The Dark Side of Operational Wi-Fi Calling Services

Tian Xie[1], Guan-Hua Tu[1], Chi-Yu Li[2], Chunyi Peng, Mi Zhang[1]

[1]Michigan State University

[2]National Chiao Tung University

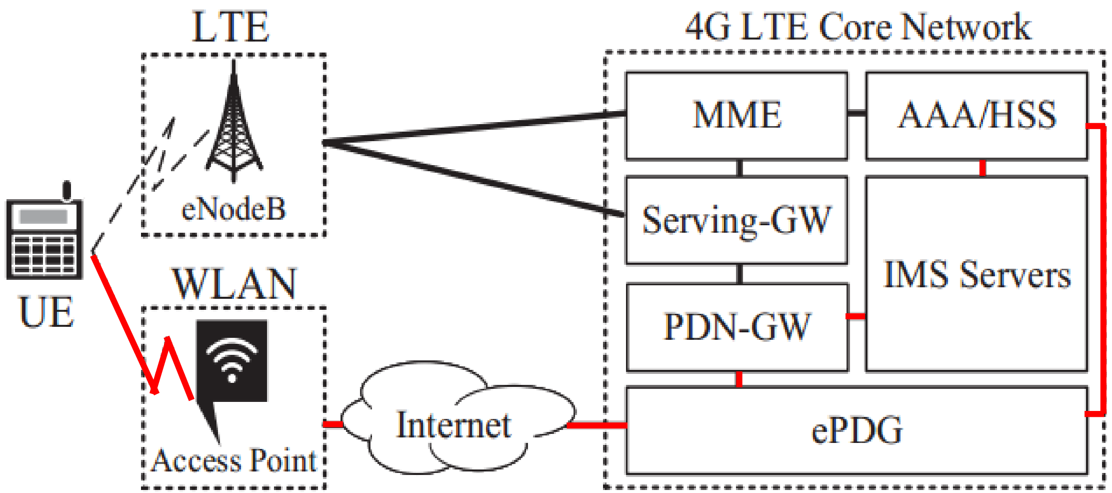
[3] Purdue University

Wi-Fi Calling Services

- Wi-Fi Calling services empower mobile users to access voice and text services over **Wi-Fi** instead of **cellular networks.**
- All of four U.S. major operators have launched Wi-Fi calling services since 2016 – Verizon, AT&T, T-Mobile, and Sprint.
- By 2020, Wi-Fi calling services will take **53%** of mobile IP voice service usage including VoLTE (26%) and others (21%).

Wi-Fi Calling Services Primer

- Specifically, they are **SIP-based** voice and text services, however, they are using a 3GPP-modified version.
  - Developed on top of 3GPP **IMS** (IP Multimedia Subsystem)
    - Operators use IMS to provide users with IP-based services such as VoIP
  - It uses **the same infrastructure** for VoLTE (Voice over LTE) users.



- Radio Access Network (RAN)
  - **Wi-Fi Access Point (Wi-Fi Calling)**
  - eNodeB (VoLTE)
- LTE Core Network (CN)
  - **ePDG (Evolved Packet Data Gateway, Wi-Fi calling)**
  - PDN-GW (Public Data Network Gateway)
  - AAA (Authentication, Authorization, and Accounting)
  - IMS (IP Multimedia Subsystem)

Wi-Fi Calling Security Mechanisms

- Using well-examined 3GPP Authentication and Key Agreement (AKA) and SIM-based security adopted by VoLTE – symmetric cryptography.
- All Wi-Fi calling signaling and voice/text packets are delivered through IPsec (Internet Protocol Security) – ciphering and integrity protection.

How Does It Go Wrong?

Finding 1: Wi-Fi calling devices will activate Wi-Fi calling services over an insecure Wi-Fi network

Vulnerability: Wi-Fi calling devices do not exclude insecure Wi-Fi networks – (design defect of standards)

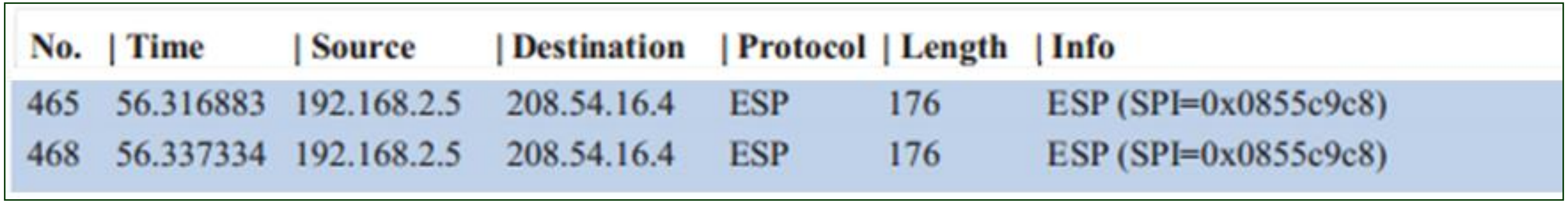
- Vulnerability – **Wi-Fi calling standards don’t exclude insecure Wi-Fi**
  - Two Wi-Fi access point selection modes do not consider security factors yet!!
  - Manual (use a prioritized list)
  - Automated (ANDSF, Access network discovery and selection function)
- Validation:
  - Deploy an insecure Wi-Fi network using a Wi-Fi router which is vulnerable to ARP spoofing attack – <u>foundation of a variety of MITM attacks</u>
    - I.e., victim’s WIFI packets will be intercepted and delivered to adversaries
  - We test whether the Wi-Fi calling devices keep connecting to the above Wi-Fi router

All tested Wi-Fi calling devices connected to the insecure Wi-Fi router!!!

