Lecture 10 - Jamming

Friday, 17 March 2023 08:40

Jamming is wireless denial of service by ***intentionally*** injecting interference (via high-powered signals) on the communication frequencies. This makes the signal-to-noise ratio $SNR = \frac{P_s}{P_n}$ too large to have meaningful communication. *Noise is every signal which is not the intended communication signal (in a given context).* SNR should be smaller than a threshold T for communication to work.

The 'bad FCS' (i.e. bad frame check sequence) issue seen in the labs is related to (unintentional) interference.

Types of jamming

1. Generic jamming
    a. Objective: block network activity
    b. Consumes more energy
    c. Less efficient, since the adversary must be present constantly
2. Smart jamming
    a. Objective: target a specific packet within a protocol, based on its important role
    b. Relatively energy-friendly
    c. More efficient, since the adversary only needs to be active during the protocol
    - Example: block/jam CTS packets in IEEE 802.11 (Wi-Fi), which prevents anyone from starting transmission

More specific jamming types

1. Frequency-based jamming
    a. Spot jamming
        i. All transmission power on a single frequency
        ii. Easy to detect, since the channel is always noisy
        iii. Easy to avoid by changing channels
    b. Sweep jamming
        i. Target multiple frequencies, one at a time
        ii. Can affect multiple frequency, but has limited effectiveness, since it only targets each frequency for a part of the time
        iii. Harder to detect than spot jamming
        iv. Still easy to avoid by changing channels, or by waiting for the frequency to be jamming-free
    c. Barrage jamming
        i. Jam a range of frequencies at the same time
        ii. Power injected on each frequency may be different (i.e. lower)
        iii. Easy to detect, since there will always be noise on the channel
        iv. Might be hard to avoid, depending on the ratio between jammed frequencies and the number of available frequencies
2. Signal type-based jamming
    a. Random noise jamming
        i. Inject random noise on the channel
        ii. Adversary does not care about detection
        iii. Easy to discover in quiet environment, hard to discover in busy environment
        iv. Very effective, since injecting noise with sufficient power is always successful to jam transmission-reception link
    b. Deceptive jamming
        i. Inject spoofed/replayed message on target link
        ii. Adversary does not want to be detected
        iii. Usually hard to detect, very effective and may lead to energy depletion
        iv. However, this require previous knowledge on e.g. modulation scheme or channel access
3. Time-based jamming
    a. Constant jamming
        i. Always on, irrespective of time/channel activity
        ii. Easy to implement and very effective
        iii. Inefficient, easy to detect and easy to localize
    b. Alternate jamming
        i. Proactive/Random-time jamming
            1) Randomly select group of frequencies per time in advance
            2) More energy efficient and might be harder to detect & localize
            3) However, does not guarantee success
        ii. Reactive jamming
            1) Jam only when activity is detected on the channel
            2) Very hard to detect & localize, energy efficient and very effective
                a) What makes this incredibly hard to detect is the fact that nodes generally either transmit or receive, but not both (so the transmitter does not know jamming occurred, since they are not receiving simultaneously)
            3) However, is hard to realize and expensive (due to the specialized hardware required)

'Positive' variants of jamming

1. Friendly jamming
    a. The jammer is the only person/group who knows when jamming is active
    b. By letting friends (i.e. your own soldiers) know when jamming will occur, you can communicate at the times known to be jamming-free
2. Cooperative jamming
    a. Jamming used to prevent an eavesdropper (and only the eavesdropper) from listening to packets
    b. Usable when location of benign and adversarial identities are known.

Detecting jamming

Jamming detection is important because it can raise situational awareness, reduce energy consumption and allows for carefully selecting a countermeasure.

Jamming detection strategies consider:

1. Channel quality indicators
    a. Signal-to-noise ratio
    b. Noise floor levels
2. Traffic quality indicators
    a. Bit error rate
    b. Packet delivery ratio
    c. Throughput

The number of IP/MAC addresses in the network is not a reasonable metric for detecting jamming, since the jammer is not part of the network (they do not receive an IP address, and they may spoof MAC addresses).

Constant and proactive jammers are easy to detect, whereas deceptive and reactive jammers are hard to detect. Note that easy-to-detect jammers are not necessarily easy to avoid.

Detection strategies can be applied on existing devices (which makes it easier to take action, but costs energy) or on dedicated devices (which have fewer limitations, but have need to communicate under jamming (to instruct devices how to avoid the jamming)).

Avoiding jamming

Critical aspects in jamming avoidance are:

1. Jamming time
2. Jamming frequencies
3. Jamming power
4. Jammed area
5. Control over the devices/network (i.e. whether it is possible to replace hardware, update software, etc.)

Anti-jamming strategies can be hardware-based or software-based.

Hardware-based anti-jamming

Hardware-based techniques use information from the physical layer of the device or the real world. They typically require access to the radio of the device, which requires specific hardware (since commercially available hardware does not provide this information). Information used on this level could indicate the received signal strength (RSS), the phase of the received signal relative to the expected one, the I-Q samples from the wireless channel or the variation of carrier frequency of the received signal.

Direct Sequence Spread Spectrum (DSSS): roughly mixes data with pseudo-random noise and uses a wider bandwidth. This minimizes interception capability and the required SNR for communication. Also, multiple networks can co-exist on the same frequency. Since DSSS involves convolution, it requires dedicated hardware.

An alternative solution is antenna polarization, which relies on physical characteristics of antennas (by having e.g. linear, circular or elliptical EM fields). While this is low cost, it still requires dedicated antennas, synchronization mechanisms (when polarization can be changed by nodes) and introduces additional management overhead.

Directional transmission enhances range along a given direction. It still requires dedicated hardware, and it introduces complex MAC-layer protocols and more difficult multipath routing, but it gives several advantages: the performance is increased, the sensitivity is higher, the interference (from unwanted sources) is reduced and eavesdropping becomes more difficult.

Software-based anti-jamming

Frequency Hopping Spread Spectrum (FHSS) spreads communicated to different channels/frequencies over time. This has similarities with TSCH in IEEE 802.15.4 (TSCH occurs at MAC-layer, while FHSS occurs at PHY-layer). An important disadvantage is that synchronization is needed between devices (to agree a function that describes how to switch channels).

For reactive jamming, FHSS does not work. As an alternative, a hardly-detectable communication scheme can be used, in which it is difficult for the adversary to learn when they need to jam. One such technique is based on postambles; that is, to move the preamble of the PHY-layer packet to the end, so that the jammer does not know when a transmission occurs. However, this does lead to increased energy consumption (possibly up to 20×), since the receiver needs to oversample the channel.
Another technique is based on side channels, where silence is encoded as a 0 and jammed communication is encoded as a 1. The main disadvantage is that this has a low bit-rate. This technique only works with reactive jamming (and, after some modifications, possibly with proactive jamming), but not with constant jamming.

In general, mixed hardware-/software-based techniques are used. Some ideas could include to route around jammed areas.

Jamming in IoT is particularly challenging to mitigate because of cost and deployment (i.e. energy) constraints.