Wireless Network Security and Privacy
Autumn 2023

Xiaoyu Ji

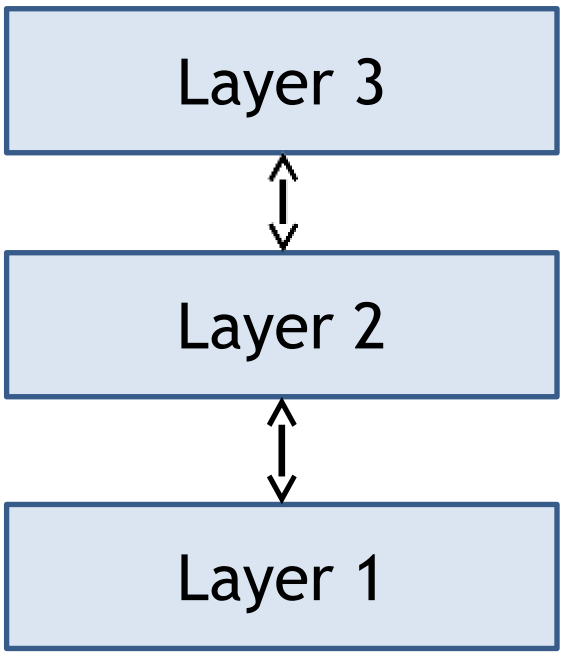
Cross-layer attacks & defenses

Agenda

- Cross-layer design
- Attacks using cross-layer data
- Cross-layer defenses / games

Layering

- **Layering simplifies network design**
- Layered model:

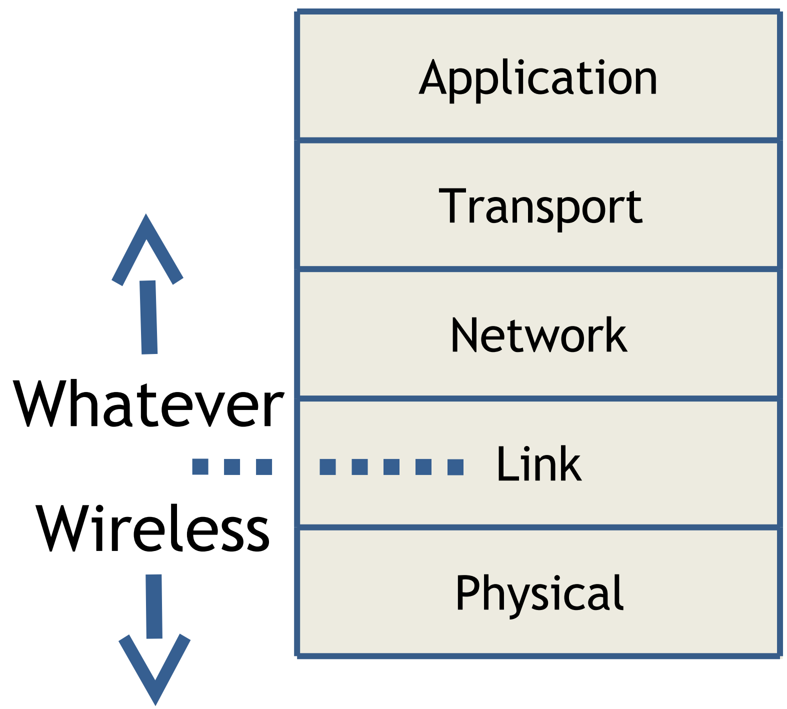


Lower layer provides a service to higher layer

Higher layer doesn't care (or even know, sometimes) how service is implemented: **lack of visibility**

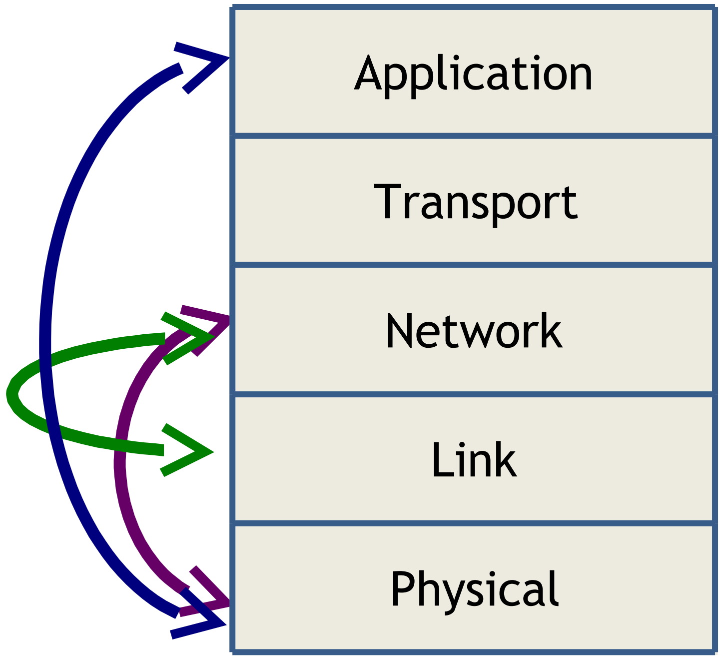
Layering in Wireless

- Layering impacts wireless protocols
  - Hiding physical layer → upper layers see wired
  - Cannot leverage advantages of wireless
- Layering is not appropriate for many wireless systems



