Off-Path TCP Hijacking in Wi-Fi Networks: A Packet-Size Side Channel Attack

Ziqiang Wang, Xuewei Feng, Qi Li, Kun Sun, **Yuxiang Yang**,
Mengyuan Li, Ganqiu Du, Ke Xu, Jianping Wu

Overview


Threat Model


Background


Attack Procedure


Empirical Study


Mitigation


Conclusion

Threat Model

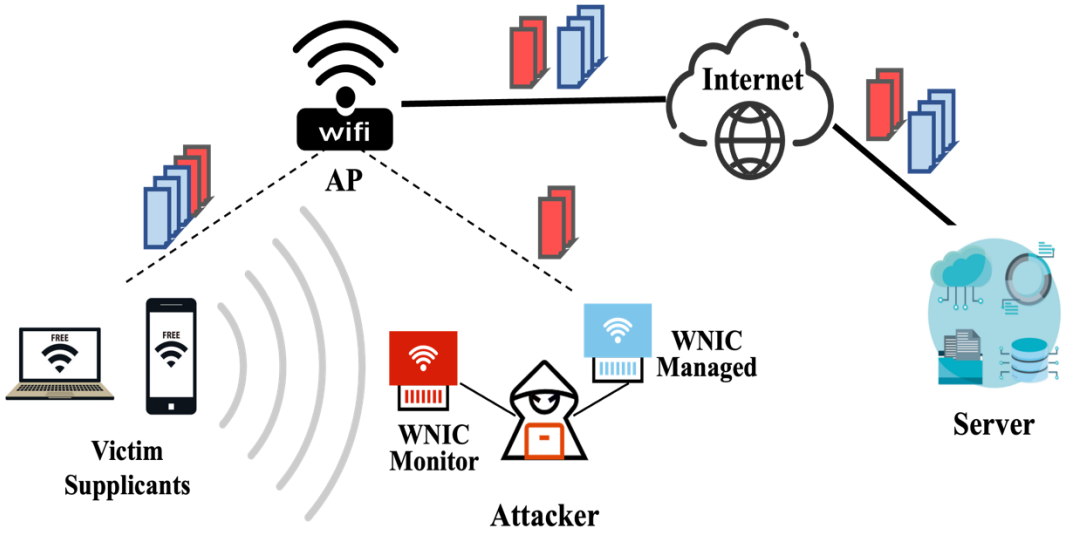
Threat Model

Consists of:

- A remote **server** that provides web services or SSH services
- An **AP** which provides Wi-Fi services and encrypts Wi-Fi frames with WPA2/WPA3
- A victim **client** who connects to Wi-Fi and establishes a TCP connection to the remote server
- An off-path **attacker** who connects to the same Wi-Fi network and does not have AP management privileges

The attacker can:

- **Terminate** the victim's **TCP connection**
- **Inject** some malicious data to the **TCP connection**



Background

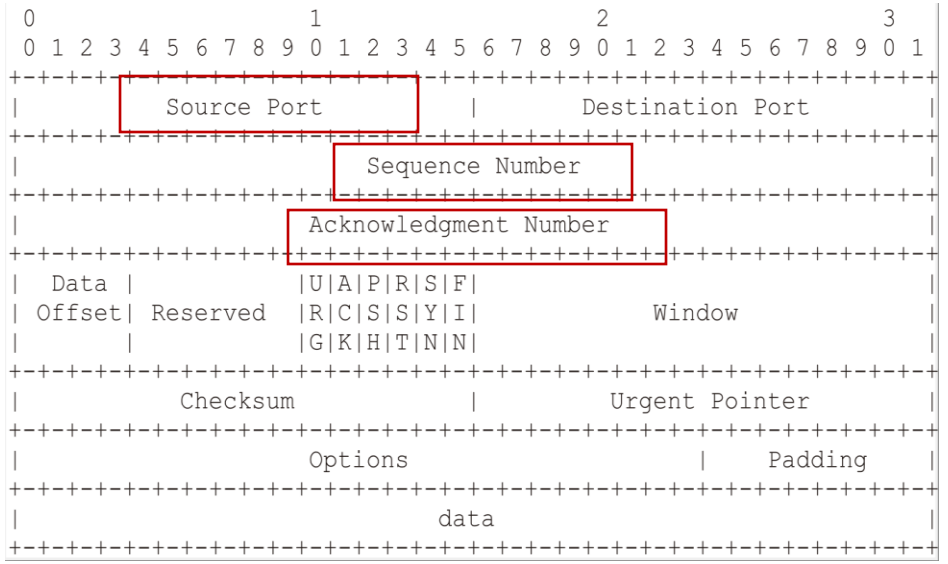
Off-Path TCP Hijacking Attacks

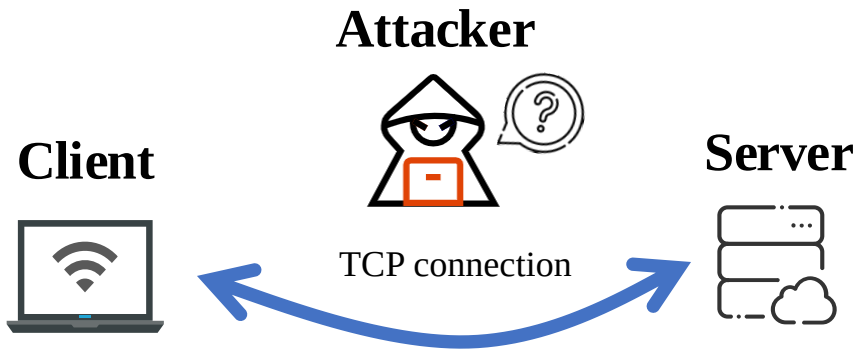
🛠 **Given a target server, the attacker already knows:**

- Dst IP address: server IP
- Dst Port number: service at server (e.g. 80)

