

Introduction to Computer Networks

COSC 4377

Lecture 22

Spring 2012

April 11, 2012

Announcements

- HW10 due this week
- HW11 is out
- Student presentations

HW10

- Latency measurements
- Plotting latency

- Get your user id soon

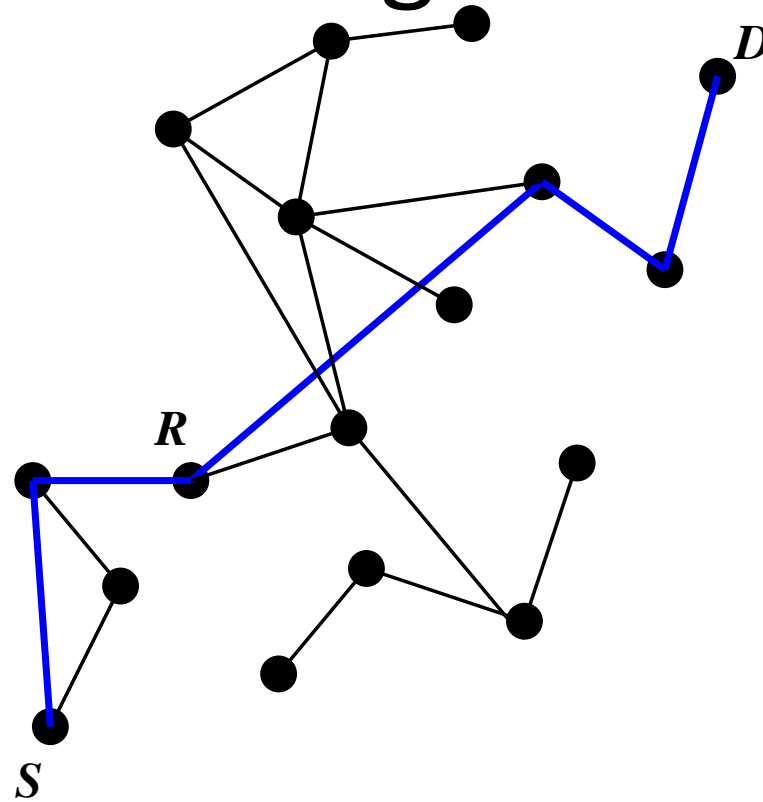
Today's Topics

- Multi-hop Wireless Networks
- Security
- RPL

Many Challenges

- Routing
 - Link estimation
- Multihop throughput dropoff

The Routing Problem



- Find a route from *S* to *D*
- Topology can be very dynamic

Routing

- Routing in ad-hoc networks has had a lot of research
 - General problem: any-to-any routing
 - Simplified versions: any-to-one (base station), one-to-any (dissemination)
- DV too brittle: inconsistencies can cause loops
- DSDV
 - Destination Sequenced Distance Vector

DSDV

- Charles Perkins (1994)
- Avoid loops by using sequence numbers
 - Each destination increments own sequence number
 - Only use EVEN numbers
 - A node selects a new parent if
 - Newer sequence number or
 - Same sequence number and *better* route
 - If disconnected, a node increments destination sequence number to next ODD number!
 - No loops (only transient loops)
 - Slow: on some changes, need to wait for root

Many Others

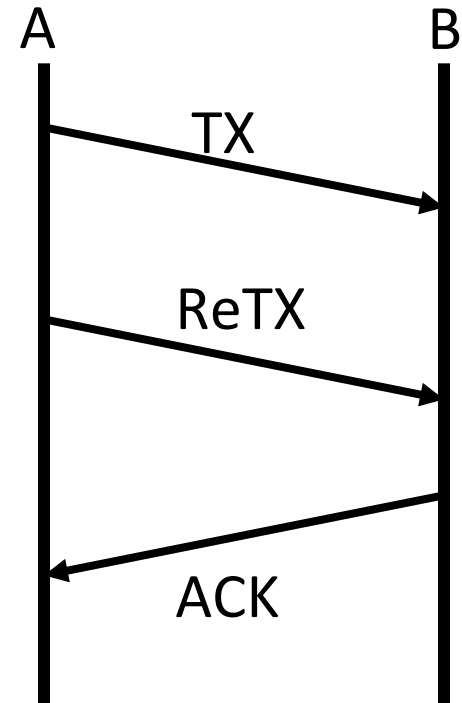
- DSR, AODV: on-demand
- Geographic routing: use nodes' physical location and do greedy routing
- Virtual coordinates: derive coordinates from topology, use greedy routing
- Tree-based routing with on-demand shortcuts
- ...

