CE 817 - Advanced Network Security
Wireless Security II

Lecture 24

Mehdi Kharrazi
Department of Computer Engineering
Sharif University of Technology

Acknowledgments: Some of the slides are fully or partially obtained from other sources. Reference is noted on the bottom of each slide, when the content is fully obtained from another source. Otherwise a full list of references is provided on the last slide.

802.11 Denial of Service Attacks: Real Vulnerabilites and Practical Solutions, J. Bellardo, and S. Savage, Usenix Security 2003.

802.11 DoS Attacks

- In 802.11, the goal of DoS attack is to prevent legitimate users from accessing the wireless LAN
- 2 major types of Attacks
  - RF attacks
  - 802.11 Protocol attacks

RF Attacks on 802.11

- Layer 1 attack (jamming)
- Involves attacker using some type of radio transmitter to generate noise in the 2.4 Ghz frequency
- Transmission disruption occurs when signal-to-noise ratio reaches certain level
- Attacks can be effective, but equipment is expensive
- Not a major attack focus

802.11 Protocol Attacks

- Level 2 attacks
- Based on vulnerabilities in 802.11 protocol
- Require only a laptop or PDA with wireless NIC
- Attacks based on Two kinds of vulnerabilities
  - Identity vulnerabilities
  - Media Access Control vulnerabilities

Identity Vulnerabilities

Identity Vulnerabilities

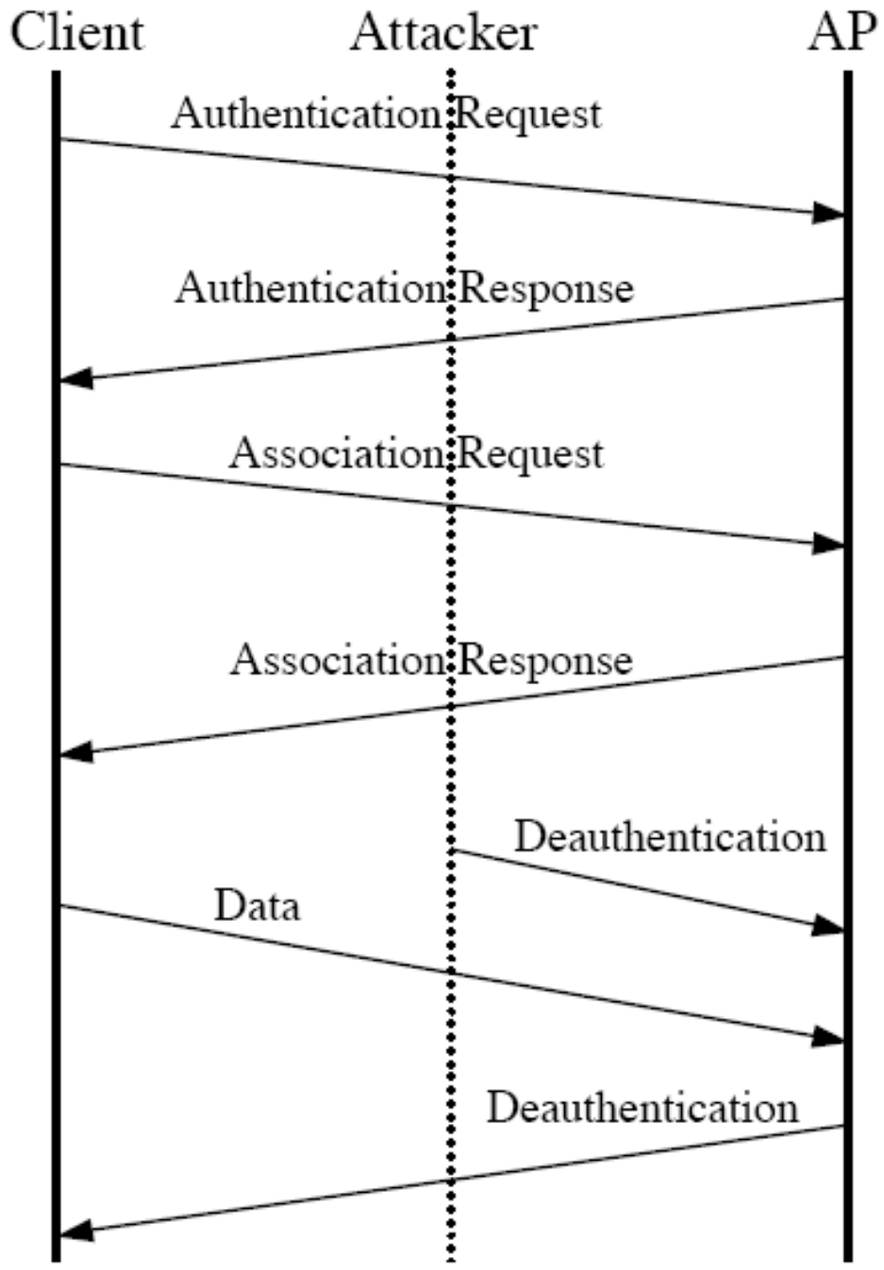
- Arise from implicit trust placed in a speaker's source address
- 802.11 nodes are identified at MAC layer by unique address as wired nodes are.
- Frames are not authenticated, meaning an attack can change his MAC address and spoof other nodes (similar to what is done in ARP spoofing)
- Causes different kinds of attacks:
  - Deauthentication attack (most effective)
  - Disassociation attack

Deauthentication Attack

- Authentication Procedure
  - After selecting an AP for communication, clients must authenticate themselves to the AP with their MAC address
  - Part of Authentication framework is a message allowing clients to explicitly deauthenticate from the AP
- Vulnerability
  - An attacker can spoof the deauthentication message causing the communication between AP and client to suspend, causing a DoS
- Result
  - Client must re-authenticate to resume communication with AP

Deauthentication Attack (Cont.)

- Client authenticates then associates
- Attacker needs to only send 1 spoofed packet to AP
- Client forced to re-authenticate with AP
  - Unfortunately, this message itself is not authenticated using any keying material.



Deauthentication Attack (Cont.)

- By repeating attack, client can be kept from transmitting or receiving data indefinitely
- Attack can be executed on individual client or all clients
- Individual Clients
  - Attacker spoofs clients address telling AP to deauthenticate them
- All Clients
  - Attacker spoofs AP telling all clients to deauthenticate

Disassociation Attack

- Disassociation Procedure
  - After Authentication, a client must associate with AP to allow the AP to forward packets on the clients behalf
  - As with deauthentication, 802.11 provides a disassocation request to tell AP to stop handling the client's traffic
- Vulnerability
  - Attacker can spoof disassociation message causing the AP to disassociate the client, resulting in DoS
  - Attack is nearly identical to deauthentication attack
- Result
  - Client must re-associate with AP to resume communication

Which method is more effective?

- Both Deauthentication and Disassociaton provide similar DoS results but Deauthentication is more effective due extra work required to return to associated state
- Authentication happens before association, therefore a deauthentication attack will require a client to re-authenticate and re-associate
  - Results in 2 RTT
- Disassocaton attack only requires a client to re-associate but not re-authenticate.
  - Results in 1 RTT

Media Access Vulnerabilities

Media Access Control Layer

- 802.11 MAC layer controls how the medium is access by clients to allow for free collision fast transmission
- To prevent collisions, a combination of physical carrier-sense and virtual carrier- sense mechanisms is used
- Physical carrier-sense
  - Uses CSMA/CA with Time windows
- Virtual carrier-sense
  - Uses RTS/CTS with NAV

CSMA/CA

- CSMA/CA stands for Carrier Sense Multiple Access with Collision Avoidance
- Works like wired Ethernet except uses Collision Avoidance instead of Collision Detection
- In addition, Time windows are used to prioritize access to the medium
- Before sending, clients must observe a quiet medium for one of the time windows
- The two most import Time windows are:
  - Short Interframe Space (SIFS)
  - Distributed Coordination Function Interframe Space (DIFS)

Time Windows

- DIFS
  - Defines the time the medium must be free before a client can transfer
- SIFS
  - Used to separate transmission belonging to the same dialog
  - Shorter time than DIFS
- To avoid all nodes transmitting immediately after DIFS expires, time after DIFS subdivided into slots
- Each client randomly picks a slot to transmit in, if collision occurs then random backoff algorithm is used before resending

