Network Security (NetSec)

Summer 2015
Chapter 06: Link Level Security
Module 04: Wireless Network Fairness Issues

Prof. Dr.-Ing. Matthias Hollick

Technische Universität Darmstadt
Secure Mobile Networking Lab - SEEMOO
Department of Computer Science
Center for Advanced Security Research Darmstadt - CASED

Mornewegstr. 32
D-64293 Darmstadt, Germany
Tel.+49 6151 16-70922, Fax. +49 6151 16-70921
http://seemoo.de or http://www.seemoo.tu-darmstadt.de

Prof. Dr.-Ing. Matthias Hollick
matthias.hollick@seemoo.tu-darmstadt.de

Learning Objectives & Outline

Discussion of fairness issues in WLANs

- MAC regulates access to medium, understand fairness issues and solutions addressing these

Outline

(1) Recap: Operating principles of IEEE 802.11

(2) Selfish behavior in hotspots (infrastructure mode)

Please note: some slides in this chapter are courtesy and copyright of Levente Buttyán and Jean-Pierre Hubaux © 2007

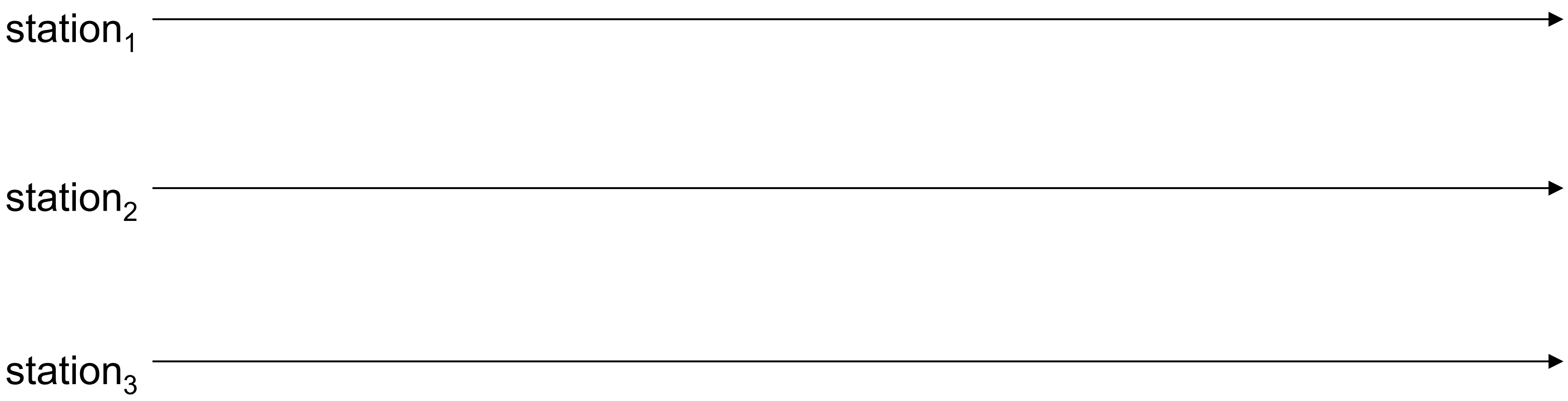
Their textbook is freely available as a download at http://secowinet.epfl.ch

Chapter 06, Module 04

IEEE 802.11 in a Nutshell

MAC

- Supports priorities:
  - SIFS/PIFS/DIFS in .11b,
  - additionally AIFS in .11e
- CSMA/CA
  - Binary exponential backoff algorithm