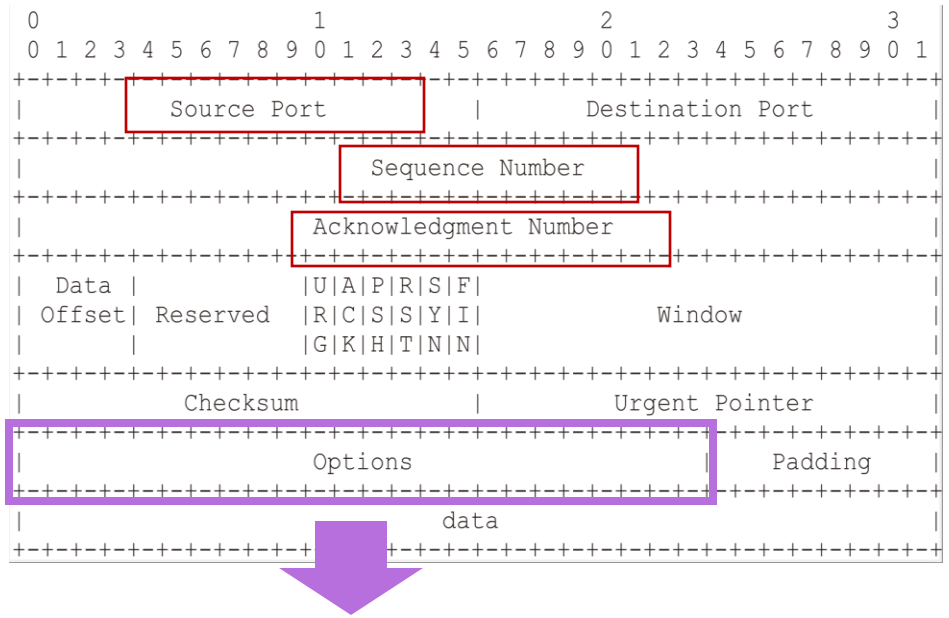
🛠 **The attacker still needs to know:**

- **Src IP address:** client's IP
- **Src port number:** A random port at client
- **SEQ number:** Track data sequence based on an initial random number
- **ACK number**: Acknowledge data order using an initial random number





TCP Options



Timestamp: improve RTT measurement and prevent sequence wrap

SACK: enable efficient retransmission by acknowledging discontinuous data blocks

Packet type	TCP options		Packet size (Byte)	Frame size (Byte)
	Timestamp	SACK		
RST	-	-	54	56
ACK	+	-	66	68
SACK-ACK	+	+	78	80

+ represents carrying the option, while - represents not carrying the option.

The TCP packet size in IPv4

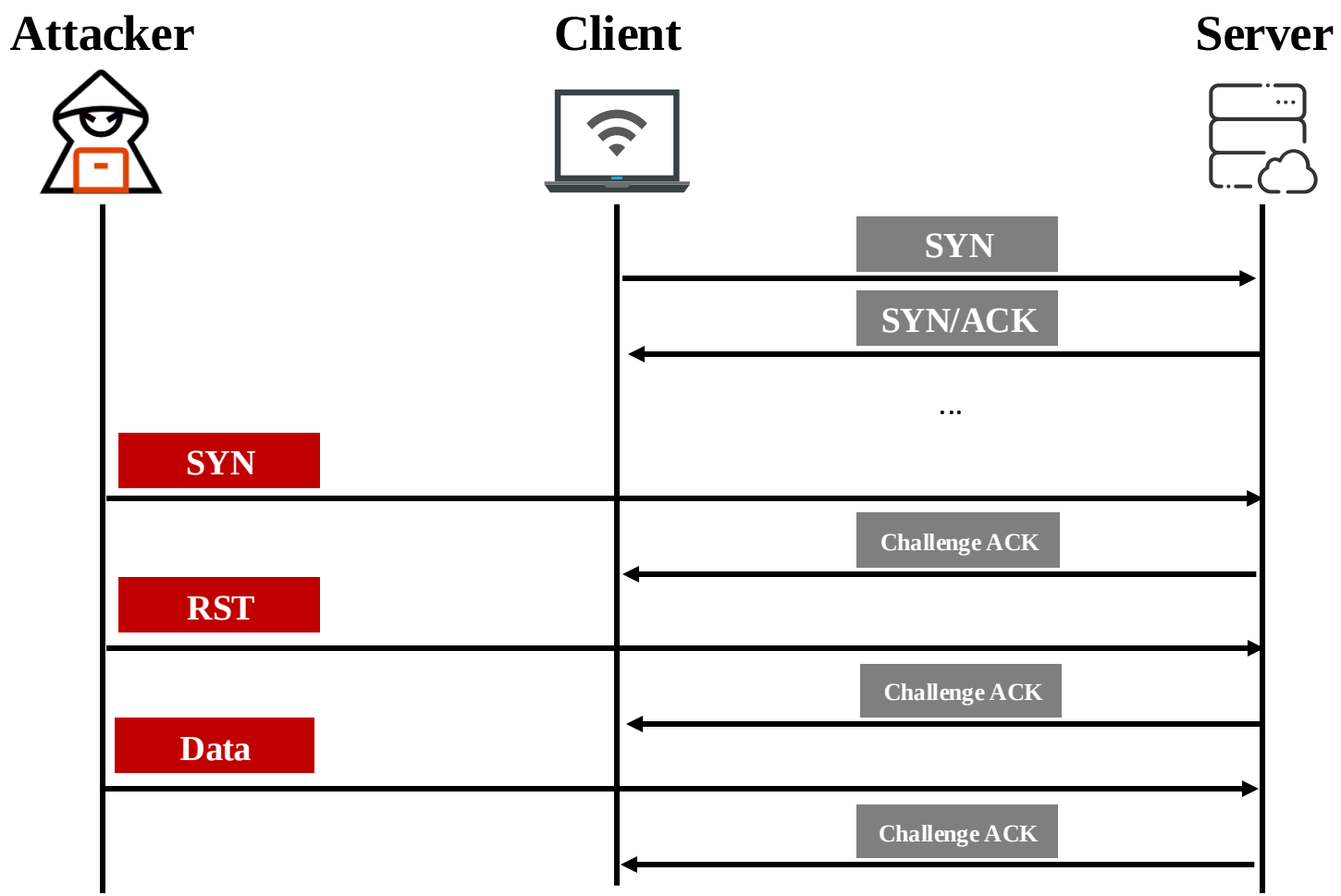
TCP options affect packet size

Challenge ACK Mechanism

RFC 5961

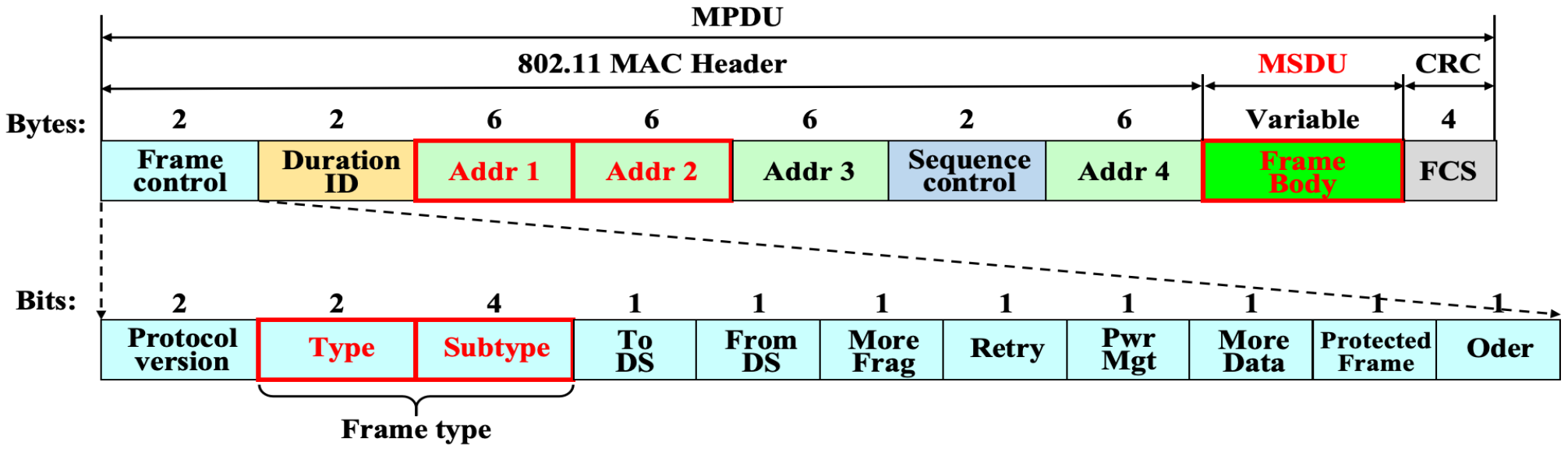
- SYN attack protection
- RST attack protection
- Data injection protection

