ulm university universität
uulm

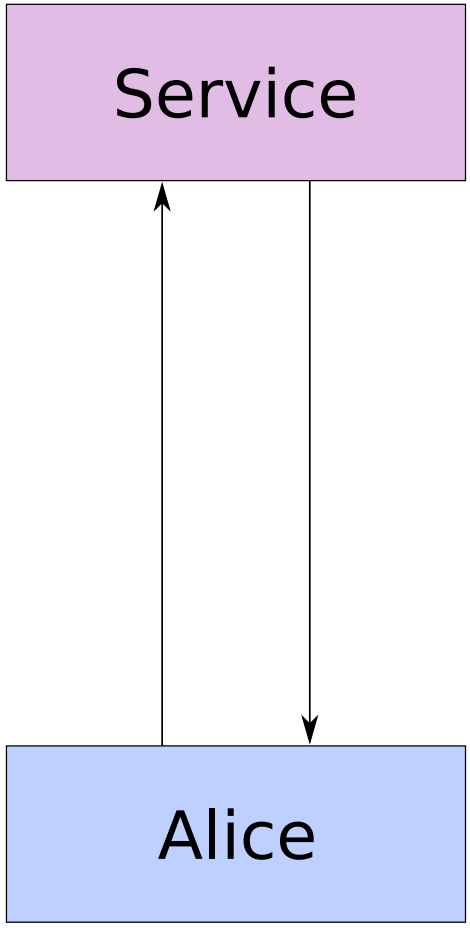
Evaluation of the 802.11w Amendment for existing DoS attacks

Dominik Lang | September 14, 2011

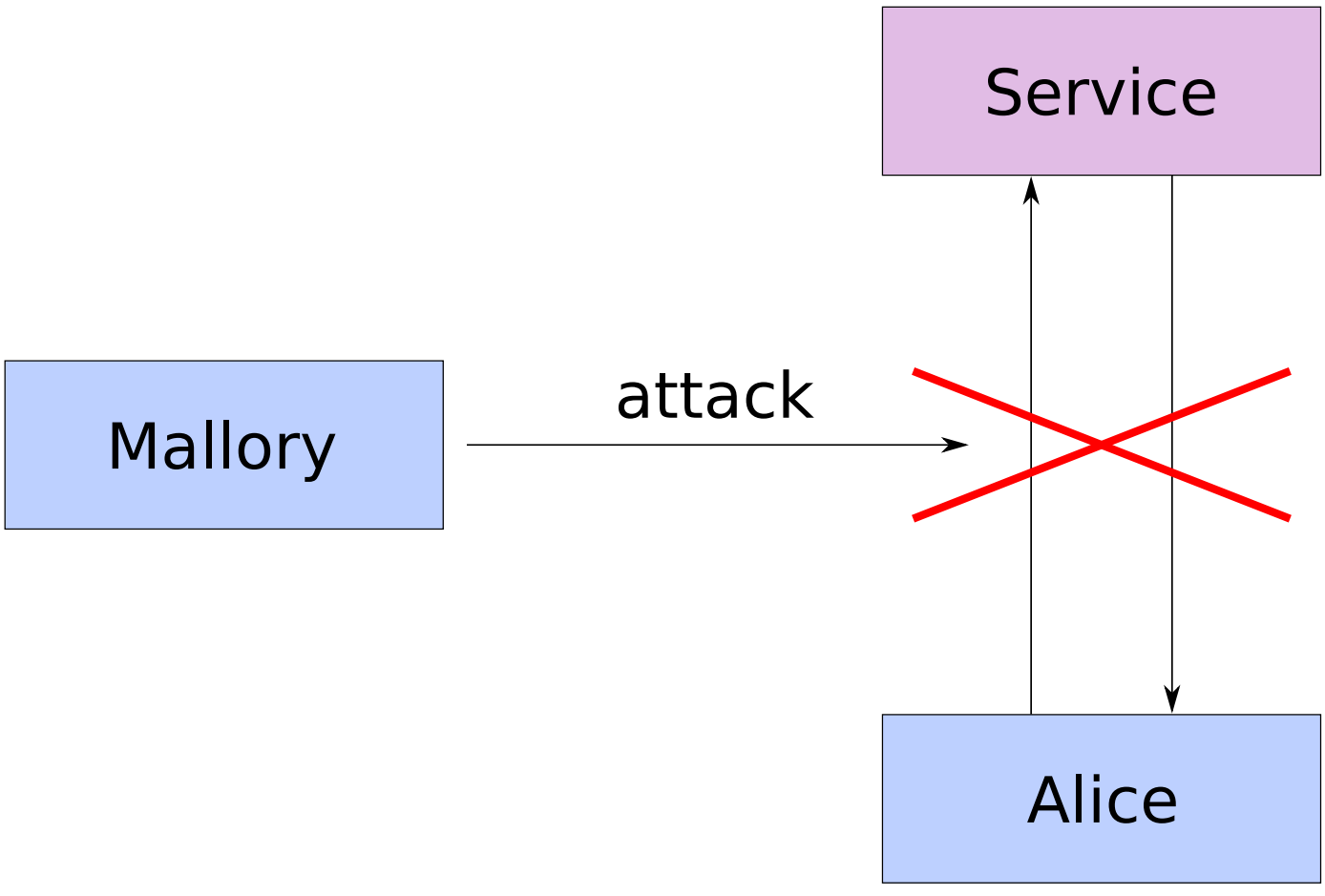
Overview

Evaluation of the 802.11w Amendment for existing DoS attacks

Denial of Service (DoS) attacks



Denial of Service (DoS) attacks



Implications for WLANs

- Disconnect somebody from the network for fun and profit
- Disconnect services
  - Monitoring services
  - Alarm services
  - Security services
- Compromise of infrastructure

Evaluation of the 802.11w Amendment for existing DoS attacks

IEEE 802.11 brief overview

Frame Types

- Data frames
  - Actual data

IEEE 802.11 brief overview

Frame Types

- Data frames
  - Actual data
- Control frames
  - Insures reliability
  - For example:
    - ACK
    - RTS
    - CTS

IEEE 802.11 brief overview

Frame Types

- Data frames
  - Actual data
- Control frames
  - Insures reliability
  - For example:
    - ACK
    - RTS
    - CTS
- Management frames
  - Compensates openness of the radio medium
  - Provides information of the WLAN
  - For example:
    - Authentication / Deauthentication
    - Association / Disassociation
    - Beacon

IEEE 802.11 brief overview

Security services

- Data frames
  - Pre-RSNA:
    - WEP
    - Open System authentication
    - Shared Key authentication

IEEE 802.11 brief overview

Security services

- Data frames
  - Pre-RSNA:
    - WEP
    - Open System authentication
    - Shared Key authentication
  - RSNA:
    - TKIP (WPA)
    - CCMP (WPA2)
    - 802.1X / EAP

IEEE 802.11 brief overview

Security services

- Data frames
  - Pre-RSNA:
    - WEP
    - Open System authentication
    - Shared Key authentication
  - RSNA:
    - TKIP (WPA)
    - CCMP (WPA2)
    - 802.1X / EAP
- Control frames
  - None
- Management frames
  - None

Attacks

Deauthentication attack

- Forge Deauthentication frame from / to a target station

Attacks

Deauthentication attack

- Forge Deauthentication frame from / to a target station

Association Request attack

- Forge an invalid Association Request
- AP may deauthenticate the target station as a result

Attacks

Deauthentication attack

- Forge Deauthentication frame from / to a target station

Association Request attack

- Forge an invalid Association Request
- AP may deauthenticate the target station as a result

Channel Switch attack

- Forge Channel Switch Announcement
- Trick stations to change to a channel out of reach

Attacks

Deauthentication attack

- Forge Deauthentication frame from / to a target station

Association Request attack

- Forge an invalid Association Request
- AP may deauthenticate the target station as a result

Channel Switch attack

- Forge Channel Switch Announcement
- Trick stations to change to a channel out of reach

Quiet attack

- Forge Quiet functionality
- Trick stations to be silent for a period of time

Evaluation of the 802.11w Amendment for existing DoS attacks

802.11w

- Adds protection for Management frames
- RSNA CCMP (WPA2) required
- Protection varies for:
  - Unicast frames
  - Multicast frames
- Protects:
  - Deauthentication frames
  - Disassociation frames
  - Action frames

Unicast Protection

- Same protection as for unicast Data frames
  $\rightarrow$ CCMP
- Security Association (SA) Query procedure to protect against Association Request attacks

Multicast Protection

Broadcast Integrity Protocol (BIP)

- New integrity and replay protection protocol
  - Message Integrity Code (MIC)
  - Integrity Packet Number (IPN)
- No confidentiality and authentication

Multicast Protection

Broadcast Integrity Protocol (BIP)

- New integrity and replay protection protocol
  - Message Integrity Code (MIC)
  - Integrity Packet Number (IPN)
- No confidentiality and authentication

General implications for attacks

- Prevents outsider attacks
- Insider attacks still possible

802.11w in the real world

Proprietary vendor support

- None
- Matthew Gast: Vendor Support soon
  - WiFi Alliance working on Vendor support [a]
  - 802.11w code should show up soon [b]

---

[a] https://mobile.twitter.com/matthewsgast/status/83337692632465408
[b] https://mobile.twitter.com/matthewsgast/status/104252556695453698

802.11w in the real world

Proprietary vendor support

- None
- Matthew Gast: Vendor Support soon
  - WiFi Alliance working on Vendor support [a]
  - 802.11w code should show up soon [b]

[a] https://mobile.twitter.com/matthewsgast/status/83337692632465408
[b] https://mobile.twitter.com/matthewsgast/status/104252556695453698

Cisco CCXv5 MFP

- Based on an early draft
- Protection of Deauthentication, Disassociation and QoS frames
- Broadcast frames are forbidden