Finding 2: Wi-Fi calling devices do not employ security defense against the common Wi-Fi ARP spoofing attacks

Vulnerability: Wi-Fi calling devices do not defend against ARP spoofing attacks –(implementation issue of devices)

- Vulnerability -Wi-Fi calling devices always accept **ARP Reply** message
  - **All packets sent by Wi-Fi calling devices can be redirected to adversaries**
- Validation
  - We use EtterCap to send ARP reply message to Wi-Fi calling devices.



No.	Time	Source	Destination	Protocol	Length	Info
465	56.316883	192.168.2.5	208.54.16.4	ESP	176	ESP (SPI=0x0855c9c8)
468	56.337334	192.168.2.5	208.54.16.4	ESP	176	ESP (SPI=0x0855c9c8)

Adversaries can capture all Wi-Fi packets sent by the victim

Finding 3: Wi-Fi calling devices and infrastructure indeed deploy extra security mechanisms for malicious Wi-Fi attacks, however, it is not enough.

A system-switch mechanism for Wi-Fi Calling Service DoS Attacks

- With the aforementioned two findings, adversaries can launch Wi-Fi Calling service DoS attacks
  - Discarding all intercepted Wi-Fi signaling and voice/text packets
- System-switch (Wi-Fi-> Cellular)
  - **If an user fails to dial a Wi-Fi voice call,** the mobile device will switch to use cellular-network-based voice services.
  - **If Wi-Fi calling service operators cannot route an incoming call to users by Wi-Fi calling**, the operators will switch it to use cellular-network-based one.

For users, they are free of voice/text DoS attacks.

Vulnerability: Service continuity is not revised accordingly – (design defect of standards)

- Service continuity can **seamlessly** switch an ongoing Wi-Fi calling call to back to cellular-network-based voice call
- However, it is only **triggered** while **the quality of Wi-Fi radio signals is bad**

What if Wi-Fi radio quality is good but Wi-Fi calling service quality is poor?

- We start dropping all Wi-Fi calling packets after the call conversation is started (Wi-Fi radio quality is good)

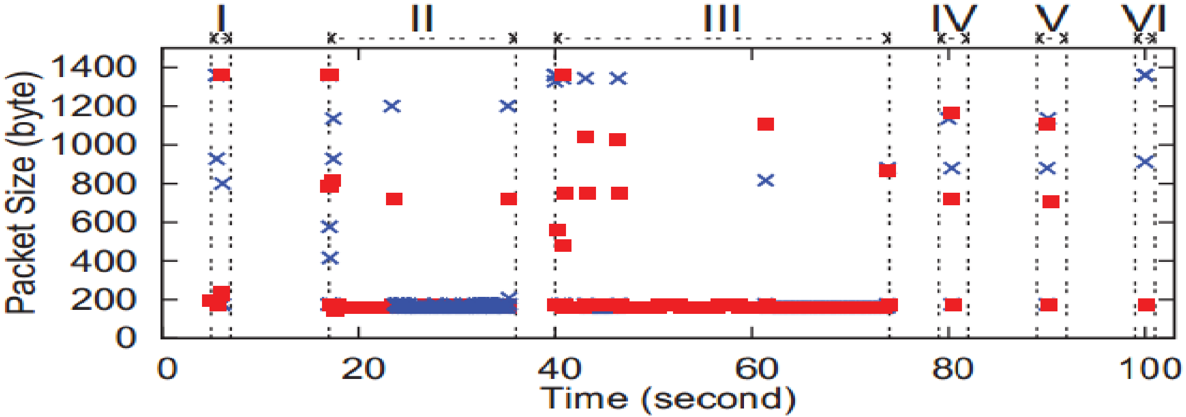
The system-switch security mechanism is bypassed!!

No cellular-based voice call is initiated.

Finding 4: Wi-Fi calling service operators do not take extra security mechanisms to protect the encrypted Wi-Fi calling packets

Vulnerability : The Wi-Fi calling traffic is vulnerable to side-channel attacks – (operational slip of operator)