Attack on Time Windows

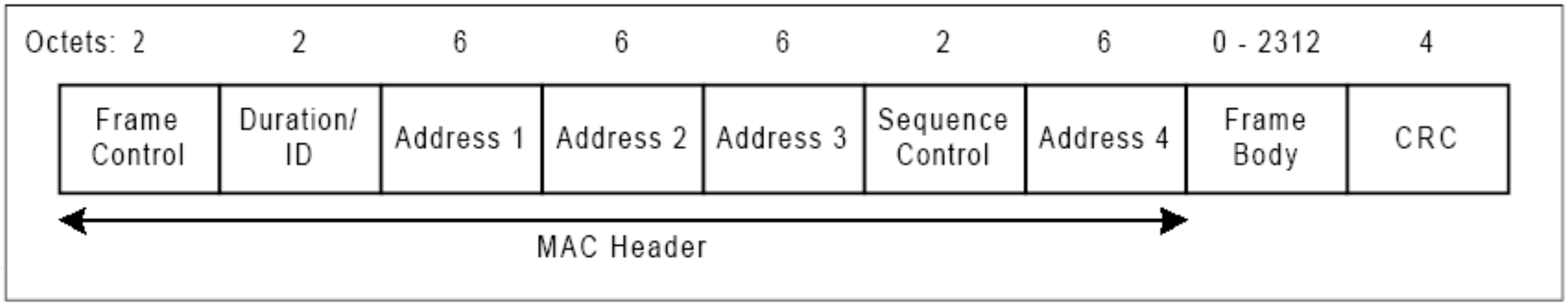
- Every transmitting client must wait at least an SIFS interval or longer
- An Attacker can completely monopolize the channel by sending a signal before the end of every SIFS interval
- Attack is limited
  - Very resource intensive – SIFS is 28 μs (802.11b), the attacker will have to send 50,000 packets per sec to disable network

Virtual Carrier Sense

- Mechanism needed in preventing collision from two clients not hearing each other (hidden terminal problem)
- RTS/CTS
  - A client wanting to transmit a packet first sends a RTS (Request to Send)
  - RTS includes source, destination, and duration
  - A client will respond with a CTS (Clear to Send) packet

Virtual Carrier Sense (Cont.)

- MAC data frame



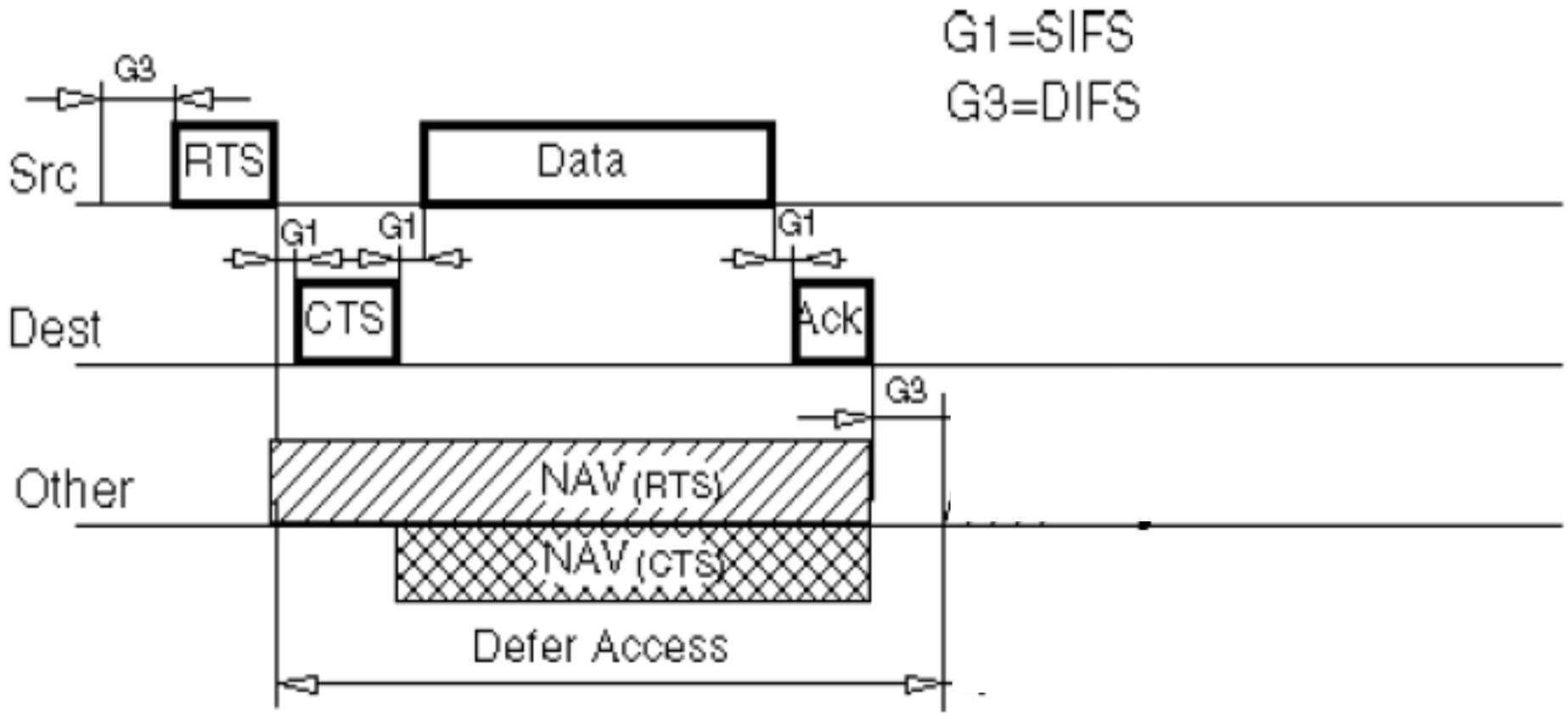
- Indicates number of μs the channel is reserved
- Used in the exchange of RTS/CTS sequencing packets

Virtual Carrier Sense (Cont.)

- All clients receiving either RTS and/or CTS will set their Virtual Carrier Sense indicator called a Network Allocation Vector (NAV)
- Clients will use this information together with the Physical Carrier Sense when sensing the medium
- Only when a client's NAV reaches 0 is it allowed to transmit over the medium

Virtual Carrier Sense (Cont.)

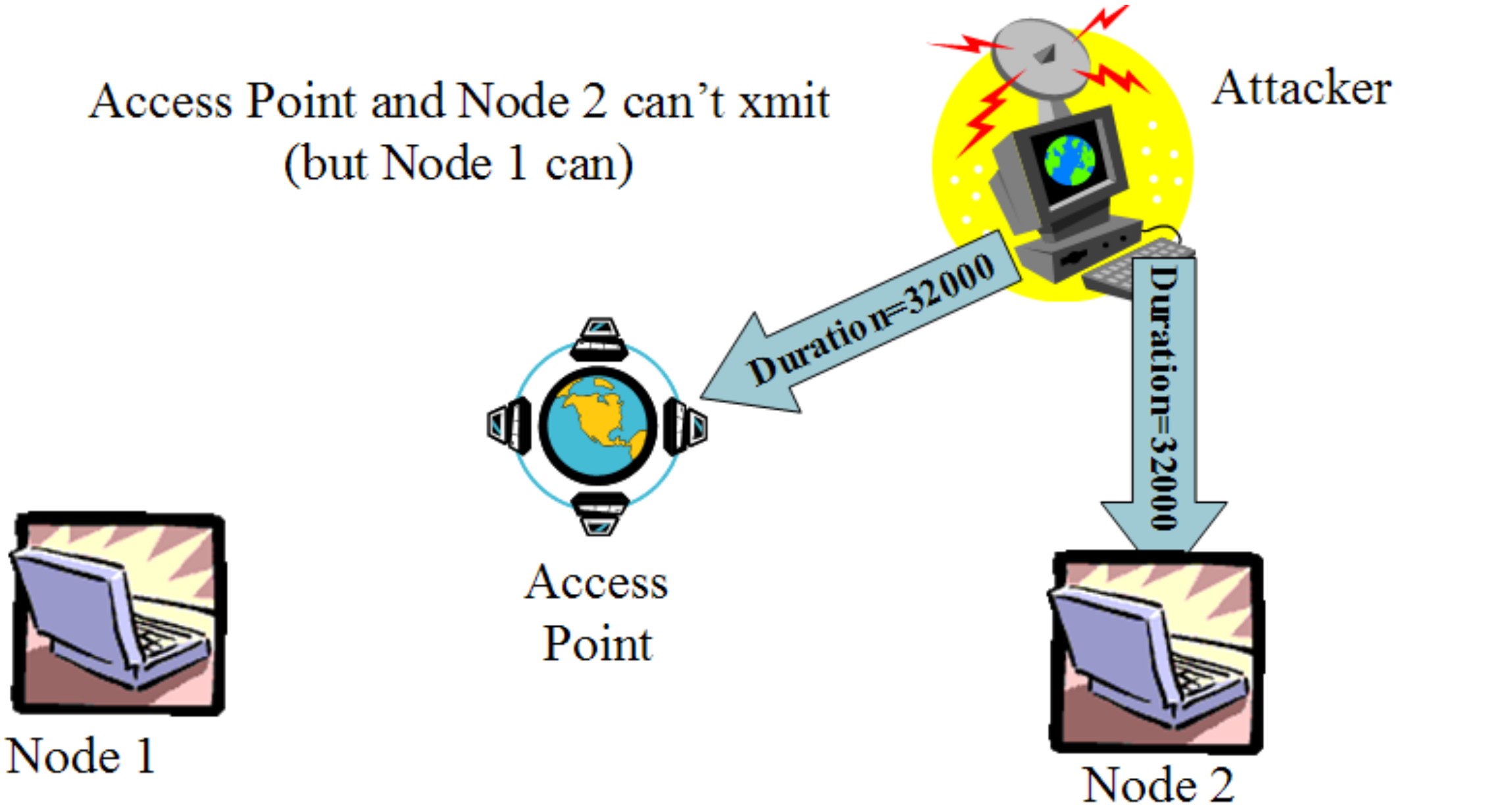
- Transaction between two stations and the NAV settings of the neighbors



