Channel Surfing and Spatial Retreats: Defenses against Wireless Denial of Service

Wenyuan Xu, Timothy Wood, Wade Trappe, Yanyong Zhang
WINLAB, Rutgers University

IAB 2004
Roadmap

- Motivation and Introduction
- Detection
  - MAC Layer Detection
  - PHY Layer Detection
- DoS Defenses
  - Channel Surfing
  - Spatial Retreat
- Conclusions
- Ongoing works
Jamming Style DoS

Bob

Hello ...

Hi ...

Alice
Jamming Style DoS

Bob
@#$%%$#@& ...

Alice

Mr. X
Jamming Style DoS

- Alice and Bob are DoS attacked by malicious Mr. X.

- A story for the problem of wireless denial of service attack we focus on.
  - Alice and Bob → two communicating nodes, A and B.
  - Mr. X → an adversarial interferer X.
  - Mr. X’s insane behavior → the jamming style DoS.
  - People and nodes in wireless network both communicate via shared medium.

- **Jamming style DoS Attack:**
  - Behavior that prevents other nodes from using the channel to communicate by occupying the channel that they are communicating on.
DoS: An attack on a system or portion of a system that results in at least the temporary inability of others to use the system for its intended purpose

wennyuan, 9/22/2004
Jamming Style DoS

Jamming style DoS: 2 styles
- MAC-layer DoS
  - Bypass the MAC protocol, repeatedly send out packets
  - Introduces packet collision
- PHY-layer DoS
  - Jam transmission channel by emitting energy in the frequency band corresponding to the channel

Australian CERT [0]:

Previously, attacks against the availability of IEEE 802.11 networks required specialized hardware and relied on the ability to saturate the wireless frequency with high-power radiation, an avenue not open to a discreet attack. This vulnerability makes a successful, low cost attack against a wireless network feasible for a semi-skilled attacker.

A common example: turning on the Microwave is a piece of cake.

Our Jammers

- **MAC-layer Jammer**
  - Mica2 Motes (UC Berkeley)
    - 8-bit CPU at 4MHz,
    - 512KB flash, 4KB RAM
    - 916.7MHz radio
    - OS: TinyOS
  - Disable the CSMA
  - Keep sending out the preamble

- **PHY-layer Jammer**
  - Waveform Generator
  - Tune frequency to 916.7MHz
Handling Jamming: Strategies

- **What can you do when your channel is occupied?**
  - In wired network you can cut the link that causes the problem, but in wireless...
  - Make the building as resistant as possible to incoming radio signals?
  - Find the jamming source and shoot it down?
  - Battery drain defenses/attacks are not realistic!

- **Protecting networks is a constant battle between the security expert and the clever adversary.**

- Therefore, we take motivation from “The Art of War” by Sun Tze:
  - He who cannot defeat his enemy should retreat.

- Detection Strategies
  - MAC Detection
  - PHY Detection

- Retreat Strategies:
  - Spectral evasion
  - Spatial evasion
Detection: MAC Layer and PHY Layer
Idea:
- Want to use channel state information to detect whether a jamming has occurred.

**Adversary Model:** There is one *stationary* adversary, who *continuously* blasts on a *single* channel at a time.
- We assume there is only one stationary adversary, who blasts on a single channel at any time.

Observation:
- Normal scenario: nodes can pass the CSMA after some time
- DoS scenario: nodes might never pass the CSMA

Challenges:
- How to discriminate a legitimate traffic jam from illegitimate traffic?
- What is a good model to minimize the probability of a false positive?

Thresholding is the “bread and butter” of detection theory (Neyman-Pearson, Bayesian inference).
- Sensing time?
Empirically setting the threshold

- Problem with theoretically setting threshold: It's hard to model more complicated MACs!
- Let each network device collect statistics regarding waiting time $D$
- Experiment
  - ns-2 simulator
  - 802.11 protocol
  - Disabled the MAC layer retransmission
  - Two nodes, A and B, collected the statistical data
  - Using some streams (from sender $S_i$ to receiver $R_i$) to increase the interfering traffic
- Observation:
  - When only a few streams exist, A can get the channel quickly with high probability
  - As the number of streams increases, the competition for channel becomes more intense, thus taking longer for A to acquire the channel
DoS Detection – PHY Layer

- **Idea:**
  - Want to use PHY layer information to detect whether a jamming has occurred

- **Observations:**
  - Ambient noise levels in normal (including congested) scenarios and abnormal scenarios are statistically different.

