Exploiting Sequence Number Leakage: TCP Hijacking in NAT-Enabled Wi-Fi Networks

Yuxiang Yang, Xuewei Feng, Qi Li†, Kun Sun*, Ziqiang Wang**, and Ke Xu
Tsinghua University, George Mason University*, Southeast University**

Network and Distributed System Security Symposium (NDSS '24)

2024.02.22.

GyeongHeon Jeong(ghjeong@mmlab.snu.ac.kr)

Index

Introduction

- **Wi-Fi** has emerged as one of the most popular technologies for providing Internet access
- Wi-Fi networks are often exploited by malicious attackers to launch various attacks
  - Eavesdropping, Evil-Twin, ARP poisoning attack, …
- Most of the prior attacks have been mitigated
  - WPA2, WPA3, AP isolation, ARP prevention, and Rogue AP detection

- Proposed Attack: **off-path TCP hijacking attack in Wi-Fi networks** that exploits vulnerabilities in the NAT mapping strategies of routers

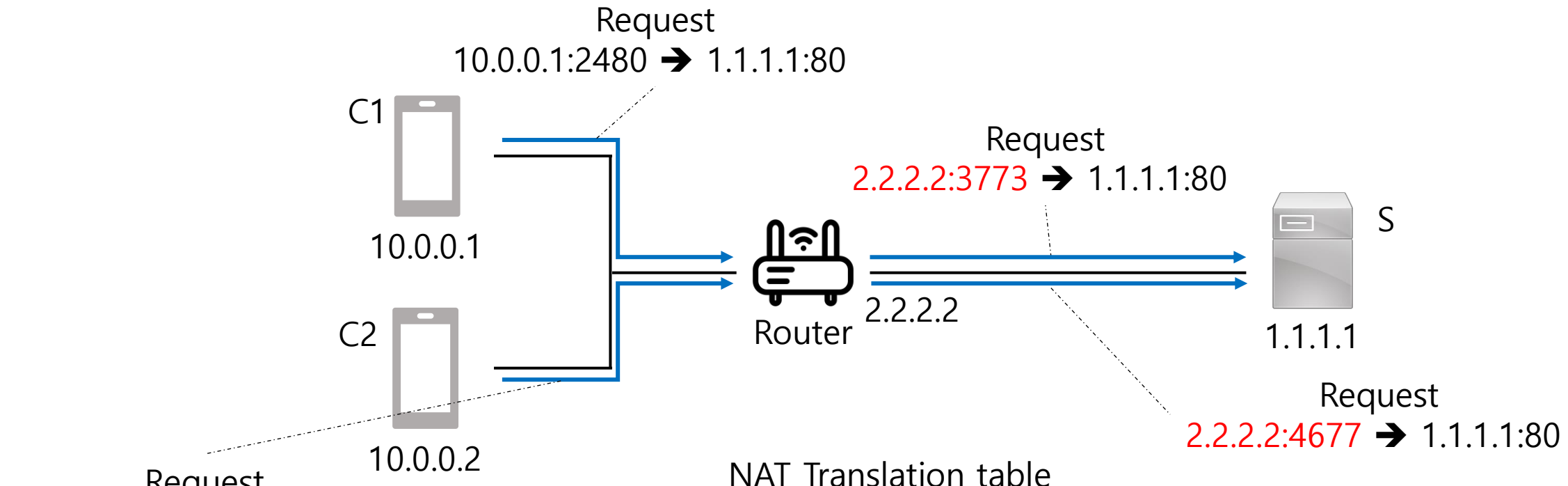
NAT (Network Address Translation)

- NAT is technique for transmitting network traffic through a router, rewriting the TCP/UDP port numbers and source/destination IP addresses of IP packets

- It is widely used to save IPv4 address space
  - After attaching to the same Wi-Fi network enabling NAT, clients share the external IP address to access the Internet

- When it takes the upper protocols (e.g., TCP and UDP) into consideration, the router will create NAT mappings to keep track of the connections
  - Router tries to keep the layer-4 information the same as the originators, such as the TCP source port

NAT (cont.)