Utilized to elicit diverse responses



Wi-Fi Encryption and Frames

- The AP typically use WPA2/WPA3 to **encrypt users' Wi-Fi frames** at the link layer
- Attackers can only observe **unencrypted fields** (e.g., address and type) in the Wi-Fi frame header

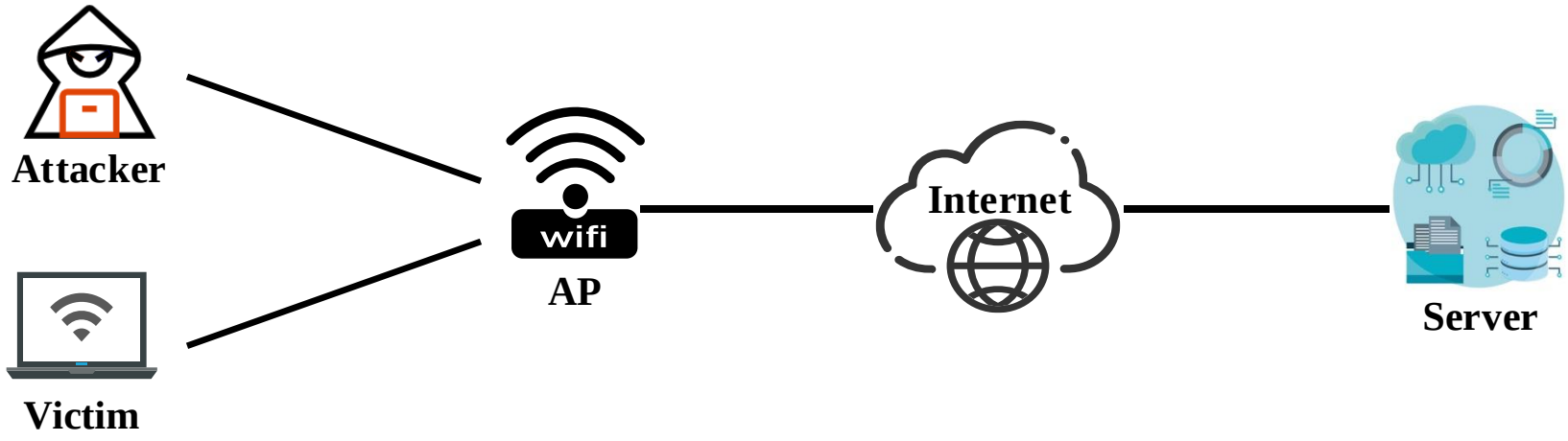


ATTACK PROCEDURE

Attack Overview

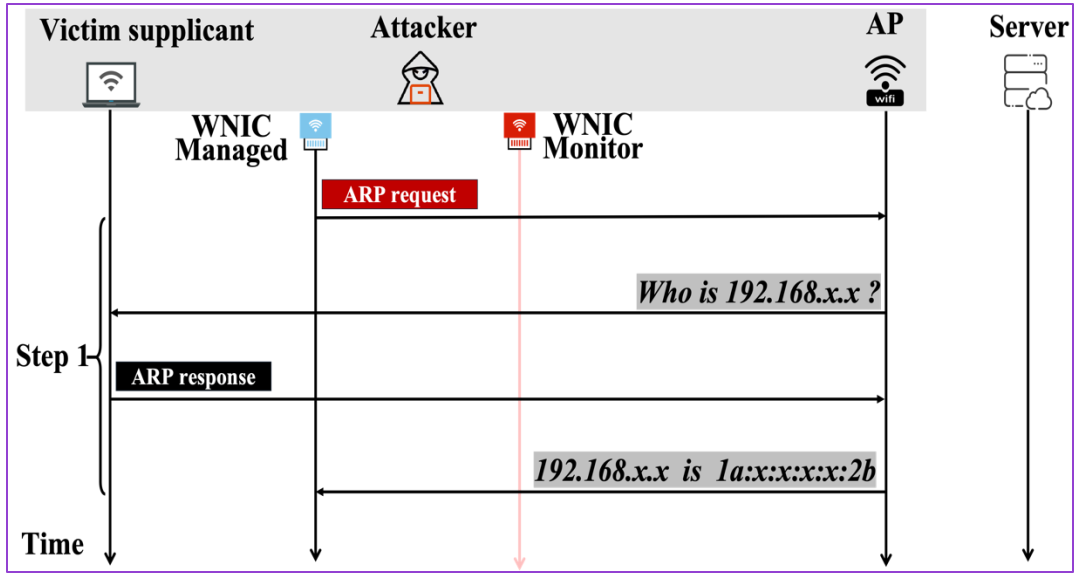
Attack Steps：

- Step 1: Probing the Wi-Fi network (to get the **client's IP** address and **MAC** address)
- Step 2: Detecting active TCP connections (to infer the client's **source port** number)
- Step 3: Inferring sequence number (by exploiting **TCP SACK** options)
- Step 4: Inferring acknowledgment number (by exploiting **challenge ACK** mechanism)