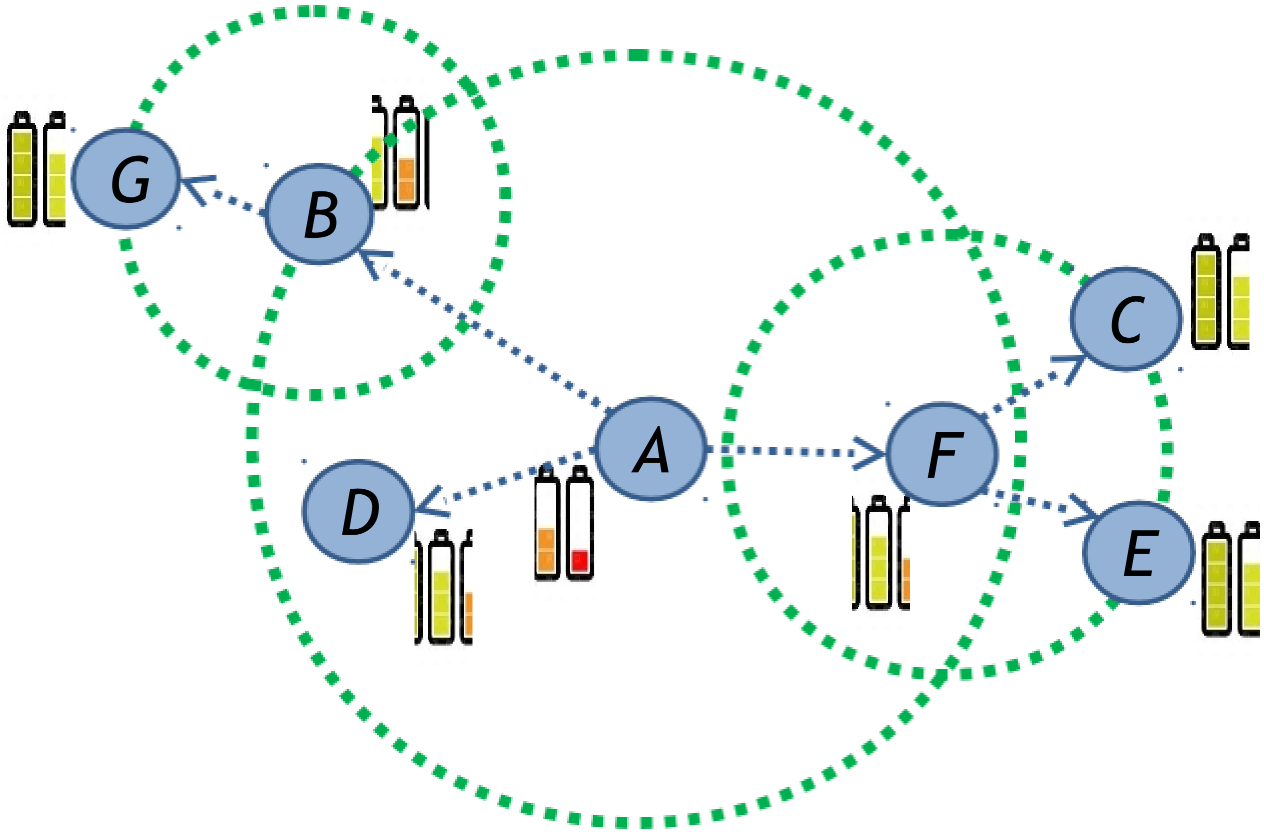
Cross-Layer Design

- Cross-layer design
  - Sharing info helps performance
  - Visibility restored
  - Design is more challenging



Max-Lifetime Broadcast Routing

- **Cross-layer example:**
  - How to broadcast to everyone to balance network lifetime given that wireless allows “overhearing”?

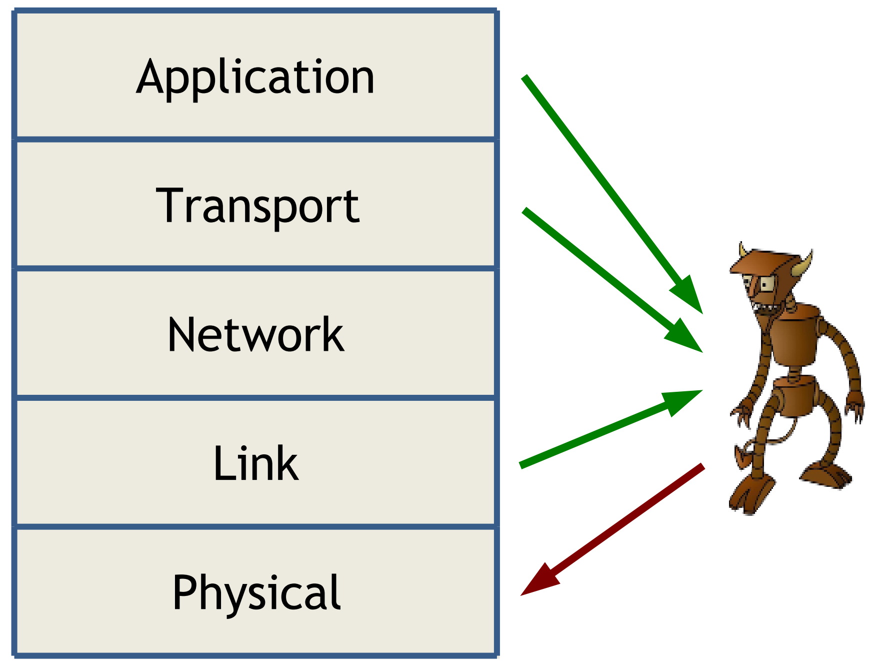


Cross-Layer Information Use

- Most network protocols were designed in the layered architecture
  - Leverage modularity for simple & efficient design
  - But...
    - Attackers don't have to follow the layering assumptions
    - Can learn significantly more about network operations and behaviors by monitoring/probing/interacting with multiple layered protocols
- → Attackers using cross-layer information may be "smarter" than the networks under attack

Cross-Layer Attacks

- Cross-layer attacks
  - Sharing information across protocol layers to improve attack performance
    - For any definition of performance
  - Planning and optimizing attacks may be much more challenging



Cross-Layer Attacks

Definition: a *cross-layer attack* is any malicious behavior that explicitly leverages information from one protocol layer to influence or manipulate another

Examples

1. MAC-aware jamming attacks

2. MAC misbehavior targeting transport-layer performance

3. Application-aware packet dropping attacks

4. Traffic-aware collaborative jamming attacks

Examples

1. MAC-aware PHY jamming attacks

2. MAC misbehavior targeting transport-layer performance

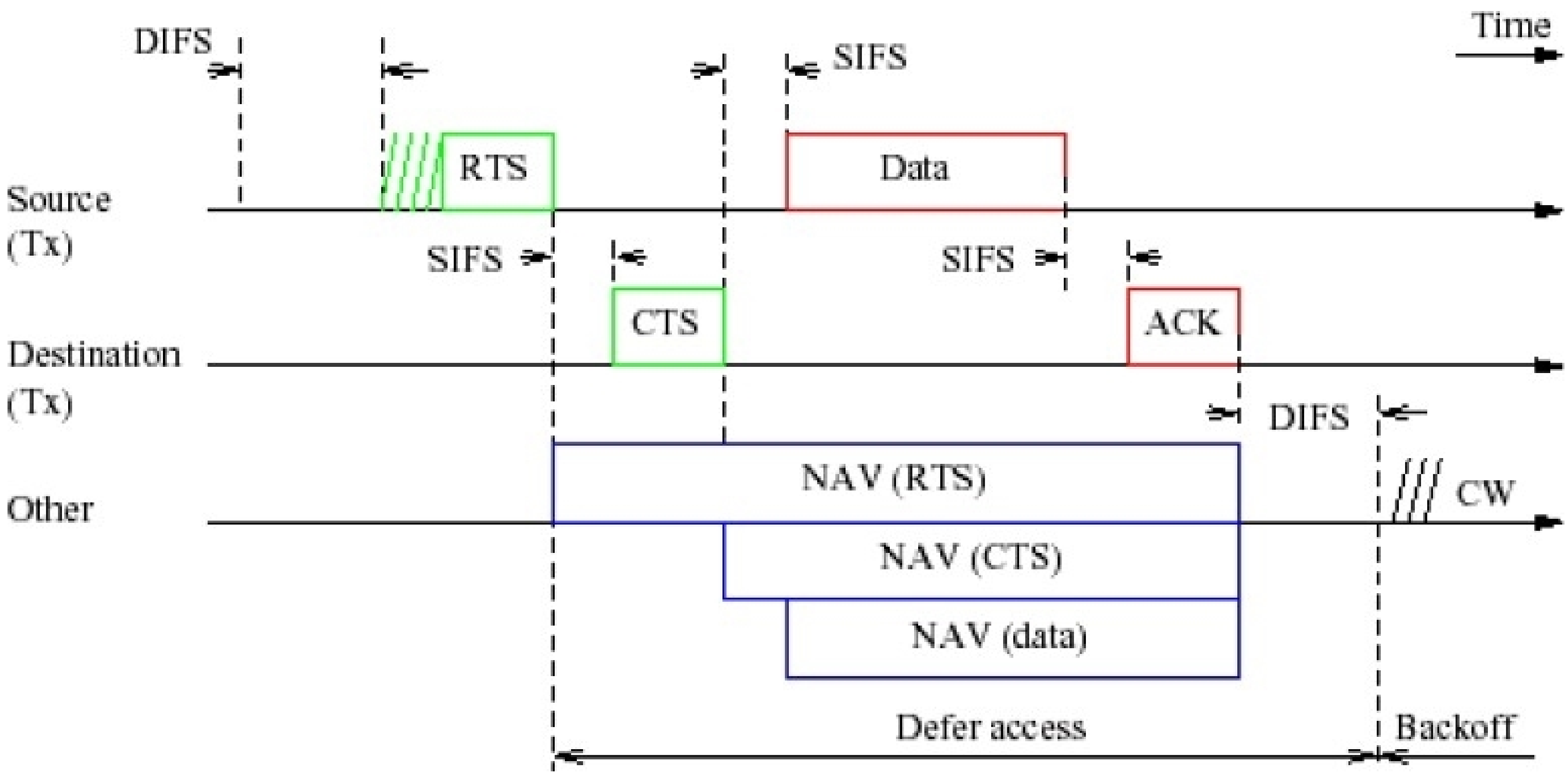
3. Application-aware packet dropping attacks