NAT Translation table

Outside Port	Inside Port	Inside IP address

Protocol, session state, and mapping timeout can be included

How to set port number?
➔ Port allocation strategy

Port Allocation Strategies

- **Port preservation**
  - NAT device attempts to preserve the source port if possible.
  - When a collision happens, the NAT device should resolve the collision by selecting a new port (e.g., another random unused port)
- **Random selection**
  - NAT device translates the source port to another random port from a pool of available ports
- **Sequential selection**
  - NAT device selects a random port for the first connection to each destination and translates the ports of subsequent packets to that destination consecutively
- **Port overloading**
  - NAT device always uses port preservation even in the case of collision

TCP Window Tracking in Routers

- The router can record the connection information for subsequent packet delivery as a middle device
  - However, router cannot record all of the information due to many reasons
- The real world router does not track the current TCP window of the connection, and thus it does not check the sequence and acknowledgment numbers of TCP packets strictly
  - Most of the routers in the market also disable the TCP window tracking strategy by default
- Disabling TCP window tracking can be abused by an off-path attacker to clean the NAT mappings of other clients with forged RST packets

Reverse Path Validation

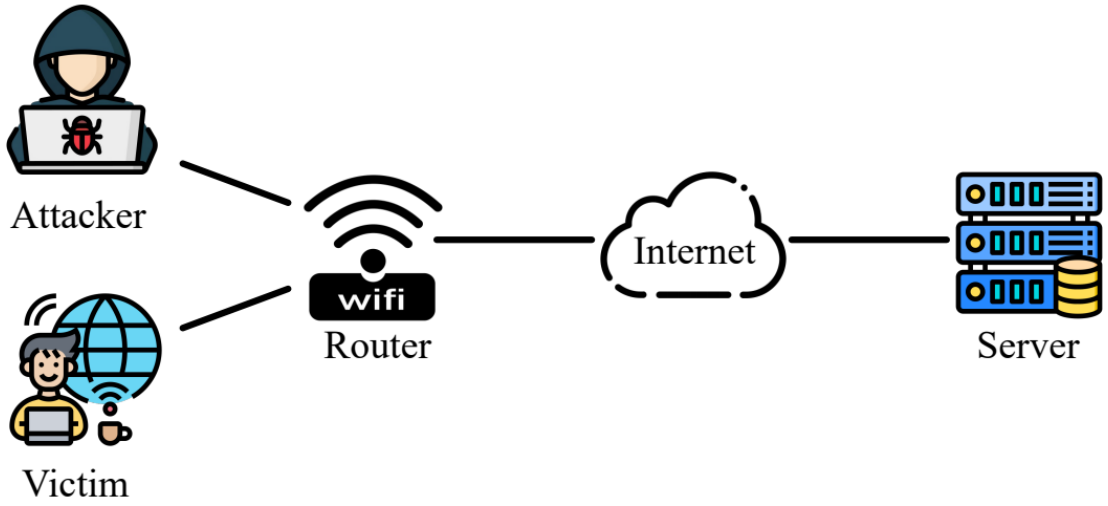
- The router verifies the authenticity of inbound traffic by checking whether the source IP address can be routed back via the interface on which packets are received against the routing table
  - Only if the packets can be routable back from the incoming interface will they be processed by the kernel and routed to their destinations

- Most routers do not run reverse path validation, thus they will not drop packets with spoofed source addresses matching a connection in the NAT mappings and will accept them on any interface

- The router without reverse path validation will process spoofed packets in the kernel mistakenly and thus change the state of the NAT mappings, leading to attack

Threat model

- Threat model of off-path TCP attacks in Wi-Fi networks
- Requirements
  - The attacker should be able to probe the external IP address of the router
  - The attacker tests whether AP isolation is enabled in the network
  - The router adopts the port preservation strategy, and no reverse path validation
  - The victim client does not communicate with the server frequently