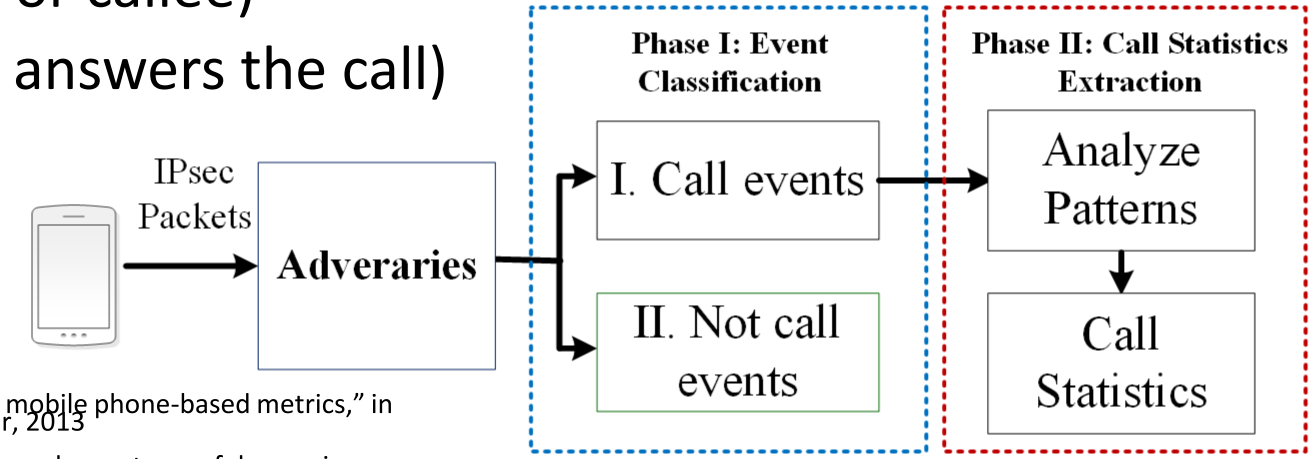
- Vulnerability -Wi-Fi calling is the **only service** that is carried by the IPSec channel between the mobile device and ePDG.
  - Adversaries may infer various Wi-Fi calling events such as dialing calls, receiving calls, etc.
- Validation
  - Apply C4.5 to analyze IPSec traffic patterns
  - We are able to infer six Wi-Fi calling events
    - Evt I: Activating Wi-Fi calling service
    - Evt II: Receiving an incoming call
    - Evt III: Dialing an outgoing call
    - Evt IV: Sending a text
    - Evt V: Receiving a text
    - Evt VI: Deactivating Wi-Fi calling service



Two Proof-of-concept Attacks

Attack 1: User privacy leakage

- The **call statistics** has been proven effective to infer user privacy including **personality[1], mood[2], malicious behaviors[3], etc**.
- Devising WiCA (Wi-Fi Calling Analyzer) to infer a Wi-Fi calling user's call statistics
    - Who initiates the call (an incoming call or an outgoing call)
    - Who hangs up the call first (caller or callee)
    - Ringing time (how long the callee answers the call)
    - Call conversation time



WiCA: WiFi-Calling Analyzer

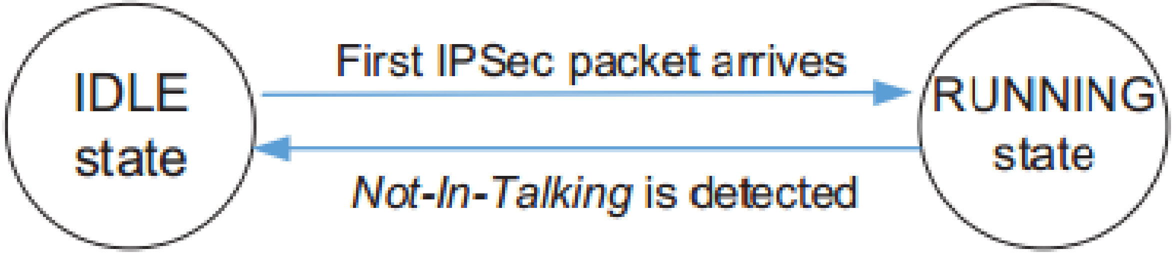
[1] Y.-A. de Montjoye, J. Quoidbach, F. Robic, and A. S. Pentland, "Predicting personality using novel mobile phone-based metrics," in International conference on social computing, behavioral-cultural modeling, and prediction. Springer, 2013

[2] S. Thomee, A. H´ arenstam, and M. Hagberg, "Mobile phone use and ¨ stress, sleep disturbances, and symptoms of depression among young adults-a prospective cohort study," BMC public health, vol. 11, no. 1, p. 66, 2011.

[3] V. Balasubramaniyan, M. Ahamad, and H. Park, "Callrank: Combating SPIT using call duration, social networks and global reputation," in CEAS'07, 2007

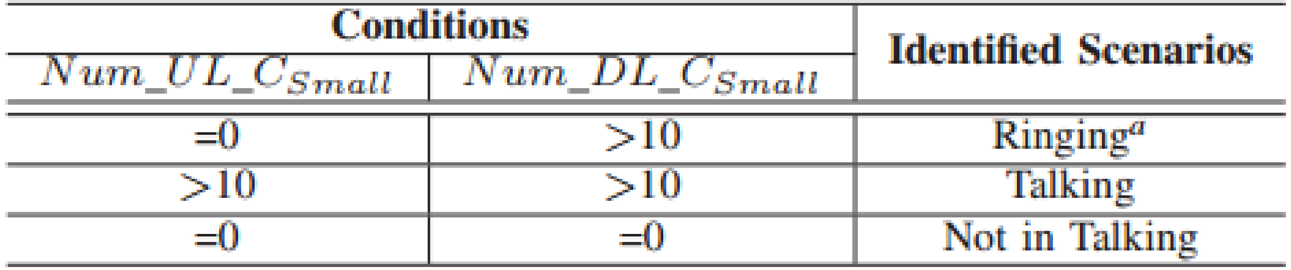
Infer call statistics@WiCA

- WiCA’s finite state machine



  - Record the number of **Uplink** and **Downlink** packets transmitted every 2 seconds
  - Classify them into three categories by packet size:
    - **Small** (<200 bytes), **Medium**(200-800 bytes), **Large** (>800 bytes)