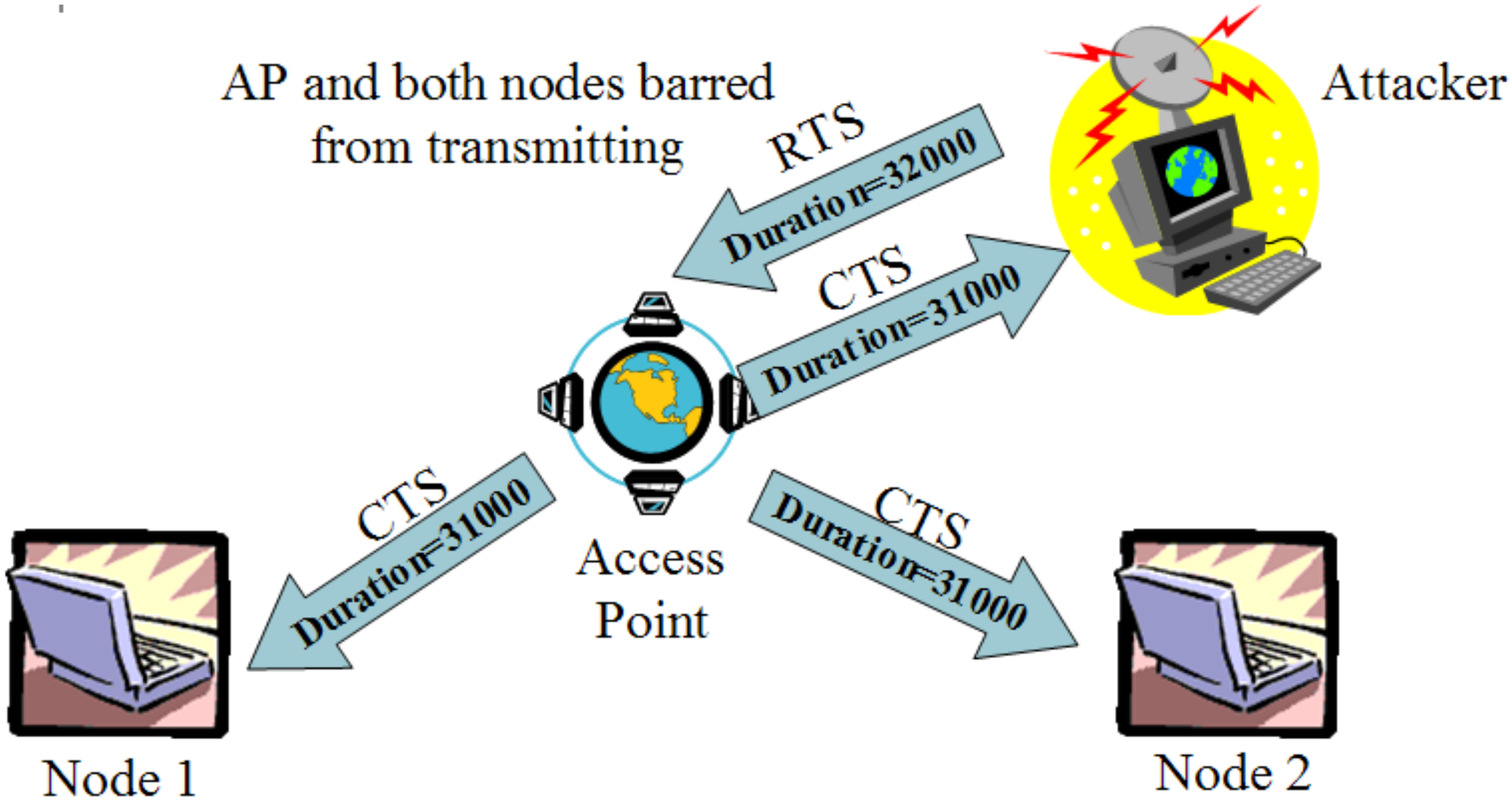
Attack on NAV

- Arises from forging the duration field of a MAC packet
- Attacker can set Duration field to high values causing NAV values to be incremented and preventing channel access to others
  - Maximum of 32767, equals to about 32 ms
  - Attacker needs to transmit only 30 times per second
- Attack is improved if duration of RTS is forged, clients will propagate attack with CTS response

NAV Attack Example



NAV Attack Example with RTS/CTS



Practical Perspective

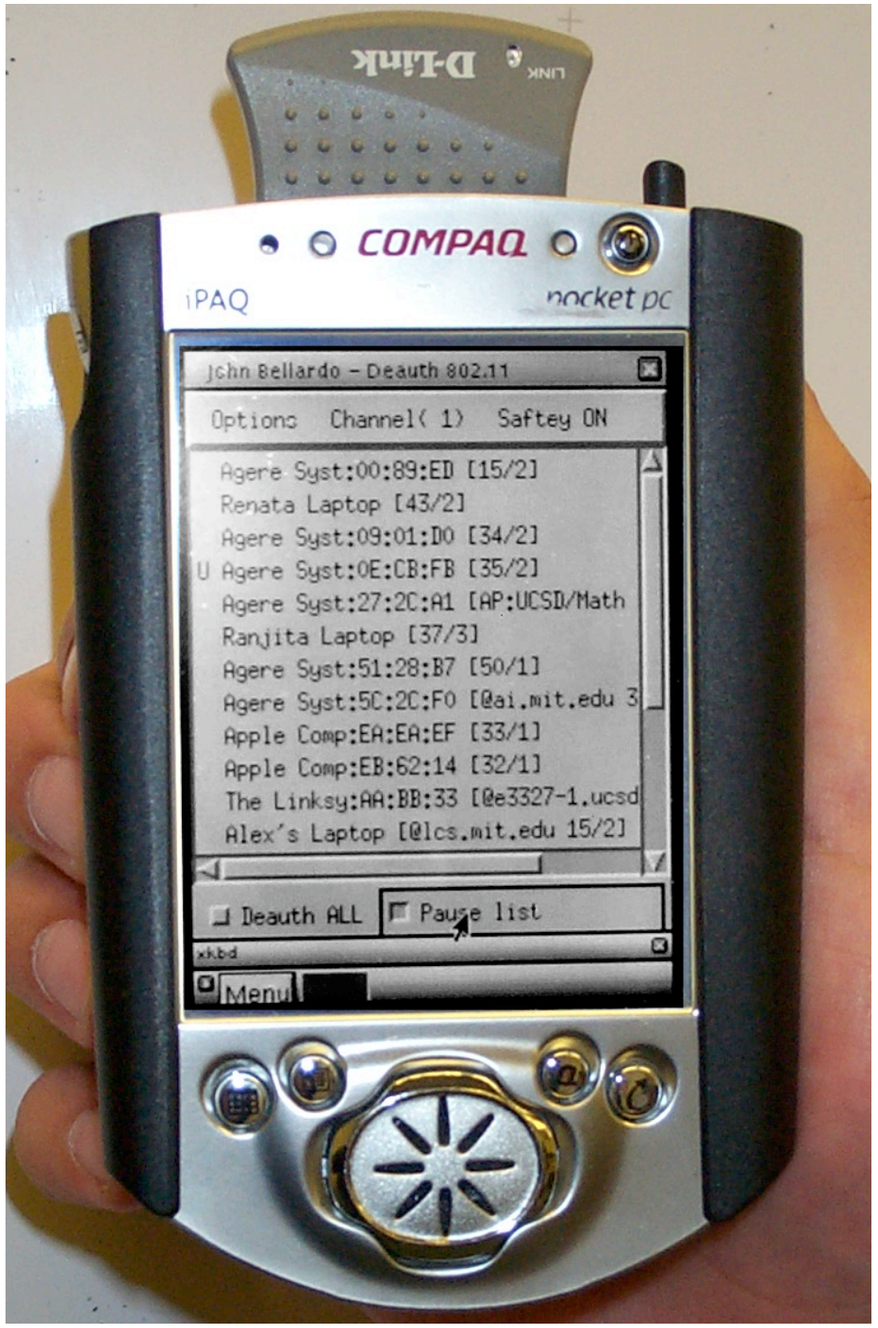
- Theoretically attacks work, but what about in actual practice on commodity hardware?
  - Yes, after testing can be done with NIC tweaking
- Most NICs allow generation of management frames to exploit the identity attacks (deauthentication & disassociation)
- Most NICs do not, however, allow generation of control frames (required for NAV attack) due to firmware restrictions
  - But, there is still away around this