Attack Procedure

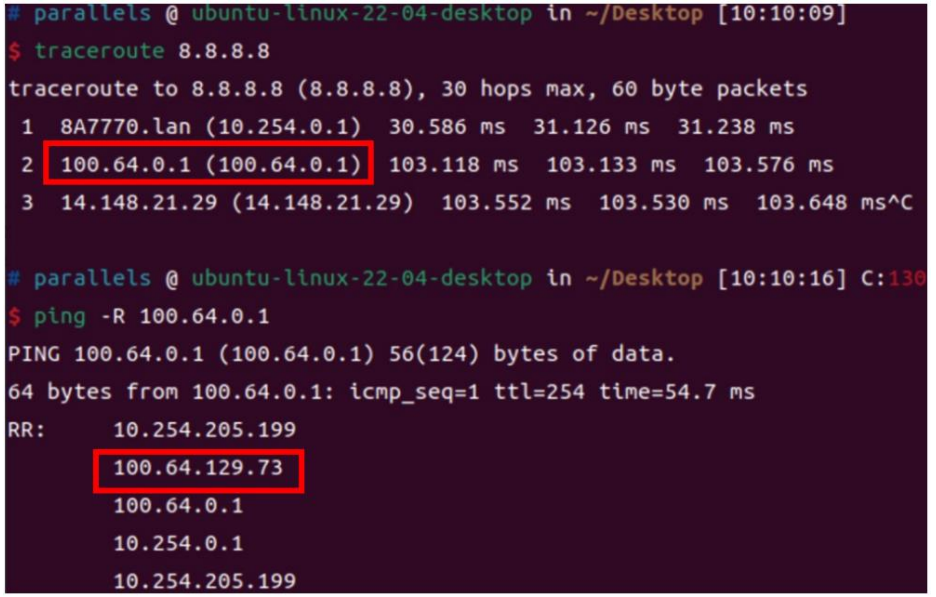
1. Probe the router's external IP address and identify whether AP isolation is enabled, thus finding potential victim clients

2. Make inferences about whether there is any active connection from the LAN to the server

3. Remove and construct NAT mappings at the router and then intercept the sequence and acknowledgment numbers from the replies to unsolicited packets from the server

Phase 1: Probing the Network

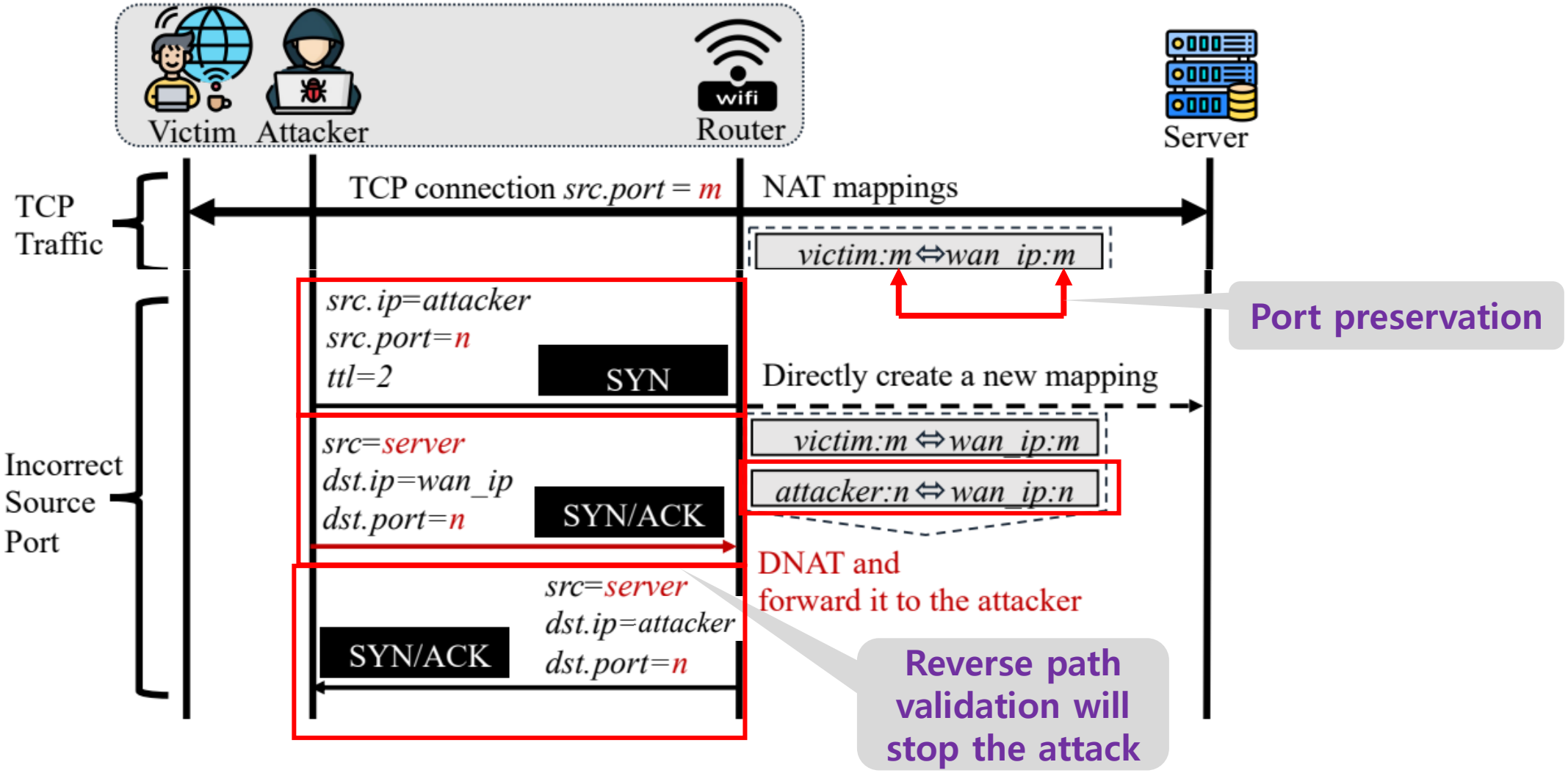
- Probing the external IP address of the router
  - (1) The attacker gets the gateways along the way to any outside host (e.g., 8.8.8.8) through Traceroute
  - (2) The attacker issues the ping command to the second gateway with the RECORD ROUTE option, which will record the passed routes