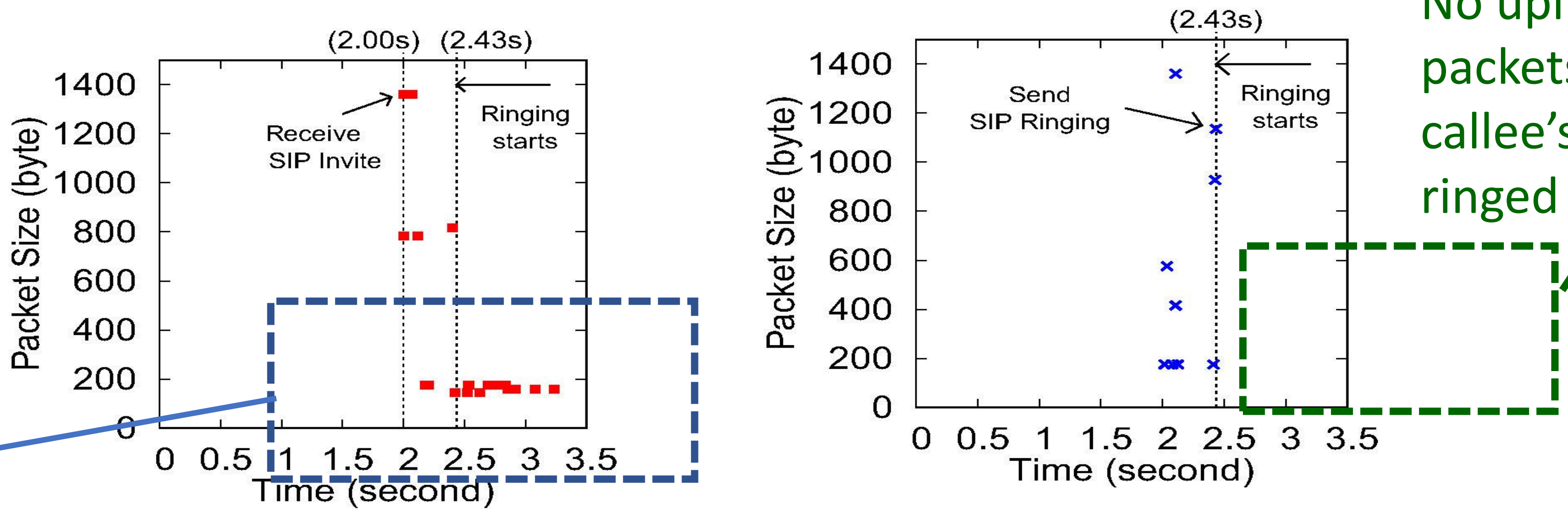
- Our observations on **small packets**



Conditions		**Identified Scenarios**
$Num\_UL\_C_{Small}$	$Num\_DL\_C_{Small}$	
=0	>10	Ringing[a]
>10	>10	Talking
=0	=0	Not in Talking

Ringing time inference

- We observe that Wi-Fi calling service servers will keep sending small packets to both of caller and callee after SIP RINGING message is sent by the callee.