Routing Metrics

- How to choose between routes?
- Hopcount is a poor metric!
 - Paths with few hops may use long, marginal links
 - Must find a balance
- All links do *local retransmissions*

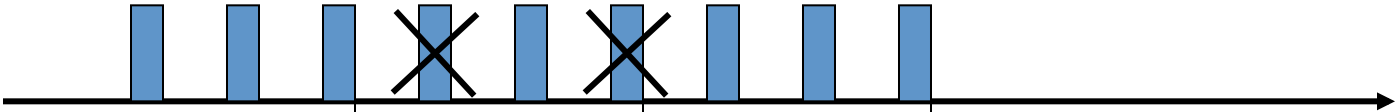
Link Quality Estimation

$$ETX(L) = \frac{1}{PRR(f) * PRR(b)}$$



ETX Estimation Example

Beacons



1.0 3.0 1.0

ETX Estimate
(alpha = 0.8)



Routing Metrics

- Idea: use expected transmissions over a link as its cost!
 - $ETX = 1/(PRR)$ (Packet Reception Rate)
 - Variation: ETT, takes data rate into account

Multihop Throughput



- Only every third node can transmit!
 - Assuming a node can talk to its immediate neighbors
 - (1) Nodes can't send and receive at the same time
 - (2) Third hop transmission prevents second hop from receiving
 - (3) Worse if you are doing link-local ACKs
- In TCP, problem is worse: data and ACK

Sometimes you can't (or shouldn't)
hide that you are on wireless!

TCP over wireless

- How to handle
 - Link losses
 - Hop-by-hop retransmissions
 - Congestion vs lossy links

Security

From: Internal Revenue Service [mailto:admin@irs.gov]

Sent: Wednesday, March 01, 2006 12:45 PM

To: john.doe@jdoe.com

Subject: IRS Notification - Please Read This .



Internal Revenue Service

United States Department of the Treasury

After the last annual calculations of your fiscal activity we have determined that you are eligible to receive a tax refund of **\$63.80**. Please submit the tax refund request and allow us 6-9 days in order to process it.

A refund can be delayed for a variety of reasons. For example submitting invalid records or applying after the deadline.

To access the form for your tax refund, please [click here](#)




Regards,
Internal Revenue Service

Microsoft Security Warning



Antivirus 360 Web Scanner detected dangerous spyware on your system!

Detected malicious programs can damage your computer and compromise your privacy. It is **strongly recommended** to remove them immediately.

Name	Type	Risk level
 Spyware.IEMonster.b	Spyware	CRITICAL
 Zlob.PornAdvertiser.Xplisit	Spyware	High
 Trojan.InfoStealer.Banker.s	Trojan	Medium

Remove All

Ignore

Basic Requirements for Secure Communication

- **Availability:** Will the network deliver data?
 - Infrastructure compromise, DDoS
- **Authentication:** Who is this actor?
 - Spoofing, phishing
- **Integrity:** Do messages arrive in original form?
- **Confidentiality:** Can adversary read the data?
 - Sniffing, man-in-the-middle
- **Provenance:** Who is responsible for this data?
 - Forging responses, denying responsibility
 - Not who sent the data, but who created it