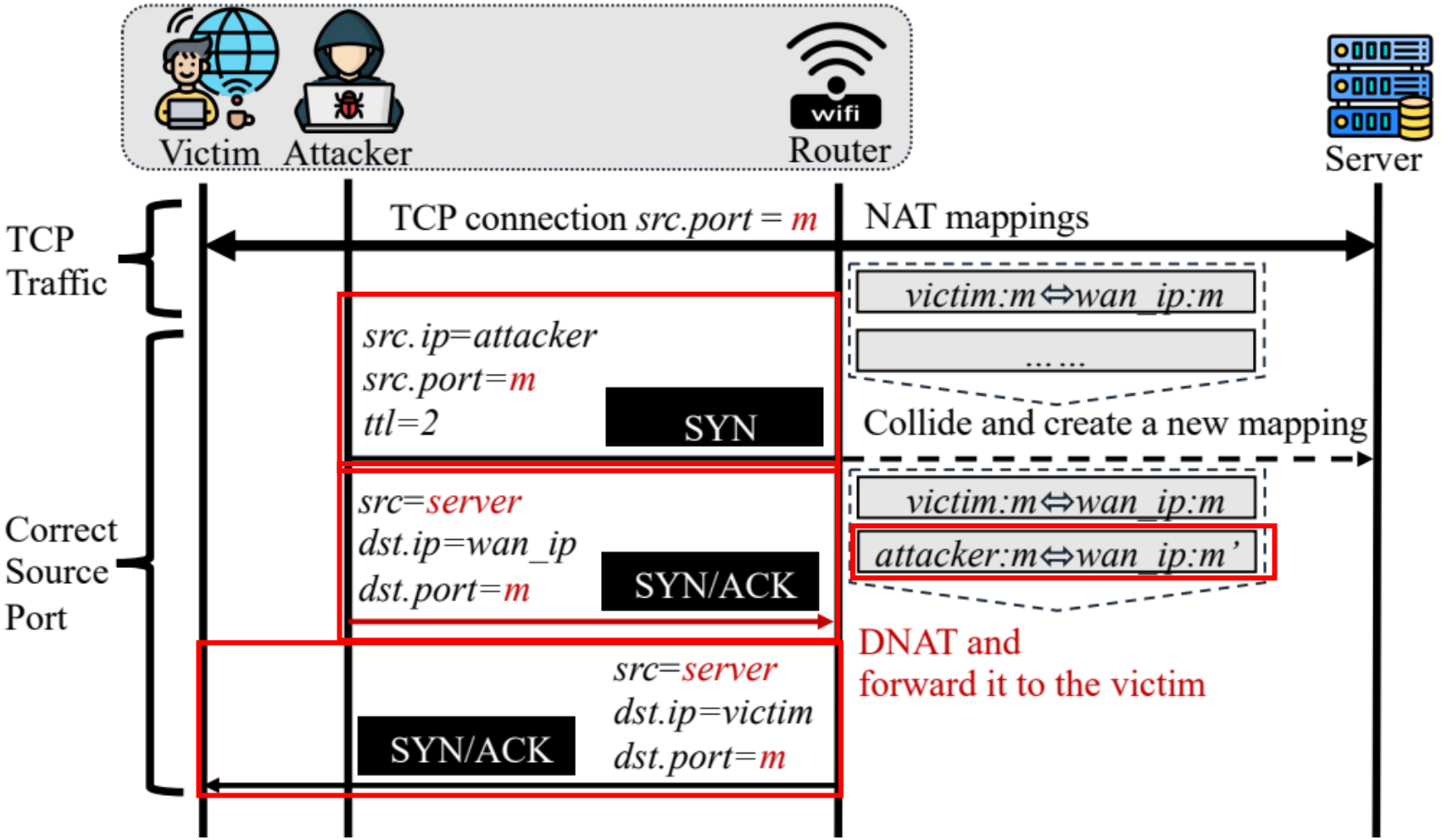
- Identifying the status of AP isolation in the network
  - The attacker detects whether AP isolation is enabled via network scanning tools (e.g., Nmap)