4. Traffic-aware collaborative jamming attacks

MAC-Aware Jamming

[Thuente & Acharya, MILCOM 2006]

- Protocol-aware jammers can optimize jamming actions based on protocol structure, e.g., MAC



Jamming Attack Metrics

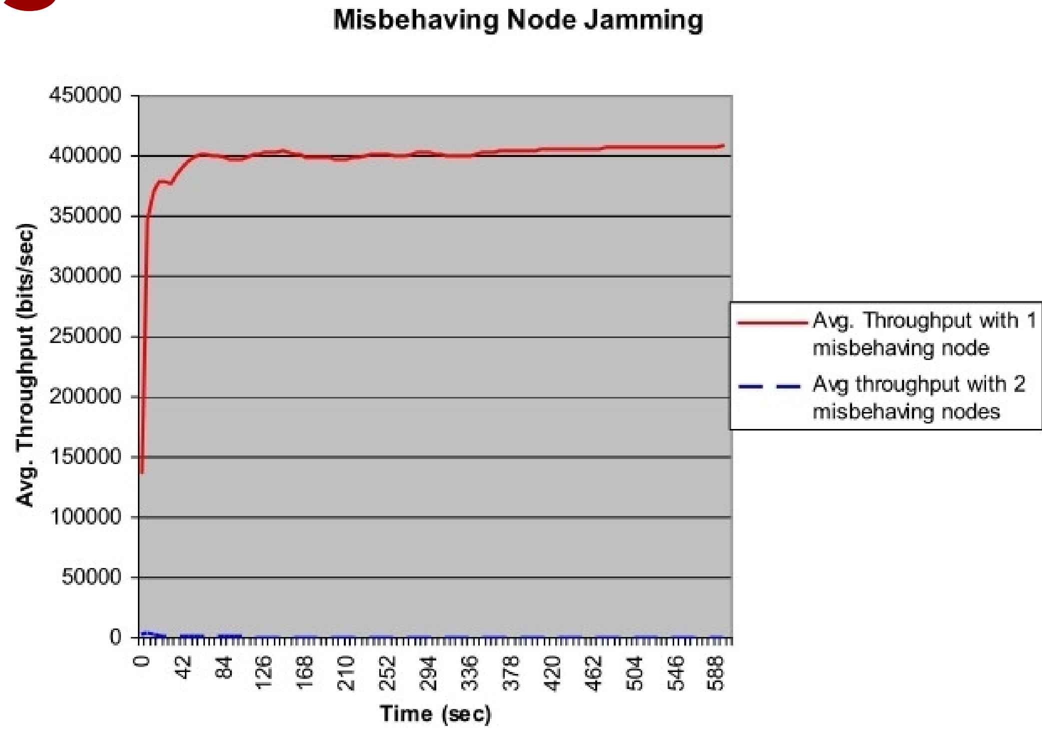
- *Attacks can be optimized in terms of:
  - Energy efficiency
  - Low probability of detection
  - Stealth
  - DoS strength
  - Behavior consistency with/near protocol standard
  - Strength against error correction algorithms
  - Strength against PHY techniques (FHSS, DHSS, CDMA)

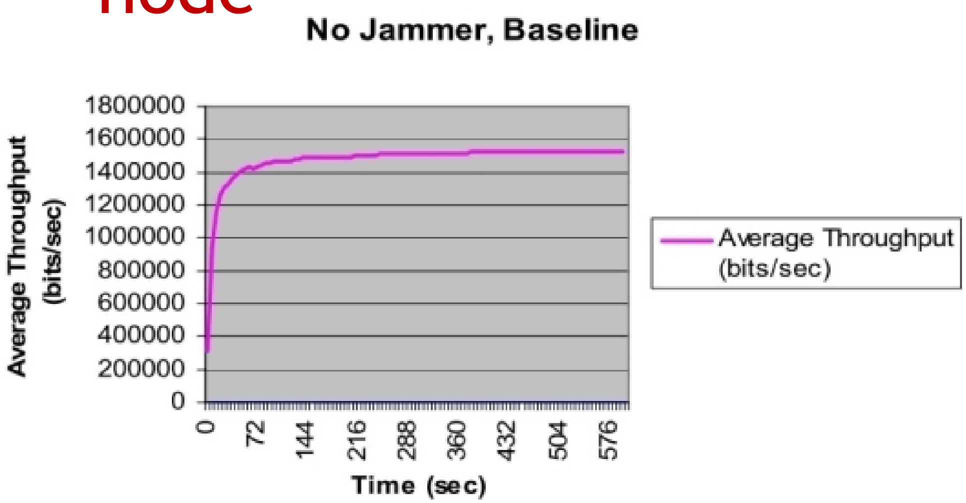
Jamming 802.11 Networks

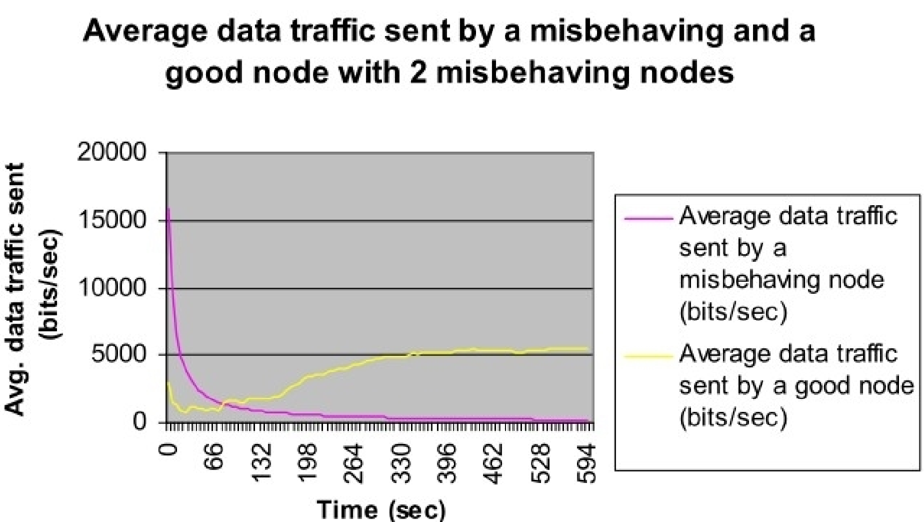
- Cross-layer jamming attacks
  - CTS corruption jamming
    - Jam CTS control packets to deny access and cause low channel utilization, knowing that CTS follows RTS
  - ACK corruption jamming
    - Jam ACK control packets to cause excess retransmission and low utilization, knowing that ACK follows DATA
  - DATAcorruption jamming
    - Attempt to jam data packets to reduce throughput, knowing that DATAfollows CTS control packet or previous ACK
  - DIFS wait jamming
    - Generate a short jamming pulse during DIFS time slots to prevent protocol continuation, no utilization