Small downlink packets can be used to detect Ringing

No uplink small packets after callee’s phone is ringed

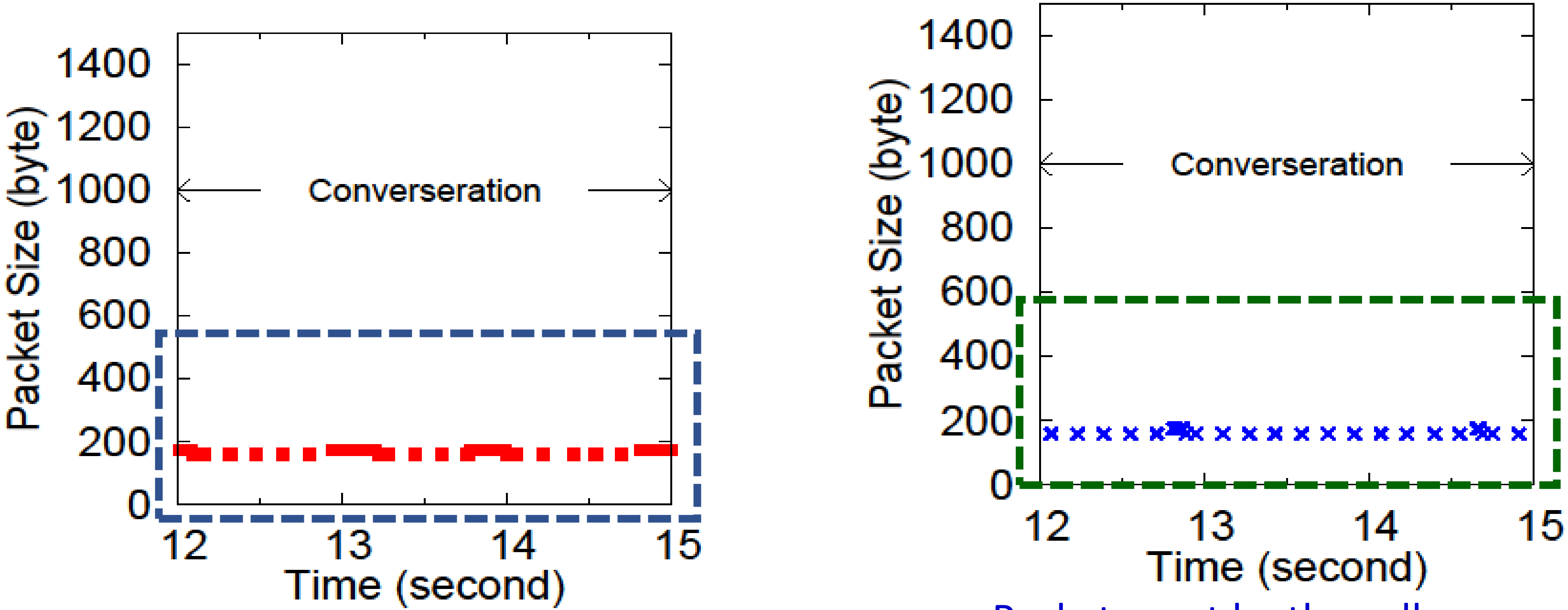
Packets sent by Wi-Fi calling server

Packets sent by the callee

Packet arrivals for the event ‘receiving a call with a ringtone’ (callee perspective).

Conversation time inference

- We observe small packets on the uplink and downlink during the call conversation



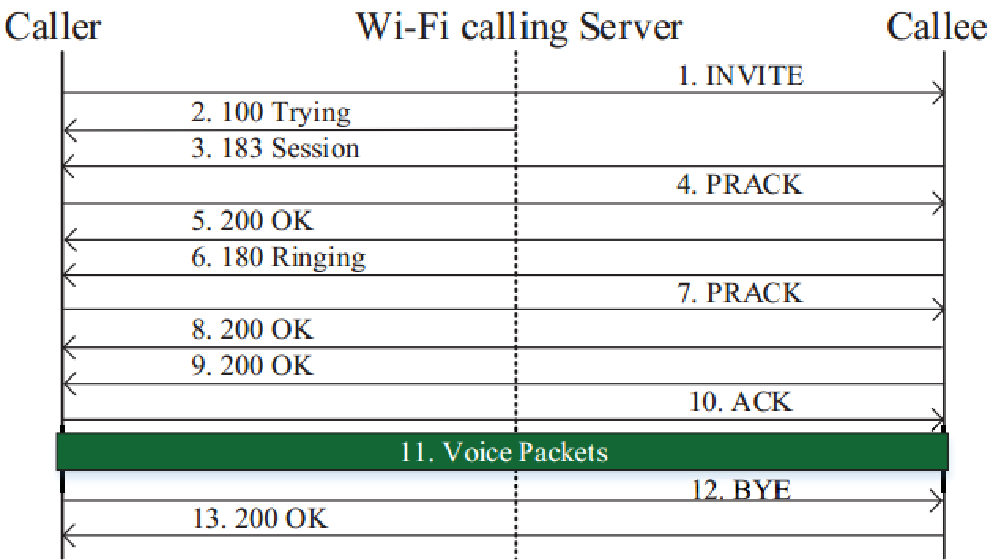
Packets sent by Wi-Fi calling server

Packets sent by the callee

Packet arrivals for ‘Talking’ (callee perspective).

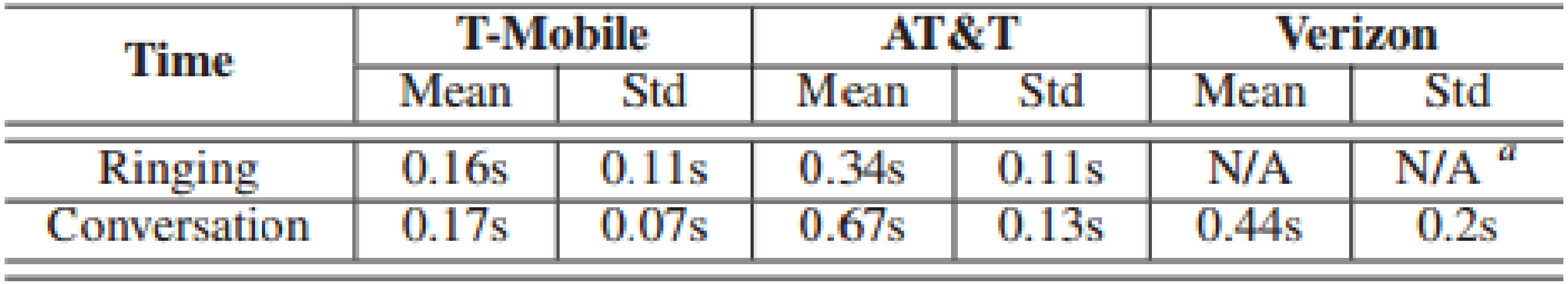
Call initiation and termination inference

- Relying on the directions and patterns of large packets
  - E.g., if the ringing or talking event is detected and the first large packet (SIP INVITE) is sent by the monitored Wi-Fi user => **It is an outgoing call**
  - E.g., if the talking and not-talking events are detected and the last large packet (200 OK) is sent by the Wi-Fi server => **the monitored Wi-Fi user terminates call first**



Performance of WiCA

- Who initiates, Who ends call first : 100% accurate
- Ringing time and conversation time
  - Maximum error is less than **0.8** seconds.