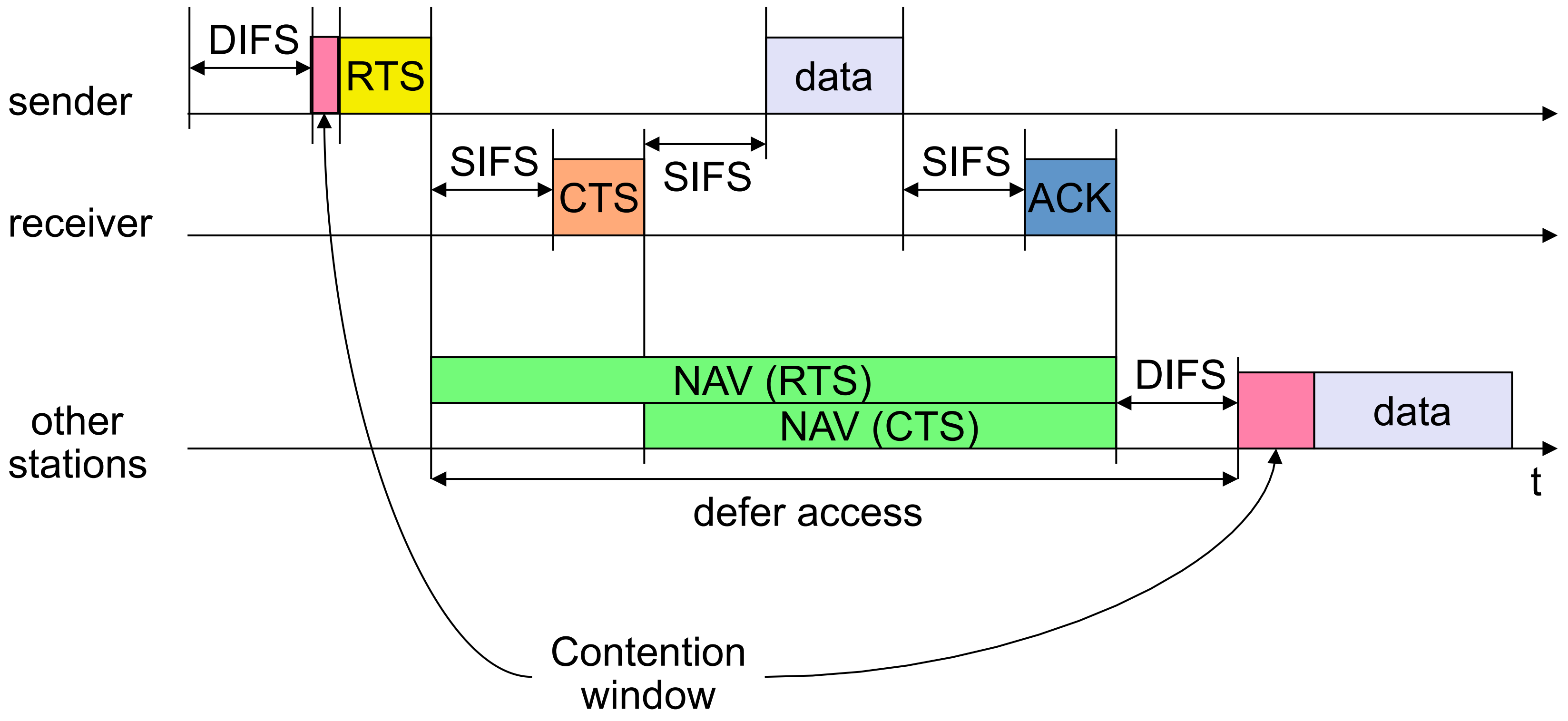


station_1

station_2

station_3

IEEE 802.11 in a Nutshell



Motivation for Cheater

Scenario: Internet access through public hotspots

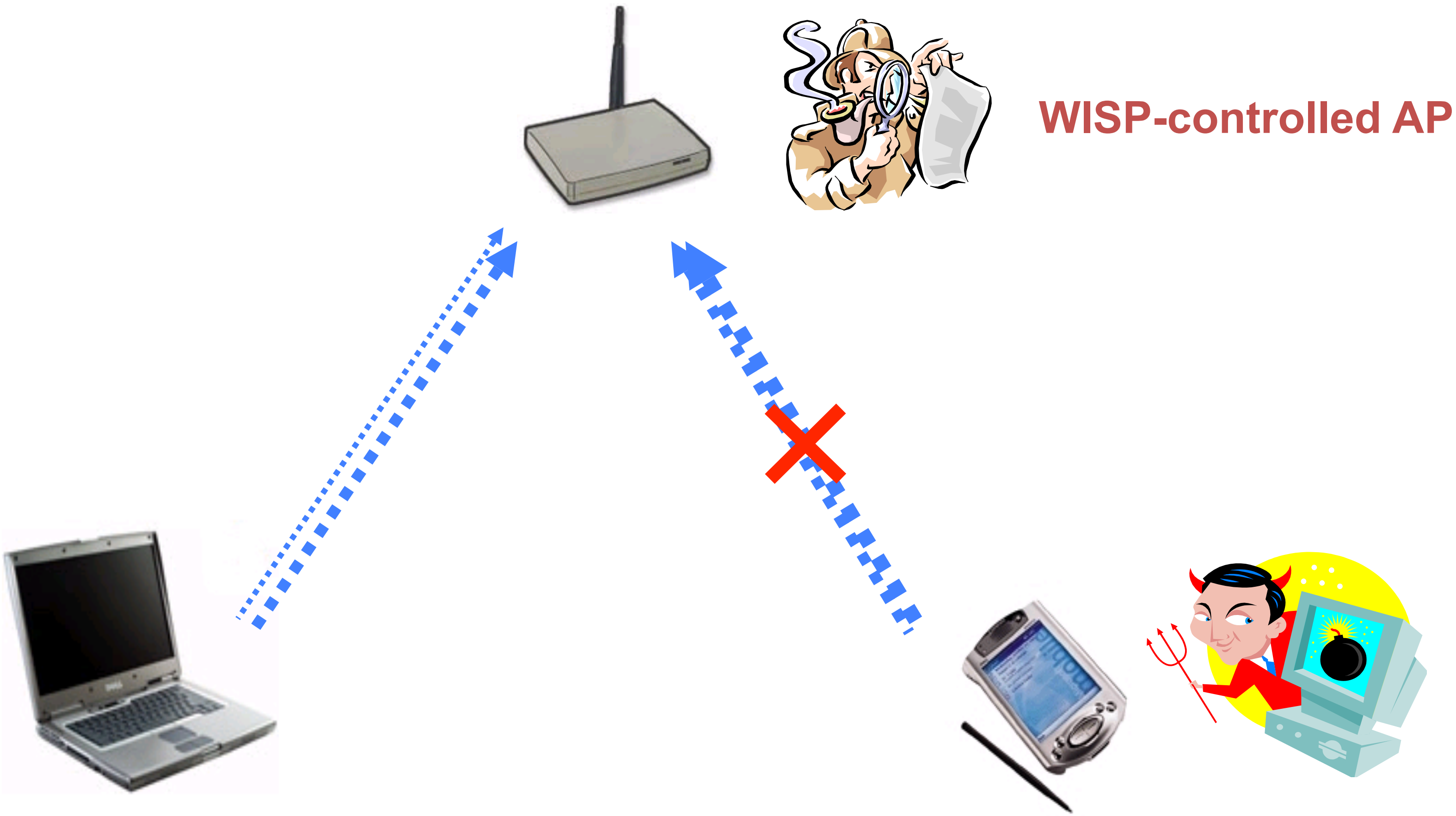
System model:

- Infrastructure mode, DCF (Distributed Coordination Function)
- Single trusted AP operated by a WISP
- Problem: misuse of protocols
  - Misbehavior is greedy as opposed to malicious
- What about MAC-layer misbehavior?
  - Considerable bandwidth gains
  - Hidden from the upper layers
  - Always usable

If the misbehavior is detected, the WISP can take measures

- But how to detect?