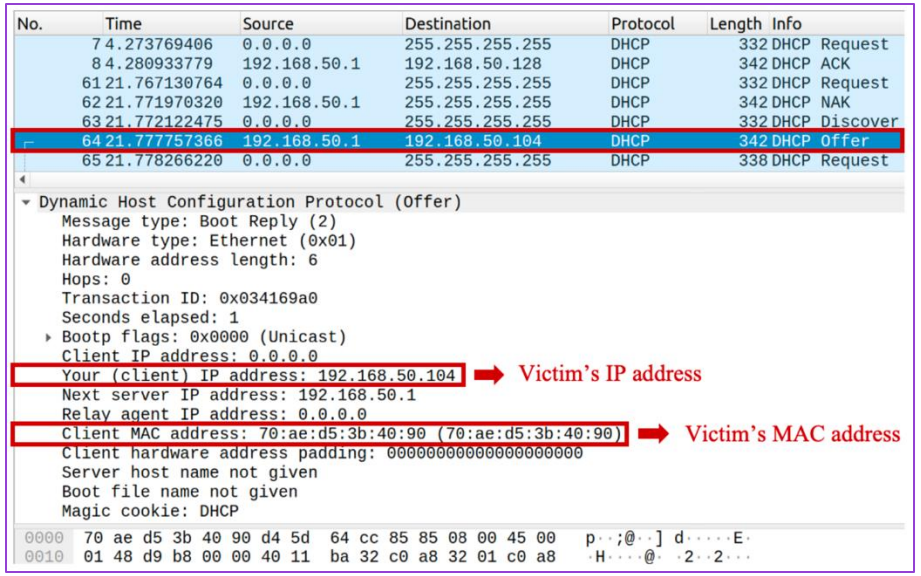


Probing the Wi-Fi Network

🛠 **Identifying the client's MAC/IP addresses through ARP request or DHCP mechanism**



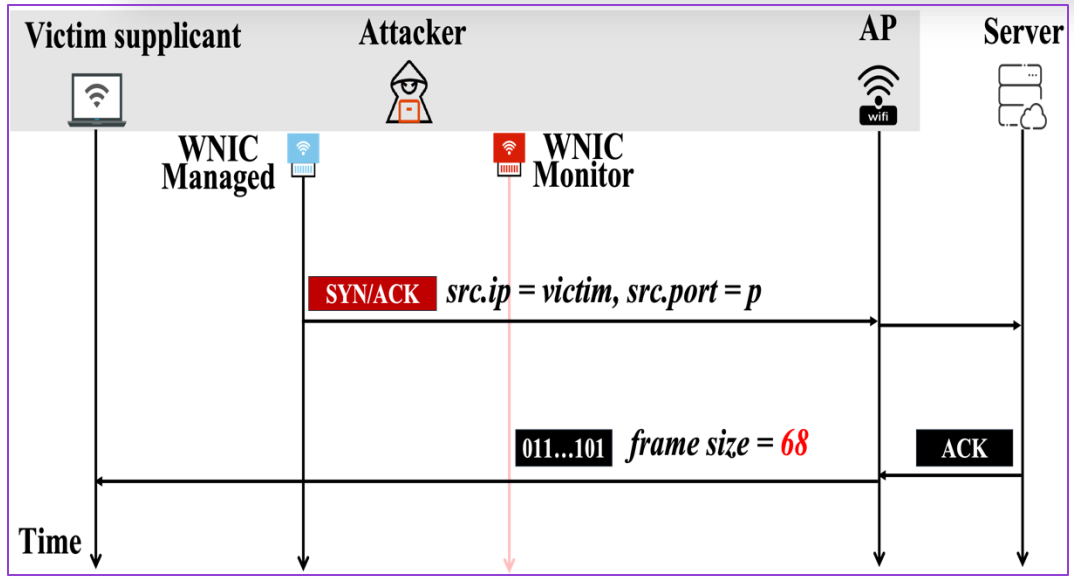
ARP request



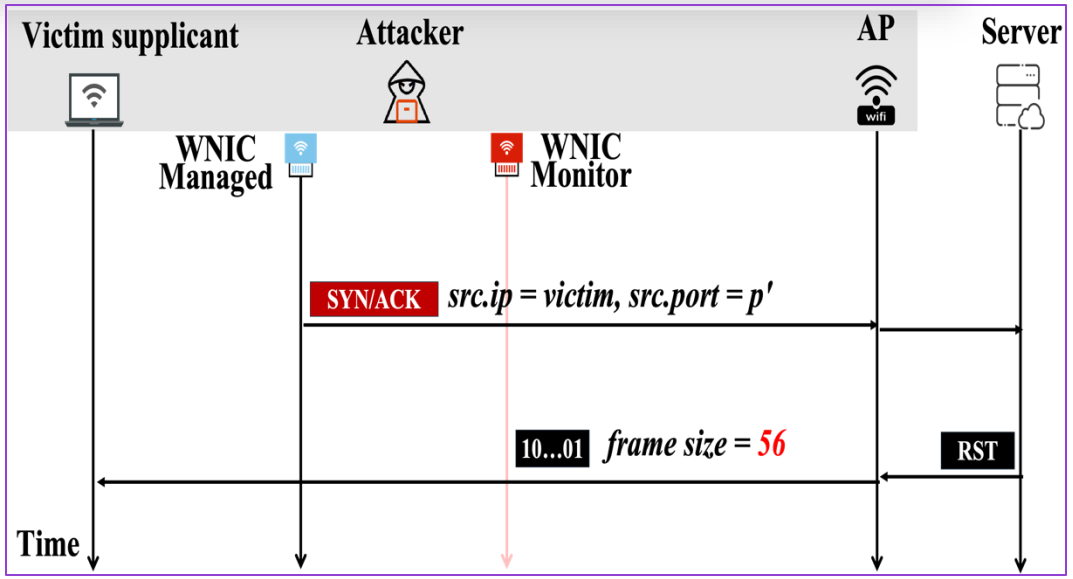
DHCP mechanism (AP-isolated)

Inferring Source Port Number

- Sending **SYN/ACK packets** with **guessed source ports**
- Sniffing and **analyzing the sizes** of encrypted frames



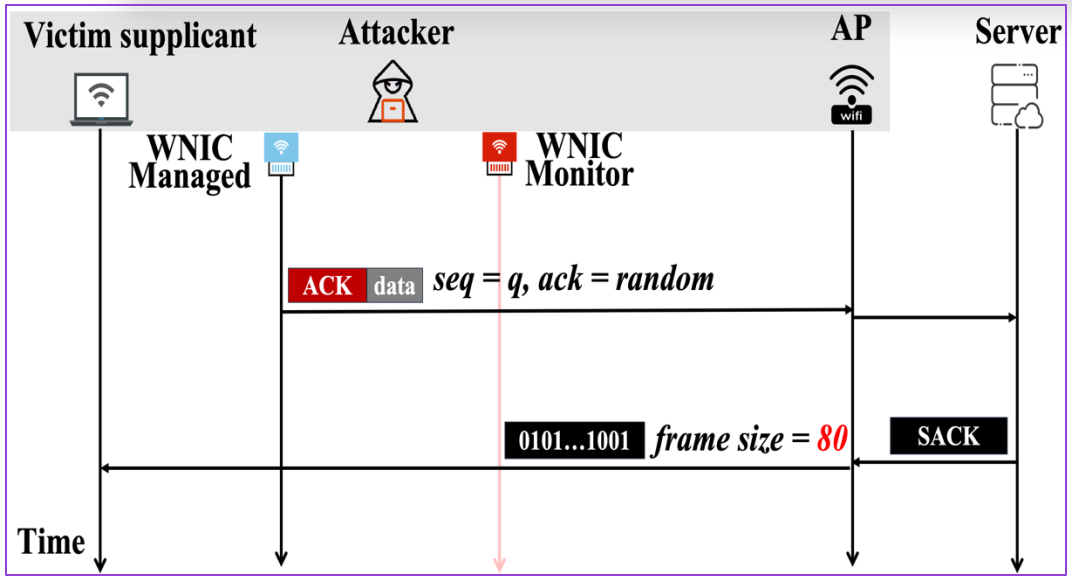
- Guess **the correct source port** number
- The server will respond with a **challenge ACK**
- ACK packet will carry with **timestamp option**
- Resuting in frame **size of 68**