Time	T-Mobile		AT&T		Verizon	
	Mean	Std	Mean	Std	Mean	Std
Ringing	0.16s	0.11s	0.34s	0.11s	N/A	N/A [a]
Conversation	0.17s	0.07s	0.67s	0.13s	0.44s	0.2s

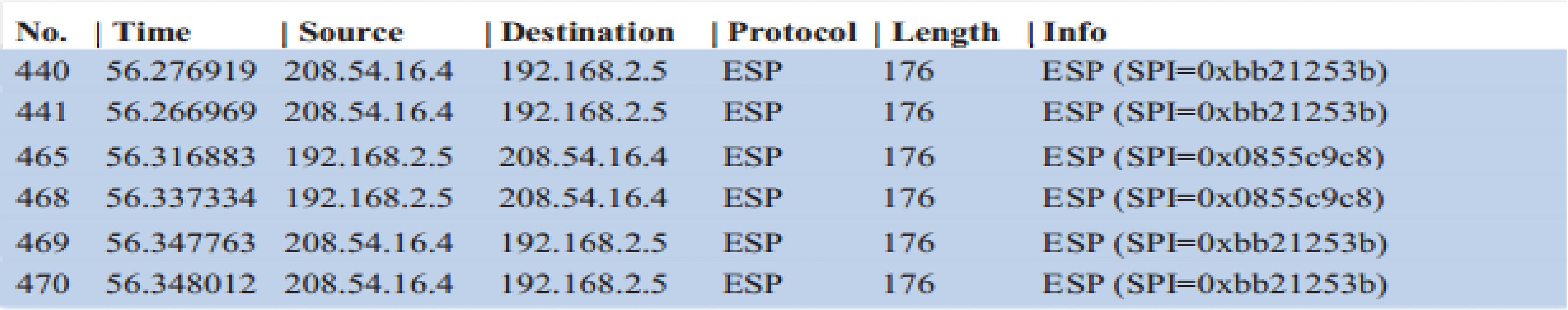
Another application of WiCA

- By face recognition, It is not difficult to identify who you are

- How about their IP addresses if they are using free public WiFi?

Xie?

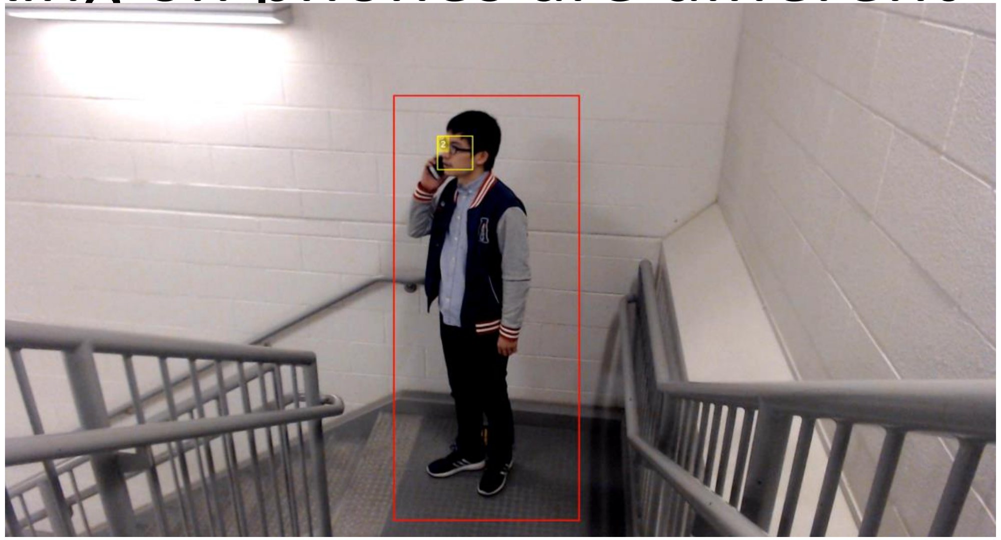
Peng?



No.	Time	Source	Destination	Protocol	Length	Info
440	56.276919	208.54.16.4	192.168.2.5	ESP	176	ESP (SPI=0xbb21253b)
441	56.266969	208.54.16.4	192.168.2.5	ESP	176	ESP (SPI=0xbb21253b)
465	56.316883	192.168.2.5	208.54.16.4	ESP	176	ESP (SPI=0x0855c9c8)
468	56.337334	192.168.2.5	208.54.16.4	ESP	176	ESP (SPI=0x0855c9c8)
469	56.347763	208.54.16.4	192.168.2.5	ESP	176	ESP (SPI=0xbb21253b)
470	56.348012	208.54.16.4	192.168.2.5	ESP	176	ESP (SPI=0xbb21253b)

WiCA with visual recognition system

- With the mature visual recognition system, WiCA's call statistics can help to identify both of user identities and their IP addresses
- The ways people are surfing and talking on phones are different