802.11w in the real world

Open Source

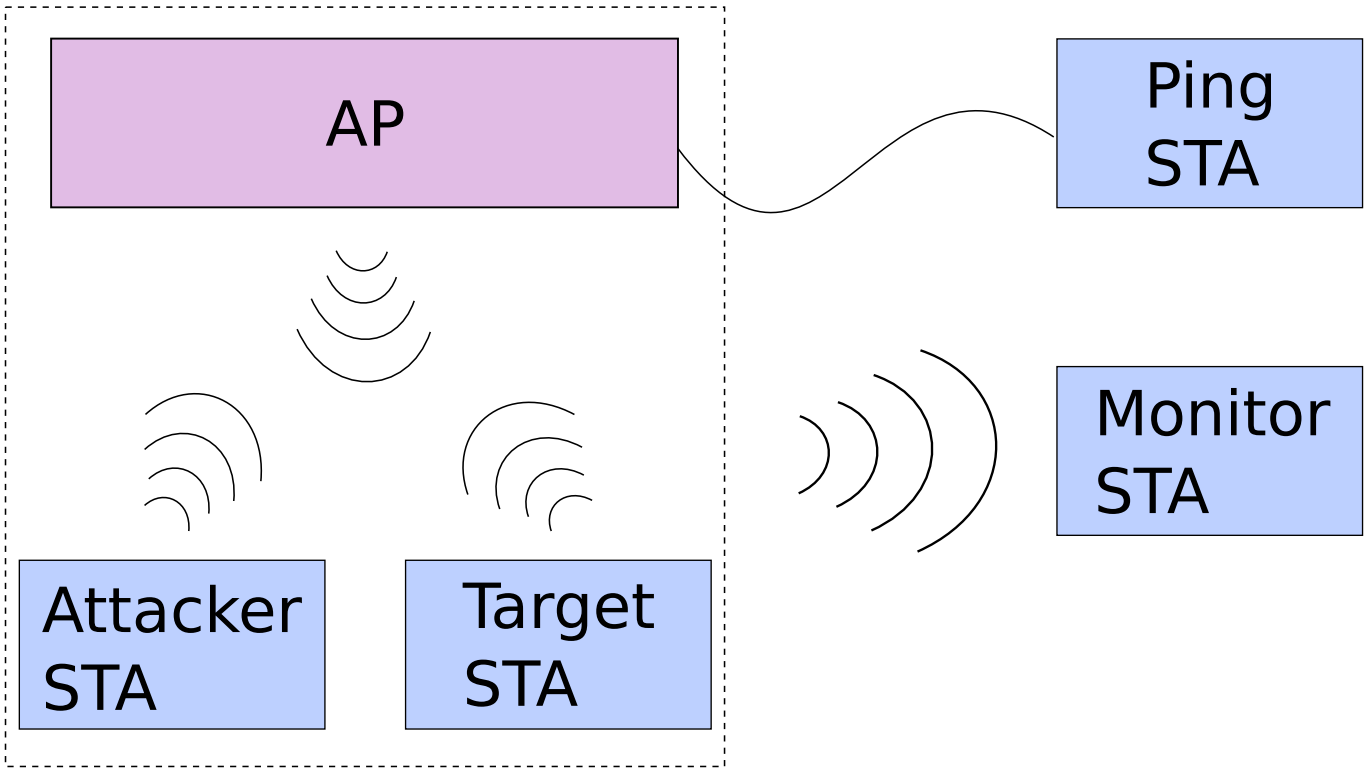
- Linux:
  - mac80211
  - wpa_supplicant / hostapd
- OpenBSD:
  - Not used by drivers
    $\rightarrow$ Established connection between drivers and 802.11w code

Evaluation of the 802.11w Amendment for existing DoS attacks

Practical Tasks

- Implementation of various tools
  - Attack tools
  - Analysis tools
- Test with and without 802.11w
- Get 802.11w up and running

Test setup



Test setup

Some further details

- Pre-802.11w tests:
  - RSNA CCMP
- 802.11w tests:
  - RSNA CCMP as amended by 802.11w
- Ping and Monitor were the same device

Test procedure for station attacks

Reference value measurement

- 5 seconds of traffic capture

Test procedure for station attacks

Reference value measurement

- 5 seconds of traffic capture

Deauthentication attack

- Unicast, 10 per second
- Broadcast, 10 per second

Test procedure for station attacks

Reference value measurement

- 5 seconds of traffic capture

Deauthentication attack

- Unicast, 10 per second
- Broadcast, 10 per second

Channel Switch attack

- Valid channel out of reach
- Invalid channel out of reach

Test procedure for station attacks

Reference value measurement

- 5 seconds of traffic capture

Deauthentication attack

- Unicast, 10 per second
- Broadcast, 10 per second

Channel Switch attack

- Valid channel out of reach
- Invalid channel out of reach

Quiet attack

- Duration field set to 1000 (= 1.024 sec.)
- Duration field set to 65535 (= 67.11 sec.)

Test procedure for access point attacks

Test procedure

- Wild things happen

Test procedure for access point attacks

Test procedure

- Wild things happen
- Attack ...
- ... and observe

Test procedure for access point attacks

Test procedure

- Wild things happen
- Attack ...
- ... and observe

Association Request attack variations

- invalid Supported Rates IE
- invalid Supported Rates IE + RSN IE without 802.11w
- invalid Supported Rates IE + RSN IE with 802.11w

Tested Hardware

Pre-802.11w laptops

Windows 7	Broadcom BCM4322
Windows 7	Atheros 5008X
Mac5.1 OS X 10.6.7	Broadcom BCM4322
Mac3.1 OS X 10.6.7	Atheros AR5416
Linux Ubuntu 10.04	Broadcom BCM4322
OpenBSD 4.8	Intel iwl 5100

Tested Hardware

Pre-802.11w laptops

Windows 7	Broadcom BCM4322
Windows 7	Atheros 5008X
Mac5.1 OS X 10.6.7	Broadcom BCM4322
Mac3.1 OS X 10.6.7	Atheros AR5416
Linux Ubuntu 10.04	Broadcom BCM4322
OpenBSD 4.8	Intel iwl 5100

Pre-802.11w mobile devices

Android 2.3.4	HTC Desire
Android 2.3.4	Nexus S
iOS 4.3.3	iPhone 3gs
iOS 4.3.3	iPod Touch 2
iOS 4.3.3	iPad2

Tested Hardware

802.11w stations

- Modified OpenBSD 4.8 with an iwn driver (Intel)
- Linux with an ath9k driver (Atheros)

Tested Hardware

802.11w stations

- Modified OpenBSD 4.8 with an iwn driver (Intel)
- Linux with an ath9k driver (Atheros)

Pre-802.11w access points

- Airport Express
- OpenWrt (TP-Link)
- Vodafone DSL-EasyBox 602
- Netgear DGND330B

Tested Hardware

802.11w stations

- Modified OpenBSD 4.8 with an iwn driver (Intel)
- Linux with an ath9k driver (Atheros)

Pre-802.11w access points

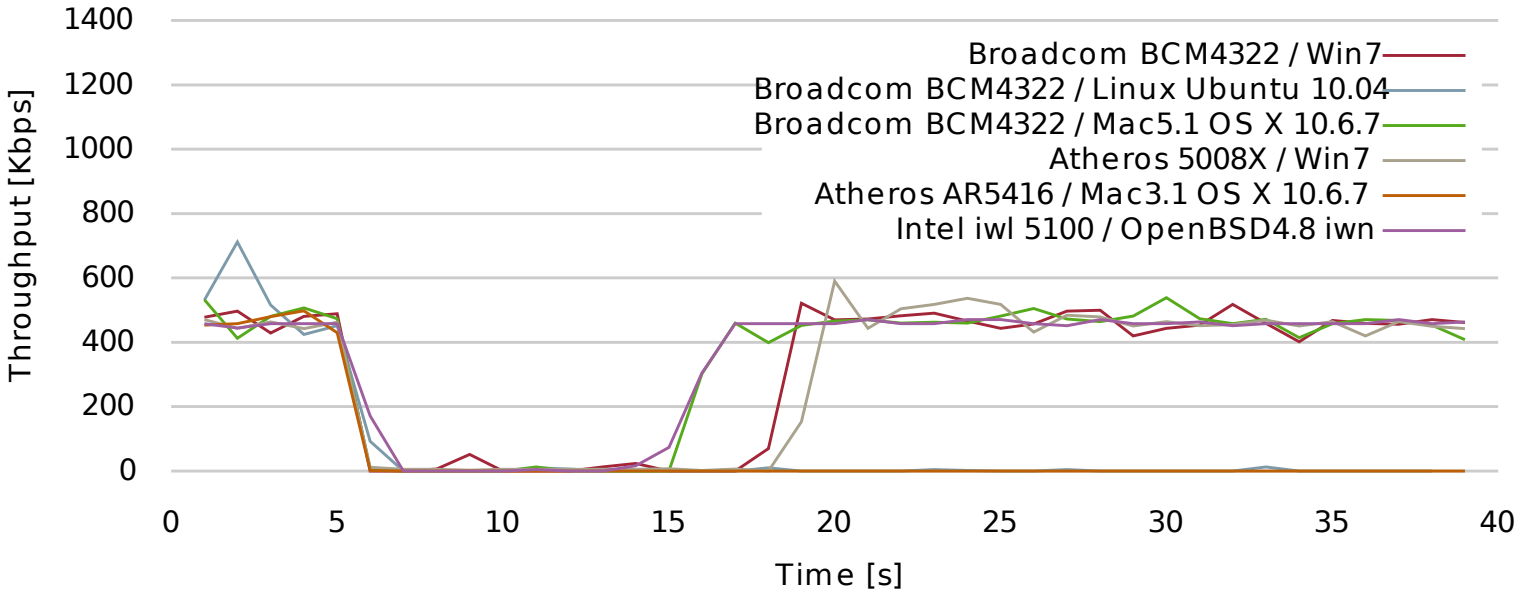
- Airport Express
- OpenWrt (TP-Link)
- Vodafone DSL-EasyBox 602
- Netgear DGND330B