Colluding Attackers

- Nodes can collude to decrease probability of attack detection
- Energy required for 2 nodes is only slightly more than single node







Examples

1. MAC-aware jamming attacks

2. MAC misbehavior targeting transport-layer performance

3. Application-aware packet dropping attacks

4. Traffic-aware collaborative jamming attacks

Stasis Trap

[Bian et al., GLOBECOM 2006]

- Attacker uses MAC-layer misbehavior to target performance degradation in TCP flows
  - Based on MAC layer back-off manipulation, but only periodically, say on the order of a TCP timeout
    - Similar to a JellyFish attack, only executed at a lower layer
  - Overall, Stasis Trap has little effect on MAC layer performance, so MAC misbehavior detection will not be able to identify the attack
  - Attacker can target multiple flows to further reduce detectability

Examples

1. MAC-aware jamming attacks

2. MAC misbehavior targeting transport-layer performance

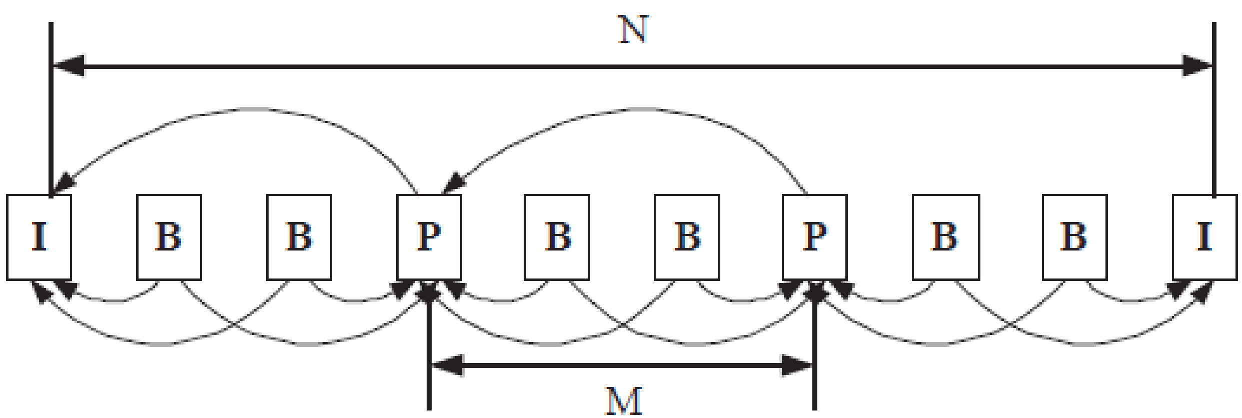
3. Application-aware packet dropping attacks

4. Traffic-aware collaborative jamming attacks

App-Aware Packet Dropping

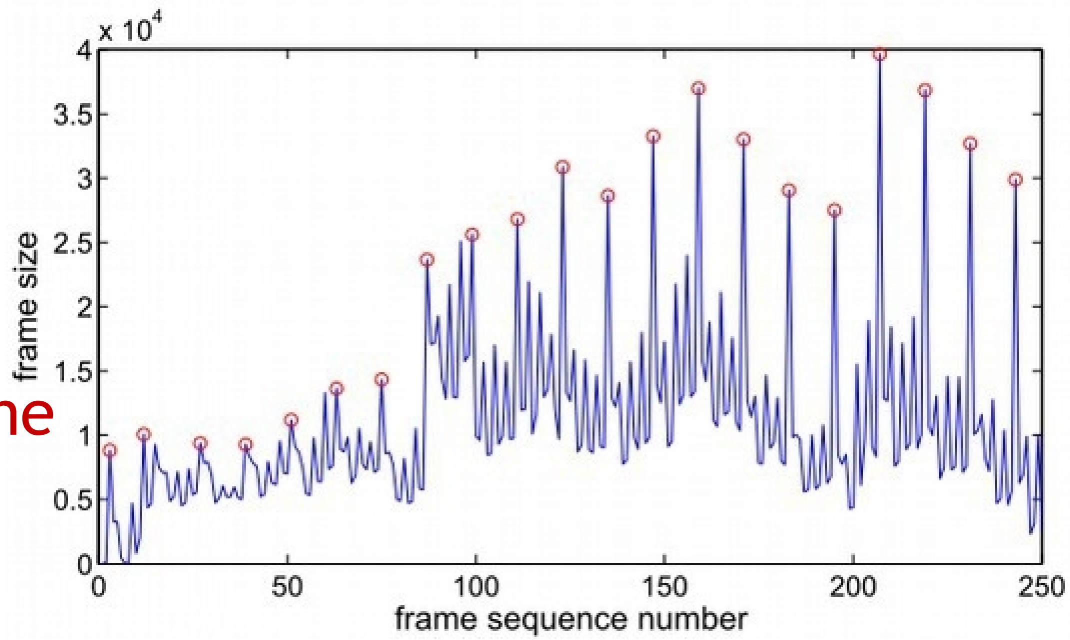
[Shao et al., SecureComm 2008]

- Attackers can use application-layer information to improve attack performance at lower layers
  - Attackers can drop the most valuable packets
  - Example: MPEG video
    - I-frames are more valuable to MPEG decoding capability and video quality than B- or P- frames
    - Cross-layer attackers can identify which packets contain I-frame data, and drop a small number of them

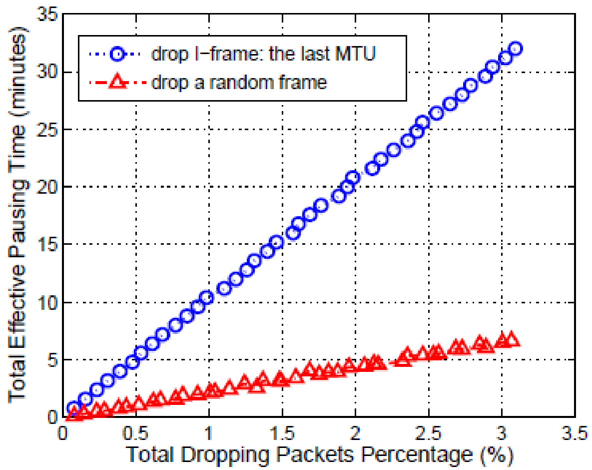


Sensing I-Frame Packets

- Router can observe frame sizes and attempt to identify which packets belong to I-frames
  - Analyzing frame size statistics reveals I-frame period N
  - Additional check tell router whether each packet is from an I-frame with high probability