- **Challenges:**
  - How to capture the time variant properties efficiently?
  - What is a good model to use for minimizing the probability of a false positive?

- **Network devices can sample noise levels prior to DoS attack and build a statistical model describing usual energy levels in the network.**
  - Discrimination between normal noise level measurements and abnormal data by employing the various features of the data.

- **Tools:**
  - $\psi^2$ statistics: Spectral Discrimination
  - $\chi^2$ statistics: Distributional Discrimination
DoS Detection – PHY Layer

- **Platform:**
  - Mica2 Motes (UC Berkeley)
  - Use RSSI ADC to measure the signal strength
  - The values are in inverse relationship to power (signal strength)

- **Three scenario**
  - No communicator
  - Three communicators (obey CSMA)
  - Use waveform generator as jammer

The noise level time series with a jammer and without a jammer are different.
Defenses: Channel Surfing and Spatial Retreats
Network Types

- DoS detection can be employed by a single node, however, DoS defenses are group activities.

- Three different network scenarios are concerned:
  - Two party radio communication
    - Baseline case
  - Infrastructured wireless network
    - Consist of two types of device: access points and mobile devices
    - Access points communicate with each other via wired infrastructure
    - Mobile devices communicate via the access point to other mobile devices
  - Mobile Ad Hoc Wireless Networks
    - Composed of mobile devices without access points
    - Mobile devices can communicate to each other via multi-hop routing protocol
Dos Defenses—Channel Surfing

- **Adversary Model:**
  - We assume there is only one stationary adversary, who blasts on a single channel at any time.

- **Adversary Model:** There is one *stationary* adversary, who *continuously* blasts on a *single* channel at a time.

- **Channel Surfing:**
  - If we are blocked at a particular channel, we can resume our communication by switching to a different (and hopefully safe) channel that does not overlap current channel.
  - Inspired by frequency hopping techniques, but operates at the link layer

- **System Issues:**
  - Must have ability to choose multiple “orthogonal” channels:
    - Prevents Interference
    - Practical Issue: PHY specs do not necessarily translate into correct “orthogonal” channels
    - Example: MICA2 Radio recommends: “choose separate channels with a minimum spacing of 150KHz” but.....
Throughput VS. Channel Assignment

- Sender sends the packet as fast as it can.
- Receiver counts the packet and calculates the throughput.
- The radio frequency of the sender and receiver was fixed at 916.7MHz.
- Increased the interferer’s communication frequency by 50kHz each time.
- When the Jammer’s communication frequency increases to 917.5MHz, there is almost no interference.
Throughput VS. Channel Assignment

Throughput vs. Jammer Frequency (Source-Receiver at 916.7Mhz)

Throughput vs. Wave Generator Frequency (Source-Receiver at 916.7Mhz)
Dos Defenses– Channel Surfing

- **System Issues (cont.):**
  - “Orthogonal” channels:
    - The fact is that we need at least 800KHz to escape the interference.
    - Therefore, explicit determination of the amount of orthogonal channels is important.
  - How to determine which channel to hop?
    - The adversary X may periodically stop its interference and try to find the new channel the nodes are currently on.
    - Goal: Maximize the delay before X finds out the new channel
    - Therefore, using next available channel is NOT good!
    - Use a (keyed) pseudo-random channel assignment!

- **Basic Channel Surfing Algorithm:** Both parties detect DoS independently, and change to a pre-determined channel and establish communication there
Two Party Radio Communication

- Prototype:
  - Two Berkeley motes A and B
  - A sends out a packet to B every 200msecs
  - Measure the packet delivery rate = \#recv/\#sent
  - Used waveform generator as jammer X
  - A and B try to detect the DoS attack periodically

- Code:
  ```
  task void checkDos() {
    sent = call SendMsg.send(
      TOS_BCAST_ADDR,
      sizeof(uint16_t),
      &beacon_packet);
    if(!sent){
      if(++failures< thresh)
        post checkDos();
      else post changeChan();
    } else {
      failures = 0;
    }
  }
  ```

![Channel Surfing Experiment graph]
DoS Defenses – Spatial Retreats

- **Adversary Model:**
  - We assume there is only one stationary adversary, who blasts on a single channel at any time.

**Adversary Model:** There is one **stationary** adversary, who **continuously** blasts on a **single** channel at a time.

