CIS 700/002 : Special Topics : Wireless Security

A survey on wireless security: Technical challenges, recent advances, and future trends

Y Zou, J Zhu, X Wang, L Hanzo - Proceedings of the IEEE, 2016

Konstantinos Gatsis

CIS 700/002: Security of EMBS/CPS/IoT

Department of Computer and Information Science

School of Engineering and Applied Science

University of Pennsylvania

< date >

Wireless Security

- Broadcast nature of wireless medium: new vulnerabilities compared to wired
- Each layer has its own vulnerabilities, countermeasures (higher layers same in wired)

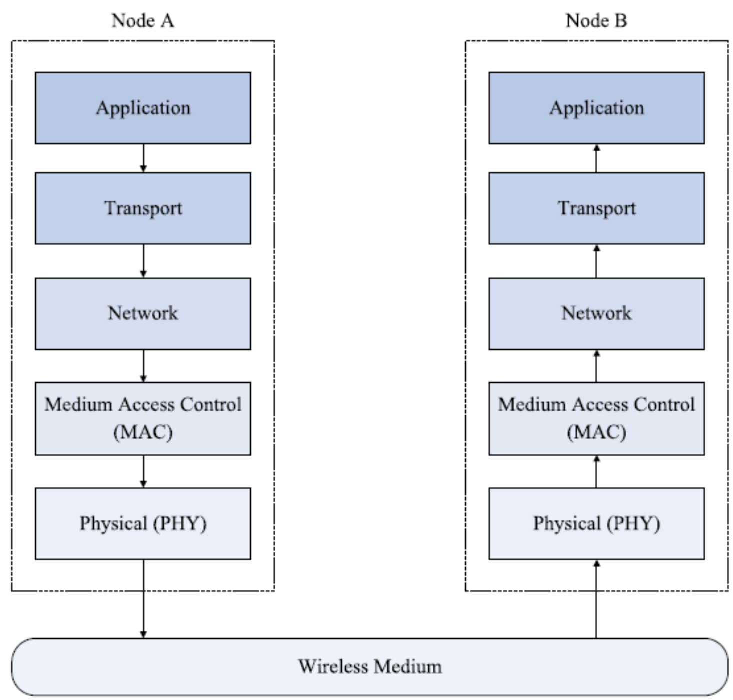


Fig. 2. ***Generic wireless OSI layered protocol architecture consisting of the application layer, the transport layer, the network layer, the MAC layer, and the physical layer.***

Wireless Security

- Broadcast nature of wireless medium: new vulnerabilities compared to wired
- Each layer has its own vulnerabilities, countermeasures (higher layers same in wired)
- Wireless security requirements:

1) Authenticity (e.g. device MAC address)
2) Confidentiality (e.g. against eavesdroppers)
3) Integrity (e.g. compromised node)
4) Availability (e.g. jamming)

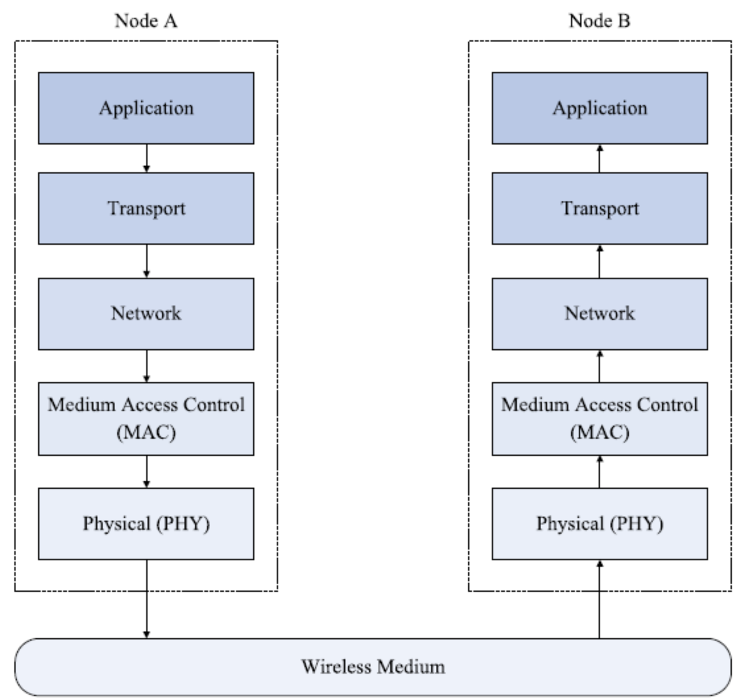
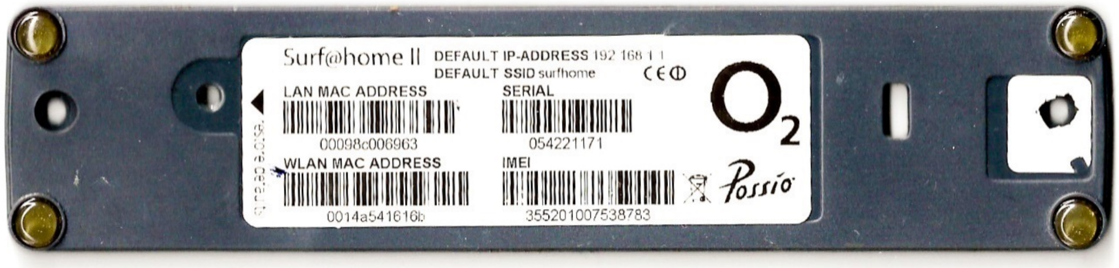