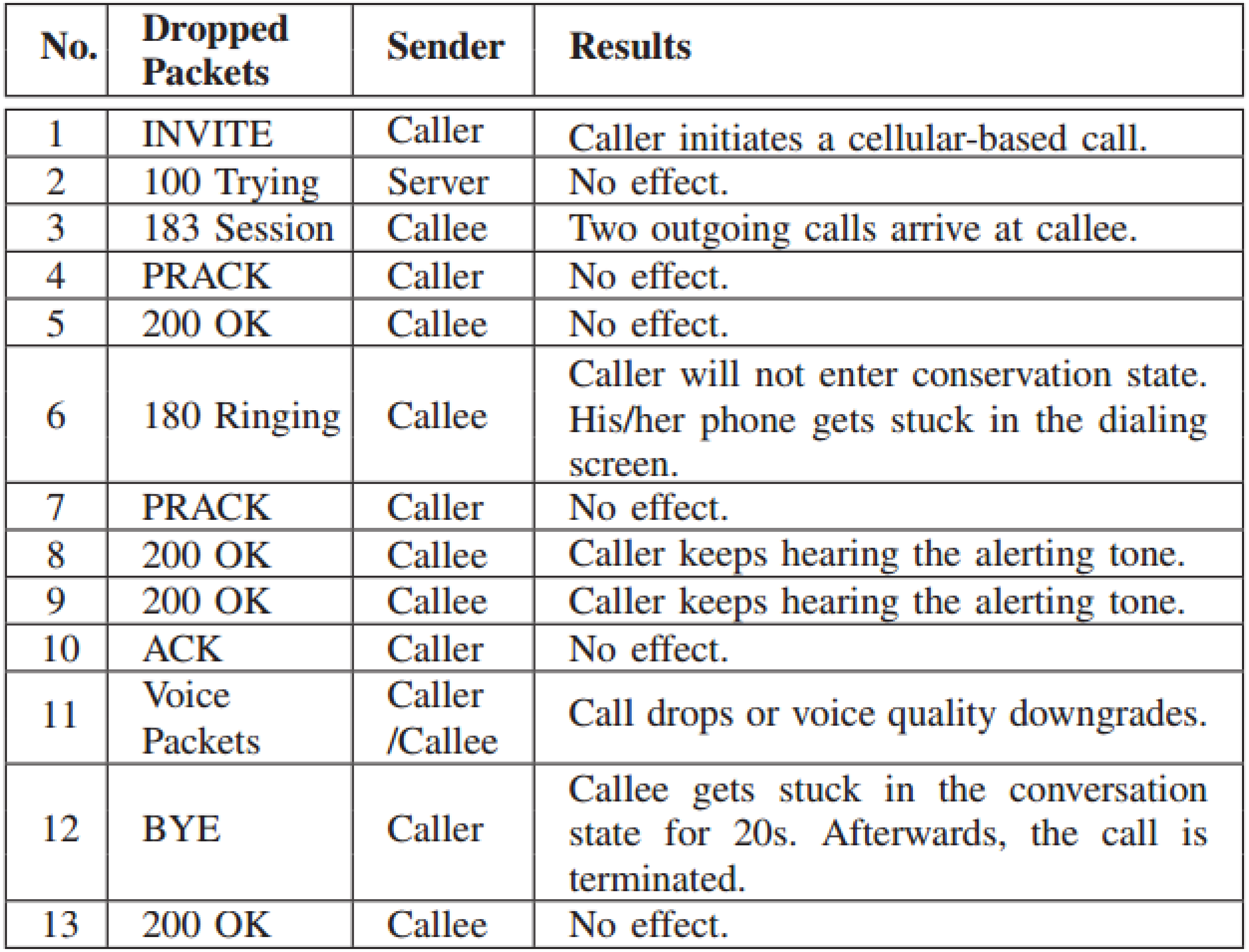


We know which of IP addresses is to initiate Wi-Fi calling call and its call statistics.

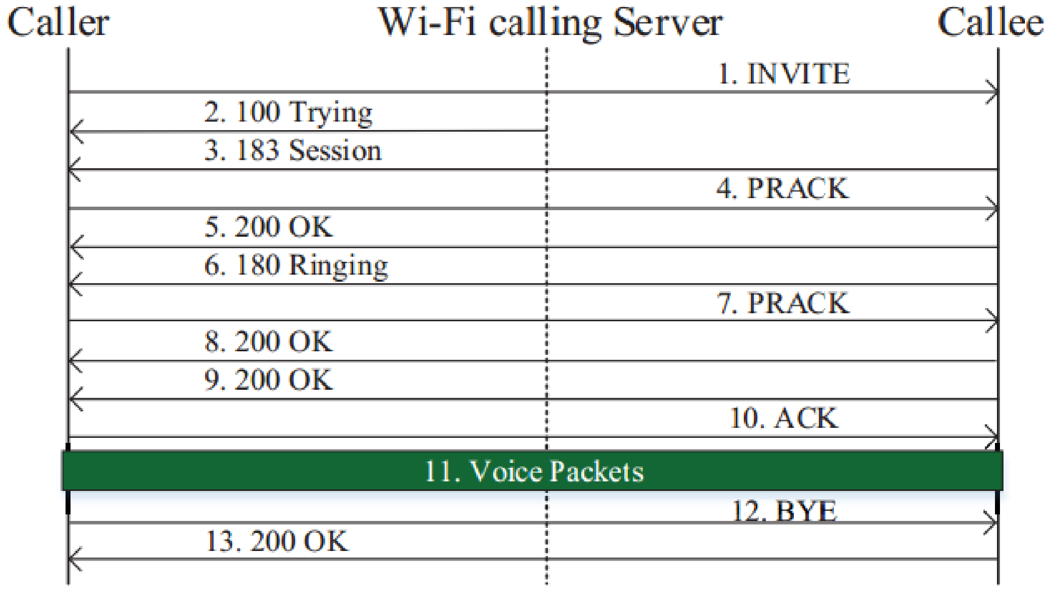
Attack 2: Telephony harassment or denial of voice service attack (THDoS)

- We devise a telephony harassment or denial of voice service attack against Wi-Fi calling users.
  - It can bypass the security defenses deployed on Wi-Fi calling devices and the infrastructure.
  - The attack is based on the manipulation of the delivery of Wi-Fi calling signaling and voice packets for an ongoing call.
  - It contains several variants.