802.11w access point

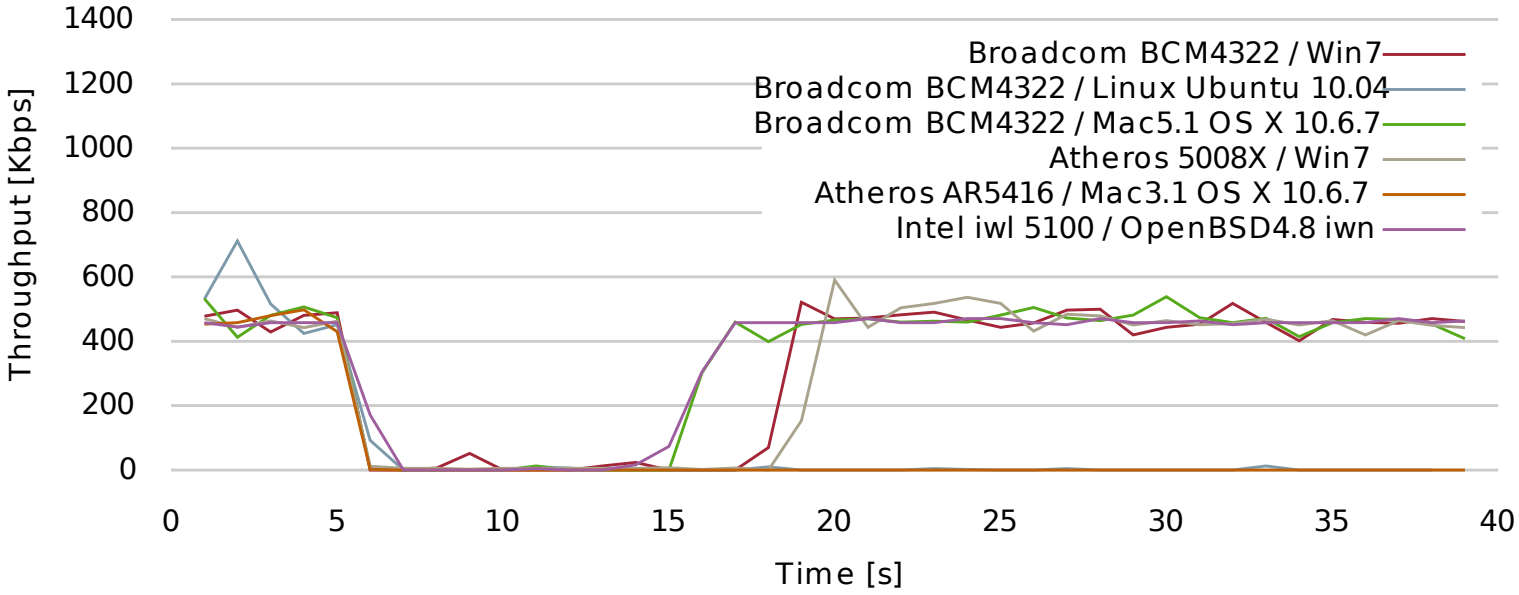
- OpenWrt (TP-Link)

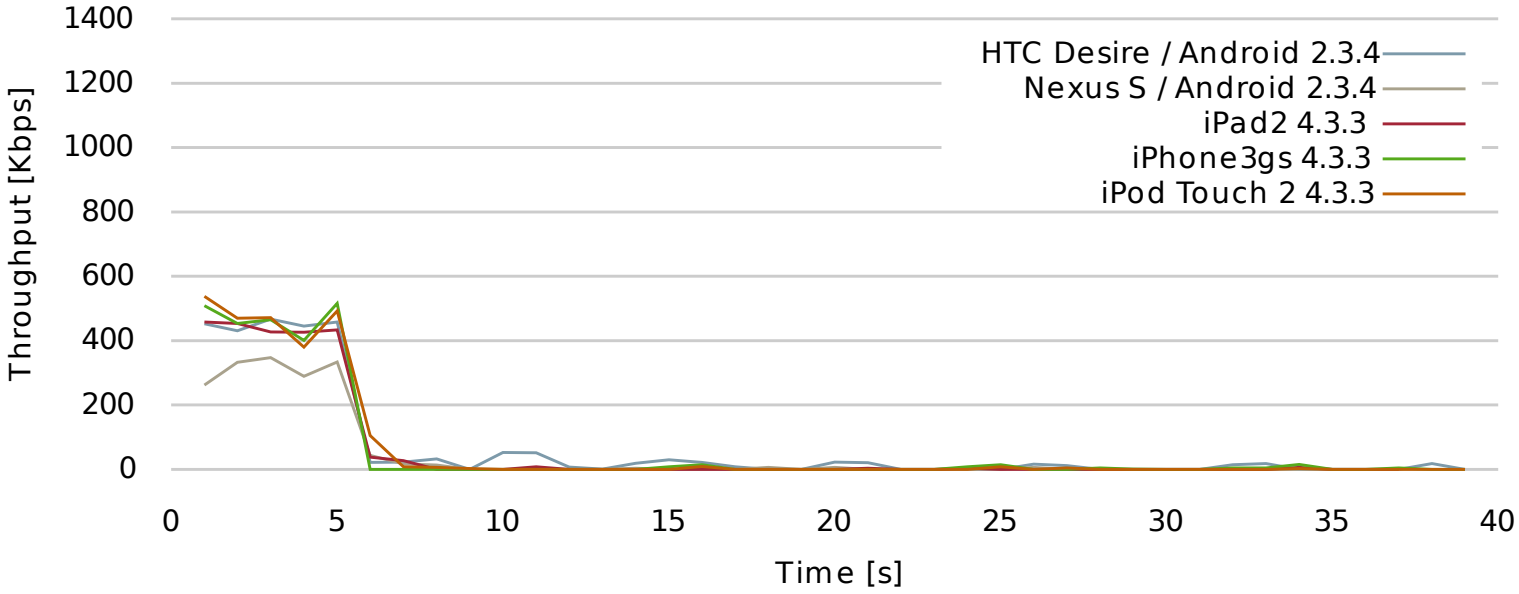
Evaluation of the 802.11w Amendment for existing DoS attacks