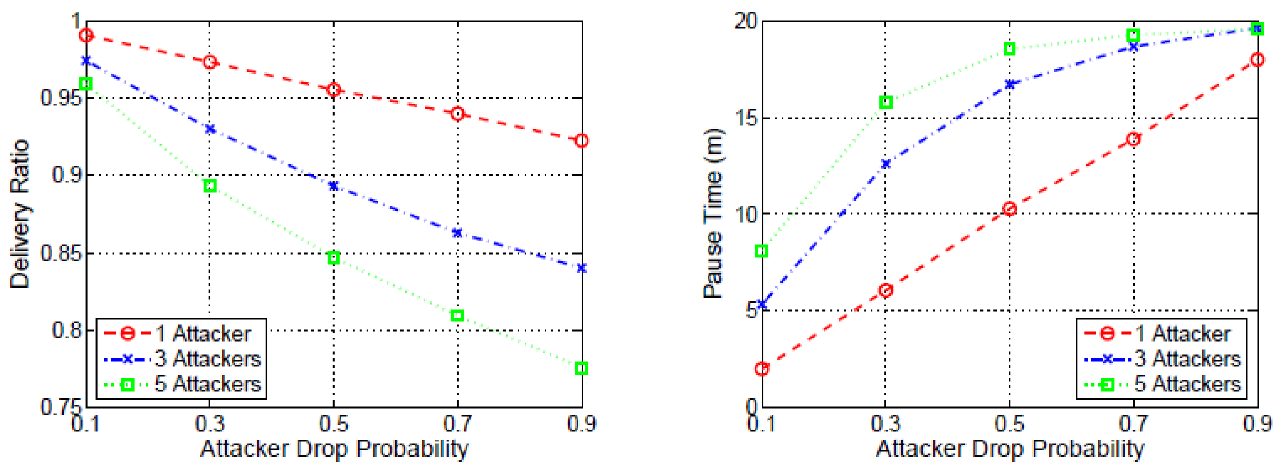


I-Frame Packet Dropping



Application-aware attack degrades video performance much more effectively compared to blind attack

Collaboration between multiple attackers yields further degradation



Examples

1. MAC-aware jamming attacks

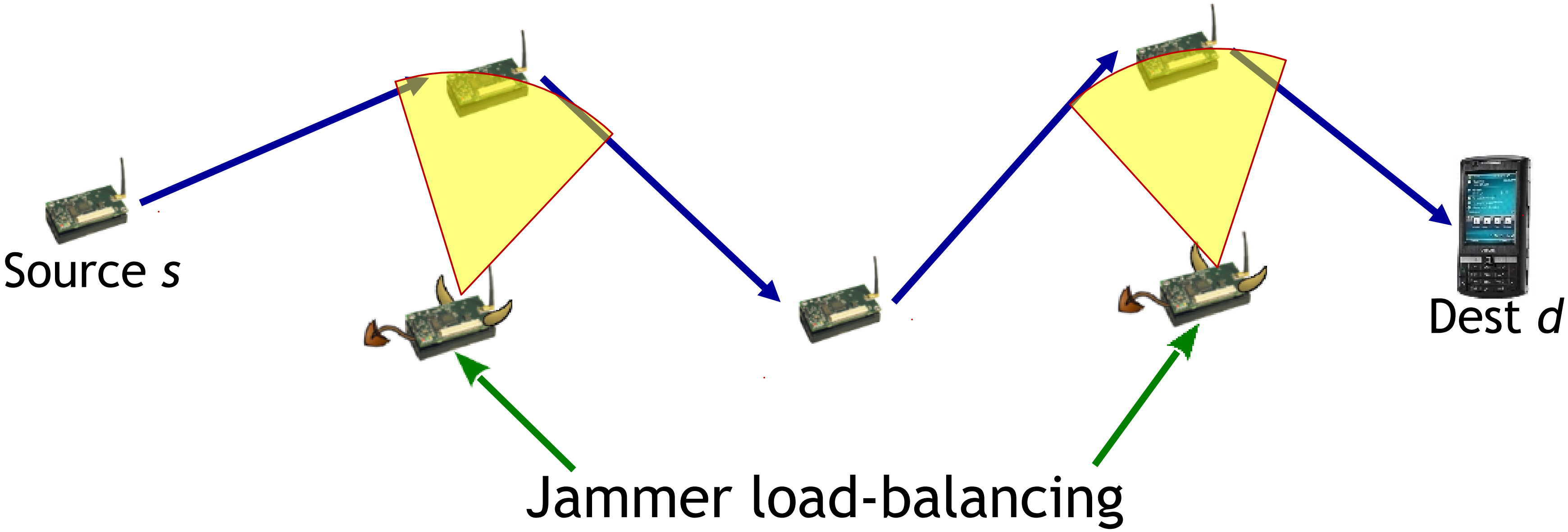
2. MAC misbehavior targeting transport-layer performance

3. Application-aware packet dropping attacks

4. Traffic-aware collaborative PHY jamming attacks

Traffic-Aware Jamming
[Tague et al., WiOpt 2008]

- Collaborating jammers with information about network flow topology and traffic rates can load-balance to control end-to-end flow



What about cross-layer defenses?

Layered Defenses for Layered Attacks

- Layered Attack vs. Layered Defense
  - This is what I consider "classical" network security
  - Layer *n* protocols protect against layer *n* vulnerabilities
  - Little/no protection from *cascading attack impacts*

Layered Defenses for Cross-Layer Attacks

- Cross-Layer Attack vs. Layered Defense
  - Advanced attacks developed against "classical" network defenses
  - Most likely, the attackers are going to win
    - At a cost, of course

Cross-Layer Defenses for Layered Attacks

- Layered Attack vs. Cross-Layer Defense
  - “Classical” attacks applied to advanced networking
  - If well designed, defenses should come out ahead
    - Again, at a cost

Cross-Layer Defenses for Cross-Layer Attacks

- Advanced Attack vs. Advanced Defense
  – Most interesting case where there isn't much work yet
  – How "advanced" do defenses need to be to keep up with the "advanced" attacks?
    - Hard question...
  – Can we come up with a general framework to allow a defender to learn and adapt to what it sees?
    - Attacker can do the same thing…
    - …now we have a game

