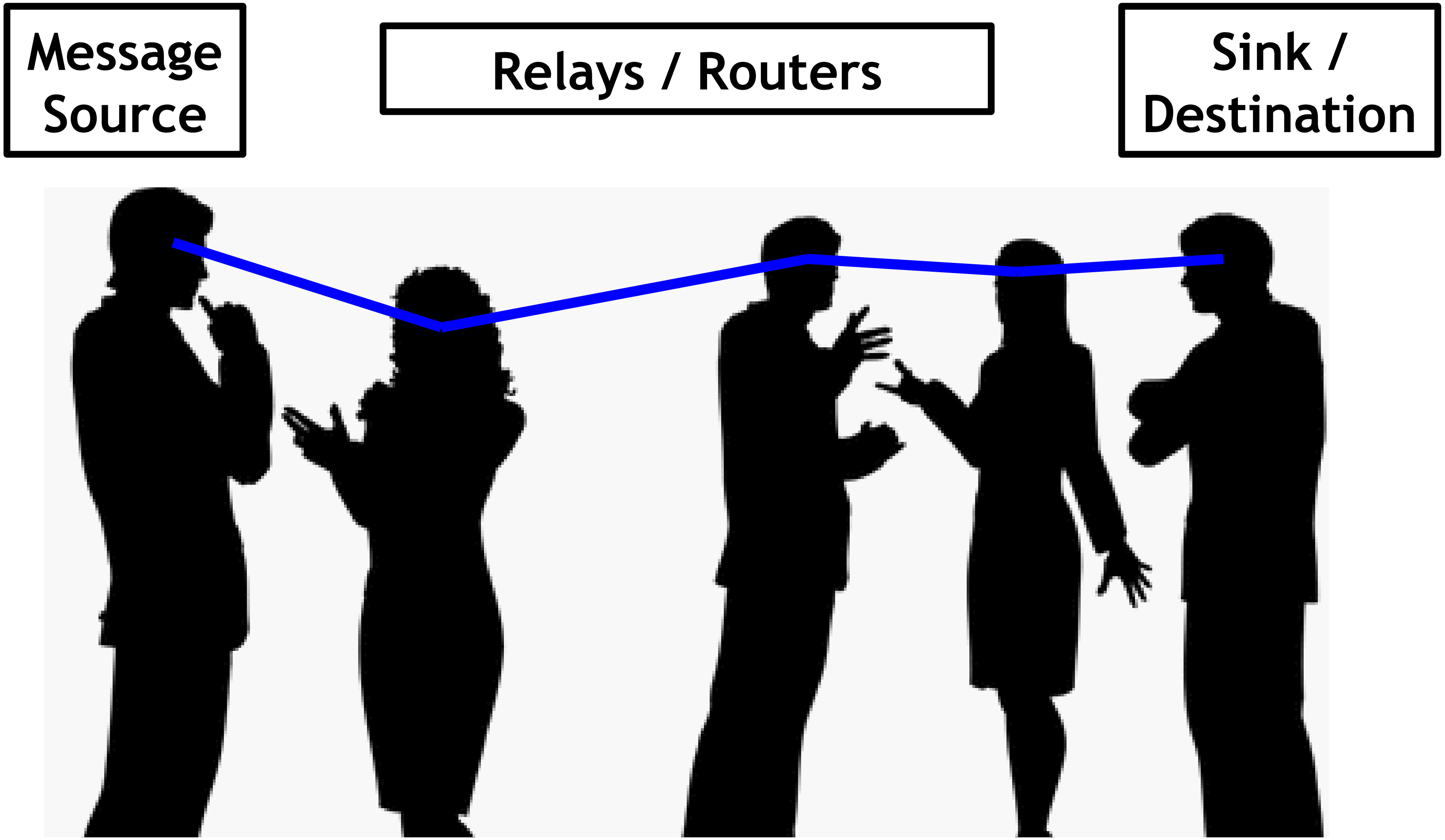
Averaging over Runs



- repeat = 20

©2016 Patrick Tague

Wireless Networking



Message Source

Relays / Routers

Sink / Destination

Network Layer Functionality

- The network layer is primarily responsible for establishing end-to-end paths and delivering packets over them