Example scenario



WISP-controlled AP

Well-behaved node

Well-behaved node

Cheated node

Misbehavior techniques – Overview

Uplink traffic (stations → AP)

- Example scenarios: backup, webcam, …

Downlink traffic (AP → stations)

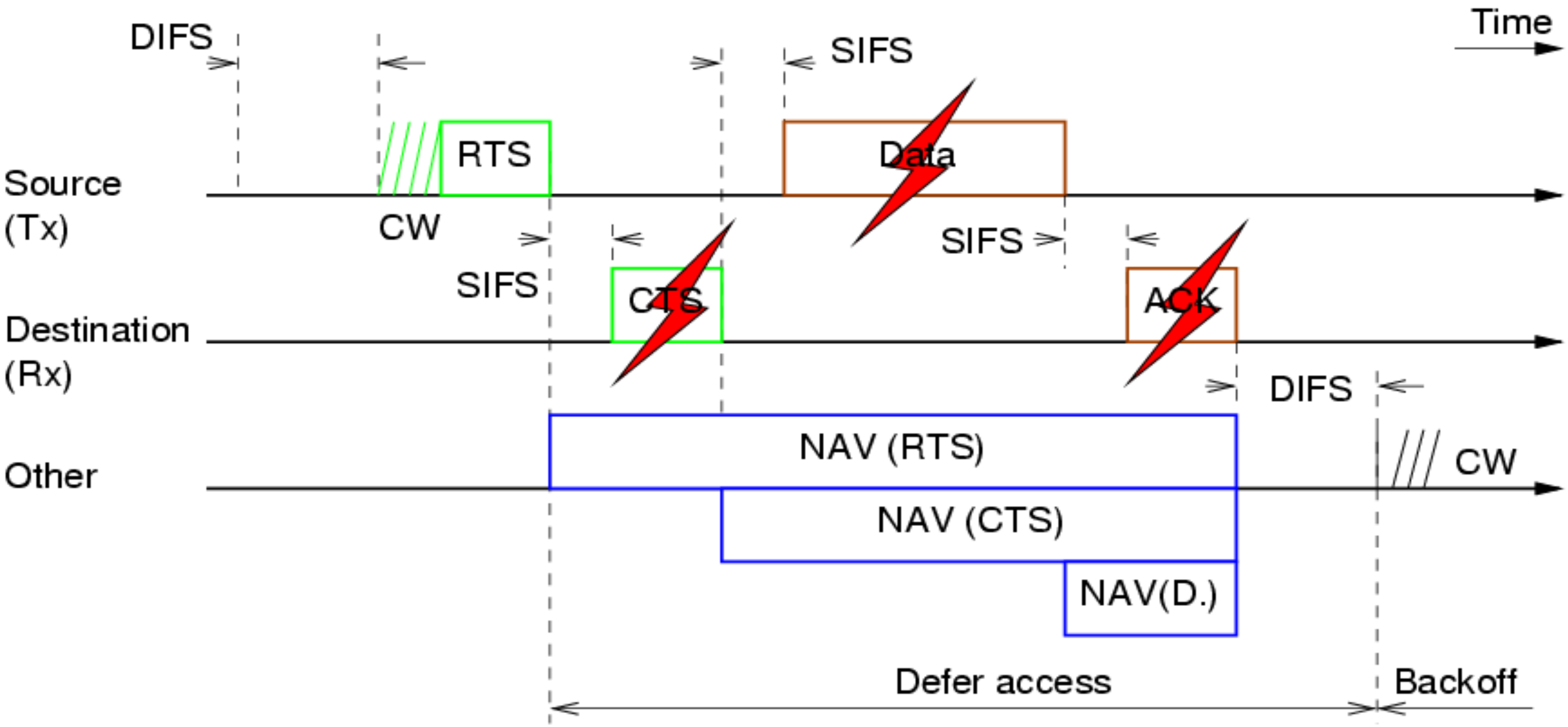
- Constitutes most of the wireless traffic
- Over 90% is TCP
- Example scenarios: Web browsing, FTP, video streaming, …

Subsequently, we discuss various kinds of greedy misbehaviour

One solution addressing these is:

- **http://domino.epfl.ch**

Uplink traffic – Frame scrambling



CW: Contention Window
SIFS: Short Inter–Frame Spacing
DIFS: Distributed Inter–Frame Spacing

RTS / CTS: Request To Send / Clear To Send
ACK: ACKnowledgement
NAV: Network Allocation Vector