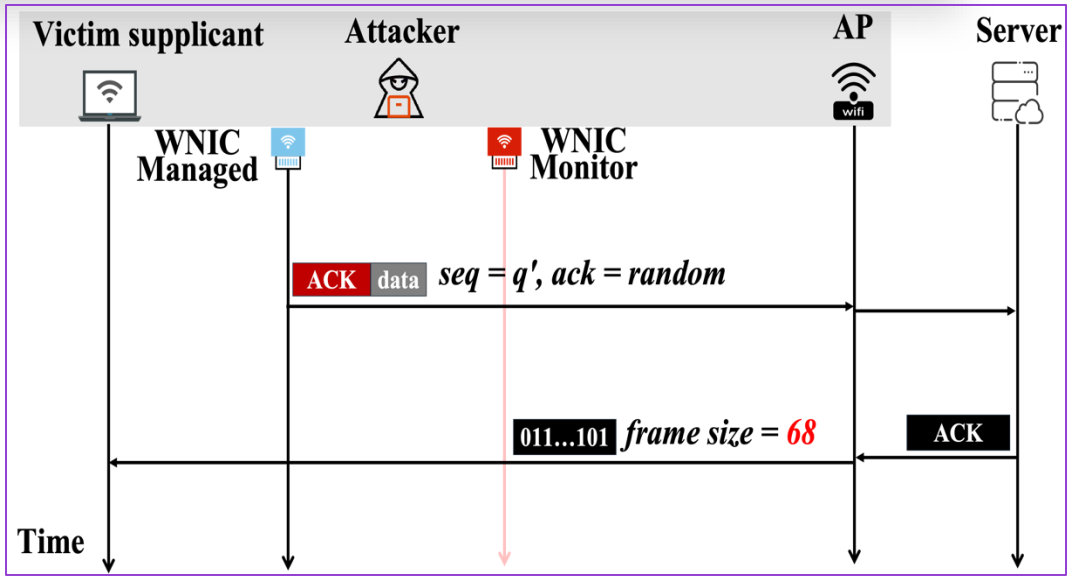
- Guess **an incorrect source port** number
- The server will respond with **a RST packet**
- RST packet will **not carry any option**
- Resuting in frame **size of 56**

Inferring Sequence Number

- Sending **ACK packets** with **guessed sequence numbers**
- Sniffing and **analyzing the sizes** of encrypted frames



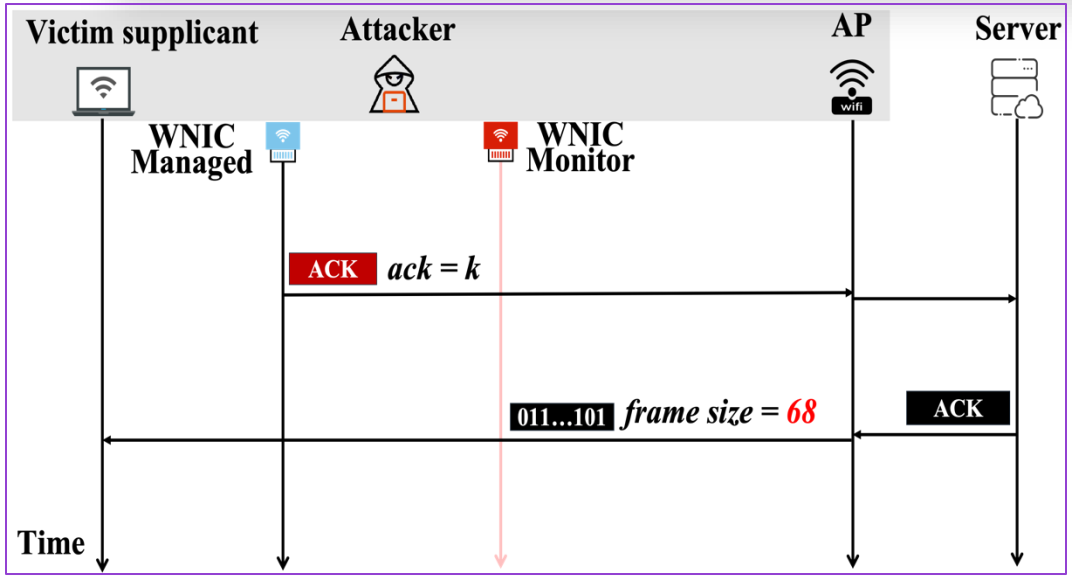
- Sequence number **less than** RCV.NXT
- The server will respond with a **SACK-ACK**
- Carry with **timestamp and SACK** option
- Resuting in frame **size of 80**



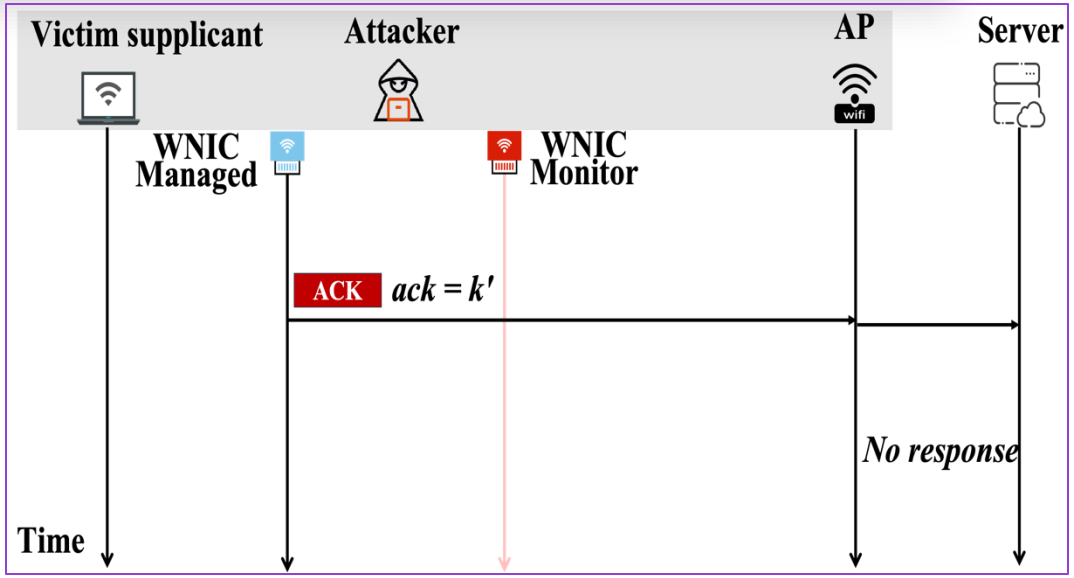
- Sequence number **greater than** RCV.NXT
- The server will respond with an **ACK**
- Carry with **only timestamp** option
- Resuting in frame **size of 68**