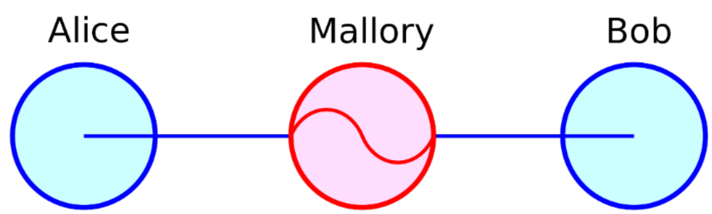
Fig. 2. *Generic wireless OSI layered protocol architecture consisting of the application layer, the transport layer, the network layer, the MAC layer, and the physical layer.*

MAC Layer Attacks

- Each wireless device has a unique hard-coded MAC for authentication



1) MAC spoofing attack: attacker hides true identity or impersonates someone else by stealing legitimate MAC
2) MITM attack: establish connection with a pair of legitimate nodes by impersonating both

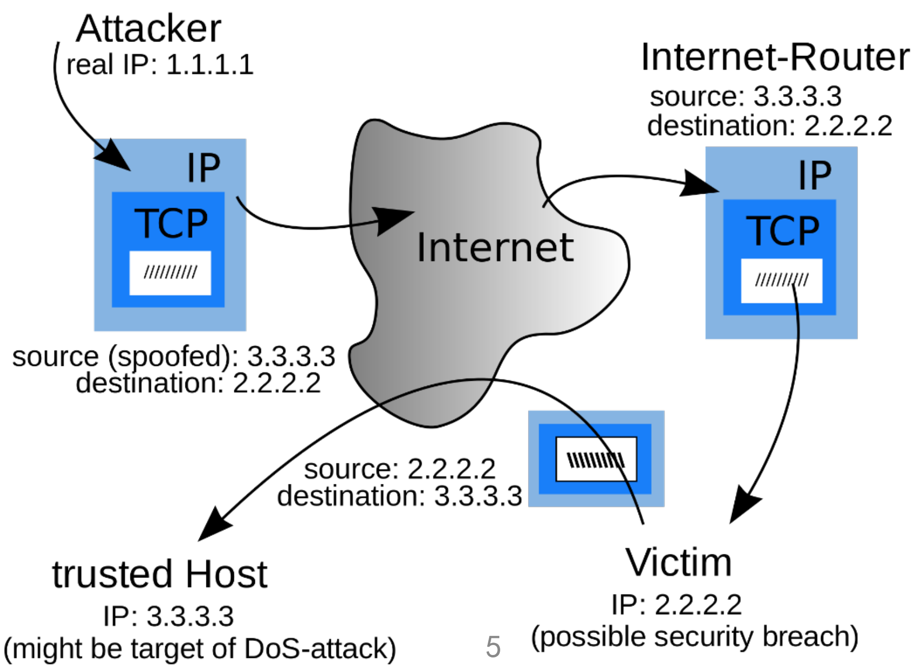


3) Network injection attack: inject forged network reconfiguration commands, may paralyze network
   - Detect by firewall (?)