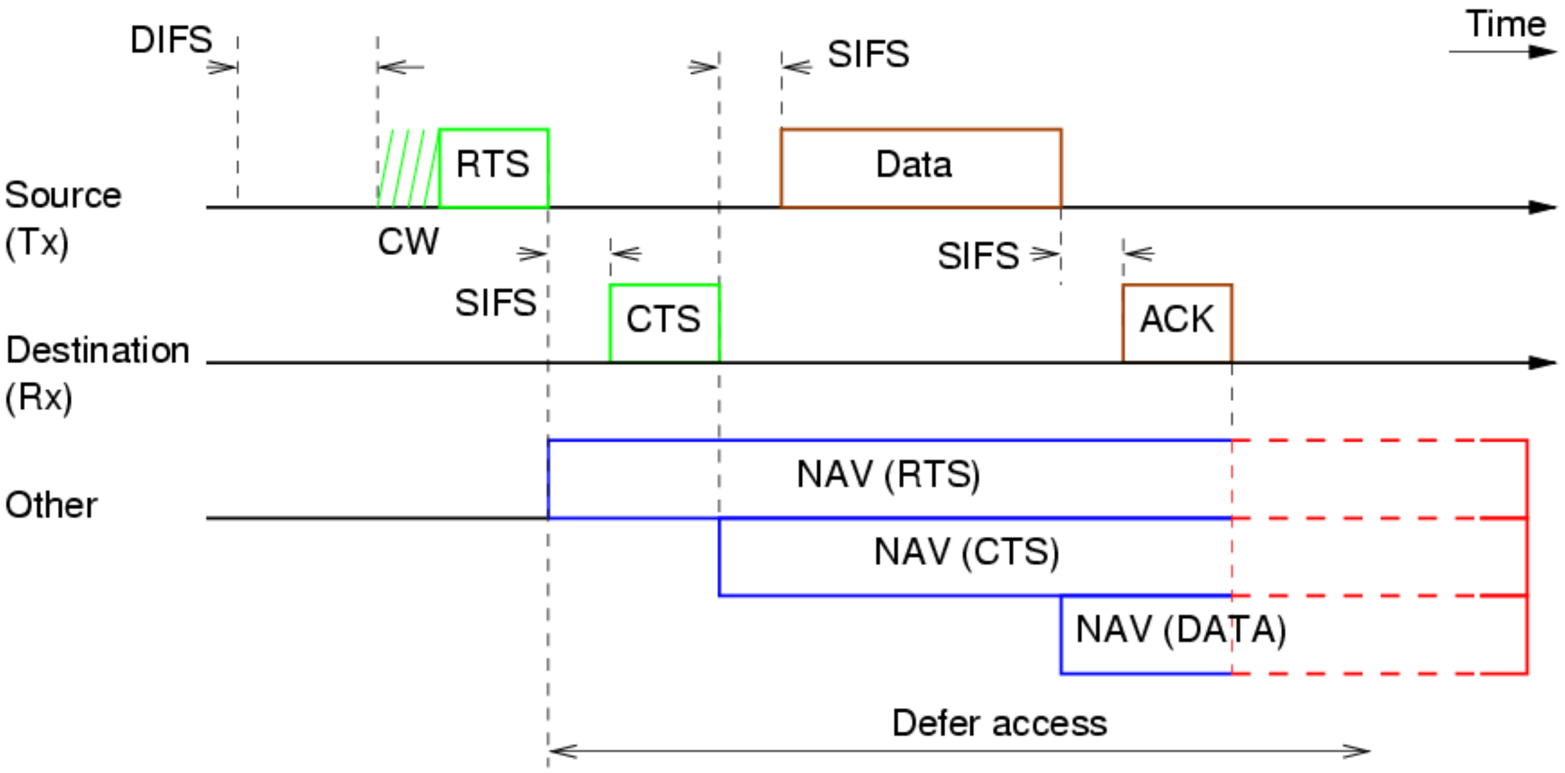
Problem & Solution
Frame scrambling

How to detect?

Solution: Number of retransmissions

- Lost frames are retransmitted
- Sequence numbers in the MAC header distinguish retransmissions
- Cheater's retransmissions are fewer than those of well-behaved stations
- By counting retransmissions, the AP can single out the cheater

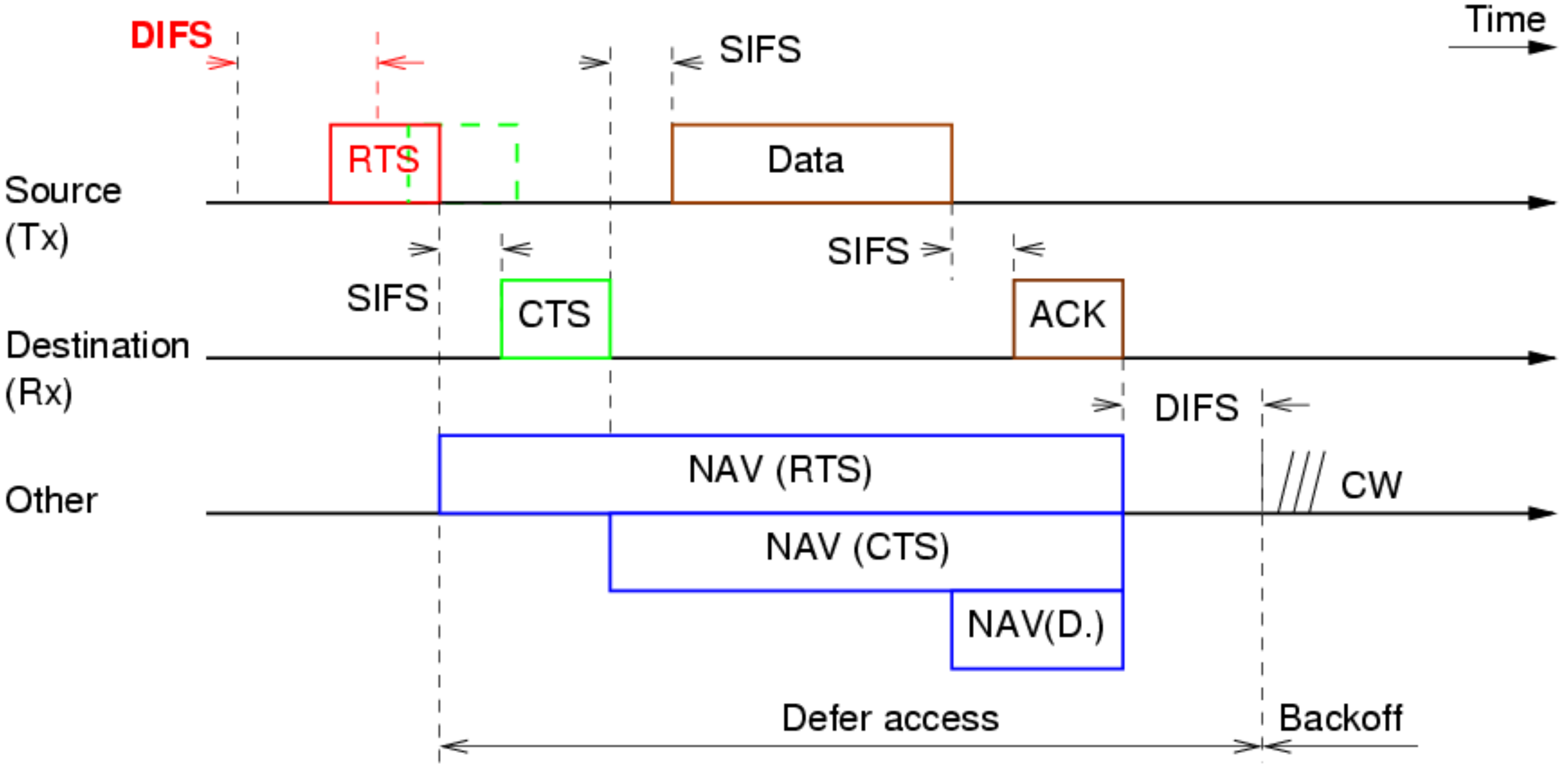
Uplink traffic – Oversized NAV



CW: Contention Window
SIFS: Short Inter–Frame Spacing
DIFS: Distributed Inter–Frame Spacing

RTS / CTS: Request To Send / Clear To Send
ACK: ACKnowledgement
NAV: Network Allocation Vector

Uplink traffic – Short DIFS



CW: Contention Window
SIFS: Short Inter–Frame Spacing
DIFS: Distributed Inter–Frame Spacing

RTS / CTS: Request To Send / Clear To Send
ACK: ACKnowledgement
NAV: Network Allocation Vector

Problem & Solution
Oversized NAV, Short DIFS

How to detect?