- Includes several fundamental services:
  - Addressing: network ID management
  - Routing: finding/establishing paths
  - Forwarding: delivering packets

  - Interactions with Transport layer and Link/MAC layer

©2016 Patrick Tague

Addressing

- Before routing can be performed, nodes need some sort of ID or address
  - Address/ID types range from local to global, just like in the postal system (streets up to ZIP codes)
  - In very large-scale systems (e.g. Internet), addresses must have some sort of structure
    - IP addresses follow a specific hierarchy and are reused within each domain
  - Within a domain and in small-scale systems (e.g. MANET/WSN), addresses are typically unstructured or random
    - Address management needed within a domain to prevent duplication and other failure scenarios

Addressing Threats

- Addresses can be changed arbitrarily
  - Allows for address spoofing
    - Masquerading as other node(s)
    - Potential for a large number of attacks
  - Changing identity to prevent detection/punishment
- Attackers can infiltrate address management protocols (ARP, DHCP) to cause problems
  - Inducing address duplication
  - Forcing frequent address changes
  - Manipulating forwarding schemes

Routing

- Routing = path management
  - Routing does not involve actual sending of packets from source to destination(s), only sets up the path
  - Lives in the "control plane"
  - Involves path setup/discovery, maintenance, and tear-down
- Challenges in MANET/WSN environments
  - Route using multiple untrusted relay nodes
  - Resource and capability limitations
  - No centralized authority or monitor
  - Secure routing often relies on existing key mgmt.

©2016 Patrick Tague

Routing Threats

- Just as with other types of misbehavior, routers can be greedy, non-cooperative, or malicious
  - Greedy routers can refuse route discovery requests in order to save their own resources
  - Non-cooperative routers can choose to selectively accept route requests to specific sources/dests
  - Malicious routers can persuade route discovery protocols so paths pass through them, avoid them, or take unnecessary detours

Path Attraction

- Black-hole attack:
  - A malicious router broadcasts false claims of being "close" to the destination in order to attract all traffic and drop it
- Gray-hole attack:
  - Similar to black-hole attack, except it only drops some packets selectively
    - Ex: forward all routing control packets but drop all data
- Worm-hole attack:
  - Colluding routers create a low-latency long-distance out-of-band channel to attract routing paths and control data flow

Path Manipulation

- Detours:
  - A malicious router can modify/inject control packets to force selection of sub-optimal routes

- “Gratuitous detours”:
  - Greedy routers can avoid being on a selected route by advertising long delays or creating “virtual nodes”
    - Could be considered a form of Sybil attack, where all “personalities” are on the routing path

Route Subversion

- Targeted blacklisting:
  - In any routing protocols using blacklisting, attackers can accuse/slander/blame others to force them onto the blacklist → DoS

- Rushing attacks:
  - Attackers can quickly disseminate forged requests, causing later valid requests to be dropped

Forwarding

- Forwarding = point-to-point data management
  - Forwarding involves actual sending of packets from source to destination(s) on given routing paths
  - Lives in the “data plane”
  - Correct forwarding involves
    - Sending the correct packets
    - Maintaining packet order
    - Respecting headers and rules
    - Relaying in a timely manner
    - Respecting rate control mechanisms

Forwarding Threats

- Misbehavior in the forwarding mechanism (often called Byzantine forwarding) includes various ways of going against forwarding rules
  - Dropping packets
  - Modifying packet contents or header information
  - Injecting bogus packets on source's behalf
  - Forwarding to the wrong next hop
  - Disrespecting rate control (flooding or throttling)

Network Privacy Threats

- Routing protocols inherently reveal information to curious/malicious eavesdroppers
  - An attacker can listen to route discovery interactions and learn (1) locations of source and destination nodes, (2) type of interactions between nodes, (3) commonly used paths, (4) network events, or (5) data
  - These are all issues of location privacy, network privacy, and data privacy due solely to the routing process

Let's go through these different threats in some detail, starting with addressing

©2016 Patrick Tague

Feb 18:

Identity Mgmt.; Routing Security

©2016 Patrick Tague