- Does not need to know victim client IP

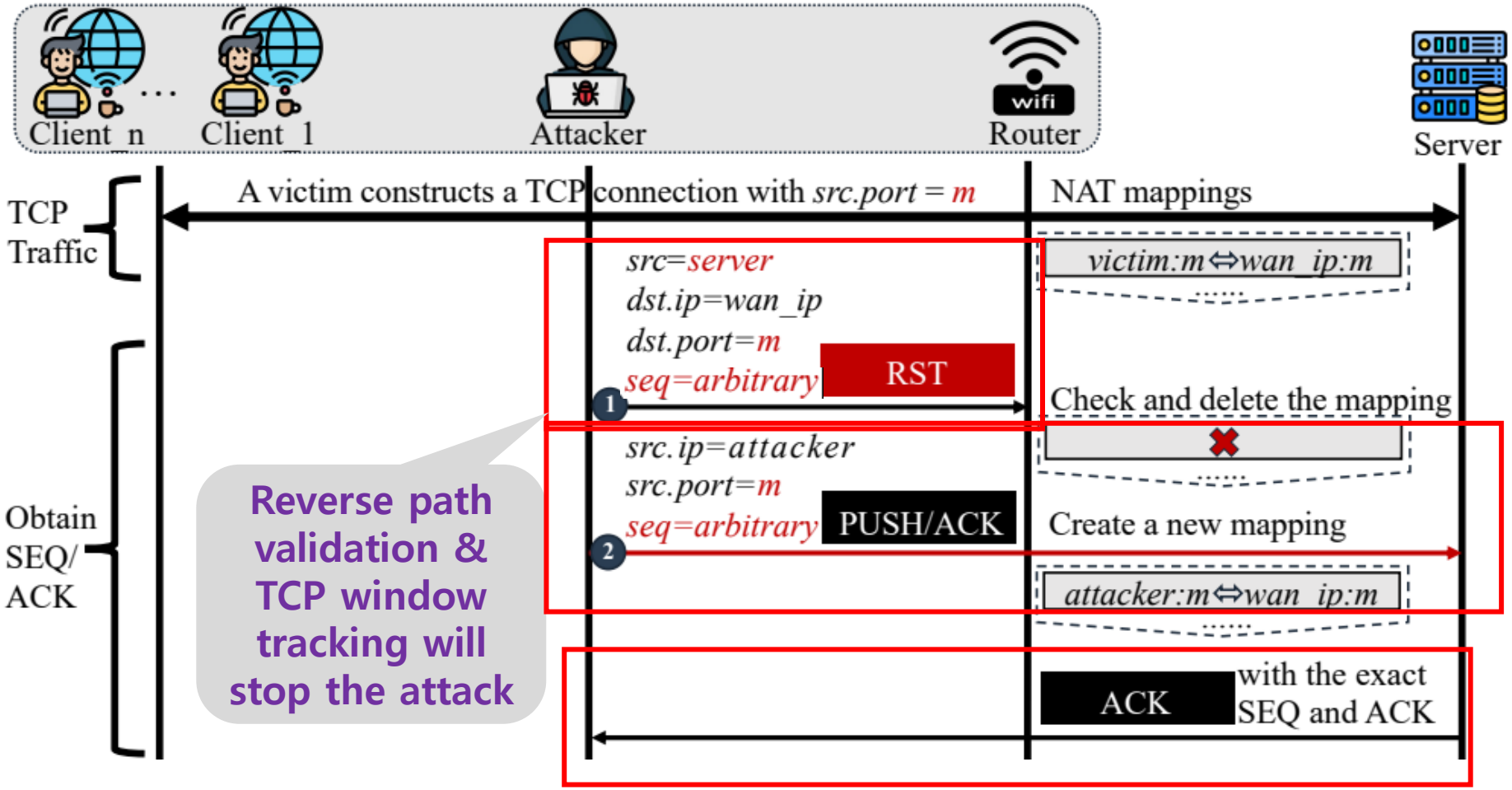
Phase 2: Making Inferences about Active Connections