Pre-802.11w unicast Deauthentication attack

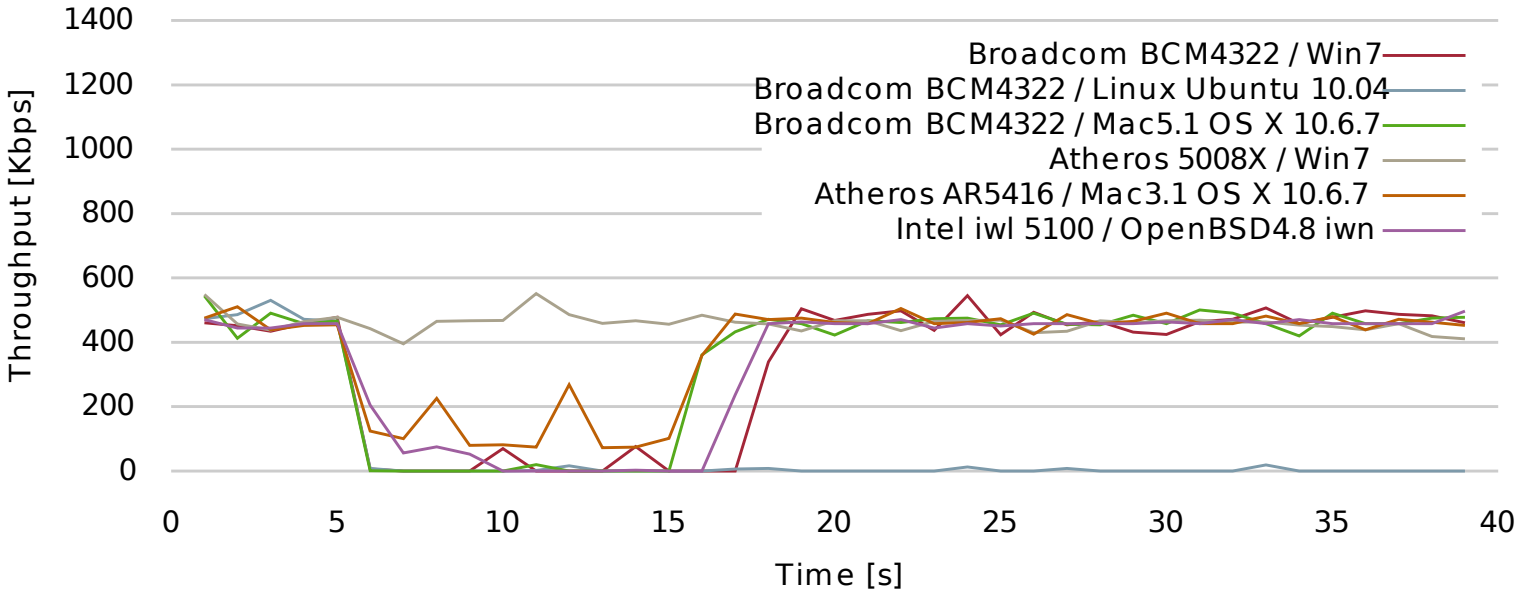


Pre-802.11w unicast Deauthentication attack

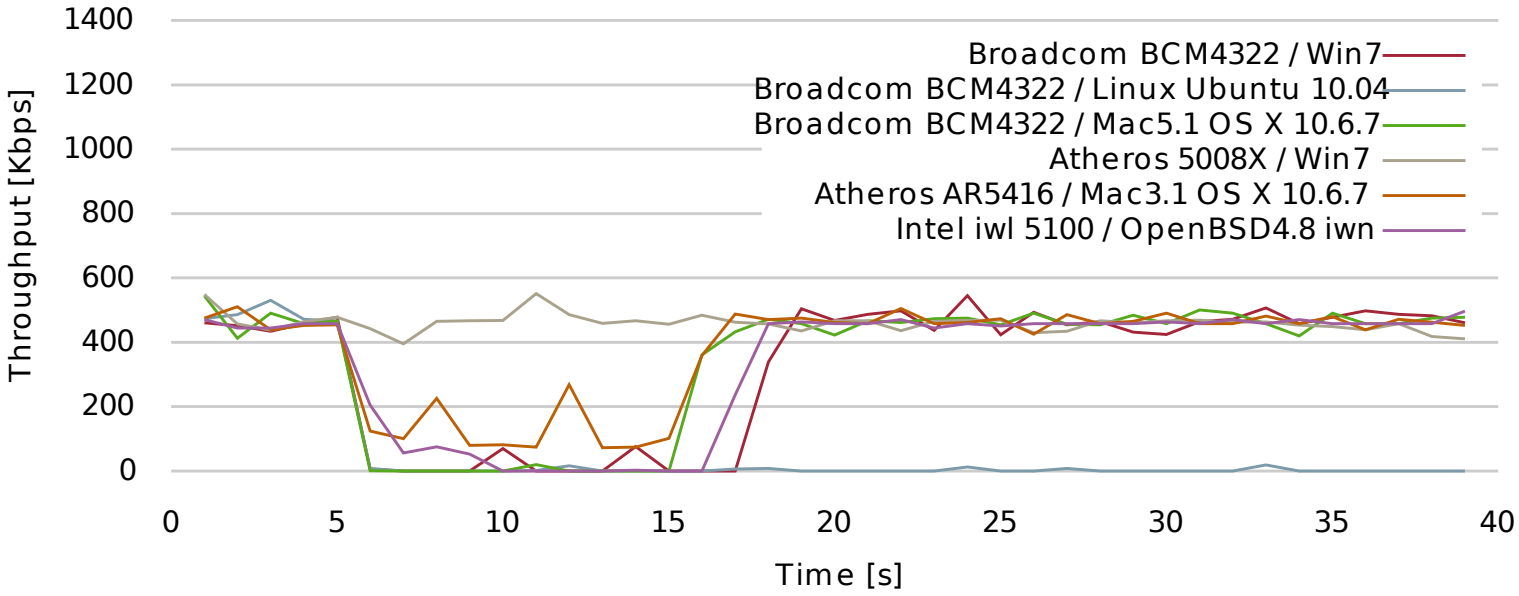


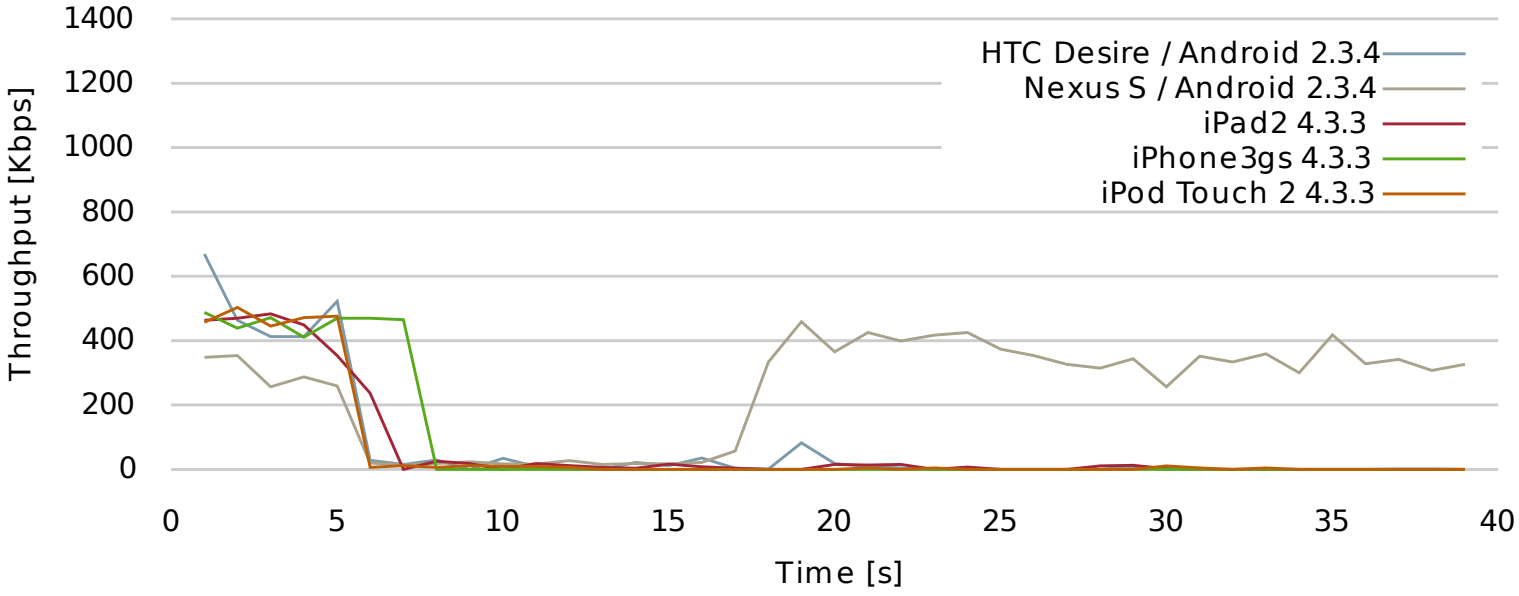


Pre-802.11w broadcast Deauthentication attack

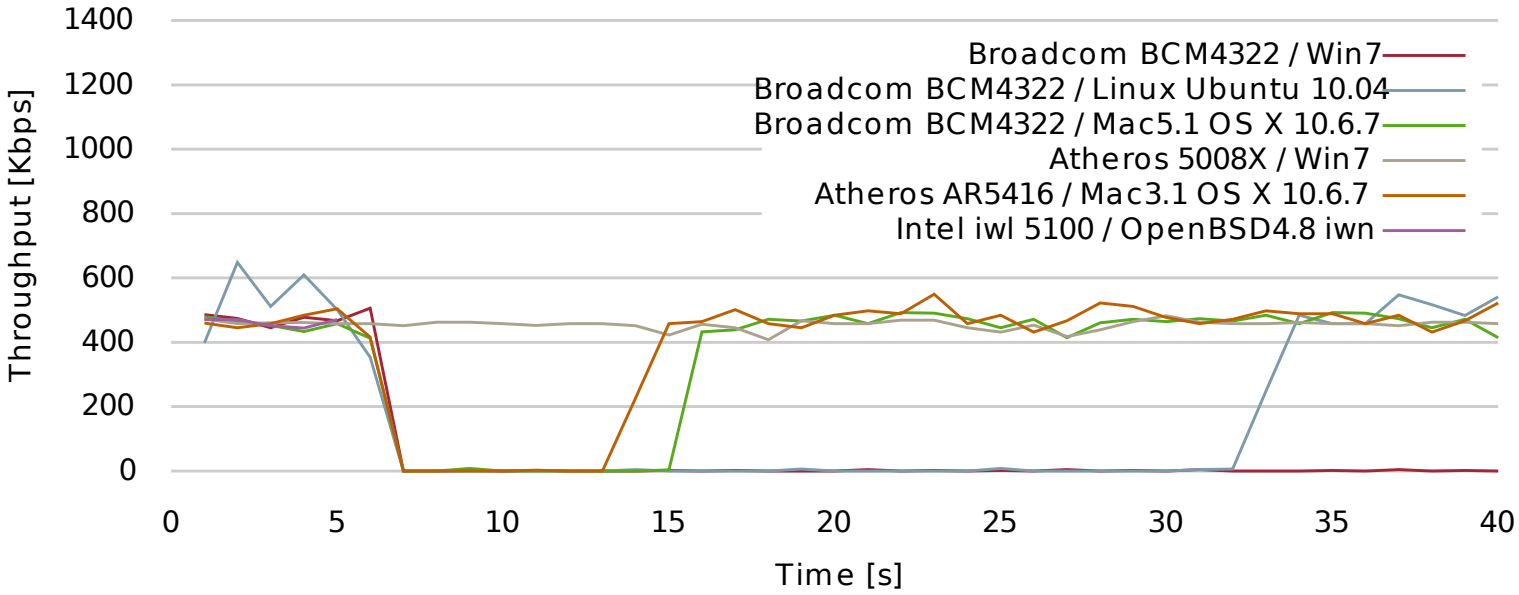


Pre-802.11w broadcast Deauthentication attack

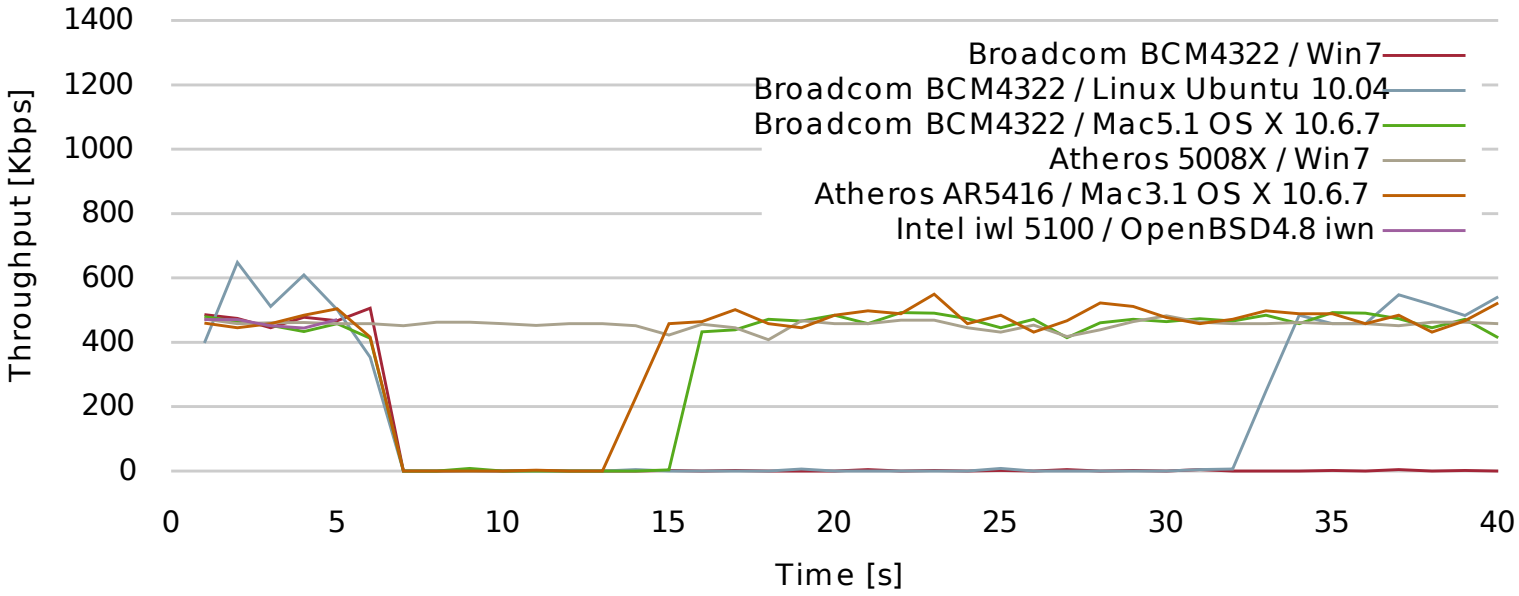


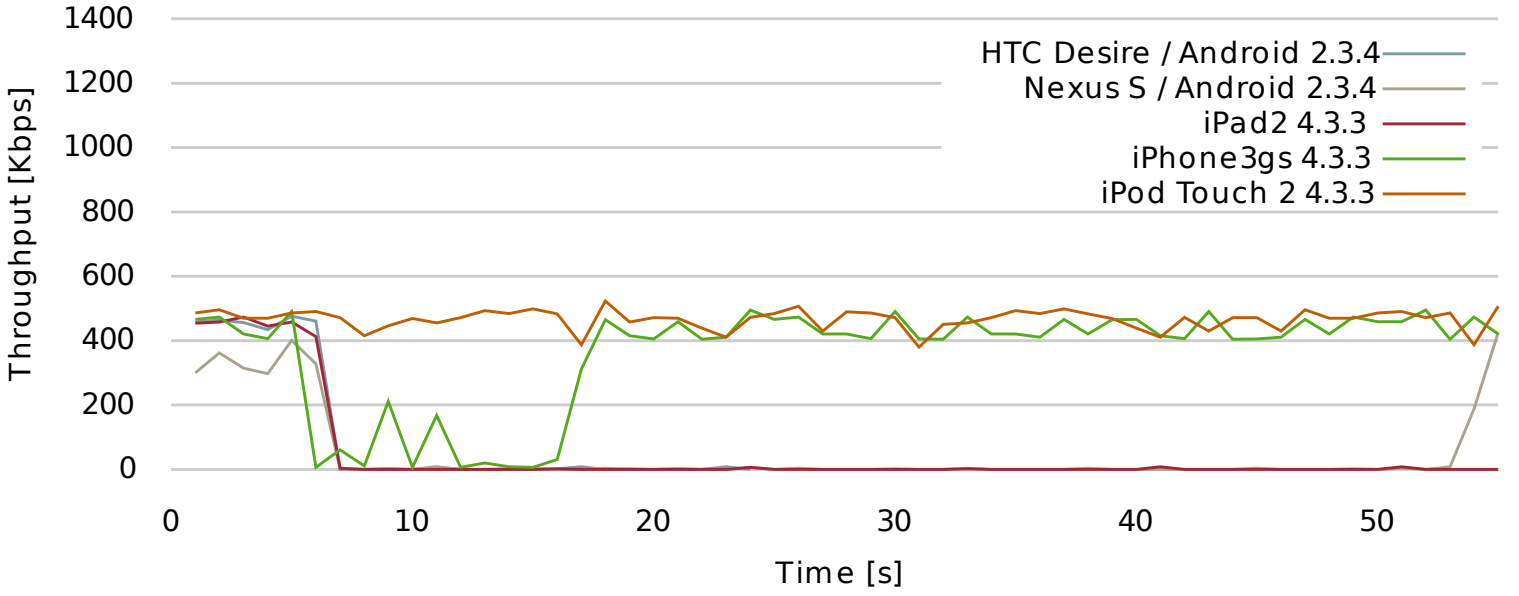


Pre-802.11w valid channel Channel Switch attack



Pre-802.11w valid channel Channel Switch attack





Pre-802.11w invalid channel Channel Switch and Quiet attack

Invalid channel Channel Switch attack

- OpenBSD 4.8 iwn
- Ignored by the rest