Other Desirable Security Properties

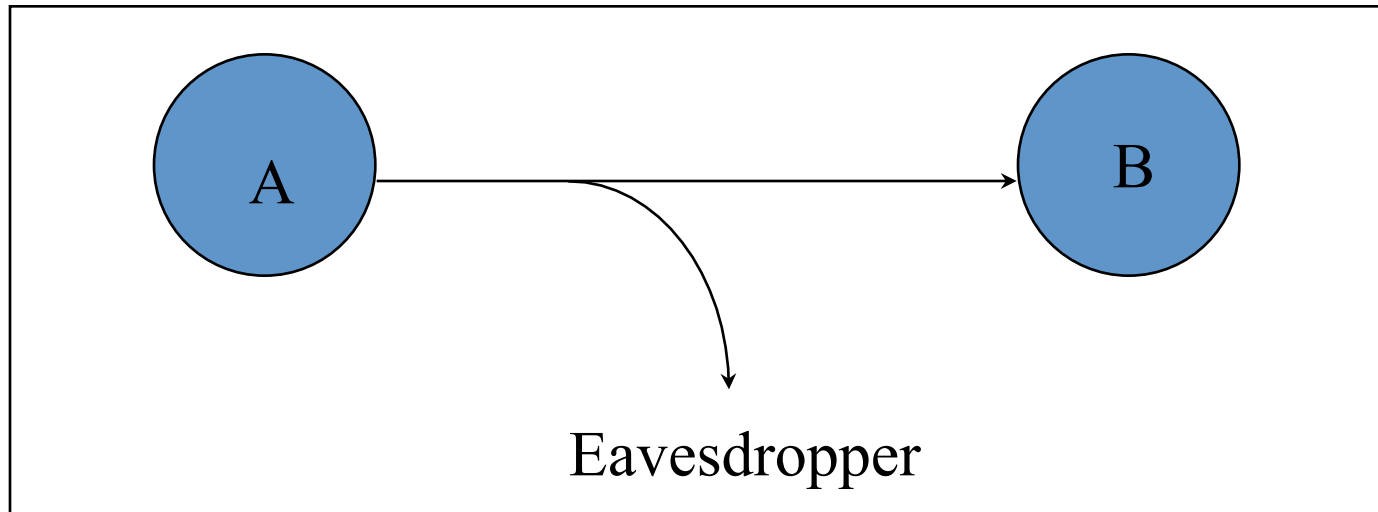
- **Authorization:** is actor allowed to do this action?
 - Access controls
- **Accountability/Attribution:** who did this activity?
- **Audit/Forensics:** what occurred in the past?
 - A broader notion of accountability/attribution
- **Appropriate use:** is action consistent with policy?
 - E.g., no spam; no games during business hours; etc.
- **Freedom from traffic analysis:** can someone tell when I am sending and to whom?
- **Anonymity:** can someone tell I sent this packet?

Internet's Design: Insecure

- Designed for simplicity in a naïve era
- “On by default” design
- Readily available zombie machines
- Attacks look like normal traffic
- Internet's federated operation obstructs cooperation for diagnosis/mitigation

Eavesdropping - Message Interception (Attack on Confidentiality)

- Unauthorized access to information
- Packet sniffers and wiretappers
- Illicit copying of files and programs

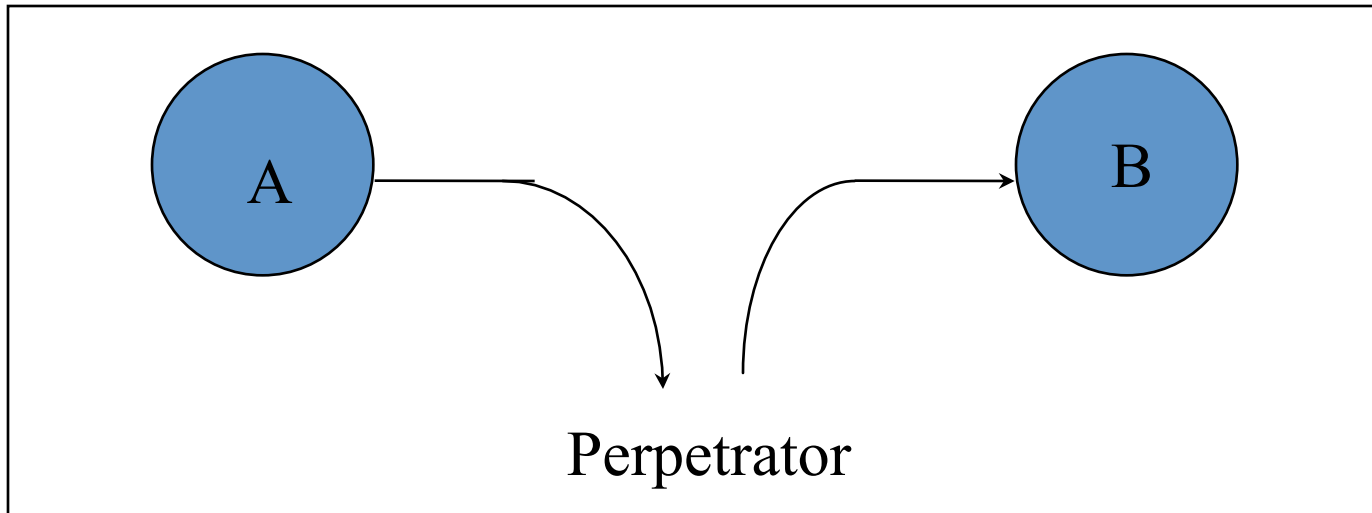


Eavesdropping Attack: Example

- tcpdump with promiscuous network interface
 - On a switched network, what can you see?
- What might the following traffic types reveal about communications?
 - DNS lookups (and replies)
 - IP packets without payloads (headers only)
 - Payloads
- How about HW9?