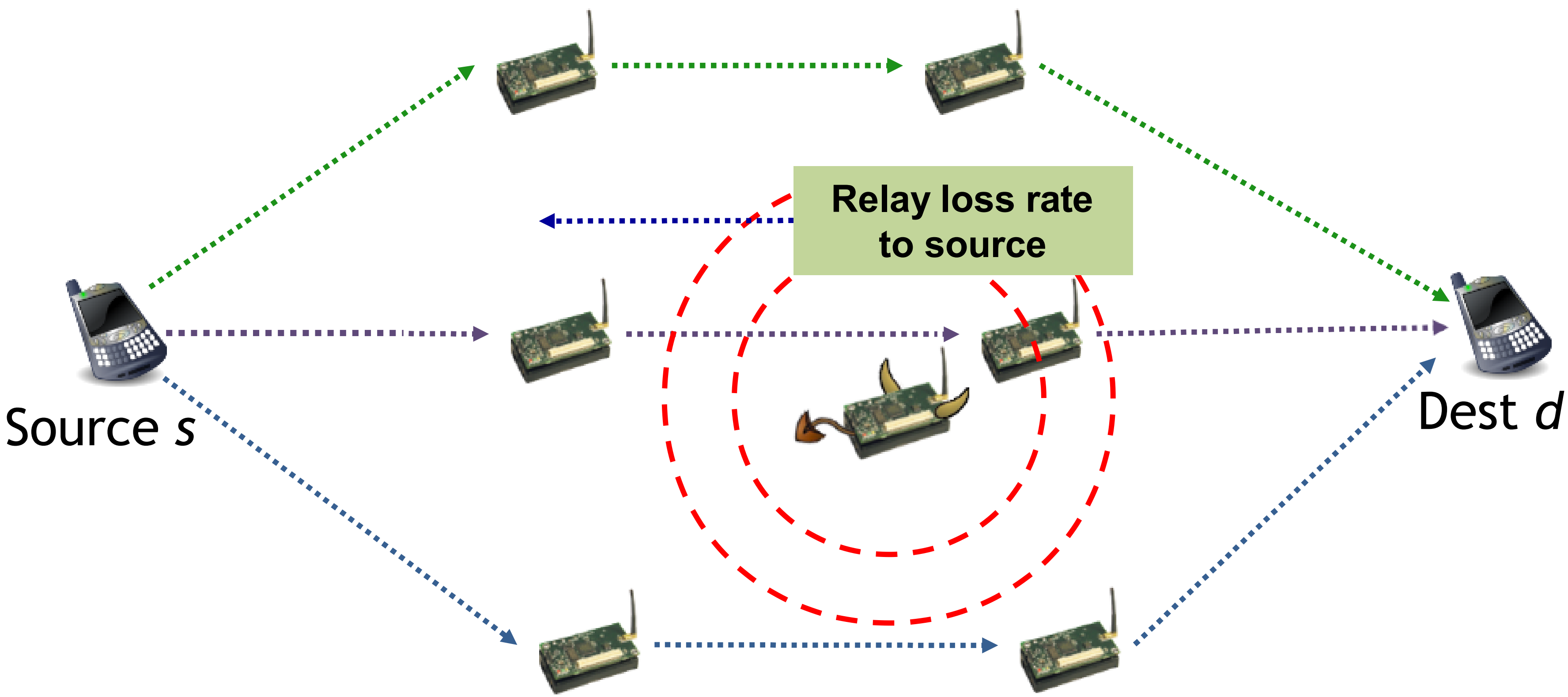
Comparison

	Layered Attack	Cross-Layer Attack
Layered Defense	Attack elements can target specific protocol performance Attacks are easy to plan, but probably sub-optimal	Attacker may be "smarter" than the network under attack Attack has fairly low cost to optimize, but likely to succeed
Cross-Layer Defense	Detection of attacks is more likely due to cross-layer impacts Defense is more costly, but likely to succeed	More difficult to characterize, optimize, predict, plan, … Attack and defense are more costly Red vs. Blue games

Jamming-Aware Traffic Flow

[Tague et al., ToN 2011]

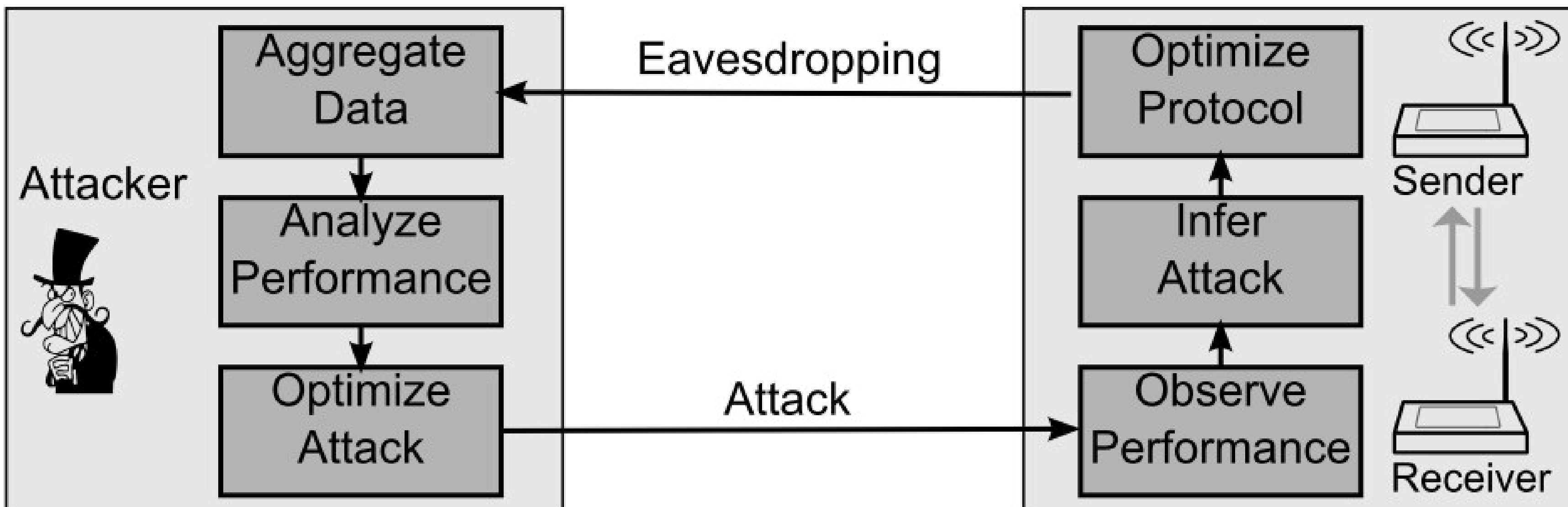
- Feedback from relay nodes allows source to dynamically adjust traffic allocation over multiple fixed routing paths



Observation-Based (Anti-)Jamming

[DeBruhl & Tague, PMC 2014]

- Opponents can observe actions, analyze what those actions mean, then adapt attack/defense algorithms accordingly



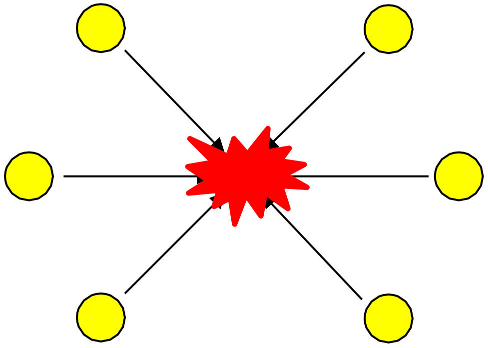
Cross-layer design can also enhance each other

For example: PHY can assist MAC collision resolution

Example: STAIRS [Ji, et, al. INFOCOM'13]

- Wireless Sensor Networks (WSNs)
  - Event-driven mode
  - Low duty cycle operating
  - Large number of nodes

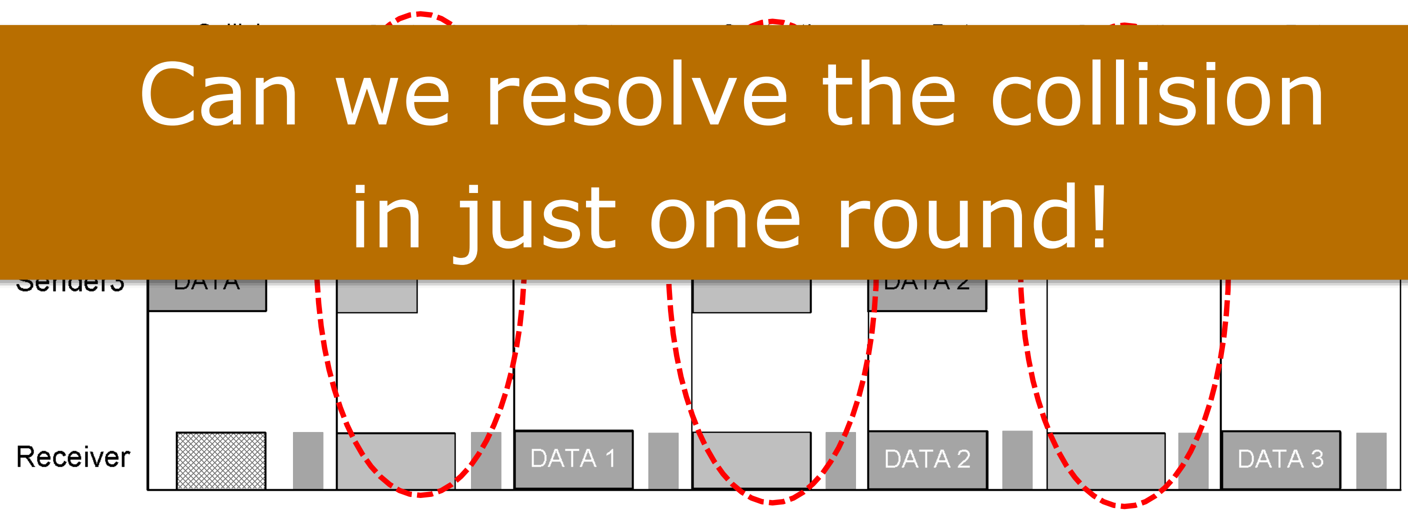
- CSMA-like protocols
  - Limitations
  - Backoff...