- **Spatial Retreats:**
  - In order to resume our communication under the jamming style attack, we should move to a place that is outside of the jamming regions.

- **System Issues:**
  - Where to move?
  - How to ensure that both parties leave the adversary’s interference range?
  - How to maintain radio connectivity following a spatial retreat?
  - How to adapt to **non-circular** jamming regions?
Two Party Radio communication

- Three stage protocol:
  - Establish Local coordinates
  - Exit the Interference Region
  - Move into Radio Range
Two Party Radio communication

- Three stage protocol:
  - Establish Local coordinates
    - Decide the initial positions prior to the introduction of adversary
    - Determine a local coordinate system
    - Agree on the direction of the retreats, for example, $y$ axis.
  - Exit the Interference Region
  - Move into Radio Range
Two Party Radio communication

- Three stage protocol:
  - Establish Local coordinates
    - Decide the initial positions prior to the introduction of adversary
    - Determine a local coordinate system
    - Agree on the direction of the retreats, for example, y axis.
  - Exit the Interference Region
  - Move into Radio Range
Two Party Radio communication

- Three stage protocol:
  - Establish Local coordinates
  - Exit the Interference Region
    - Once A and B detect the DoS scenario, they try to move away from adversary along the y-axis.
    - A and B stop, as soon as they detect that it is out of the interference range.
  - Move into Radio Range
Two Party Radio communication

- Three stage protocol:
  - Establish Local coordinates
  - Exit the Interference Region
    - Once A and B detect the DoS scenario, they try to move away from adversary along the y-axis.
    - A and B stop, as soon as they detect that it is out of the interference range.
    - Problem: A and B cannot talk to each other any more.
  - Move into Radio Range
Two Party Radio communication

- Three stage protocol:
  - Establish Local coordinates
  - Exit the interference Region
  - Move into Radio Range
    - What if they bypass each other?
      - Let B be master and A be slave. Only slave moves
      - A moves along x-axis (toward B, never beyond B)
Two Party Radio communication

- Three stage protocol:
  - Establish Local coordinates
  - Exit the interference Region
  - Move into Radio Range
    - What if they bypass each other?
      - Let B be master and A be slave. Only slave moves
      - A moves along x-axis (toward B, never beyond B)
    - What if moving into the interference range again?
Two Party Radio communication

- Three stage protocol:
  - Establish Local coordinates
  - Exit the interference Region
  - Move into Radio Range
    - What if they bypass each other?
      - Let B be master and A be slave. Only slave moves
      - A moves along x-axis (toward B, never beyond B)
    - What if moving into the interference range again?
      - stops moving along the x-axis, moving along y-axis
Conclusions:

- Due to the shared nature of the wireless medium, it is an easy feat for adversaries to perform a jamming-style denial of service against wireless networks.

- We proposed two approaches that a single node may employ to detect a DoS Attack:
  - MAC layer: monitoring the sensing time
  - PHY layer: observing the noise levels in the channel

- We have presented two different strategies to defend against the jamming style of DoS attacks:
  - Channel-surfing: changing the transmission frequency to a range where there is no interference from the adversary
  - Spatial retreat: moving to a new location where there is no interference
Ongoing works:

- Study the detection strategies
  - Jammer turns on for 95% of the time and keeps silent for the rest of 5% of the time
  - Jammer will start to jam only if someone is sending out the message

- Investigate the channel-surfing and spatial retreat algorithm in new wireless network topologies:
  - Infrastructured wireless networks
  - Ad-hoc network

- Study the defenses against DoS with other issues:
  - High mobility
  - High redundant (in sensor network)

- A large scale (approximately 50 nodes) jamming-tolerant sensor network is being developed and results will be reported soon.
Other Investigations

- Many wireless security threats are being addressed
  - Secure routing protocol, Temporal Key Integrity Protocol (TKIP), 802.1x, privacy......
  - Validation of the possibility of DDOS in wireless by mathematical models.[1]
  - Using FAIR-MAC to prevent nodes from monopolizing the channel. Prerequisite: every node follows the fair MAC protocol.[2]
  - DOMINO: System for Detection Of greedy behavior in the MAC layer of IEEE 802.11 public Networks. [3]

- However, *the jamming style DoS is not well studied*
  - Australian CERT announced the issue of MAC layer weaknesses in 802.11 MAC. [0]
  - Mapping a jamming-area for sensor networks.[4]