Wireless Network Security
Spring 2015

Patrick Tague
Class #5 - Jamming, “Physical Layer Security”
Class #5

- Jamming attacks and defenses
- Secrecy using physical layer properties
- Authentication using physical layer properties
Let's focus on Jamming
Jamming

- Conceptually, jamming is a physical layer denial-of-service attack that aims to prevent wireless communication between parties.
How Does Jamming Work?

Interference + Noise

Receiver can decode message if $SINR \geq \tau$

Jamming decreases $SINR$, causes decoding failure and packet loss

But, it's much more complicated than that...
Geometry Matters

Attacker can be MUCH quieter than speaker

SINR metric captures effects of geometry

\[
\text{SINR} = \frac{\text{(Rx signal power)}}{\text{(noise power + Rx jamming power)}}
\]

Often modeled as \( P_{tr} = k_t P_t d_{tr}^{-\alpha} \)

Typically random variable \( N_0 \)

Often modeled as \( P_{jr} = k_j P_j d_{jr}^{-\alpha} \)
Timing Matters

Can be modeled as a (random) multiplier in the “I” term of the SINR metric
Orthogonality Matters

Channel $k$ \

Channel $m \neq k$ \

DSSS encoded \

narrowband \

fail?
Generalized Jamming

• A jammer allocates energy/signal to diverse time, freq, etc. resources according to an attack strategy $S$
  – Effect $E(S)$ of the attack
  – Cost $C(S)$ of the attack
  – Risk $R(S)$ of being detected / punished

  – With other metrics, an optimization emerges
Jamming Strategies
Time Domain

Link Traffic

- Pkt
- Pkt
- Pkt
- Pkt
- P

- Constant
- Random
- Periodic
- Reactive

[Xu et al., 2006; Mpitziopoulos et al., 2009]
Jamming Strategies
Frequency Domain

Link Traffic

Ch. 1 Ch. 2 Ch. 3 ... Ch. k

Broadband

Single Ch.

Single Sub-Ch.

Multiple Sub-Ch.
How can we protect against jamming?
Jamming Detection & Defense

[Xu et al., IEEE Network 2006]

- **Goal:** detect and localize jamming attacks, then evade them or otherwise respond to them

- **Challenge:** distinguish between adversarial and natural behaviors (poor connectivity, battery depletion, congestion, node failure, etc.)
  - Certain level of detection error is going to occur
  - Appropriate for deployment in sensor networks

- **Approach:** coarse detection based on packet observation
Basic Detection Statistics

• Received signal strength (RSSI)
  – Jamming signal will affect RSSI measurements
  – Very difficult to distinguish between jamming/natural

• Carrier sensing time
  – Helps to detect jamming as MAC misbehavior
  – Doesn't help for random or reactive cases

• Packet delivery ratio (PDR)
  – Jamming significantly reduces PDR (to ~0)
  – Robust to congestion, but other dynamics (node failure, outside comm range) also cause PDR → 0
Advanced Detection

- Combining multiple statistics in detection can help
  - High PDR + High RSSI → OK
  - Low PDR + Low RSSI → Poor connectivity
  - Low PDR + High RSSI → ? → Jamming attack?

Caveat: this assumes RSSI can be accurately measured

See [DeBruhl & Tague, SECON 2013]
Jammed Area Mapping

- Based on advanced detection technique, nodes can figure out when they are jammed.
- At the boundary of the jammed area, nodes can get messages out to free nodes.
- Free nodes can collaborate to perform boundary detection using location information.
Evading Jamming

- Nodes in the jammed region can evade the attack, either spectrally or spatially
  - Spectral evasion → “channel surfing” to find open spectrum and talk with free nodes
  - Spatial evasion → mobile retreat out of jammed area
- Need to compensate for mobile jammers ability to partition the network (see figure in paper)
What about dynamic attack and defense strategies?
Optimal Jamming & Detection
[Li et al., Infocom 2007]

- **Problem setup:** each of the network and the jammer have control over random jamming and transmission probabilities
  - Network parameter $\gamma$ is probability each node will transmit in a time slot
  - Attack parameter $q$ is probability the jammer will transmit in a time slot

- Opponents can learn about goals through observation and optimize for min-max/max-min
Jamming Games
[DeBruhl & Tague, PMC 2014]

• What if both the attacker and defender are freely adapting in response to each other?
How can the properties of the wireless medium actually help to achieve secure communication?
Snooping on the Party
“Wiretapping”

- In 1975, A. D. Wyner defined the wiretap channel to formalize eavesdropping.