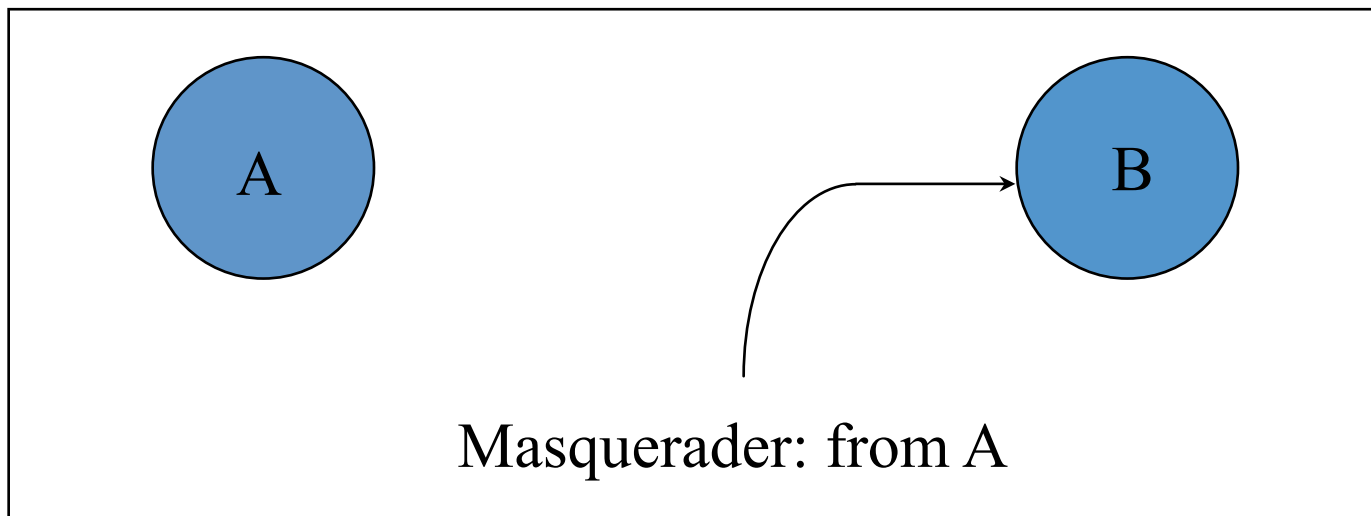
Integrity Attack - Tampering

- Stop the flow of the message
- Delay and optionally modify the message
- Release the message again



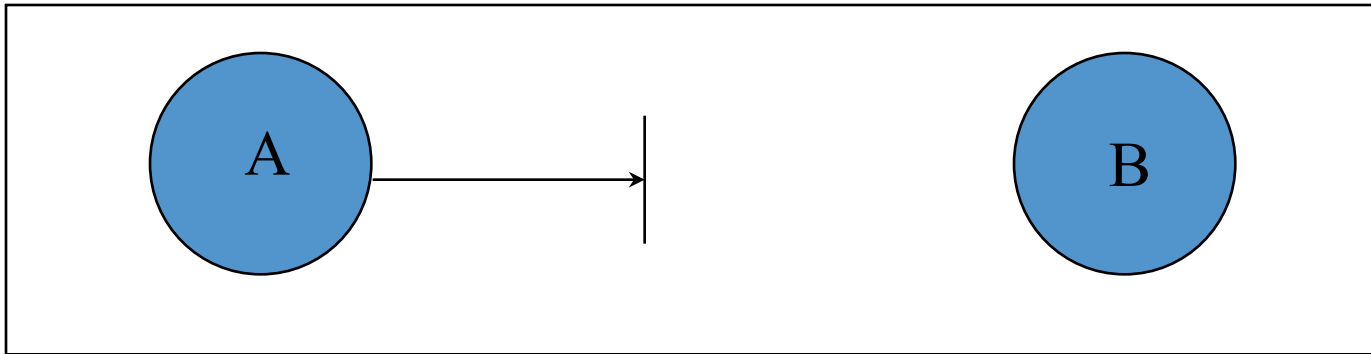
Authenticity Attack - Fabrication

- Unauthorized assumption of other's identity
- Generate and distribute objects under this identity



Attack on Availability

- Destroy hardware (cutting fiber) or software
- Modify software in a subtle way
- Corrupt packets in transit



- Blatant *denial of service* (DoS):
 - Crashing the server
 - Overwhelm the server (use up its resource)