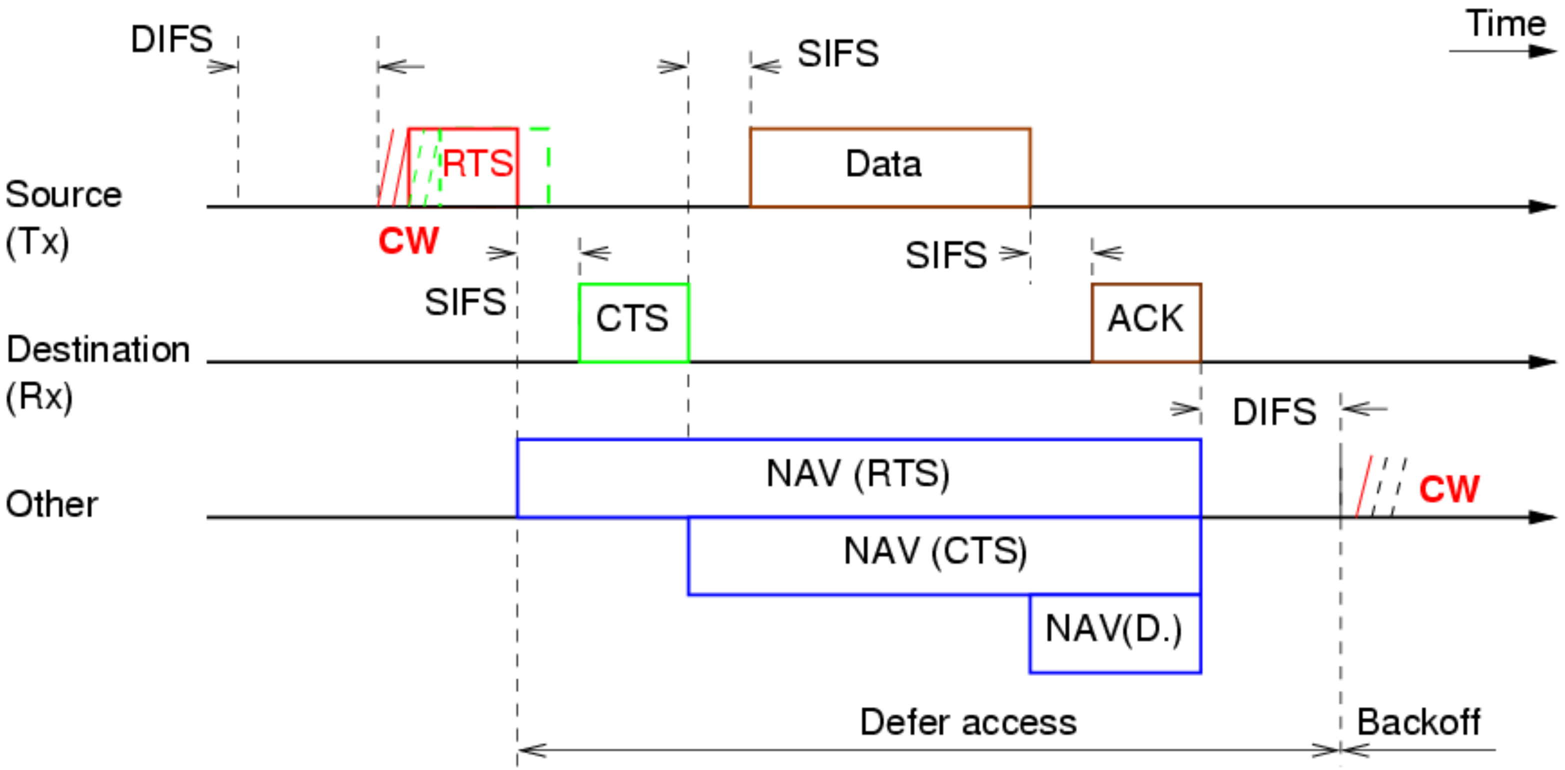
Solution: Comparison of NAVs

- AP measures the actual NAV and compares to the received one
- A repeated pattern of oversized NAVs distinguishes the cheater

Solution: Comparison of DIFS

- The value of DIFS is constant and provided by the IEEE 802.11 standard
- A short DIFS cannot be anything but the result of cheating

Uplink traffic – Backoff



CW: Contention Window
SIFS: Short Inter–Frame Spacing
DIFS: Distributed Inter–Frame Spacing

RTS / CTS: Request To Send / Clear To Send
ACK: ACKnowledgement
NAV: Network Allocation Vector

Problems & Solutions:

How to detect?

