Wireless Network Security
14-814 - Spring 2012

Patrick Tague
Class #8 - Interference and Jamming
Announcements

• Homework #1 is due today
  – Questions?

• Not everyone has signed up for a Survey
  – These are required, count for 10% of total grade
  – Class topics Feb 23 and all of March are open
    • Also, a few unspecified topics in April
  – If you haven't already, please sign up ASAP
Jamming

- **Theme:** overview of jamming attacks and defenses, focusing on (but not limited to) WSN

- **Papers:**
What is jamming, how does it work, and how can we protect wireless networks from it?
What is Jamming?

Jamming is the transmission of interfering signals to intentionally block or degrade communication over the wireless medium.

- **Sender**
- **Path Loss**
- **Receiver**

**Interference + Noise**

- Receiver can decode message if $SINR \geq \tau$
- Jamming decreases $SINR$, causes *decoding failure* and *packet loss*

But, there are numerous ways to do this.
Types of Jamming Signals

- Noise-based jamming (dates back to <1940s)
  - Attacker aims to simply raise the noise floor
  - Cause low SNR, resulting in high BER/SER/PER

- Signal-based jamming
  - Attacker injects valid-looking signal
  - Confuse receiver circuit or overpower/replace intended signal in the radio

- Packet-based jamming
  - Attacker injects well-formed packets (with or without real data)
Jamming Strategies
from [Xu et al., 2006; Mpitziopoulos et al., 2009]

- As with typical communication systems, choice of jamming strategy depends on a number of factors
  - Effectiveness of the jamming signal at achieving the attack goal
  - Cost of mounting the attack / signal generation
  - Risk of being detected and punished / destroyed
  - ... ?
Constant Jamming

Jammer sends a constant signal using a specific, fixed set of signal parameters.
Deceptive Jamming

Jammer sends a valid-looking signal using the same encoding, modulation, etc. as sender

Sender

Jammer

Pkt Pkt Pkt Pkt Pkt Pkt

Jamming signal that looks valid (pkts)

Receiver

Time

©2012 Patrick Tague
Random/Periodic Jamming

Jammer turns its signal “on” and “off” at random or fixed durations (can be constant, deceptive, etc. when on)
Reactive Jamming

Jammer turns its signal “on” only when it detects the sender's transmission
Common Misperceptions

• Jamming signals, like other wireless signals, reach/effect all receivers within a distance \( R \)
  – Neither are circular, but they're sometimes modeled that way

• All receptions within jammer's range are blocked whenever the jammer is “on”
  – Like typical communications, jamming success is probabilistic

• Jamming strategies are static
  – Nothing prevents a jammer from changing strategy in time or in response to network events
Questions

• Other than what we discussed, what can jammers do to reduce detection risk (i.e., to increase stealth?)

• What are the trade-offs?
How can a sensor network detect a jamming attack?
Jamming Detection & Defense
[Xu et al., 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

- **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
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)
Defeating Jammers

- Nodes can compete with jammers
  - Power control, adaptive modulation/coding, signal shaping, filtering, etc.
  - In general, this is a hard problem
    - Jammers can fight back: sender increases power → jammer increases power…who wins?
    - Many side-effects (e.g., increased power → increased range → increased congestion)
Questions

• What are the trade-offs between evading jamming versus trying to defeat jamming?
How is jamming different in a time-slotted communication system?
Optimal Jamming & Detection

[Li et al., 2007]

- Problem setup: each of the network and the jammer have control over their multiple access parameter (Note: we're at the MAC layer here)
  - 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
- Goal: choose $\gamma^*$ (resp. $q^*$) to minimize (resp. maximize) detection delay + response time
  - What does each “player” know about its “opponent”? 
Jamming Detection

• First, need to characterize the network's ability to detect the jammer
  – Sequential Probability Ratio Test (SPRT) yields minimum delay detection for given error bounds
    • $S_k$ is log-likelihood of jamming attack present ($H_1$) over absent ($H_0$) given a sequence of $k$ data points
    • False alarm rate $P_{FA}$ and miss rate $P_M$ yield coefficients $a, b$
      \[
      S_k \geq a \implies \text{accept } H_1,
      
      S_k < b \implies \text{accept } H_0,
      
      b \leq S_k < a \implies \text{take another observation}
      \]
  – The corresponding delay is denoted $D(q, \gamma)$
Response to Detection

• Next, need to know how long it will take for the jamming detection message to propagate out of the jammed area to a free node

  – Analysis depends on:
    • Spatial deployment pattern or statistics (neighborhood \( n \))
    • Relationship between communication and jamming range (parameter \( H \))
    • Impact of jamming on message propagation (success probability \( p_a \), dependent on \( q \) and \( \gamma \))

  – Response time

\[
W(q, \gamma) = \frac{H}{p_a} = \frac{H}{(1 - q)\gamma(1 - \gamma)^n - 1}
\]
Informed Optimization

- Attacker (with knowledge of $\gamma$):
  \[
  \max_{0 < q \leq 1} \quad D(q, \gamma) + W(q, \gamma)
  \]
  \[
  \text{s.t.} \quad qP_m \left[ D(q, \gamma) + W(q, \gamma) \right] \leq E_m
  \]
  \[
  U_{mc}(q, \gamma) \geq U^0_m
  \]

- Network (with knowledge of $q$):
  \[
  \min_{0 \leq \gamma \leq 1} \quad D(q, \gamma) + W(q, \gamma)
  \]
  \[
  \text{s.t.} \quad \gamma P \left[ D(q, \gamma) + W(q, \gamma) \right] \leq E
  \]
  \[
  U_C(q, \gamma) \geq U^0
  \]
Blind Optimization

- Attacker (no knowledge of $\gamma$):

$$\max_{0 < q \leq 1} \min_{0 \leq \gamma \leq 1} D(q, \gamma) + W(q, \gamma)$$

$$q P_m [D(q, \gamma) + W(q, \gamma)] \leq E_m$$

$$U_{mc}(q, \gamma) \geq U_m^0$$

- Network (no knowledge of $q$):

$$\min_{0 \leq \gamma \leq 1} \max_{0 < q \leq 1} D(q, \gamma) + W(q, \gamma)$$

$$\gamma P [D(q, \gamma) + W(q, \gamma)] \leq E$$

$$U_C(q, \gamma) \geq U^0.$$
Example Evaluation

- Example scenario (parameters in the paper)

<table>
<thead>
<tr>
<th>Case</th>
<th>Attacker's delay (slots)</th>
<th>Network's delay (slots)</th>
<th>Actual delay (slots)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Both blind</td>
<td>1137</td>
<td>3089</td>
<td>1206</td>
</tr>
<tr>
<td>Informed attack</td>
<td>1506</td>
<td>3089</td>
<td>1506</td>
</tr>
<tr>
<td>Informed defense</td>
<td>1137</td>
<td>414</td>
<td>414</td>
</tr>
</tbody>
</table>
Summary

- Discussed three papers that discuss different types of jamming attacks and defense strategies
  - Statistical detection, mapping, and evasion
  - Jamming strategies and countermeasures
  - Optimal attack and defense
Next Time

- Feb 16: Spread spectrum, UFH, UDSSS, etc.
  - Classical PHY protections against jamming attacks
    - We'll cover more material from [Mpitiopoulous et al., 2009]
  - Strengths and weaknesses of SS
  - Uncoordinated spread spectrum