Pre-802.11w invalid channel Channel Switch and Quiet attack

Invalid channel Channel Switch attack

- OpenBSD 4.8 iwn
- Ignored by the rest

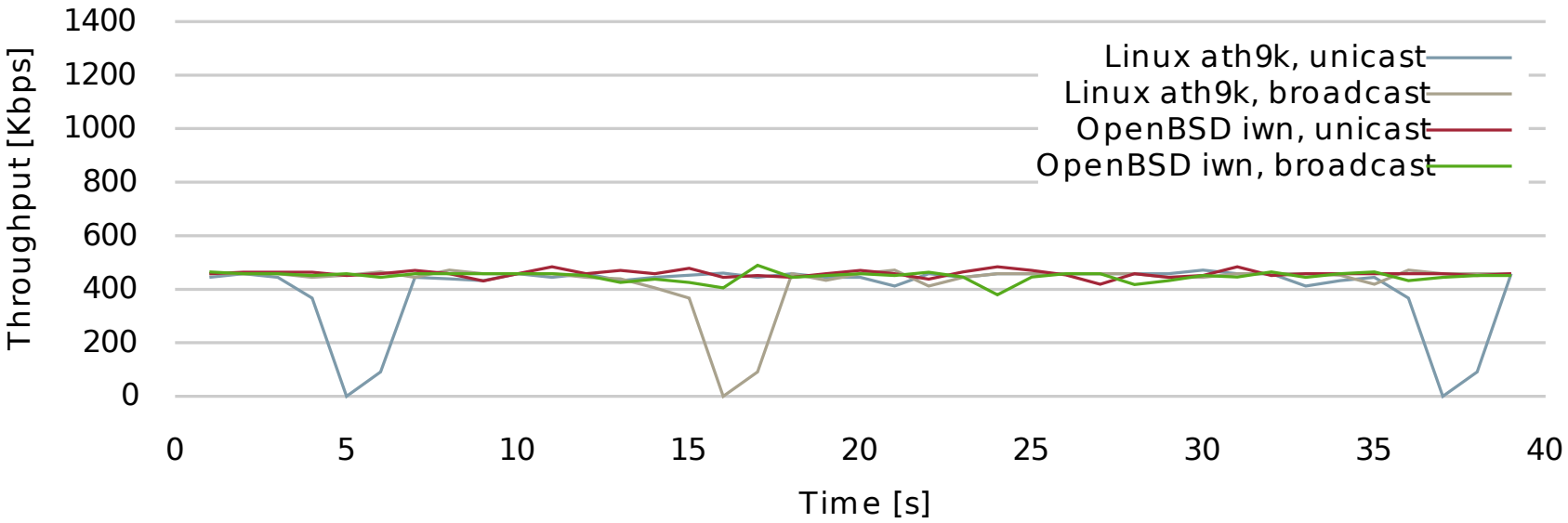
Quiet attack

- No effect at any station

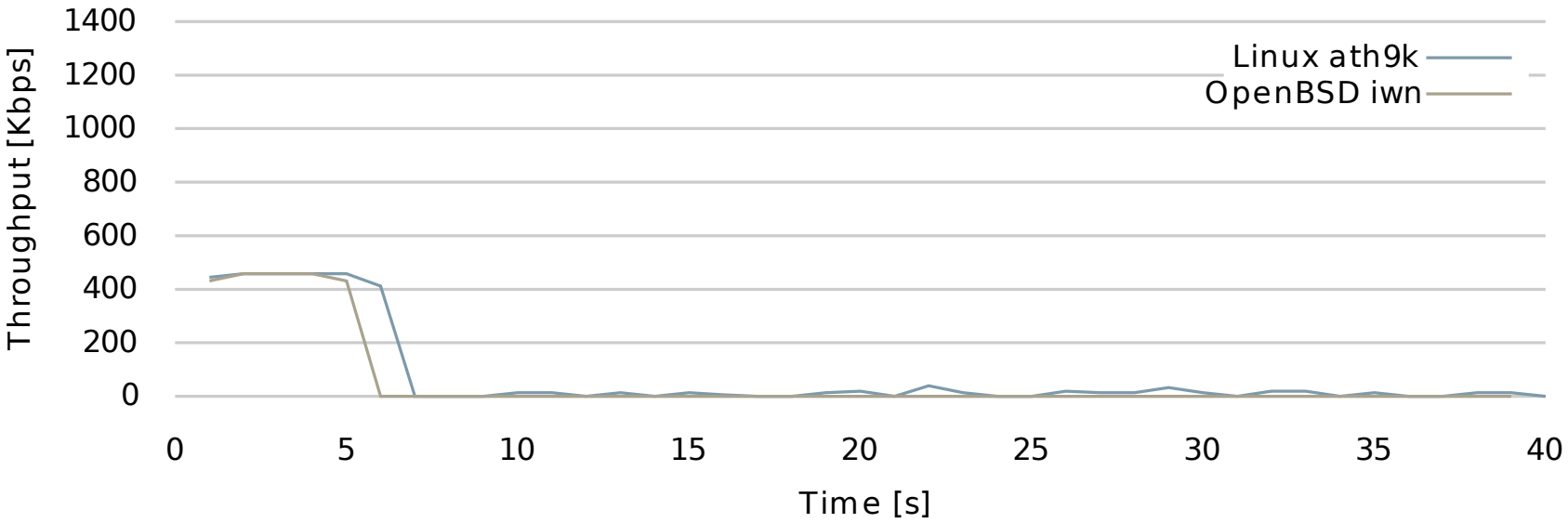
Summary

	Unicast Deauth.	Broadcast Deauth.	Channel Switch	Quiet
Broadcom BCM4322 / Win7	●	●	●	
Broadcom BCM4322 / Linux Ubuntu 10.04	●	●	●	
Broadcom BCM4322 / Mac5.1 OS X 10.6.7	●	●	●	
Atheros 5008X / Win7	●			
Atheros AR5416 / Mac3.1 OS X 10.6.7	●	●	●	
Intel iwl 5100 / OpenBSD 4.8	●	●	●	
HTC Desire / Android 2.3.4	●	●	●	
Nexus S / Android 2.3.4	●	●	●	
iPad 2 4.3.3	●	●	●	
iPhone 3gs 4.3.3	●	●	●	
iPod Touch 2 4.3.3	●	●		