Network Layer Attacks

1) IP spoofing: can generate forged IP packet, waste network capacity
2) IP hijacking: disconnects legitimate user, access to confidential info
3) Smurf attack (DoS): attacker sends huge number of network control packets to victims who send control responses, paralyze network

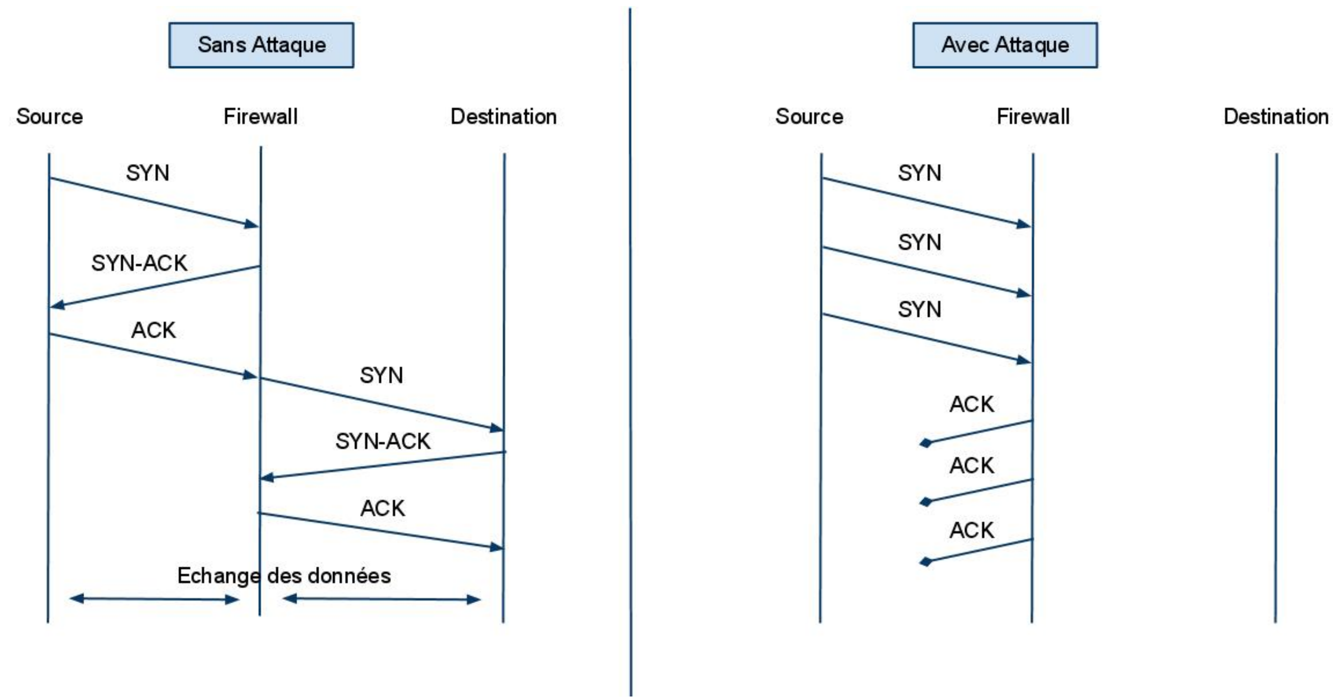
- Defend by firewall, avoid responses



Transport Layer Attacks

1) TCP flooding attack: attacker sends huge number of ping requests, victim sends ping responses, makes system unresponsive
2) TCP sequence prediction attack: attacker guesses packet sequence index of legitimate user, integrity loss
3) UDP flooding attack: attackers sends huge number of packets (not ping) to victim, who responds

- Defend by limiting response rate, firewall



Physical Layer Attacks

1) Eavesdropping attack

- Classic defense: encryption using a shared secret key
  - successful against computationally limited attackers
  - Introduces overheads
- Physical layer security defenses