The Recent Art- COMA

- COMA- Contend before data transmission
  - Contention packets reserve channel for real data packets
  - The drawback: dedicated contention packets in each round

Can we resolve the collision in just one round!



Ref: F. Osterlind, et. al, Strawman: resolving collisions in bursty low-power wireless networks," in IEEE/ACM IPSN, 2012

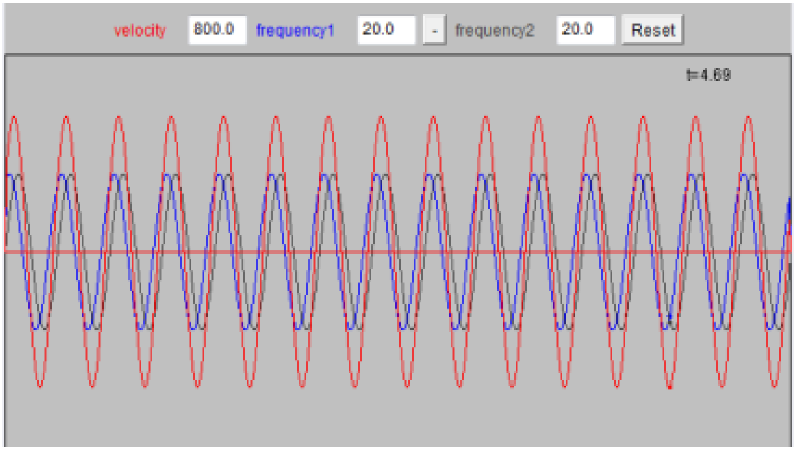
One-round Collision Resolution

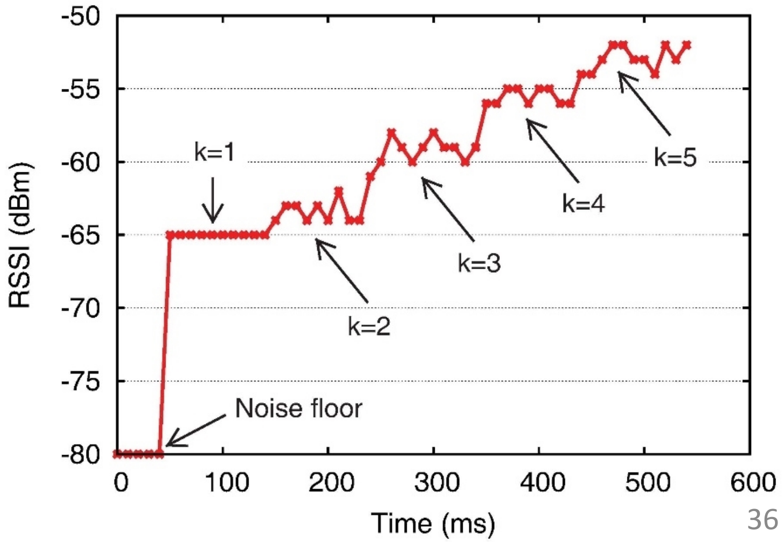
- The problem:
  - Count, identify and schedule
  - And of course in one round!

- Approach
  - Active contention
  - Virtual ID
  - Fast identification

Our weapon: RSSI *Stair* Pattern

- The observation
  - Signals can constructively collide
  - Requirements of *Constructive Interference* (CI)
    - 0.5 μs
    - Identical signal waveform





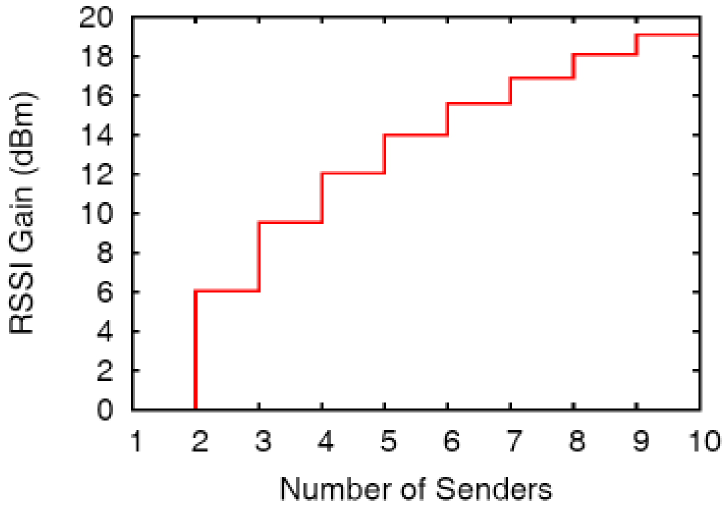
The Principle

Proposition: Given the superposed signal *CI(k)* under CI, let $A_1 = A_2 = \ldots = A$ be the amplitude and $\tau_1 = \tau_2 = \ldots = B$ denoting the phase offset with respect to the first signal generated by transmitter *i* = 1. Consider one IEEE 802.15.4 standard based communication system, $RSSI_{CI(k)}$ is equal to:

$$RSSI_{CI(k)} = 20\log\left(\sum_{i=1}^{k} A_i \cos(\omega_c \tau_i)\right)$$

Where ω_c is a constant and $\tau_1 = 0$

$$\Delta RSSI_{CI(k)-CI(k-1)} = 20\log_{10}\frac{k}{k-1}, \forall k \geq 2$$



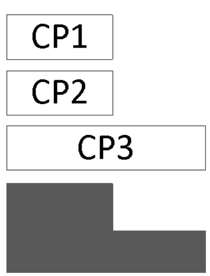
Design of STAIRS

- Overview

Through intentional contention, senders can be identified from the stair-like pattern of RSSI in one round.