Practical Attacks and Defenses

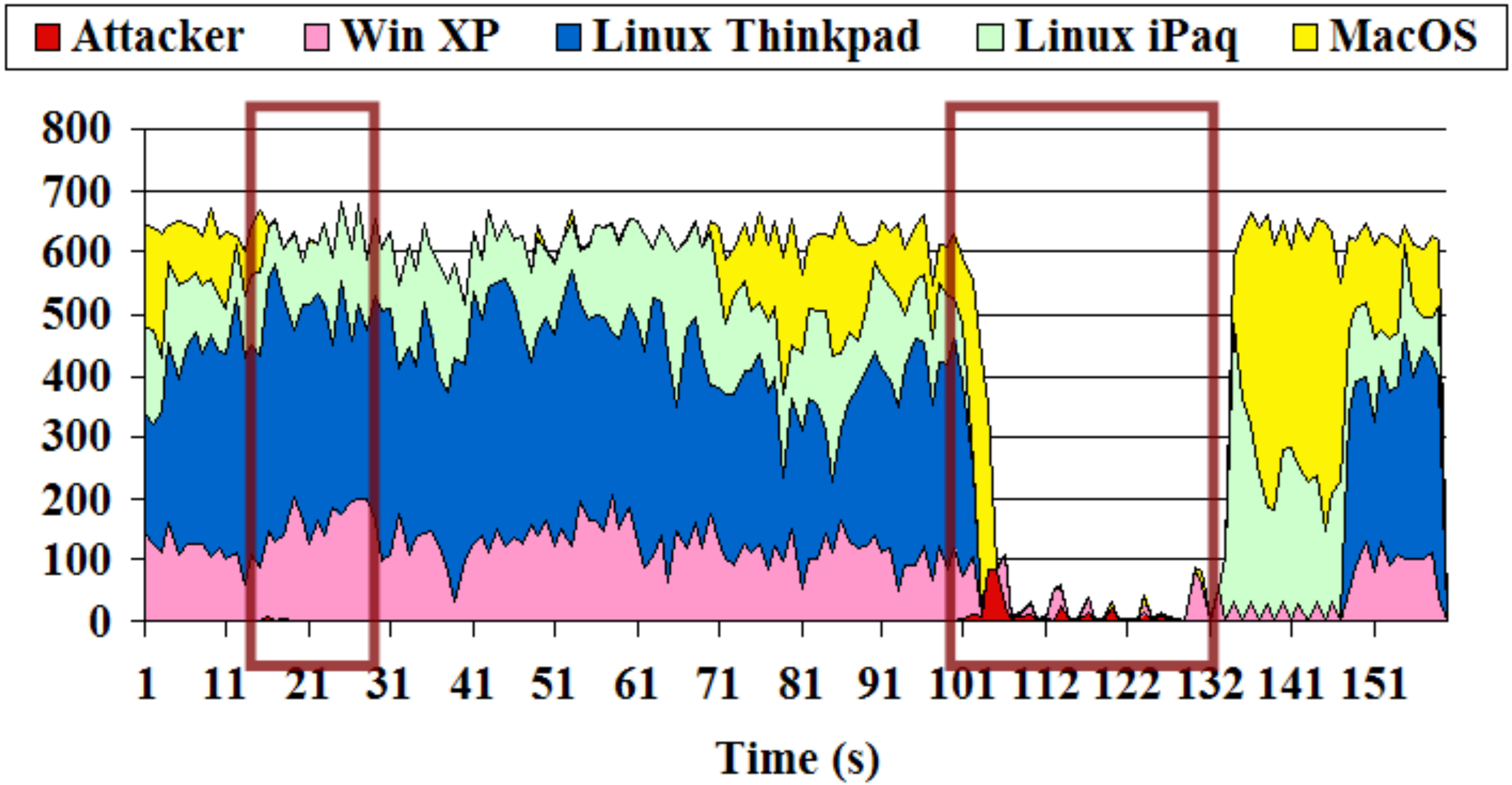
Deauthentication Attack Simulation

- Testing Hardware
  - 1 attacker (iPAQ H3600 with Dlink DWL-650 card)
  - 1 access point (built with Linux HostAP driver)
  - 4 clients (winXp, Linux Thinkpad, Linux iPAQ, MacOS X)
  - 1 monitoring station (record results of test)
- Scenario
  - Each of the 4 legitimate clients attempt to transfer a large file via ftp
- Two Attacks
  - Attack on individual client (MacOS X) at time 15 sec lasting 8 sec
  - Attack on all clients at time 101 sec lasting 26 sec

iPAQ


D-Link
COMPAQ
iPAQ
pocket pc
John Bellardo - Deauth 802.11
Options Channel(1) Saftey ON
Agere Syst:00:89:ED [15/2]
Renata Laptop [43/2]
Agere Syst:09:01:D0 [34/2]
U Agere Syst:0E:CB:FB [35/2]
Agere Syst:27:2C:A1 [AP:UCSD/Math
Ranjita Laptop [37/3]
Agere Syst:51:28:B7 [50/1]
Agere Syst:5C:2C:F0 [@ai.mit.edu 3
Apple Comp:EA:EA:EF [33/1]
Apple Comp:EB:62:14 [32/1]
The Linksy:AA:BB:33 [@e3327-1.ucsd
Alex's Laptop [@lcs.mit.edu 15/2]
Deauth ALL
Pause list
xkbd
Menu