2) Jamming attack

- Physical layer security defense

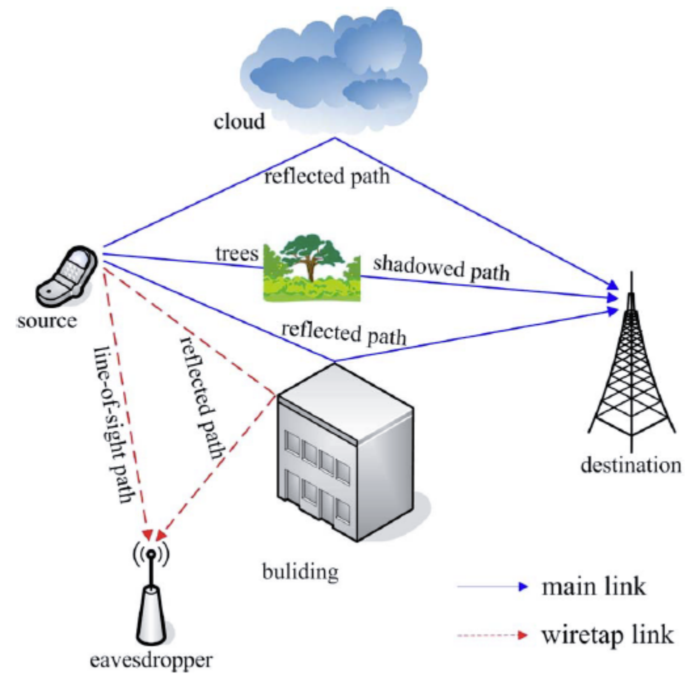


Fig. 17. ***Wireless scenario transmitting from source to destination in multipath fading environments in the presence of an eavesdropper.***

PHY Layer Security Against Eavesdroppers

- Wiretap channel (Wyner 1975):
  - Information-theoretic security (no secret keys!)
- **Theorem**: possible to communicate with secrecy if eavesdropper has a degraded channel compared to legitimate receiver (Ce < Cr)
- Criticism:
  - need to know eavesdropper's channel
  - practical coding under research
- Lots of spinoffs:
  - MIMO,
  - Broadcast with confidential messages,
  - Covert communication

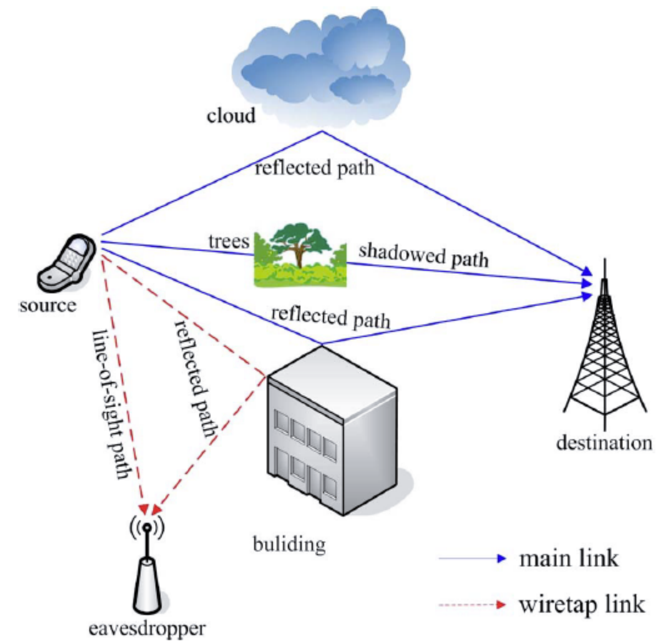
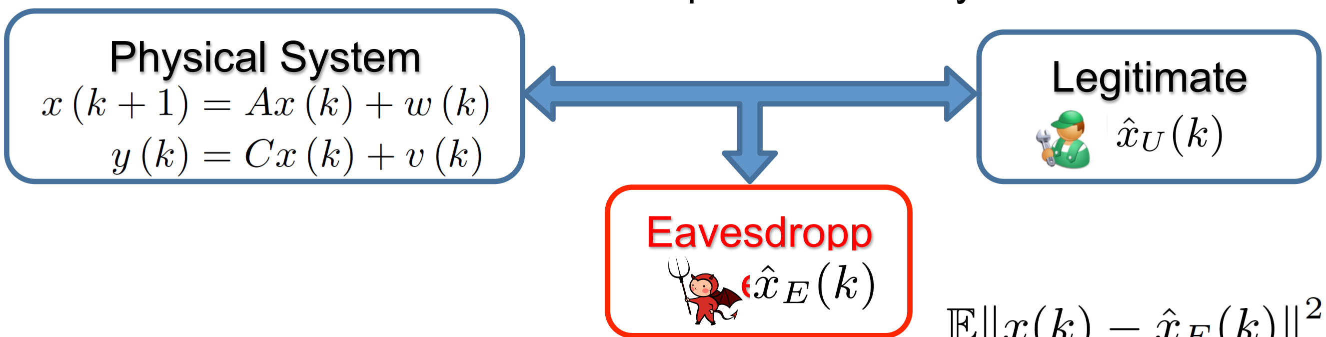