Phase 2: Making Inferences about Active Connections (cont.)

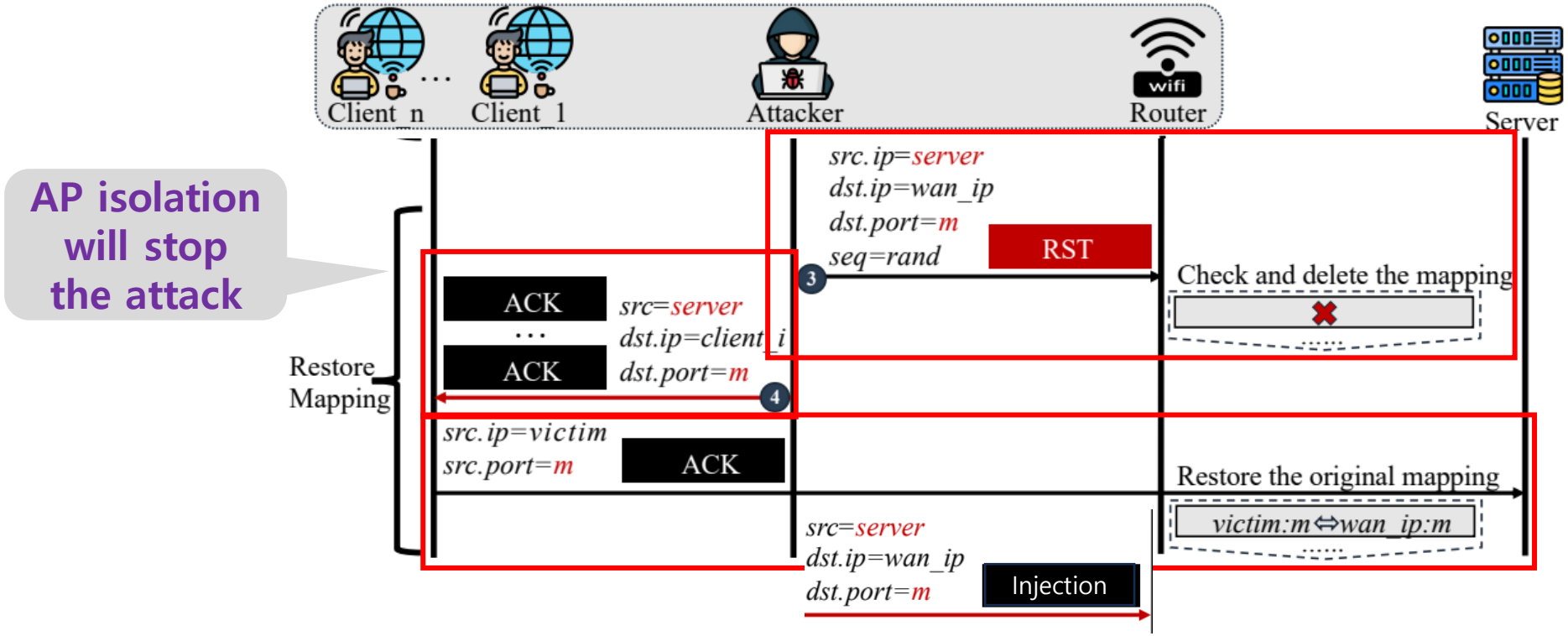


Phase 3: Hijacking Active Connections



Phase 3: Hijacking Active Connections (cont.)