Results of Discarding Wi-Fi Signaling and Voice packets



No.	Dropped Packets	Sender	Results
1	INVITE	Caller	Caller initiates a cellular-based call.
2	100 Trying	Server	No effect.
3	183 Session	Callee	Two outgoing calls arrive at callee.
4	PRACK	Caller	No effect.
5	200 OK	Callee	No effect.
6	180 Ringing	Callee	Caller will not enter conservation state. His/her phone gets stuck in the dialing screen.
7	PRACK	Caller	No effect.
8	200 OK	Callee	Caller keeps hearing the alerting tone.
9	200 OK	Callee	Caller keeps hearing the alerting tone.
10	ACK	Caller	No effect.
11	Voice Packets	Caller /Callee	Call drops or voice quality downgrades.
12	BYE	Caller	Callee gets stuck in the conversation state for 20s. Afterwards, the call is terminated.
13	200 OK	Callee	No effect.



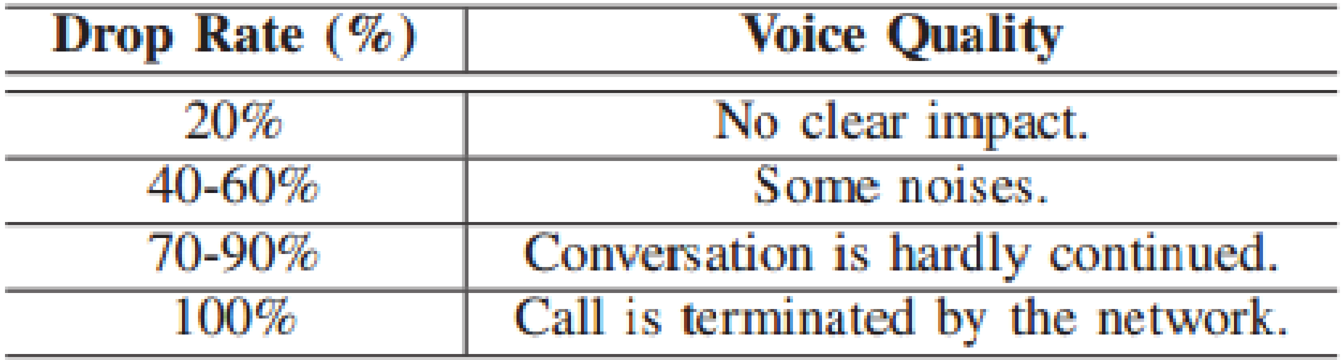
Wi-Fi calling Call Flow

Four Call Attack Variants

- Attack Wi-Fi signalings
  - Annoying-Incoming-Call Attack
    - Victim is callee:
      - He/she keeps receiving incoming calls
    - By discarding 180 Ringing message or 183 Session Progress message
  - Zombie-Call Attack – a call cannot be ended
    - Victim is caller:
      - The callee has answered the incoming call.
      - However, the caller's device gets stuck in the dialing screen and will keep hearing the alerting tone.
      - The conversation is never started.
    - By discarding 200 OK message

Four Call Attack Variants (cont.)

- Attack Wi-Fi voice packets
  - Mute Call Attack – a muted call
    - Can only mute a call for 8s, call will be terminated by network
    - Not terminate the call but only mute the call
  - Telephony Denial-of-Voice-Service Attack
    - Can make the conversation be hardly continued



Drop Rate (%)	Voice Quality
20%	No clear impact.
40-60%	Some noises.
70-90%	Conversation is hardly continued.
100%	Call is terminated by the network.

Real-world Impact

- We find that Wi-Fi calling users will suffer from the devised proof-of-concept attacks, specifically for the users who are using campus Wi-Fi
  - Usually provide their faculty, staff, students, and guests with free Wi-Fi
  - However, **they are not always secure** (cannot defend against our attacks)
    - MSU
    - New York University
    - University of California Berkeley
    - Northeastern University
    - etc

Solutions

Solutions

- Short-term: Using Virtual Private Network (VPN) service
  - It aims to increase the **difficulty** of launching side-channel attacks
  - Adversaries cannot easily infer each Wi-Fi calling service signalings/voice/text packets

- Long-term: Revisit Wi-Fi calling service standards
  - Stipulate required security mechanisms which defends against the state-of-the-art Wi-Fi based attacks
  - Empower both Wi-Fi calling device and infrastructure to detect whether users are under the attack by monitoring the quality of Wi-Fi calling services and take actions (e.g., excluding malicious Wi-Fi networks)
  - Revise the current service continuity procedure from security perspective

Conclusion

- We conducted the **first security study** on exploring the dark side of operational Wi-Fi calling services provided by three major U.S. operators as well as their commodity Wi-Fi calling devices.
- Four security vulnerabilities are discovered, which stem from **design defects** of Wi-Fi calling standards, **operational slips** of operators, and **implementation issues** of Wi-Fi calling devices.
- We demonstrate the **negative real-world impacts** (e.g., WiFi DoS) by two proof-of-concept attacks and provide recommended remedies.
- Our lessons learned can secure both Wi-Fi calling service users and operators and facilitate its global deployment, as well as provide new design insights for upcoming 5G networks.

Thank you! Questions?