802.11w Deauthentication attacks



802.11w Channel Switch attacks



Summary

	Unicast Deauth.	Broadcast Deauth.	Channel Switch	Quiet
Linux ath9k			●	
OpenBSD iwn			●	

Pre-802.11w access point Association Request attacks

Airport Express

- All variations caused same effect
- $\sim$**6 sec.** DoS at target station

Pre-802.11w access point Association Request attacks

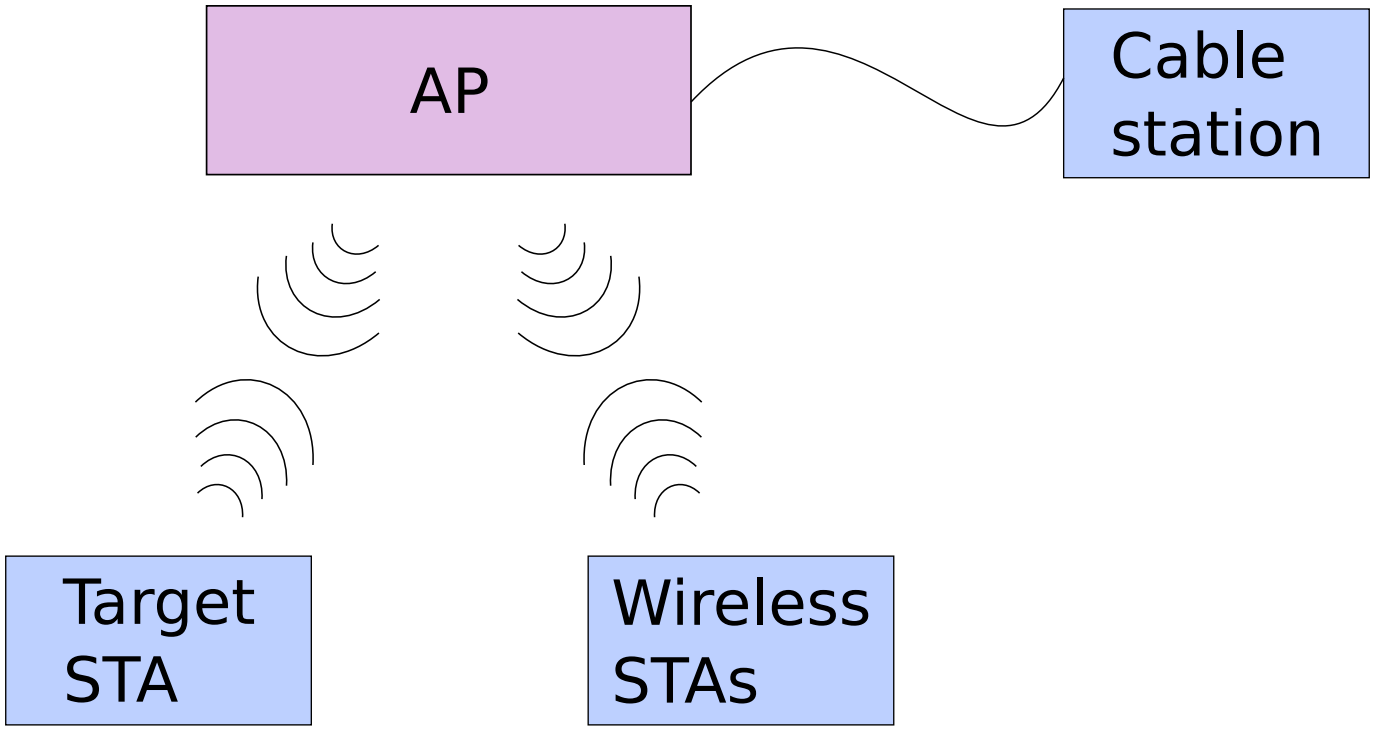
Airport Express

- All variations caused same effect
- ∼**6 sec.** DoS at target station

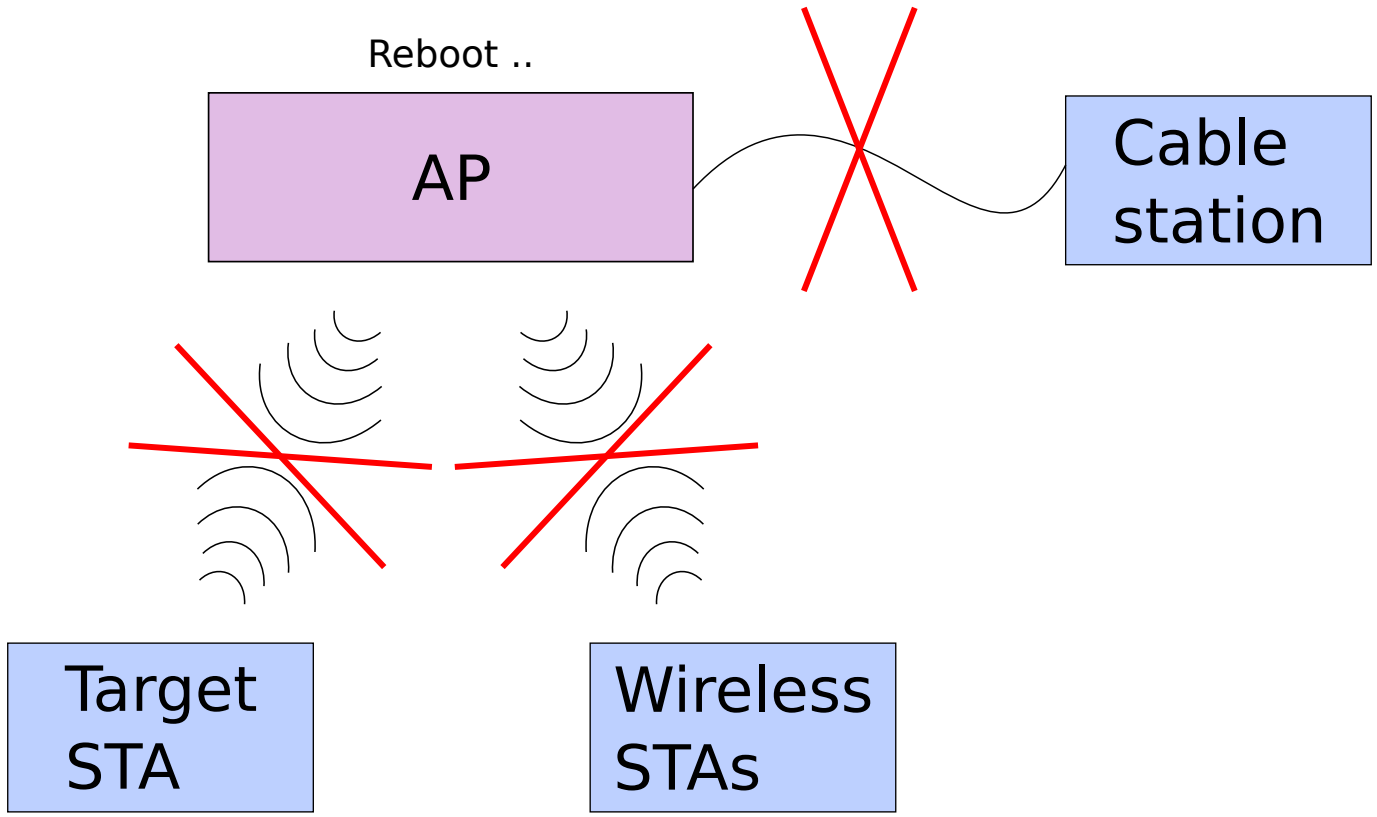
OpenWrt (TP-Link)