Inferring Acknowledgment Number

- Sending **ACK packets** with **guessed acknowledgment numbers**
- Sniffing and **analyzing the sizes** of encrypted frames



- Acknowledgment number **in window**
- The server will respond with an **ACK**
- Carry with **timestamp** option
- Resuting in frame **size of 68**



- Acknowledgment number **not in window**
- The server **will not respond**
- Resuting in **no frames**

Empirical Study

Analysis of Routers

🛠 **We perform tests on 30 mainstream wireless routers/APs from 9 vendors.**

- Xiaomi, TP-LINK, HUAWEI
- ASUS, Tenda, Netgear
- Linksys, Ruijie, H3C

Frame size side channel found in all routers

Router	Generation	WPA	IPv6 Enabled	Vendor	Built-in Firewall	Anti-Flooding	MAC-ADDR Filtering
Mi 4C	Wi-Fi 4	WPA2	No	Xiaomi	●	●	●
Redmi AC2100	Wi-Fi 5	WPA2	Yes	Xiaomi	●	●	●
AX6000	Wi-Fi 6	WPA2/WPA3	Yes	Xiaomi	●	●	●
AX9000	Wi-Fi 6	WPA2/WPA3	Yes	Xiaomi	●	●	●
TL-WR841N	Wi-Fi 4	WPA2	No	TP-LINK	●	○	●
Archer AXE300	Wi-Fi 6	WPA2/WAP3	Yes	TP-LINK	●	●	●
Archer C80	Wi-Fi 5	WPA2/WPA3	Yes	TP-LINK	●	○	●
Archer AX10	Wi-Fi 6	WPA2/WPA3	Yes	TP-LINK	●	●	●
AX3	Wi-Fi 6	WPA2/WPA3	Yes	HUAWEI	●	●	●
WS7200	Wi-Fi 6	WPA2	Yes	HUAWEI	●	●	●
WS7100	Wi-Fi 6	WPA2	Yes	HUAWEI	●	●	●
WS318N	Wi-Fi 4	WPA2	Yes	HUAWEI	●	○	○
RT-AC66U	Wi-Fi 5	WPA2	Yes	ASUS	●	●	●
RT-AC68U	Wi-Fi 5	WPA2	Yes	ASUS	●	●	●
RT-AX86U	Wi-Fi 6	WPA2/WPA3	Yes	ASUS	●	●	●
RT-AX82U	Wi-Fi 6	WPA2/WPA3	Yes	ASUS	●	●	●
AC 6	Wi-Fi 5	WPA2	Yes	Tenda	●	○	○
AC 8	Wi-Fi 5	WPA2	Yes	Tenda	●	○	●
AC 23	Wi-Fi 5	WPA2	Yes	Tenda	●	●	●
F9	Wi-Fi 4	WPA2	No	Tenda	○	○	●
AX1800	Wi-Fi 6	WPA2/WPA3	Yes	Netgear	●	○	●
AX5400	Wi-Fi 6	WPA2/WPA3	Yes	Netgear	●	○	●
E5600	Wi-Fi 5	WPA2	Yes	Linksys	●	●	●
E7350	Wi-Fi 6	WPA2/WPA3	Yes	Linksys	●	●	●
E8450	Wi-Fi 6	WPA2/WPA3	Yes	Linksys	●	○	●
RG-EW1200G PRO	Wi-Fi 5	WPA2	Yes	Ruijie	○	○	●
M32	Wi-Fi 6	WPA2	Yes	Ruijie	○	○	●
N21	Wi-Fi 5	WPA2	No	H3C	●	○	●
NX15	Wi-Fi 6	WPA2/WPA3	Yes	H3C	●	○	●
B6	Wi-Fi 6	WPA2/WPA3	Yes	H3C	●	●	●

○ indicates that the security mechanism is not supported by the router, while ● indicates that it is supported.

Details of tested wireless routers/APs

Attack Evaluation

SSH DoS Attack:

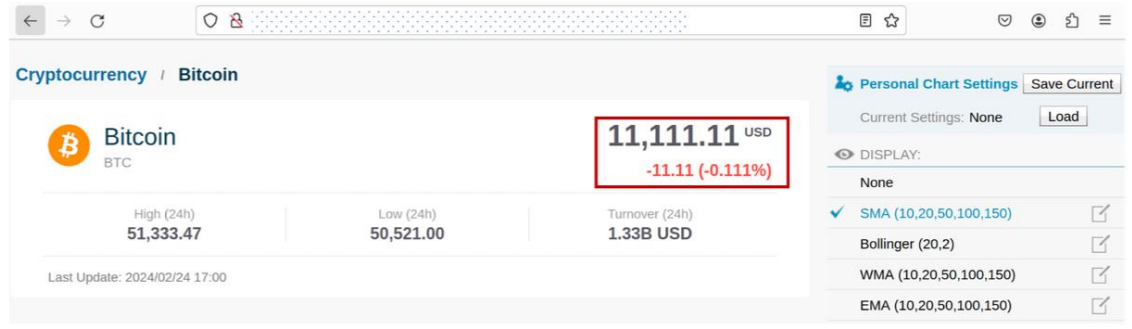
- Success rate: 84%
- Attack time: ~19s

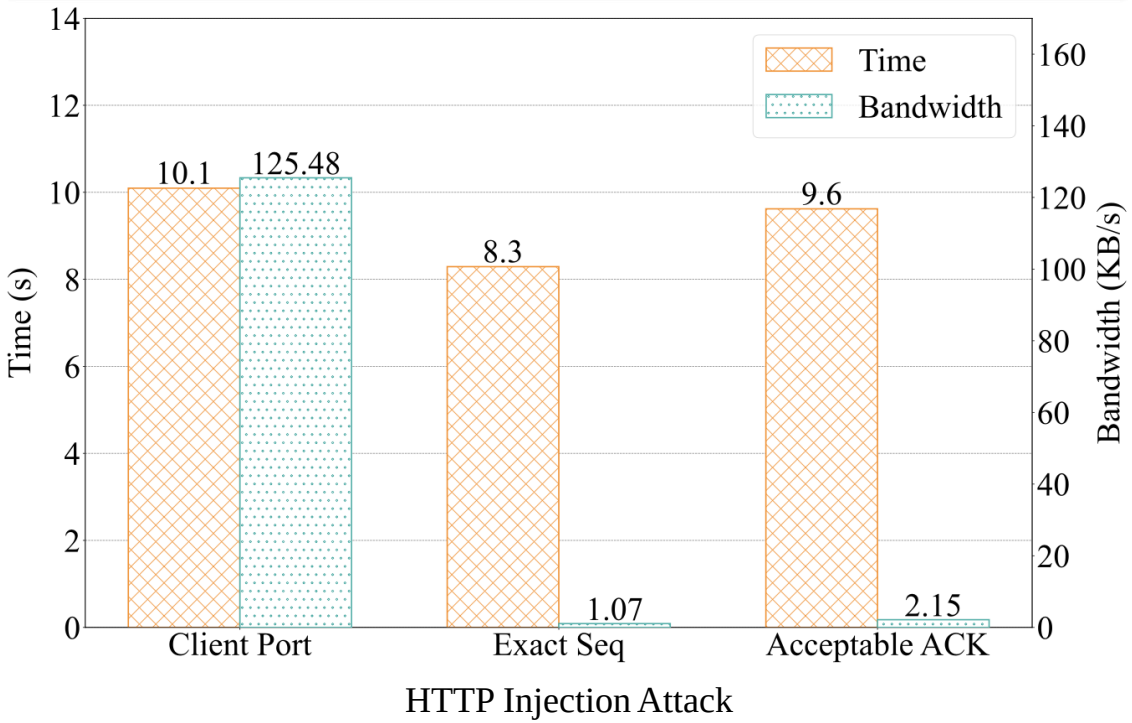
HTTP Injection Attack:

- Success rate: 72%
- Attack time: ~28s

Server address	Linux version	Time cost (s)	Bandwidth cost (KB/s)	Success rate
82.x.x.41	5.4	18.47	77.04	8/10
150.x.x.186	5.15	19.56	80.91	9/10
43.x.x.151	5.10	18.24	69.15	8/10
43.x.x.84	4.15	17.26	68.18	8/10
43.x.x.187	3.13	20.12	82.07	9/10

SSH DoS Attack





HTTP Injection Attack

Real-World Attacks

- We conduct thorough experiments of the attack in **80 various real-world** Wi-Fi networks
- We take two case studies of attacks on **SSH and HTTP** applications and measure the success rate of each attack

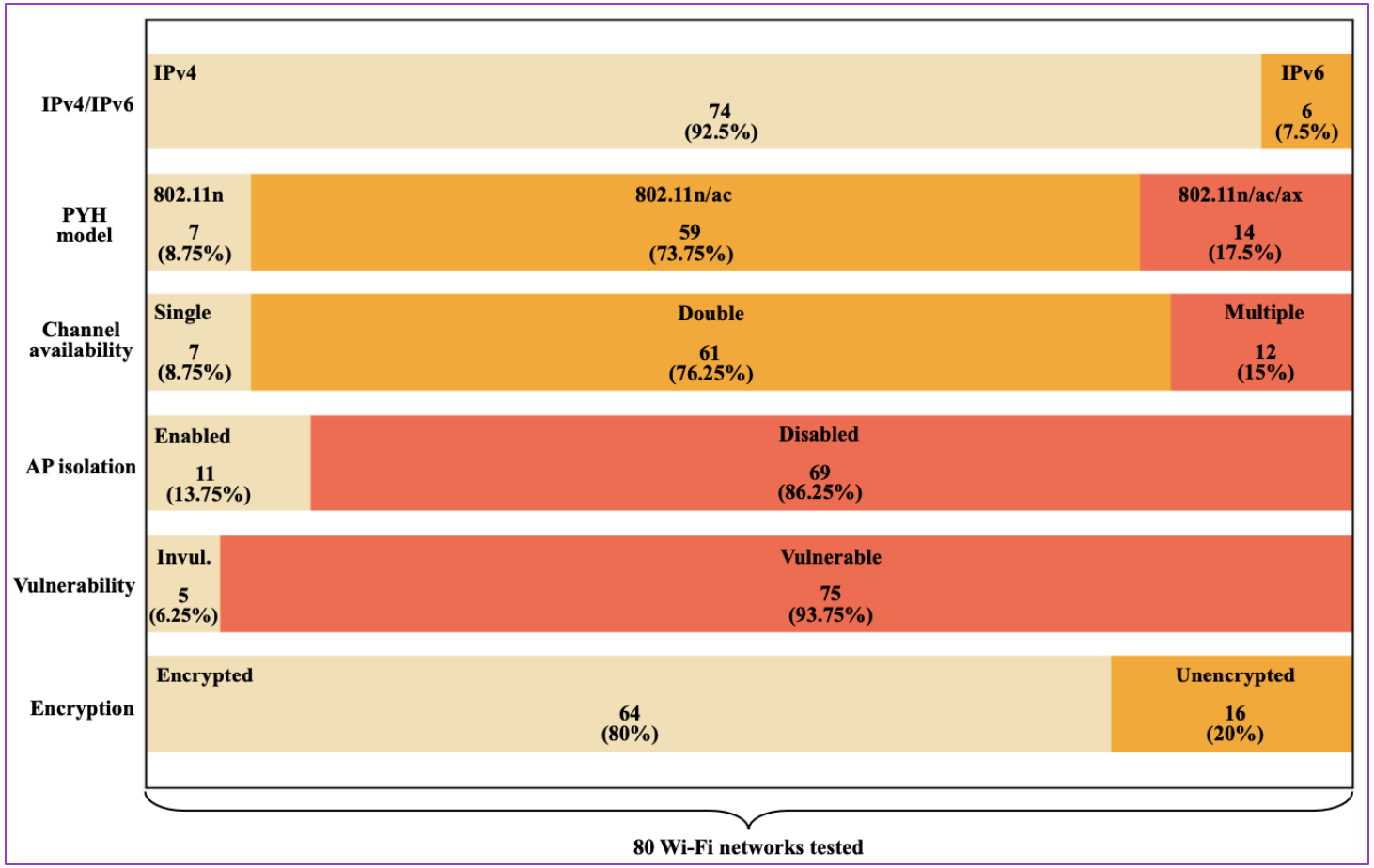
No.	SSID	AP Vendor	IPv4/IPv6	PHY model	AP isolation	Wi-Fi channel	SSH DoS	Web hijack
1	Bookstore 1	ADSLR	◐	802.11n/ac	No	6, 161	7/10	6/10
2	Bookstore 2	HUAWEI	◐	802.11n/ac/ax	No	11, 44	7/10	7/10
3	Bookstore 3	Xiaomi	◐	802.11n/ac	No	6, 149	8/10	7/10
4	Coffee Shop 1	TP-LINK	◐	802.11n/ac	No	6, 60	8/10	6/10
5	Coffee Shop 2	Wimaster	◐	802.11n/ac	Yes	1, 48	7/10	6/10
6	Coffee Shop 3	Tenda	●	802.11n/ac	No	4, 153	6/10	5/10
7	Restaurant 1	D-Link	◐	802.11n/ac	No	5, 149	7/10	5/10
8	Restaurant 2	Ruijie	◐	802.11n/ac	Yes	11, 64	6/10	4/10
9	Restaurant 3	iKuai	◐	802.11n/ac	No	1, 48	5/10	3/10
10	Office building 1	TP-LINK	◐	802.11n/ac	No	11, 36, 40	7/10	6/10
11	Office building 2	H3C	●	802.11n/ac	No	1, 48, 153	8/10	7/10
12	Office building 3	Netcore	◐	802.11n/ac	Yes	6, 149	8/10	6/10
13	Enterprise 1	TP-LINK	◐	802.11n/ac	No	6, 36	6/10	6/10
14	Enterprise 2	HUAWEI	◐	802.11n/ac	Yes	11, 157	7/10	6/10
15	Enterprise 3	Ruijie	◐	802.11n/ac	Yes	1, 11, 40, 149	6/10	5/10
16	Fast Food Restaurant 1	Wimaster	◐	802.11n/ac/ax	No	6, 161, 149	6/10	4/10
17	Fast Food Restaurant 2	TP-LINK	◐	802.11n/ac	No	3, 157	7/10	6/10
18	Fast Food Restaurant 3	Ruijie	◐	802.11n/ac	No	1, 44	6/10	6/10
19	Cinema 1	HUAWEI	◐	802.11n/ac	No	1, 157	7/10	6/10
20	Cinema 2	Ruijie	◐	802.11n	No	6	7/10	6/10
21	Cinema 3	H3C	◐	802.11n/ac	No	10, 149	7/10	5/10
22	Hotel 1	HUAWEI	◐	802.11n/ac	No	6, 44	8/10	7/10
23	Hotel 2	D-Link	◐	802.11n/ac	No	1, 48	6/10	5/10
24	Hotel 3	Xiaomi	◐	802.11n	Yes	1	5/10	4/10
25	Experience Store 1	HUAWEI	◐	802.11n/ac	No	1, 36	7/10	6/10
26	Experience Store 2	HUAWEI	◐	802.11n/ac	No	11, 149	7/10	6/10
27	Experience Store 3	Tenda	◐	802.11n/ac	No	4,153	6/10	5/10
28	Campus 1	Xiaomi	◐	802.11n/ac	No	9, 36	6/10	4/10
29	Campus 2	Ruijie	◐	802.11n/ac	No	1, 44	7/10	6/10
30	Campus 3	H3C	◐	802.11n/ac	No	1, 6, 40, 64	6/10	6/10