Fig. 17. ***Wireless scenario transmitting from source to destination in multipath fading environments in the presence of an eavesdropper.***

Wireless Secrecy for Cyber-Physical Systems

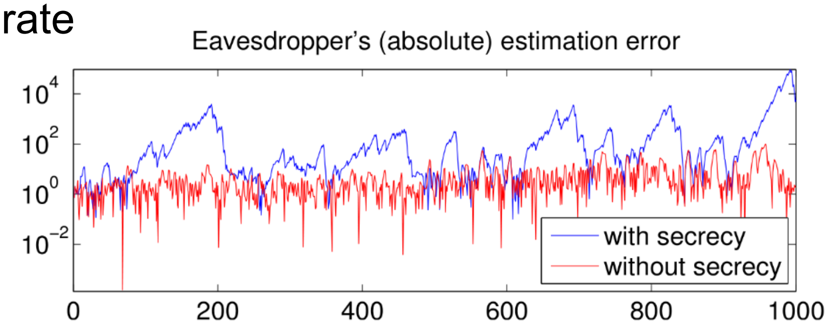
- Control-theoretic definition of perfect secrecy*



$$\mathbb{E}\|x(k) - \hat{x}_U(k)\|^2 < \infty$$

$$\mathbb{E}\|x(k) - \hat{x}_E(k)\|^2 \to \infty$$

- **Theorem**: Perfect secrecy achieved if user's packet rate > eavesdropper's interception rate



- Future goals
  - Secrecy-utility tradeoffs in CPS design
  - Secrecy in monitoring and control of smart automotive systems

Penn Engineering

* A. Tsiamis, K. Gatsis, G. J. Pappas, "Remote Estimation subject to Wireless Secrecy Constraints", submitted IFAC'17

PRECISE

PHY Layer Security Against Eavesdroppers

- Artificial-noise-aided security: add noise to transmitted signals to affect only eavesdropper, but wastes power
- Security-oriented beamforming: transmit to a particular direction to the user, hide from eavesdropper
- Diversity-assisted security, e.g. multiple antennas, relays, select the one with highest secrecy at each time

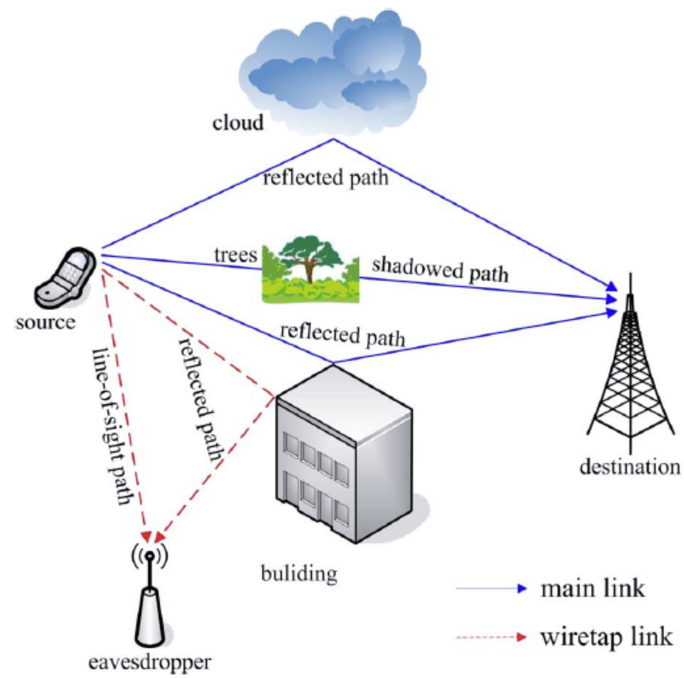


Fig. 17. *Wireless scenario transmitting from source to destination in multipath fading environments in the presence of an eavesdropper.*

Physical-layer secret key generation

- Source and destination see reciprocal random channel
- May be used to agree on a common secret key
- Eavesdropper at a different location sees an uncorrelated channel, cannot guess secret key
- Secret key length depends on 'size' of common randomness, e.g., harder in a slowly varying environment
- Practically feasible since '90s!