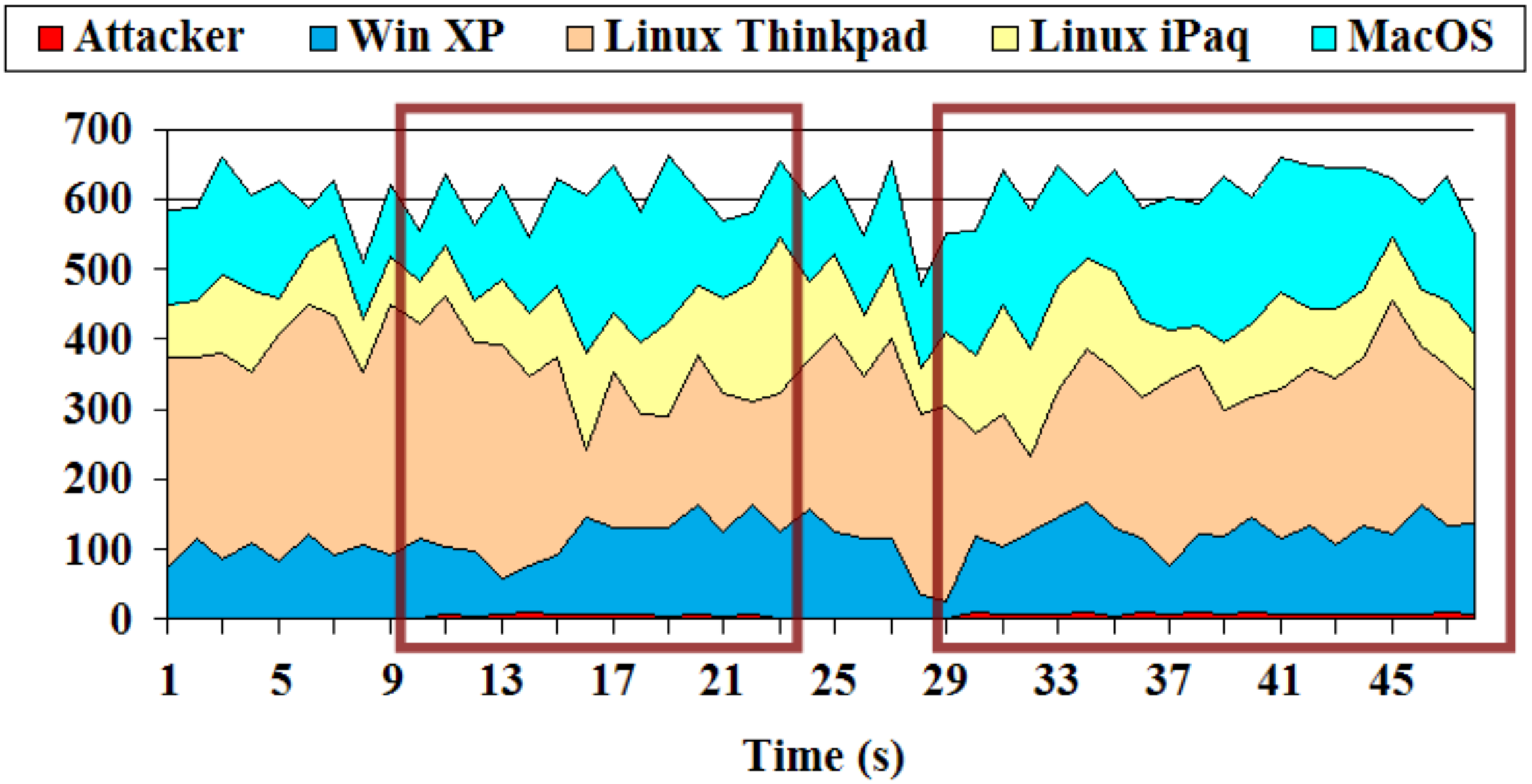
Deauthentication Attack Results



Deauthentication Attack Defense

- Two Proposed Defenses
- Defense 1: Authenticate management frames
  - Not feasible using software upgrade
  - A standardized authentication framework is required, can take time
- Defense 2: Delay honoring deauthentication request
  - Based on the observed behavior that legitimate clients do not deauthenticate then send data
  - Small delay interval (5-10 seconds)
  - If no other frames received from source then honor request
- Defense 2 more practical

Deauthentication Defense Results



Virtual Carrier Sense Attack (NAV attack)

- NAV attack simulation set up like Deauth Attack
- NAV simulation run several times with different hardware, resulted in failed attacks
  - Conclusions: many vendors do not implement the 802.11 spec correctly
- NAV attack trace

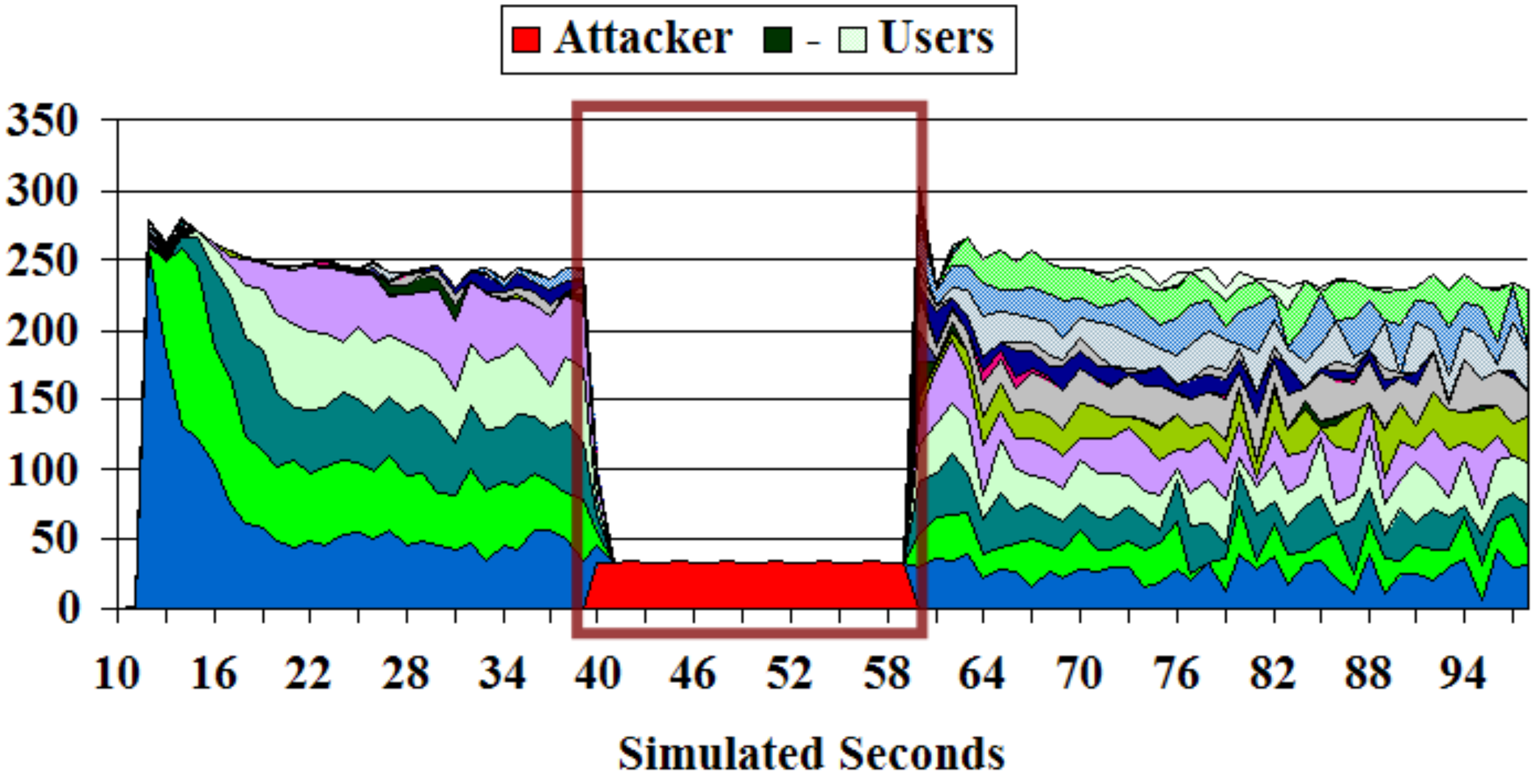
Time (s)	Source	Destination	Duration (ms)	Type
1.294020		:e7:00:15:01	32.767	802.11 CTS
1.295192	:ea:e7:0f	:93:ea:ab:df	0.258	TCP Data
1.296540		:e7:0f	0	802.11 Ack
1.297869	:9	:e7:0f	0.258	TCP Data

1.2952 - 1.2940 = 1.2 ms

NAV Attack Simulation

- Because of bug, NAV attack simulated using NS2
  - 18 Clients
  - 1 Access Point
  - 1 Attacker
- Scenario
  - Clients attempt to transfer large file via ftp
- Attack
  - Simulated attacks with ACK frames and RTS/CTS sequence
  - 30 attack frames per second
  - 37.767 ms duration per attack frame