Backoff-tests

- Compare average back-off window size

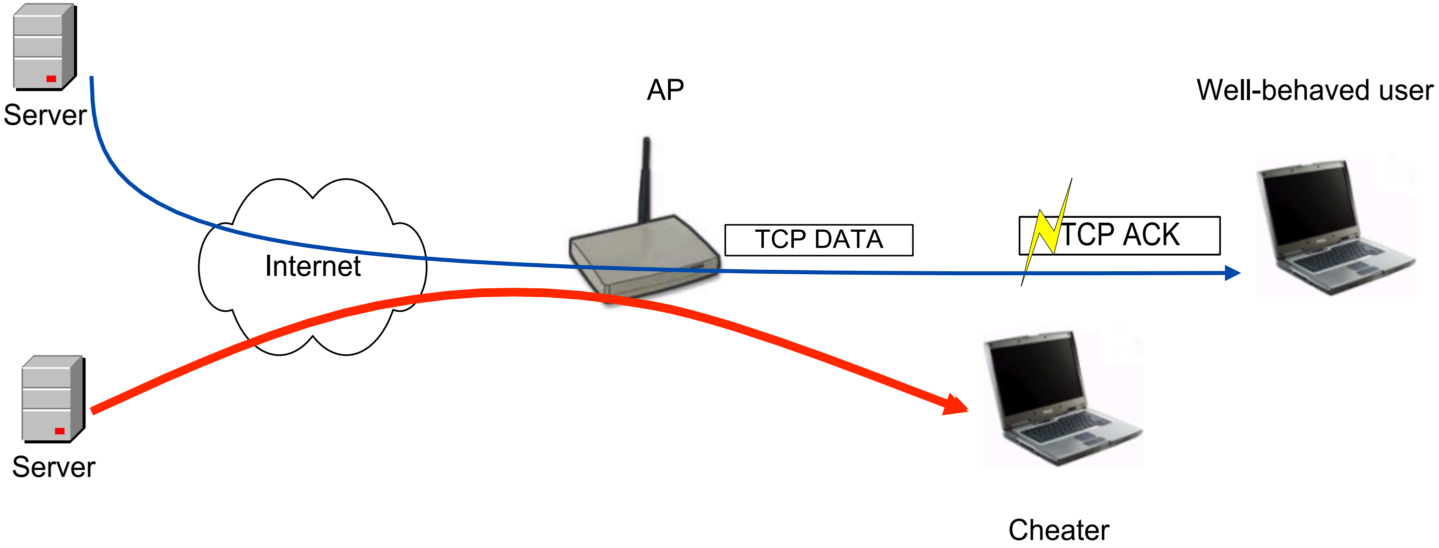
Downlink traffic – TCP ACK scrambling

Server receives no TCP ACK and slows down the TCP flow

Repeated scrambling kills the TCP connection

The AP receives less packets destined to the well-behaved station

Packets destined to the cheater are delayed less in AP’s queue

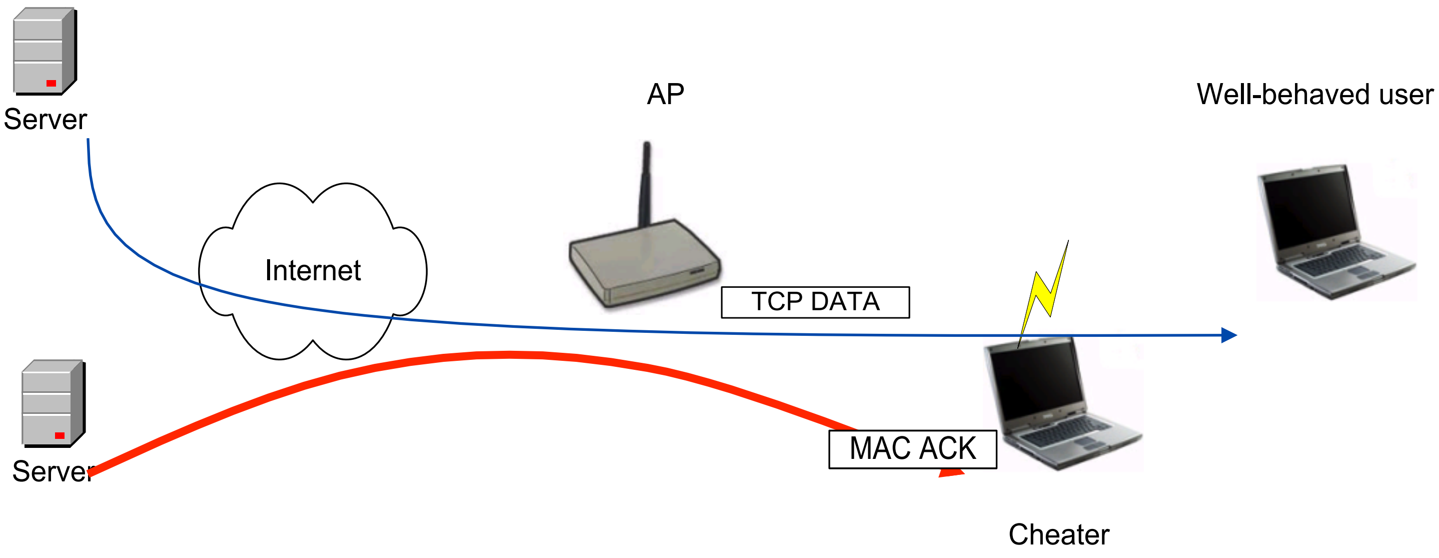


TCP DATA scrambling with MAC forging

Tries to kill the TCP connection like the previous attack

MAC ACK contains no source address

The forged MAC ACK prevents the AP from retransmitting the lost packet



Problems & Solutions:

How to detect?

Dummy frame injection

- AP periodically injects dummy frames destined to non- existing stations
- If it receives corresponding MAC ACKs, there is cheating
- Higher-layer mechanisms will identify the cheater (e.g., by monitoring the TCP flows of stations)

What Does Your Off-the-shelf Access Point Offer as Protection?

Source: http://owbg.wordpress.com/2011/04/01/zilch/

What do Commercial Vendors Offer in Terms of Protection?