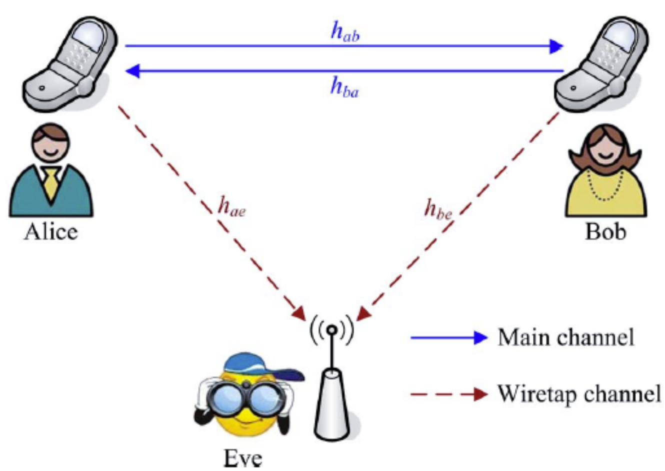


Fig. 22. *Wireless system consisting of two legitimate transceivers (Alice and Bob) in the presence of an eavesdropper (Eve).*

Penn Engineering

PRECISE

Physical-layer secret key generation

Exploiting Wireless Channel Randomness to Generate Keys for Automotive Cyber-Physical System Security, Jiang Wan, Anthony Bahadir Lopez, Mohammad Abdullah Al Faruque, ICCPS'16

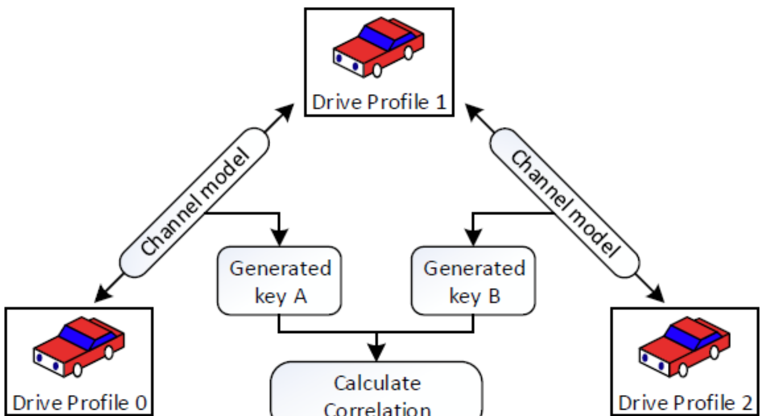
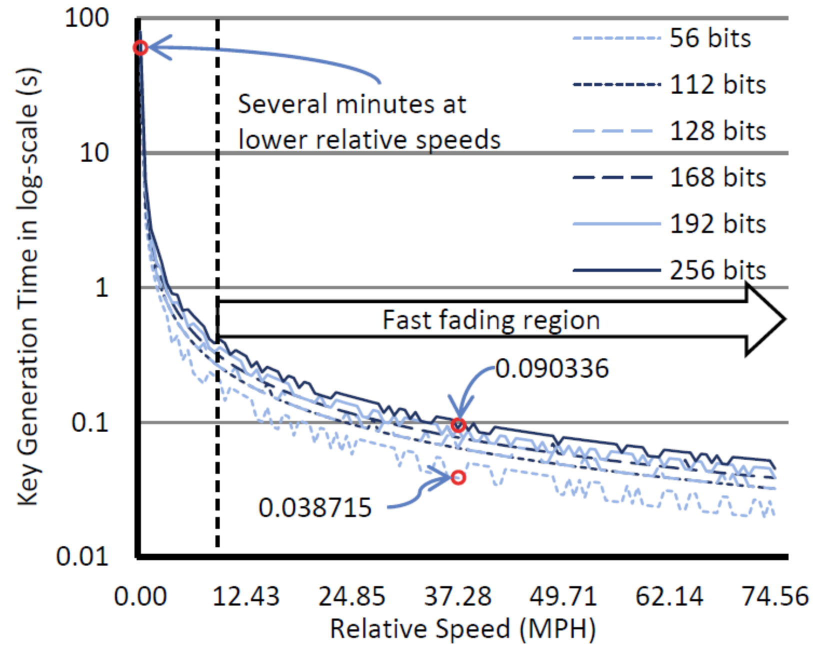


Figure 4: Simulation of Generating Two Secret Keys at the Same Time.