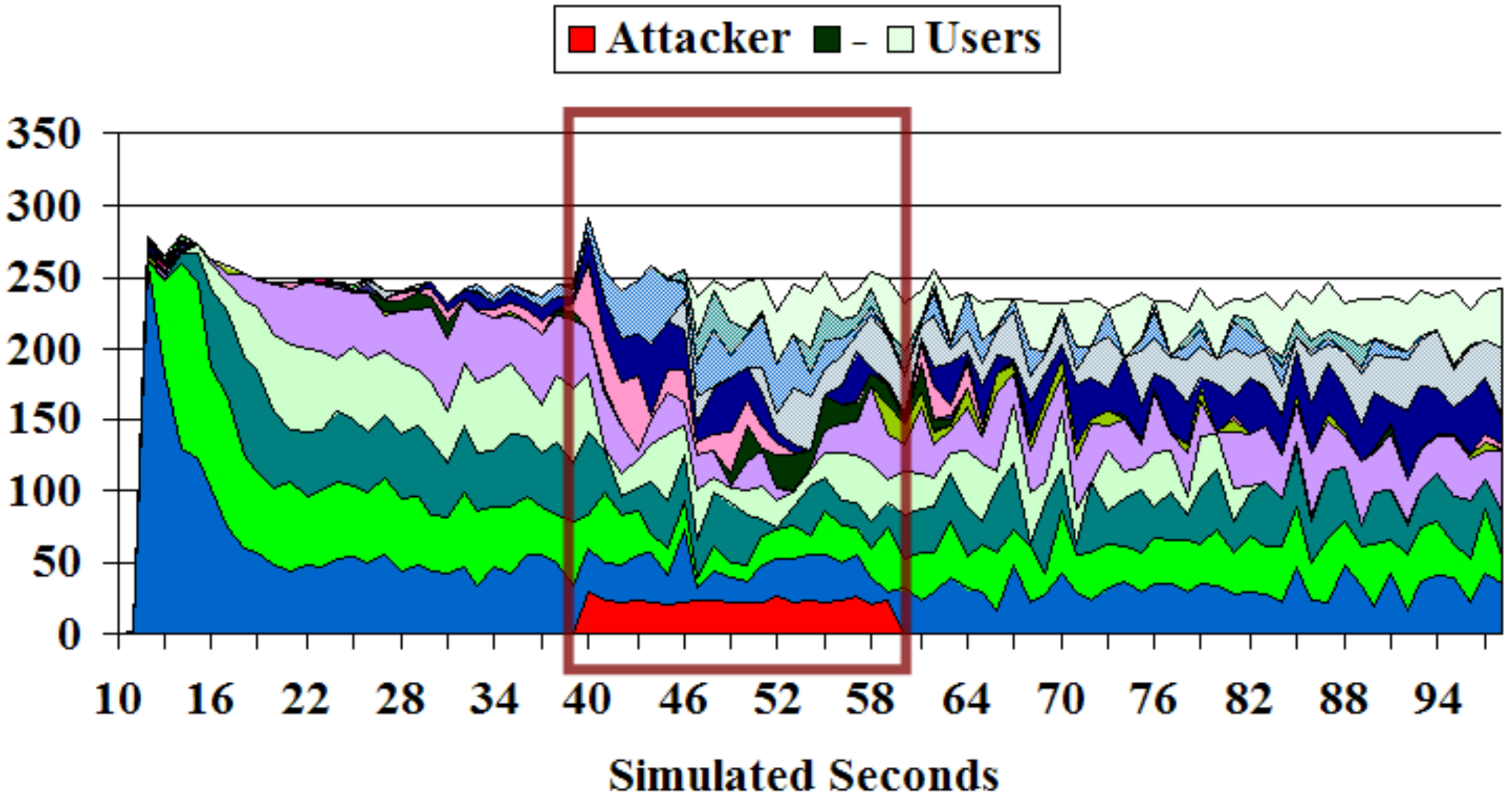
NAV Attack Results



NAV Attack Defense

- Defense based on fact that legitimate duration values are relatively small
- Put a cap on value of the max duration on received frames
- If station receives frame with duration more than cap value, truncate the duration of the cap value

Simulated NAV Defense Results



Conclusions

- 802.11 WLANs suffer from many DoS attacks not inherent in wired cousin.
- Should not depend on restricted firmware interfaces to prevent attacks
- Deauthentication attack is biggest concern
- 802.11 DoS attacks seem to stem from the IEEE's goal to provide authentication, confidentiality, and integrity and not availability
- In the future, 802.11n and 802.16(WiMax) adoption will greatly extend the range of these networks. The impact of DoS attacks at the Data-Link level could be huge.

Passive Data Link Layer 802.11 Wireless Device Driver Fingerprinting, J. Franklin, D. McCoy, P. Tabriz, V. Neagoe, J. Randwyk, D. Sicker, Usenix Security 2006.

Fingerprinting

- What is fingerprinting?
  - Process by which a target object is identified by its externally observable characteristics

Target Device

Fingerprinter

Device Driver Fingerprinting

- Utility of fingerprinting
  - Intrusion detection: detecting MAC address spoofing
  - Network forensics: narrow or verify source of network event or security incident
- Why not use the MAC Address?
  - MAC address is one way to identify a NIC manufacturer
  - Easy to change (spoof) to another legitimate, copied, or fictitious MAC

802.11 Active Scanning

- A station sends probe request frames when it needs to discover access points in a wireless network. This process is known as active scanning.

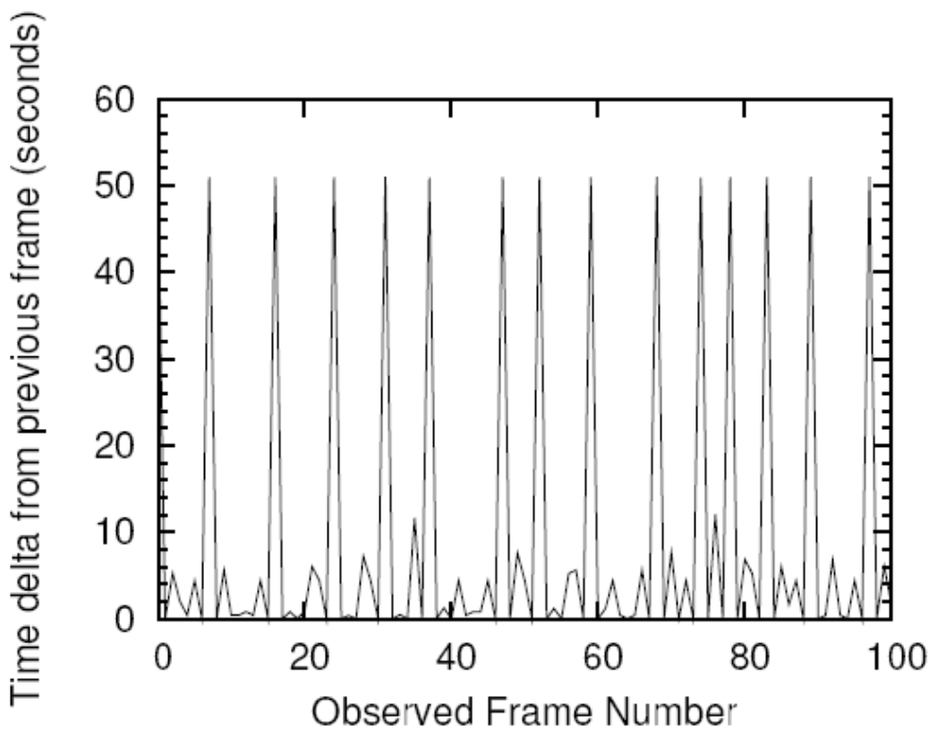
- The IEEE 802.11 standard specifies active scanning as…

```
For every channel:
Broadcast probe request frame;
Start channel timer, t;
If t reaches MinChannelTime AND current channel is IDLE:
  Scan to the next channel;
Else
  Wait until t reaches MaxChannelTime;
  Process probe response frames from current channel;
  Scan to the next channel;
```

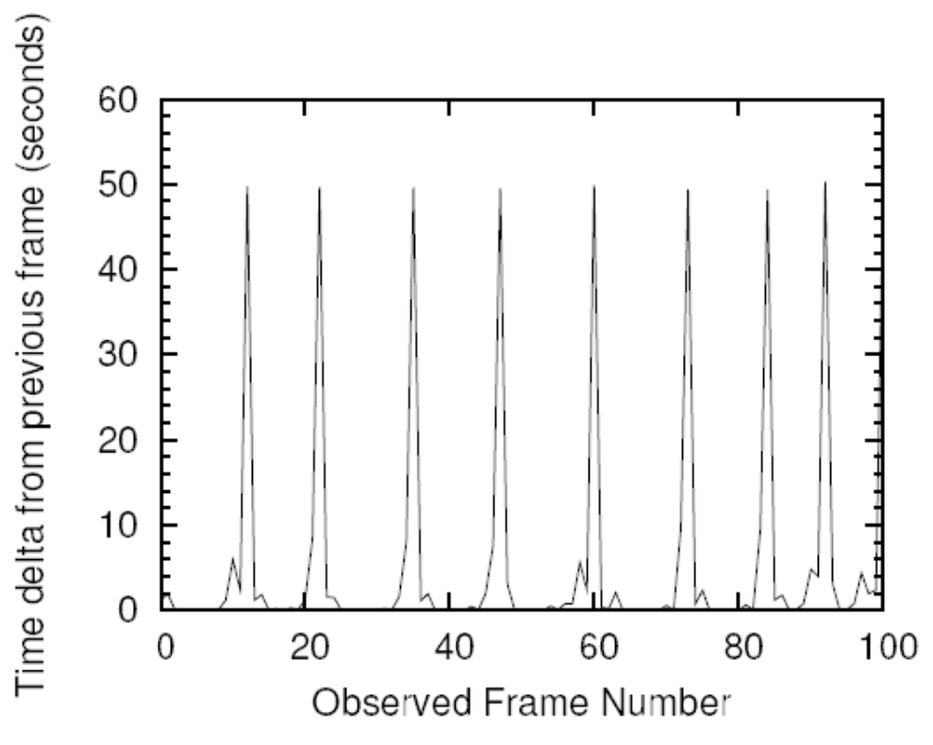
- The remaining details of this process implementation are determined by wireless driver authors…

Intuition

- As you may have guessed, we distinguish drivers based on unique active scanning!