- Without RSN IE:
  - No effect

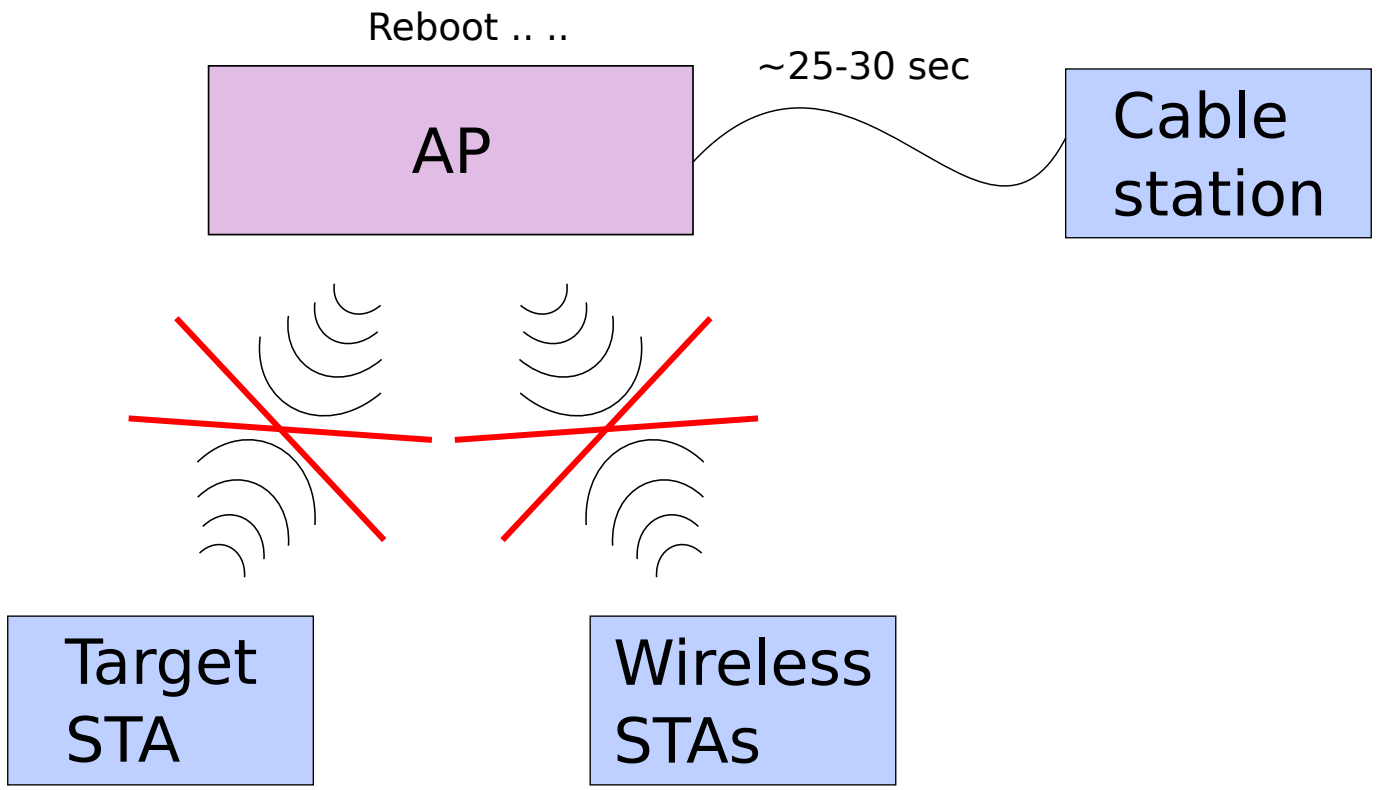
OpenWrt



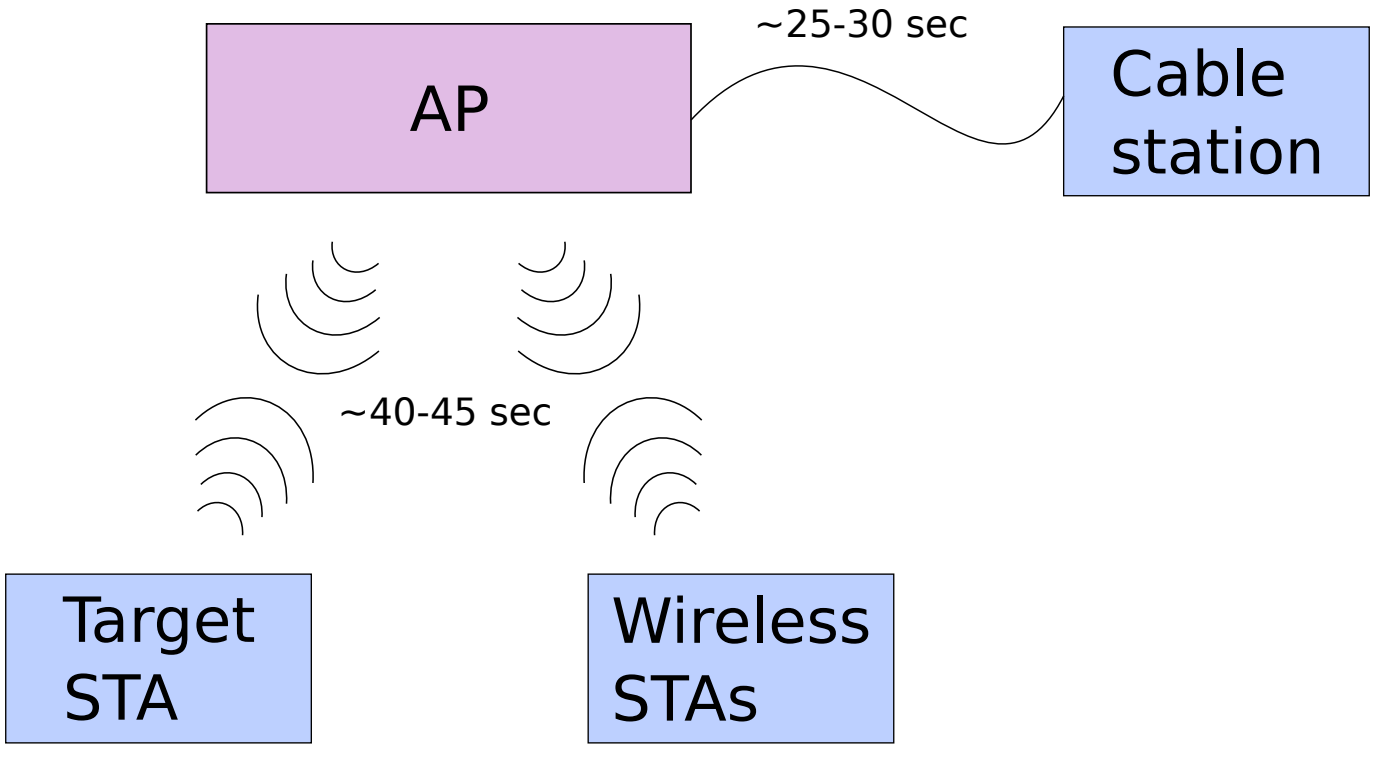
OpenWrt



OpenWrt



OpenWrt



Access point attacks

Vodafone DSL-EasyBox 602

- Without RSN IE:
  - Triggered state change to unauthenticated state at the access point
  - Disconnected forever, unless manually reconnected

Access point attacks

Vodafone DSL-EasyBox 602

- Without RSN IE:
  - Triggered state change to unauthenticated state at the access point
  - Disconnected forever, unless manually reconnected
- With RSN IE:
  - Access point sends deauthentication
  - Mac2.1 OS X 10.6.7 reconnected right away
  - Madwifi based station stays disconnected

Access point attacks

Vodafone DSL-EasyBox 602

- Without RSN IE:
  - Triggered state change to unauthenticated state at the access point
  - Disconnected forever, unless manually reconnected
- With RSN IE:
  - Access point sends deauthentication
  - Mac2.1 OS X 10.6.7 reconnected right away
  - Madwifi based station stays disconnected
- With 802.11w RSN IE:
  - Access point sends deauthentication
  - Mac2.1 OS X 10.6.7 stays disconnected
  - Madwifi based station reconnected after a while

Access point attacks

Netgear DGND330B

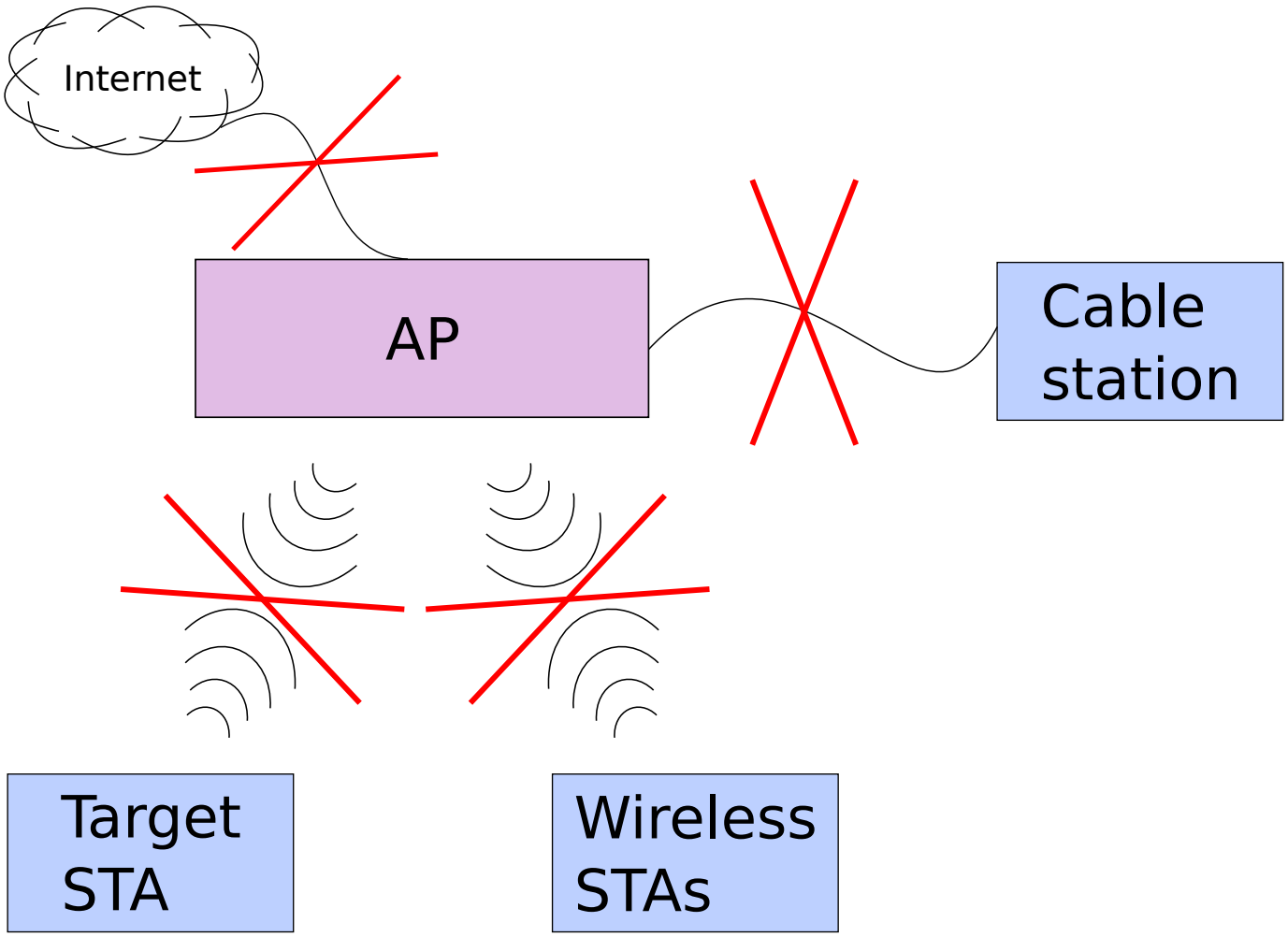
- All three variants caused one of three outcomes in seemingly random order:
- 1. outcome:
  - Triggered a reboot
  - ∼**24 sec.** DoS for stations connected by cable
  - ∼**48 sec.** DoS for wireless stations
  - ∼**2 min.** disconnected from the internet