*Not sure if eavesdropper uncorrelated assumption is verified

Wireless Jamming Attacks

1) constant jammer, where a jamming signal is continuously transmitted;
   - Requires a lot of attacker power
   - Interference corrupts signals + Legitimate transmitter finds channel busy
   - Detect by abnormal measured energy or packet error rate
   - Defend by: secret random frequency hopping
2) intermittent jammer, where a jamming signal is emitted from time to time;
3) reactive jammer, where a jamming signal is only imposed, when the legitimate transmission is detected to be active;
   - Only causes interference
   - Defend by spreading radio signal over wide frequency bandwidth, hidden from attacker
4) (ideal) adaptive jammer, where a jamming signal is tailored to the level of received power at the legitimate receiver;
   - Most power efficient for attacker
   - Attacker needs to know legitimate receiver' signal strength (unrealistic)
   - Hard to detect, defend

Wireless Jamming Attacks

5) intelligent jammer, where weaknesses of the upper-layer protocols are exploited for blocking the legitimate transmission.

- e.g. attack on MAC control packets, such as RTS/CTS,
- No need to corrupt data packets
- Detected by abnormal traffic detectors
- Defend by protocol hopping

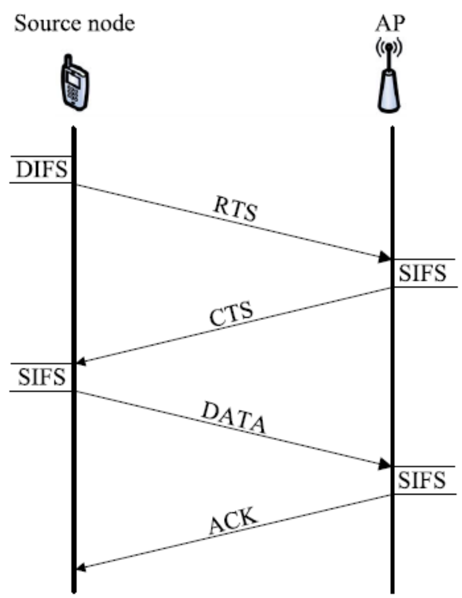


Fig. 23. IEEE 802.11 DCF process.

Penn Engineering

PRECISE

Physical Layer Authentication

- E.g. can protect against MAC spoofing
- Authentication by:
  - Hardware properties of RF devices/ fingerprints are unique among users and unforgeable, e.g., clock timing deviations
  - Wireless channel propagation statistics are unique among users and unforgeable
  - Superimpose stealthy fingerprint on data (also watermarking in control by Sinopoli et al)

Summary

- Wireless vulnerabilities due to broadcast nature of wireless medium
- Many layers have different vulnerabilities and countermeasures
- PHY Layer techniques
  - motivated theoretically
  - Not yet part of wireless security protocols
  - Require further validation
  - Can be used in combination with higher-layer security

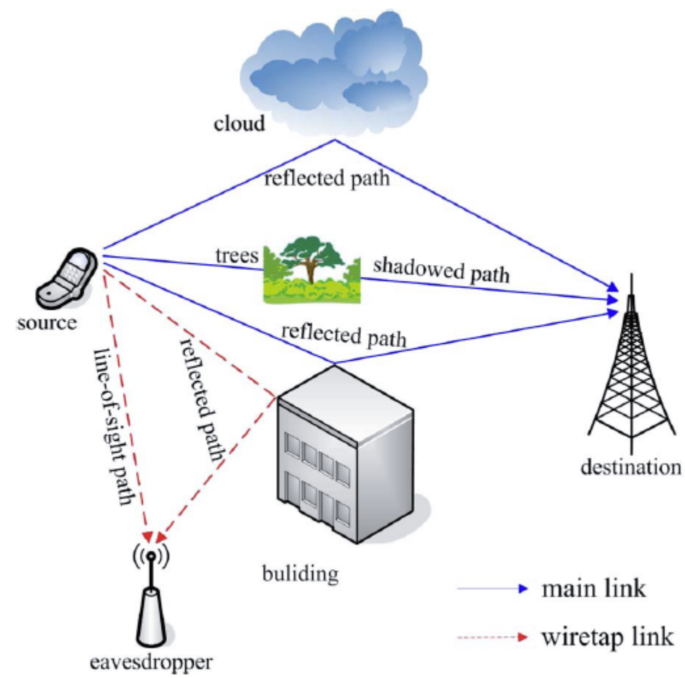


Fig. 17. ***Wireless scenario transmitting from source to destination in multipath fading environments in the presence of an eavesdropper.***