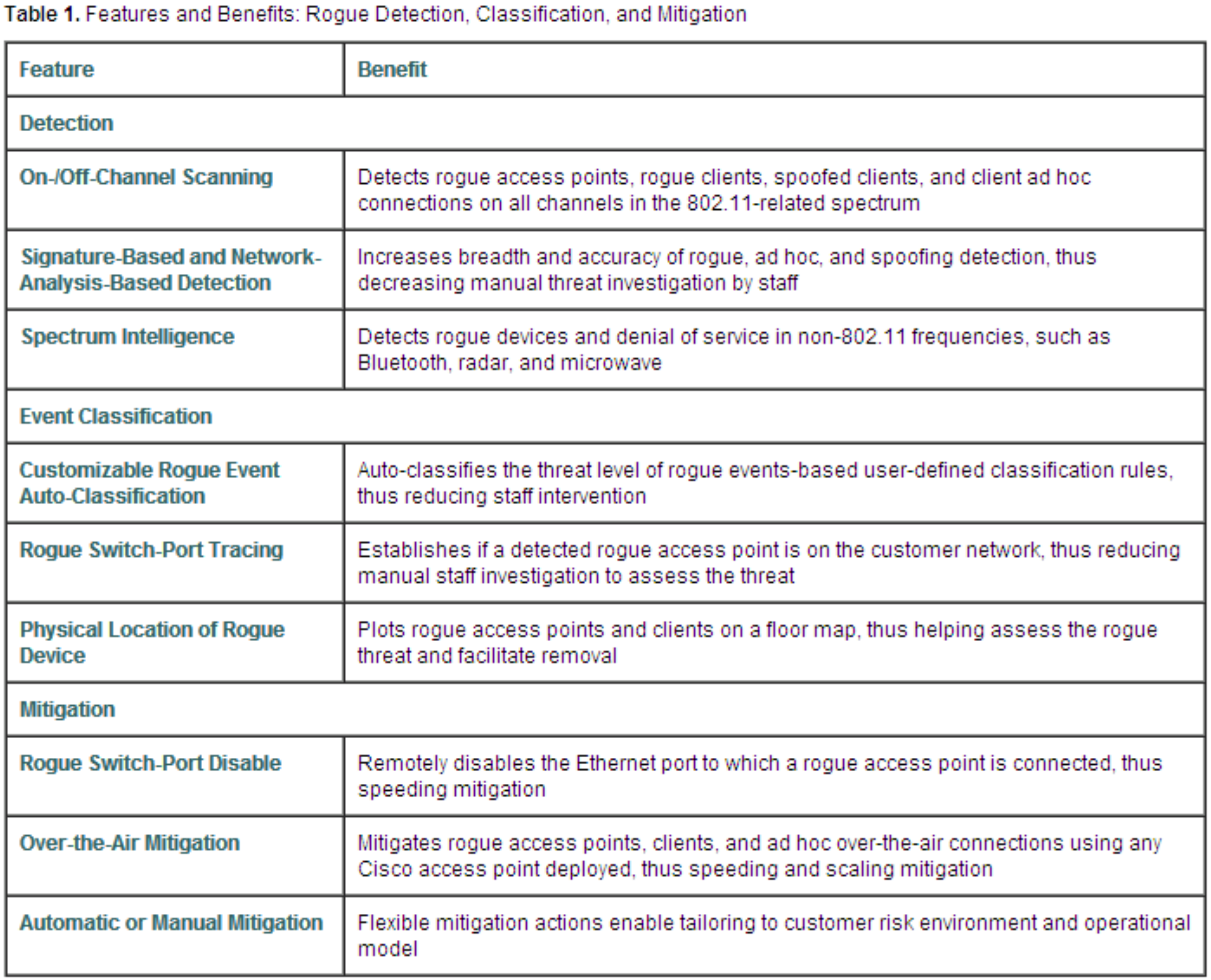


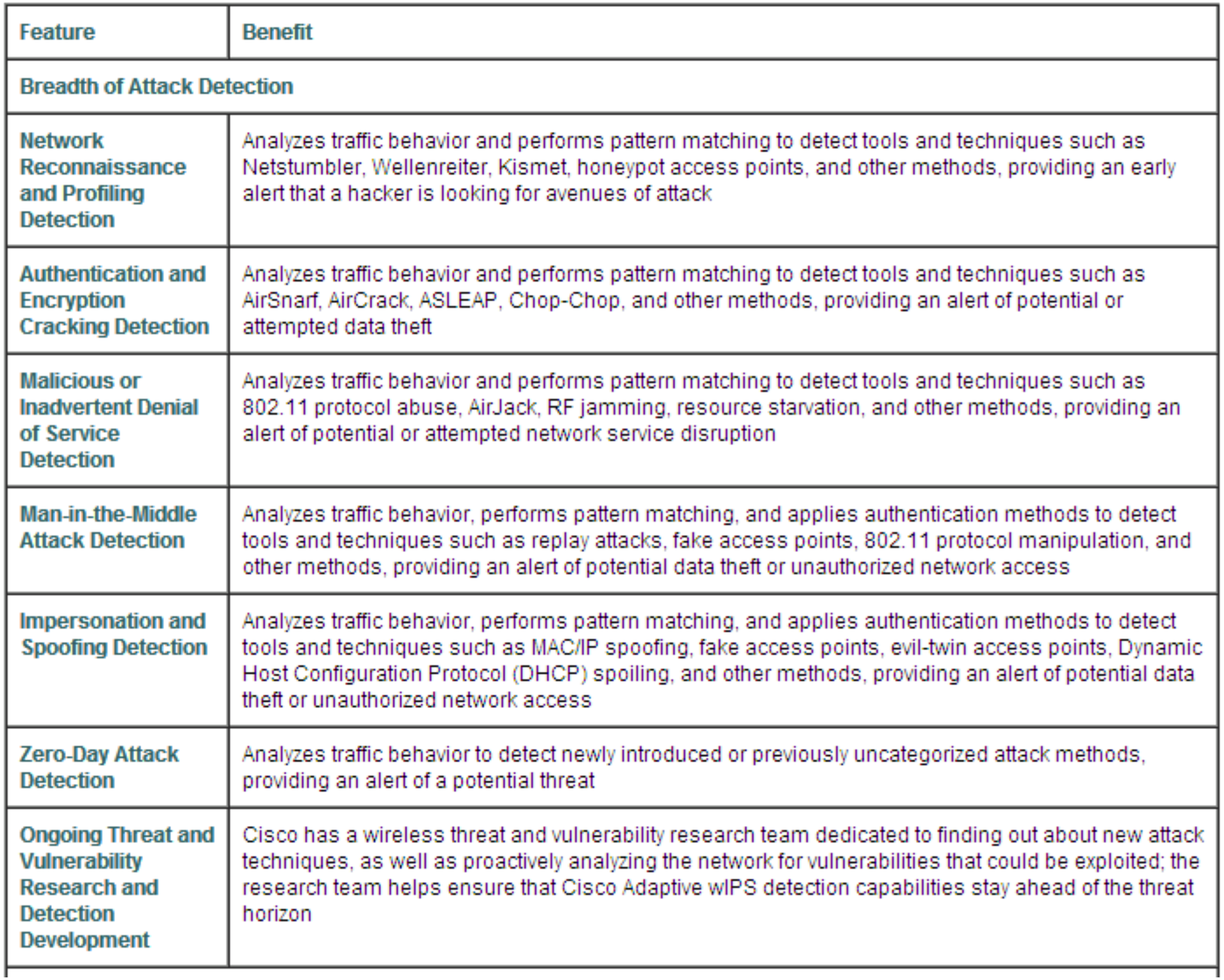
Table 1. Features and Benefits: Rogue Detection, Classification, and Mitigation