◐ means IPv4 only and ● means both IPv4 and IPv6 are supported.

Experimental Results of TCP Attacks in the Wi-Fi Networks.

Real-World Attacks

- 75 out of 80 Wi-Fi networks are vulnerable to our attack
- The attack failed in 5 WiFi networks
  - AP isolation
  - Reverse path validation

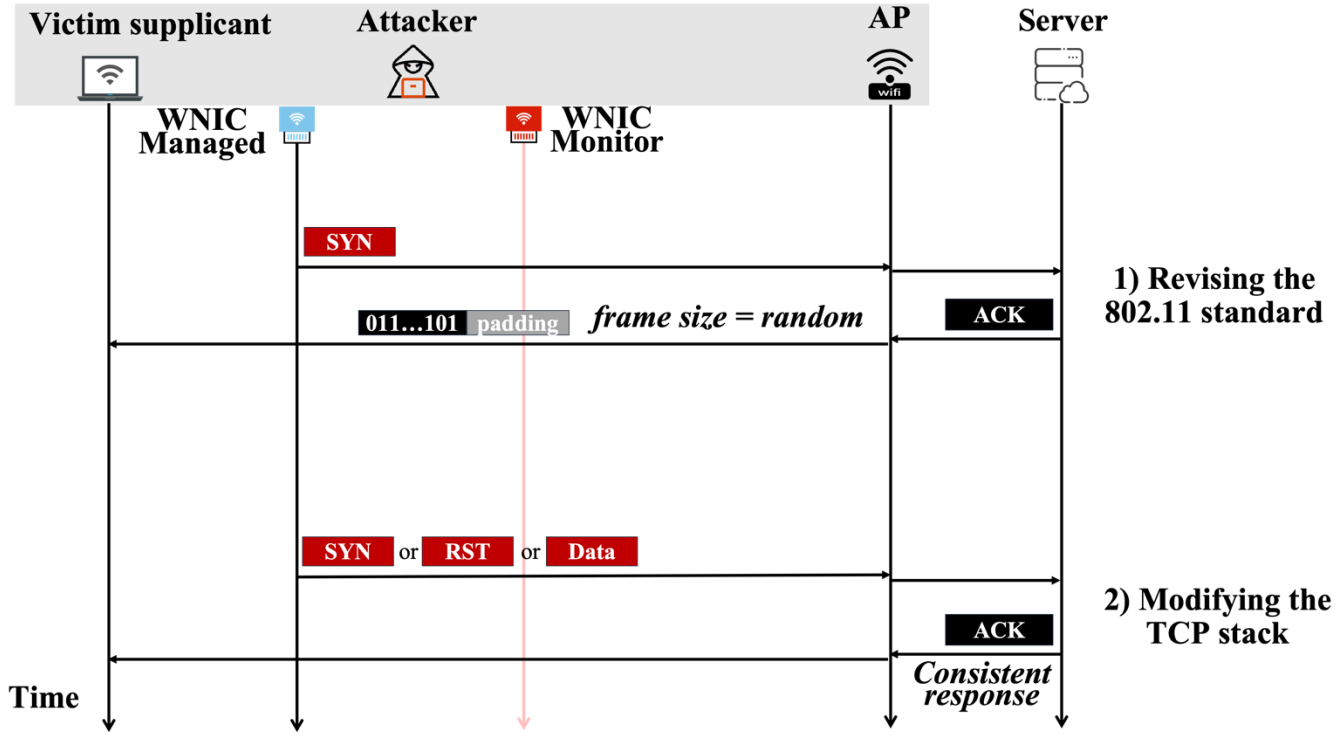


Analysis of 80 real-world WiFi networks

Mitigation

Mitigation

- Revising the 802.11 standard to support random padding for encrypted frame sizes
- Modifying the TCP protocol stack to ensure consistent response



Conclusion

- Uncovered a new side-channel (i.e., the encrypted frame size) in Wi-Fi networks to attack TCP connections
- Performed an extensive investigation against popular AP routers and real-world Wi-Fi networks
- Suggested defense countermeasures

Questions?