In Wyner's model, the wiretap channel is “degraded”, meaning Eve only sees a noisier signal than Bob sees.
Secrecy Capacity

- Since the Alice → Eve channel is noisier than the Alice → Bob channel:
  - Eve can't decode everything that Bob can decode
  - i.e., there exists an encoding such that Alice can encode messages that Bob can decode but Alice can't
  - There's a really nice Information Theory formalization of the concept of secrecy capacity, namely the amount of secret information Alice can send to Bob without Eve being able to decode
  - I'll leave the details for you to explore
Degraded Eavesdropper?

• In a practical scenario, is it reasonable to assume the eavesdropper's signal is more degraded than the receiver's?
  – Probably not.

• What else can we do to tip the scales in the favor of the Alice-Bob channel?
Diversity of Receivers

The signal emitted by a transmitter looks “different” to receivers in distinct locations.
Measurement + Feedback

• Channel State Information (CSI):
  – CSI is the term used to describe measurements of the channel condition
  – If Alice knows the CSI to Bob and to Eve, she can find an appropriate encoding using the measurements
    - If Alice and Bob interact repeatedly, the measurement and feedback actually increase the secrecy capacity
      • This can allow for secrecy capacity >0 even if Eve's channel is less noisy than Bob's channel
Jamming for Good

• If Alice has diversity in the form of multiple radios or some collaborators:
  – Alice & friends can use a jamming attack to prevent Eve from eavesdropping
  – As long as they don't jam Bob at the same time
  – Ex: if the deployment geometry is known, Alice can adjust power, antenna config, etc. so Bob's SINR is high but Eve's is low
Secure Array Transmission

[Li, Hwu, & Ratazzi, ICASSP 2006]

- Antenna control can be used for transmission with low probability of interception
Application

• Building on secrecy capacity:
  – If two devices can communicate with a high probability guarantee that eavesdroppers cannot hear them, whatever they say is secret
  – Secret messages → keys!
  – Secret key generation is now possible using inherent properties of the wireless medium
Further Reading

• For a really good summary of secrecy capacity, the formalization, secret key generation, and lots of excellent details:

  – “Physical Layer Security” by Bloch and Barros
    • Available as e-book through CMU library
    • I have a hard copy if anyone wants to borrow it
More Benefit for the Party?
Physical layer properties can help with authentication!
Diversity of Senders

Signals captured by a receiver from senders in distinct locations look “different”
• In a WLAN with multiple APs, each AP sees different characteristics of packets from each sender
  – Each AP can measure various packet features, some of which are relatively static over packets: e.g., received signal strength
  – A back-end server can collect measurements and keep history of packets from different senders
Verification & Matching

- Requirements for verification:
  - Robust to transmission power control, random fluctuations, and error
  - High correlation among signals from same sender
  - Distinct signalprints between different senders

A matching rule based on matches and mis-matches is used to declare packets from the same or different source (similar to any IDS)
Signalprint Properties

• Difficult to spoof
  – Spoofing node would require control of medium
  – Transmission power control creates lower RSS at every AP; differential analysis reveals power control

• Correlated with physical location
  – Attacker needs to be physically near target device

• Sequential packets have similar signalprints
  – RSSI values are highly correlated for stationary sender and receiver

• Note: not highly correlated with distance, but very highly correlated with subsequent transmissions
Limitations

• Signalprints with any reasonable matching rule cannot differentiate between nearby devices
  – Masquerading/spoofing attacks are possible if physical proximity is easily achieved

• Low-rate attacks cannot be detected
  – But, low-rate attacks have limited effects

• Multi-antenna attackers can cheat

• Highly mobile devices can't be printed
Summary

Interference and eavesdropping are two of the most fundamental yet least understood vulnerabilities in wireless. There's still a lot of work to be done.
Assignment #2

- Assignment #2 will be posted later today
  - Due date is February 12, 11:59pm PST

- We're asking you to do a lot of things with OMNET++ and INET that we didn't cover in the tutorial. Use the other examples and resources before asking us how to do something.
January 29:
Link Layer Threats; WiFi Security