Feature	Benefit
Detection	
On-/Off-Channel Scanning	Detects rogue access points, rogue clients, spoofed clients, and client ad hoc connections on all channels in the 802.11-related spectrum
Signature-Based and Network-Analysis-Based Detection	Increases breadth and accuracy of rogue, ad hoc, and spoofing detection, thus decreasing manual threat investigation by staff
Spectrum Intelligence	Detects rogue devices and denial of service in non-802.11 frequencies, such as Bluetooth, radar, and microwave
Event Classification	
Customizable Rogue Event Auto-Classification	Auto-classifies the threat level of rogue events-based user-defined classification rules, thus reducing staff intervention
Rogue Switch-Port Tracing	Establishes if a detected rogue access point is on the customer network, thus reducing manual staff investigation to assess the threat
Physical Location of Rogue Device	Plots rogue access points and clients on a floor map, thus helping assess the rogue threat and facilitate removal
Mitigation	
Rogue Switch-Port Disable	Remotely disables the Ethernet port to which a rogue access point is connected, thus speeding mitigation
Over-the-Air Mitigation	Mitigates rogue access points, clients, and ad hoc over-the-air connections using any Cisco access point deployed, thus speeding and scaling mitigation
Automatic or Manual Mitigation	Flexible mitigation actions enable tailoring to customer risk environment and operational model

Source: http://www.cisco.com/en/US/prod/collateral/wireless/ps9733/ps9817/data_sheet_c78-501388.html

What do Commercial Vendors Offer in Terms of Protection?

Table 2. Features and Benefits: Over-the-Air Attack Detection



Feature	Benefit
Breadth of Attack Detection	
Network Reconnaissance and Profiling Detection	Analyzes traffic behavior and performs pattern matching to detect tools and techniques such as Netstumbler, Wellenreiter, Kismet, honeypot access points, and other methods, providing an early alert that a hacker is looking for avenues of attack
Authentication and Encryption Cracking Detection	Analyzes traffic behavior and performs pattern matching to detect tools and techniques such as AirSnarf, AirCrack, ASLEAP, Chop-Chop, and other methods, providing an alert of potential or attempted data theft
Malicious or Inadvertent Denial of Service Detection	Analyzes traffic behavior and performs pattern matching to detect tools and techniques such as 802.11 protocol abuse, AirJack, RF jamming, resource starvation, and other methods, providing an alert of potential or attempted network service disruption
Man-in-the-Middle Attack Detection	Analyzes traffic behavior, performs pattern matching, and applies authentication methods to detect tools and techniques such as replay attacks, fake access points, 802.11 protocol manipulation, and other methods, providing an alert of potential data theft or unauthorized network access
Impersonation and Spoofing Detection	Analyzes traffic behavior, performs pattern matching, and applies authentication methods to detect tools and techniques such as MAC/IP spoofing, fake access points, evil-twin access points, Dynamic Host Configuration Protocol (DHCP) spoiling, and other methods, providing an alert of potential data theft or unauthorized network access
Zero-Day Attack Detection	Analyzes traffic behavior to detect newly introduced or previously uncategorized attack methods, providing an alert of a potential threat
Ongoing Threat and Vulnerability Research and Detection Development	Cisco has a wireless threat and vulnerability research team dedicated to finding out about new attack techniques, as well as proactively analyzing the network for vulnerabilities that could be exploited; the research team helps ensure that Cisco Adaptive wIPS detection capabilities stay ahead of the threat horizon

Source: http://www.cisco.com/en/US/prod/collateral/wireless/ps9733/ps9817/data_sheet_c78-501388.html

Acks & Recommended Reading

Selected slides of this chapter courtesy of

- Levente Buttyán and Jean-Pierre Hubaux , ETHZ & EPFL
- Jochen Schiller, FU Berlin

Recommended reading

- [KaPeSp2002] Charlie Kaufman, Radia Perlman, Mike Speciner: Network Security – Private Communication in a Public World, 2nd Edition, Prentice Hall, 2002, ISBN: 978-0-13-046019-6
- [Stallings2015] William Stallings, Network Security Essentials, 4th Edition, Prentice Hall, 2015, ISBN: 978-0-136-10805-4
- [Schäfer2003] G. Schäfer. Netzsicherheit - Algorithmische Grundlagen und Protokolle. dpunkt.verlag, 2003.

Copyright Notice

Contact

Prof. Dr.-Ing. Matthias Hollick
Department of Computer Science

SEEMOO
Mornewegstr. 32
64293 Darmstadt/Germany
matthias.hollick@seemoo.tu-darmstadt.de

Phone +49 6151 16-70920
Fax +49 6151 16-70921
www.seemoo.tu-darmstadt.de