Design Challenges

- Challenge 1: Synchronization
  - Requirement of CI: $\Delta \leqslant 0.5\mu s$
- Challenge 2: Falling edge detection
  - CP packets with the same length
  - External interference, e.g., WiFi signals



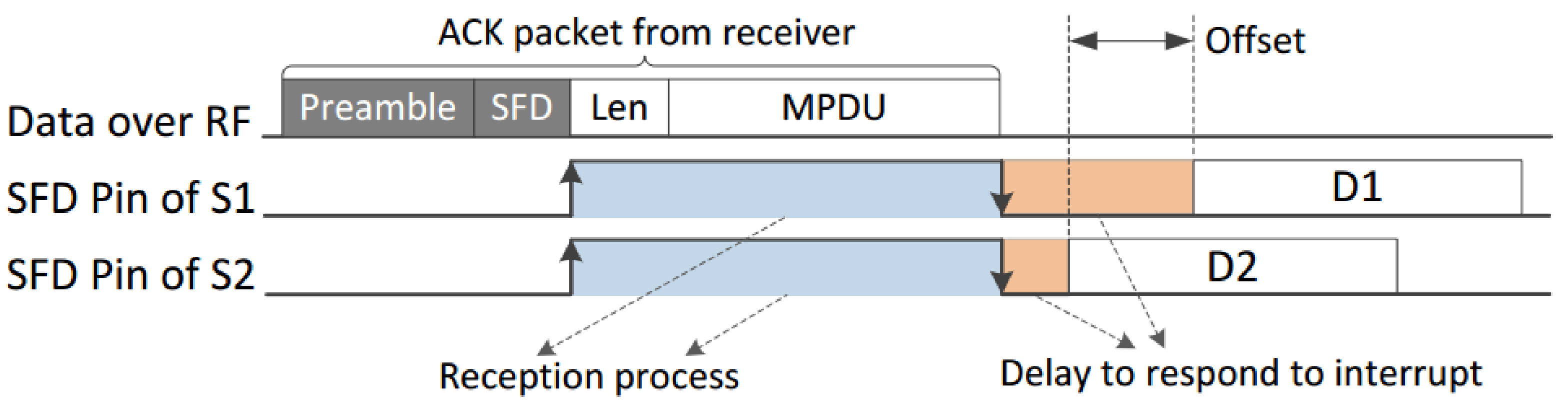
(1) False negatives

False falling edges

(2) False positives

Alignment for CP packets

- Receiver-initiated (CR)
  - Triggering transmissions of CP packets
  - Serving as ACK/NACK
  - Coping with hidden terminals
- Parallelizing *receiving* and *reading*

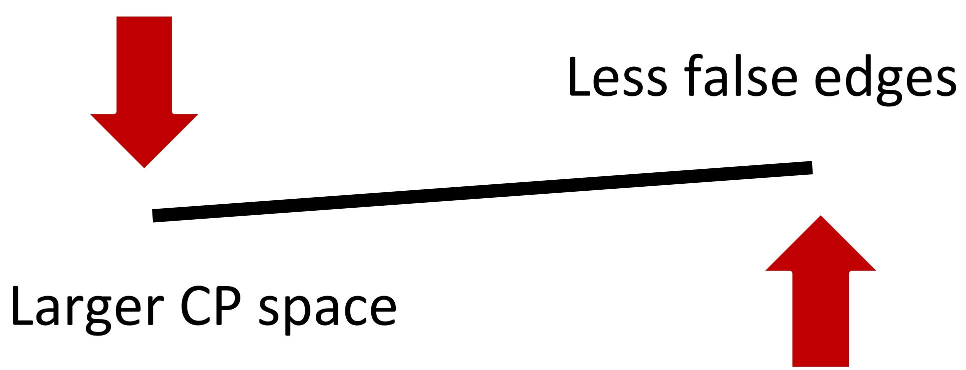


S-CUSUM Edge Detection

- Discrete lengths of CP packets
  - Total sender number *N*, maximum packet size *L*, increase step *ΔL,* length of CP is:

$$l(CP) \in \{\Delta L, 2\Delta L, 3\Delta L \ldots m\Delta L\}$$

- A paradox- how to find a good *ΔL*?



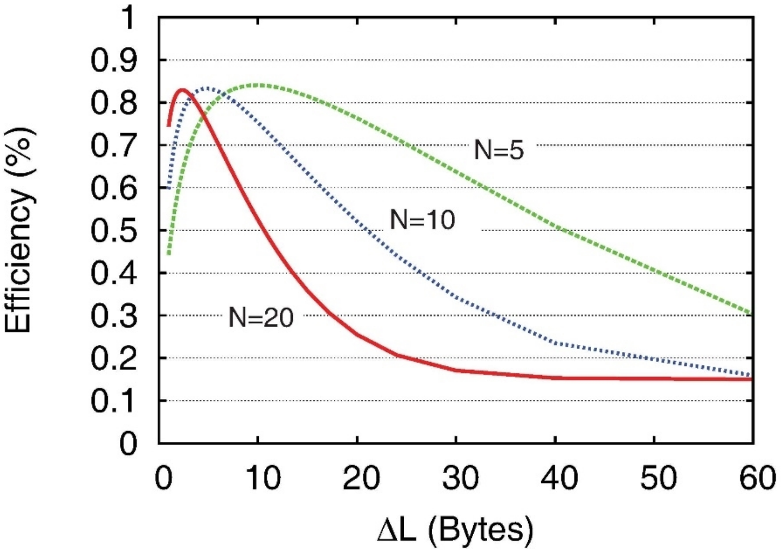
- Finding the optimal *ΔL*
  - p=1/m: choose any of the *m* lengths
  - α: the probability of false positives
- Three cases for a schedule:

$$P_i = \alpha(1-p)^N$$

$$P_s = Np(1-p)^{N-1}$$

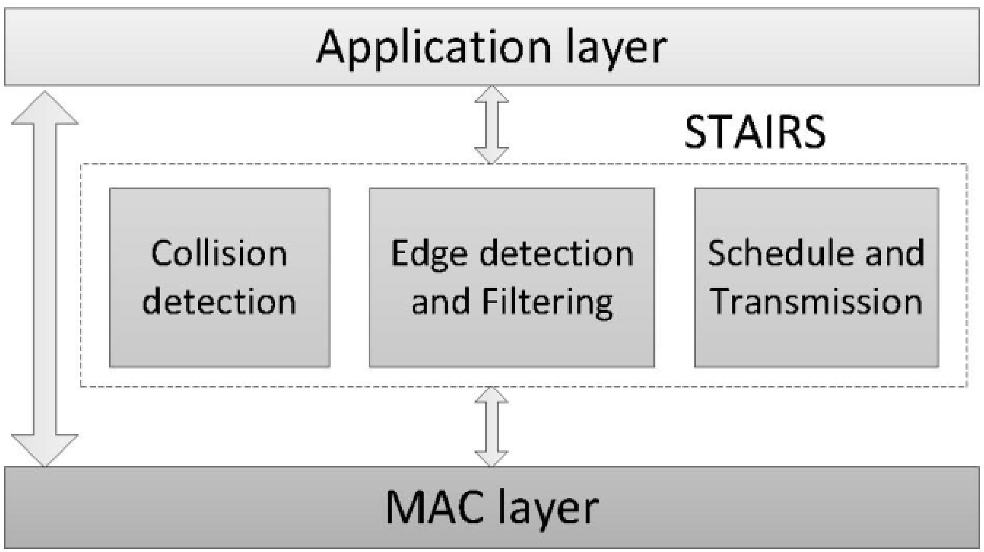
$$P_c = 1 - P_i - P_s$$

$$\Delta L^{opt} = \arg\max_{\Delta L} f\left(P_i, P_s, P_c\right)$$



Implementation

- STAIRS
  - A plug-in between APP and MAC layer
  - Invoked when collision happens
  - Three main components



Summary

- Attackers and defenders can use cross-layer information sharing to improve performance
  - Examples:
    - MAC-aware jamming, TCP-aware MAC misbehavior, APP-aware packet dropping, NET-aware jamming, PHY/LINK-aware flow control
- Adaptation in response to cross-layer observations provides further value
- Mutual adaptation is super interesting, still not really understood