- **TCP DoS attack**: Send forged TCP RST packets to the server
- **TCP hijacking attack**: Take over the NAT mapping and impersonate the client again to launch requests to the server
- **TCP injection attack**: Send forged responses by impersonating the server



Analysis of Routers

- Experiment about real-world evaluations to measure the impacts of this attack
- Investigate the default settings of routers on the market from lots of vendors
  - Test if it fits all attack conditions
- In conclusion, 52 of the 67 tested routers are vulnerable

No.	Router Model	Vendor	OS	Generation	Port Preservation	Reverse-path Validation Disabled	TCP Window Tracking Disabled	TCP Close Timeout (second)	Vulnerable
1	TL-XDR6020	TP-Link	Linux-based	Wi-Fi 6	✔	✔	✔	1	✔
2	TL-WDR7620	TP-Link	Vxworks-based	Wi-Fi 5	✔	✘	✔	1	✘
3	AX3 Pro	Huawei	EMUI (Linux-based)	Wi-Fi 6	✔	✔	✔	10	✔
4	AR6140E-9G-2AC*	Huawei	VRP (Linux-based)	-	✘	✘	✔	10	✘
5	V6G	360	360OS(Linux-based)	Wi-Fi 6	✔	✔	✔	1	✔
6	Magic R365	H3C	Comware(Linux-based)	Wi-Fi 5	✔	✔	✔	10	✔
7	W30E	Tenda	Linux-based	Wi-Fi 6	✔	✔	✔	1	✔
28	AX1800	JdCloud	Linux-based	Wi-Fi 6	✔	✔	✔	10	✔
29	Cisco Meraki 64*	Cisco Meraki	Linux-based	-	✔	✘	✘	-	✘
30	eero pro	Amazon	Linux-based	Wi-Fi 5	✔	✔	✔	10	✔
31	Google Wi-Fi	Google	ChromeOS(Linux-based)	Wi-Fi 5	✔	✔	✔	10	✔
32	GL-MT3000	GL.iNet	Linux-based	Wi-Fi 6	✔	✔	✔	10	✔
33	pfSense 2.7.0*	pfSense	FreeBSD-based	-	✘	✘	✔	90	✘

Attack Evaluation

- Experimental setup
  - Remote server
    - DoS attack - SSH server equipped with Ubuntu 22.04 (kernel version 5.15.0), OpenSSH 8.9, and OpenSSL 3.0.2.
    - Hijacking attack - FTP server equipped with Ubuntu 22.04 (kernel version 5.15.0) and vsftpd version 3.0.3.
    - Injection attack - Well-known finance website (www.ANONYMOUS.com)

- SSH DoS attack, FTP hijacking attack, and HTTP injection attack will be done after hijacking active connection

- Repeat the experiments 20 times in each tested Wi-Fi network

Experimental Results

- 81% (75/93) are vulnerable that they satisfy all of the conditions of our attacks
  - Evaluate attack against 93 real world Wi-Fi networks

- Most failure cases are due to continuous communications between the client and the server
  - During timeout, victim's communication may interfere as the mapping will be refreshed

Attack Type	Inferring Port(s)	Getting SEQ/ACK(s)	Finishing Attacking(s)	Total Time(s)	BW (pkts)	Success Rate
SSH DoS	8.1	8.4	1.0	17.5	4000	87.4%
FTP Hijacking	9.1	9.2	1.1	19.4	4000	82.6%
HTTP Injection	9.4	15.2	29.9	54.5	4000	76.1%

(Average)

Countermeasures

- **Random port allocation** (⇔ port preservation)
  - The router is recommended to use the random selection strategy when creating new NAT mappings
  - With this strategy, the attacker hard to identify whether the port has been used by other internal hosts

- **Reverse path validation** (Enable)
  - The router is recommonded to adopt the reverse path validation
  - With this strategy, the attacker cannot impersonate, but may introduce additional performance overhead

- **TCP window tracking** (Enable)
  - The router is recommonded to have to keep the necessary information about connections
  - With this strategy, the attacker cannot send packet of random sequence number, but making some performance overhead

Conclusion

- In this paper, they uncover new off-path TCP hijacking attack in the Wi-Fi networks that leverages vulnerable routers

- Malicious insider can infer the existence of TCP connections and then obtain the sequence and acknowledgment numbers by manipulating the state of NAT mappings
  - Abusing the NAT port preservation strategy and insufficient reverse path validation strategy of the vulnerable routers disabling TCP window tracking strategy

- They confirm the vulnerability in a wide range of routers from different manufacturers and evaluate the new attack in different scenarios
  - Such as SSH DoS, FTP hijacking, and HTTP injection in various Wi-Fi networks.

Thank you for listening