D-Link driver
D-Link DWL-G520 PCI Wireless NIC



Cisco driver
Aironet AIR-CB21AG-A-K9 PCI Wireless NIC

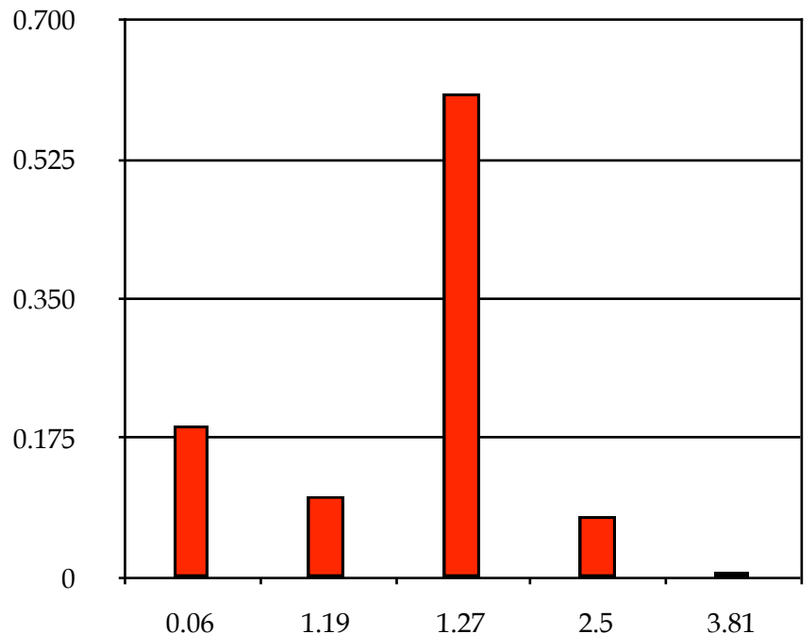
Fingerprinting Approach

Outline of Method

- Supervised Bayesian Classification:
  - Create tagged signatures (Bayesian Models)
    - 17 different device drivers
    - 12 hour traffic traces
  - Capture traffic trace for an unidentified driver
  - Compare how close the unidentified trace is to every tagged signature and identify based on nearest match

Signature Generation

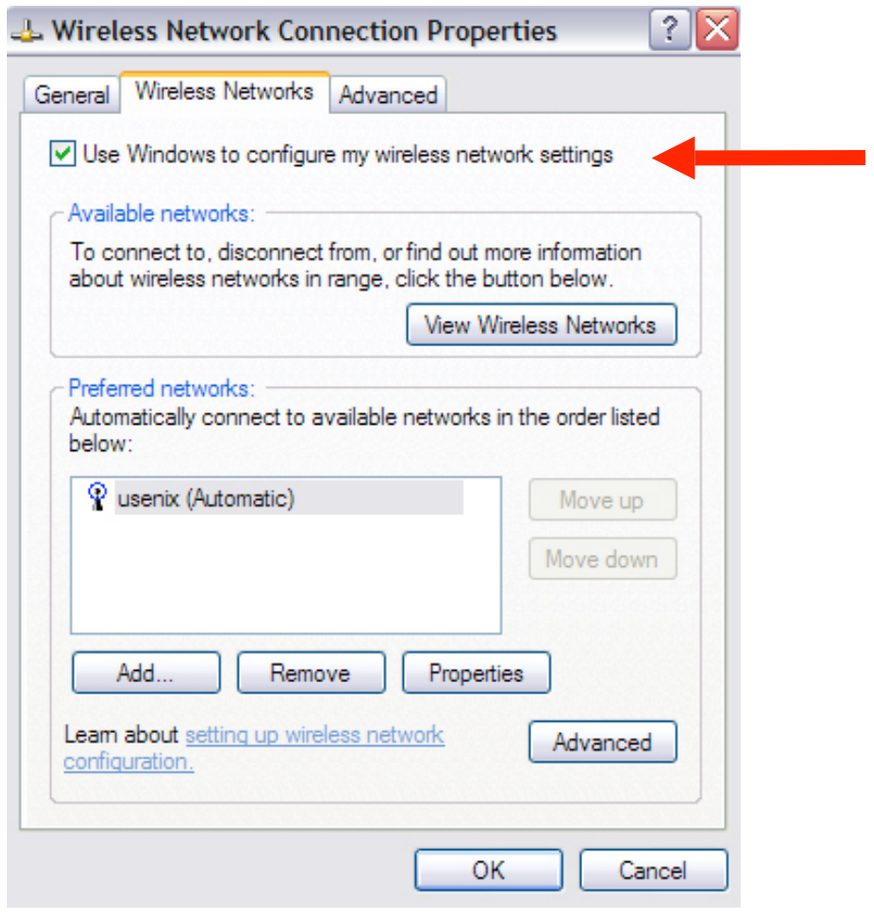
- Driver signatures are based on the delta arrival time between probe requests.
- Signatures are obtained via binning with an empirically tuned and fixed bin width.
  - Record the percentage of probe requests placed in each bin
  - Record the average, for each bin, of all actual (non-rounded) delta arrival time values in that bin
  - Generate a vector initialized with these parameters as the signature for that driver



Windows Engenius driver signature.

Factors that Effect Probing

- Association status
  - Associated to an access point
  - Unassociated
- Driver management
  - Managed by Windows
  - Managed by NIC vendor drivers



Experimental Setup

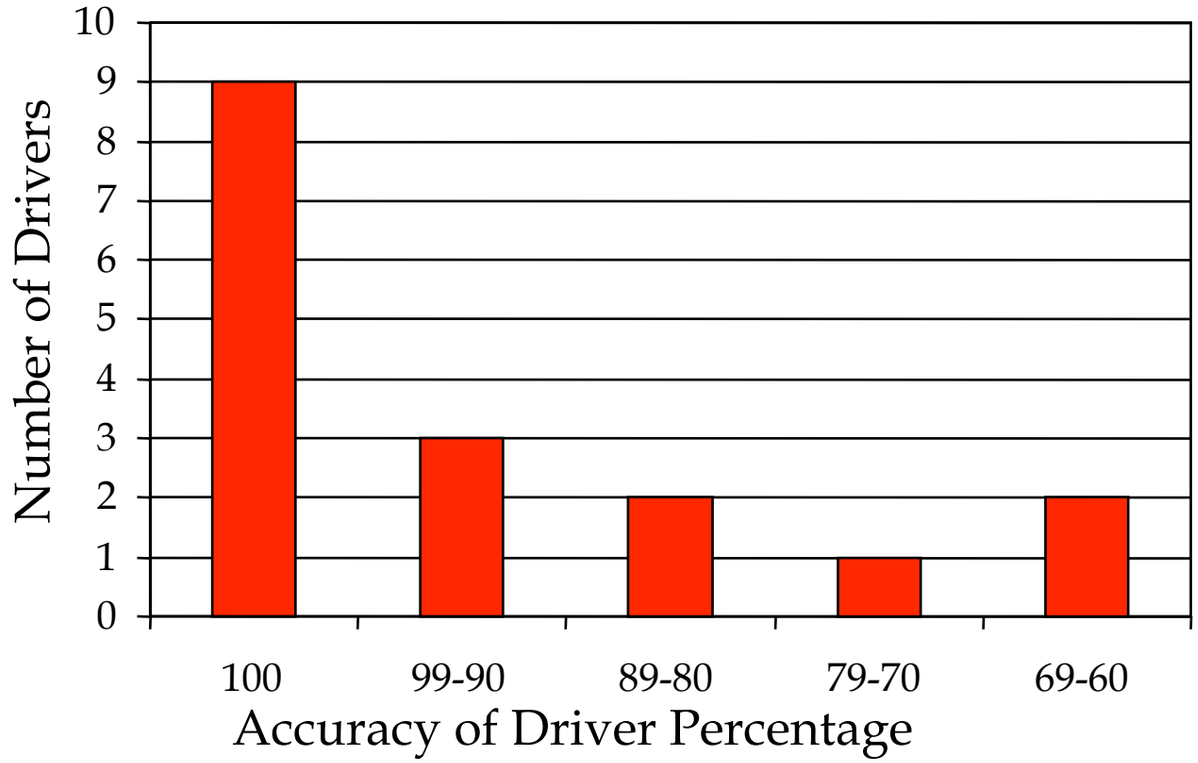
- The fingerprinter: Pentium 4 running Linux with a Cisco Aironet a/b/g wireless card
- The victims: 17 different wireless drivers, including drivers from Apple, Cisco, D-link, Intel, Linksys, Madwifi, Netgear, Proxim, and SMC
- The signature database: 31 unique driver signatures with tags and signature of the format:
  - driver assoc-status manager : (bin, % in bin, mean)