Access point attacks

Netgear DGND330B

- All three variants caused one of three outcomes in seemingly random order:
- 1. outcome:
  - Triggered a reboot
  - ∼**24 sec.** DoS for stations connected by cable
  - ∼**48 sec.** DoS for wireless stations
  - ∼**2 min.** disconnected from the internet
- 2. outcome:
  - Triggered a reboot
  - ∼**24 sec.** DoS for stations connected by cable
  - **Complete DoS for wireless stations**
  - **Complete disconnection from the internet**

Netgear DGND330B 3. outcome



802.11w access point attacks

OpenWrt (TP-Link)

- Almost the same as in pre-802.11w mode
- Exception: Pre-802.11w RSN IE is also discarded

802.11w access point attacks

OpenWrt (TP-Link)

- Almost the same as in pre-802.11w mode
- Exception: Pre-802.11w RSN IE is also discarded
- Without RSN IE / with RSN IE:
  - No effect
- With 802.11w RSN IE:
  - Triggered a reboot
  - ∼**25 - 30 sec.** DoS for stations connected by cable
  - ∼**40 - 45 sec.** DoS for wireless stations

Summary

	Target DoS	Network DoS
Airport Express	●	
OpenWrt (TP-Link) Pre-802.11w		●
Vodafone DSL-EasyBox 602	●	
Netgear DGND330B		●
OpenWrt (TP-Link) 802.11w		●

Evaluation of the 802.11w Amendment for existing DoS attacks

Conclusion

Thoughts, observations and conclusions

- WLANs are vulnerable to DoS attacks
- Buggy / poorly written code
- Difficult task to protect Management frames
- 802.11w is a first step in a promising direction
- Standard is not useful without deployment
- Only protects against a few attacks
- Long way to go

The End

Thank you for your attention!

Tools

Platforms and libraries

- BSDish platforms (tested on OpenBSD 4.8 & Mac OS X 10.6)
- Libpcap

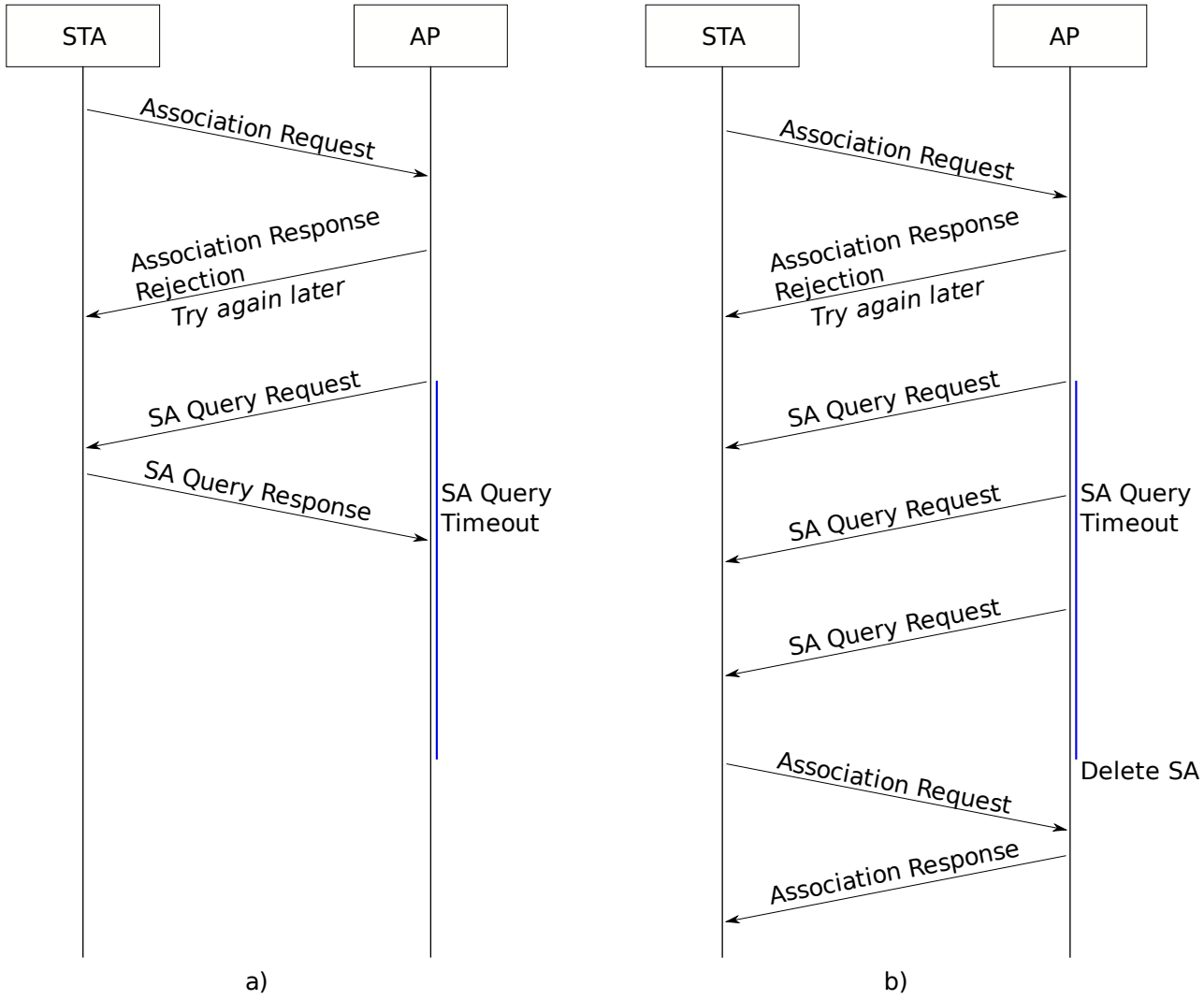
Attack tools

- deauthattack
- assocreqattack
- beaconattack

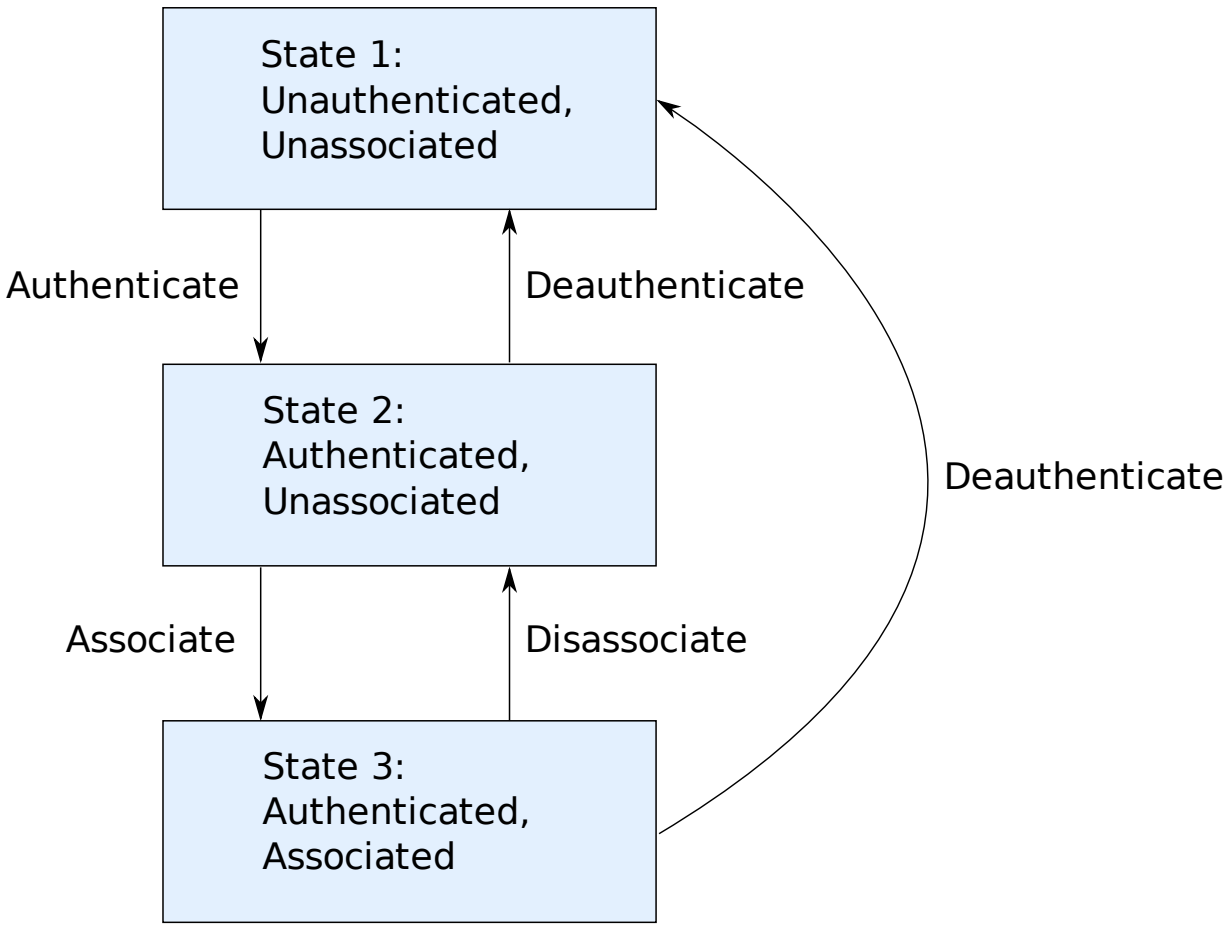
Monitor and analysis tools

- framecap
- monitor
- wlstat

SA Query procedure



Authentication and Association State machine



Association Request attack