Experimental Setup

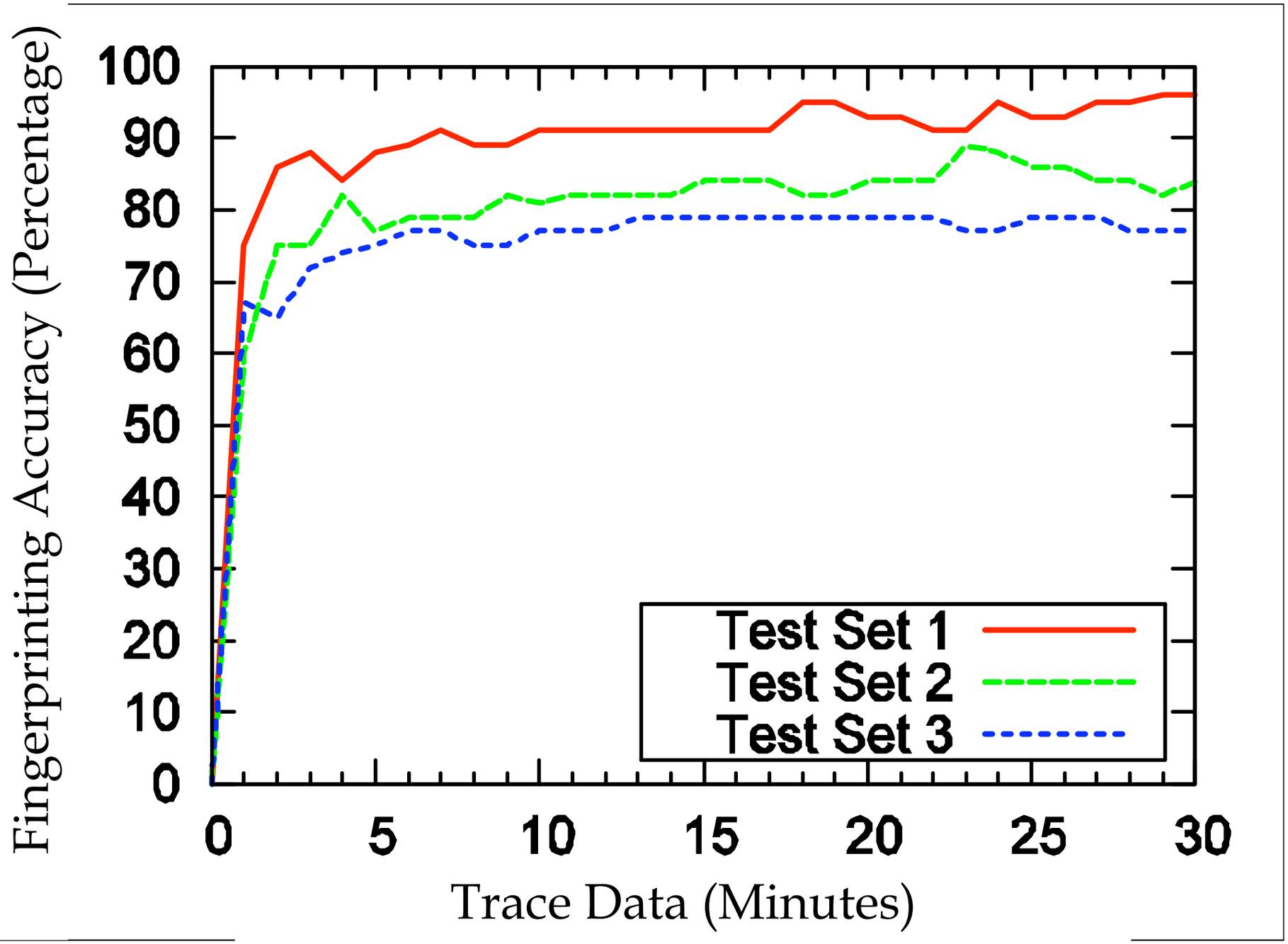
- Test set #1, Master Signature Database (Lab):
  - No background traffic
  - No obstructions
- Test set #2 (Home network):
  - No background traffic
  - Wall between fingerprinter and victim
- Test set #3 (Coffee house):
  - Background wireless traffic
  - Miscellaneous objects between fingerprinter and victim

Results

Test Set	Successful	Total	Accuracy
1	55	57	96%
2	48	57	84%
3	44	57	77%

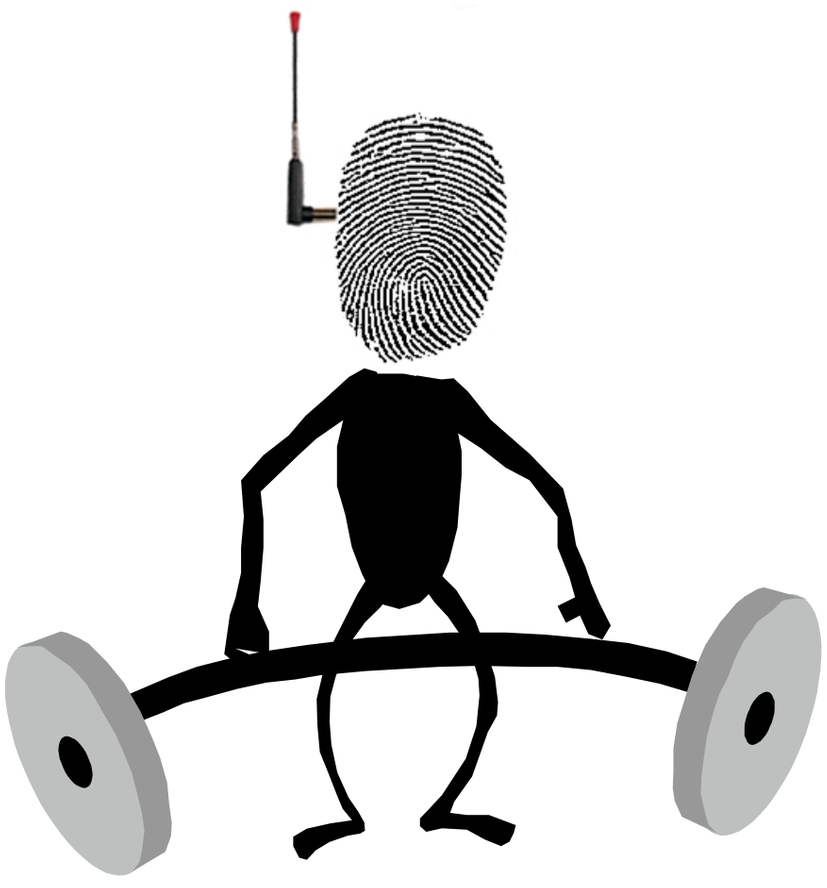


Results


Fingerprinting Accuracy (Percentage)
100
90
80
70
60
50
40
30
20
10
0
0
5
10
15
20
25
30
Trace Data (Minutes)
Test Set 1
Test Set 2
Test Set 3

Limitations

- Cannot distinguish between different driver versions
- Accuracy is sensitive to network conditions



Acknowledgments/References

- [Lindsey] CSCE790: Security and Privacy for Emerging Ubiquitous Communication system, Hal Lindsey, University of South Carolina, SPring 2008.
- [Bellardo] Presentation by John Bellardo at Usenix Security 03. (802.11 Denial-of-Service Attacks Real Vulnerabilities and Practical Solutions, John Bellardo and Stefan Savage, Usenix Security 2003)
- [Franklin] Presentation by Jason Franklin at Usenix Security 2006. (Passive Data Link Layer 802.11 Wireless Device Driver Fingerprinting, J. Franklin, D. McCoy, P. Tabriz, V. Neagoe, J. Randwyk, D. Sicker, Usenix Security 2006.)