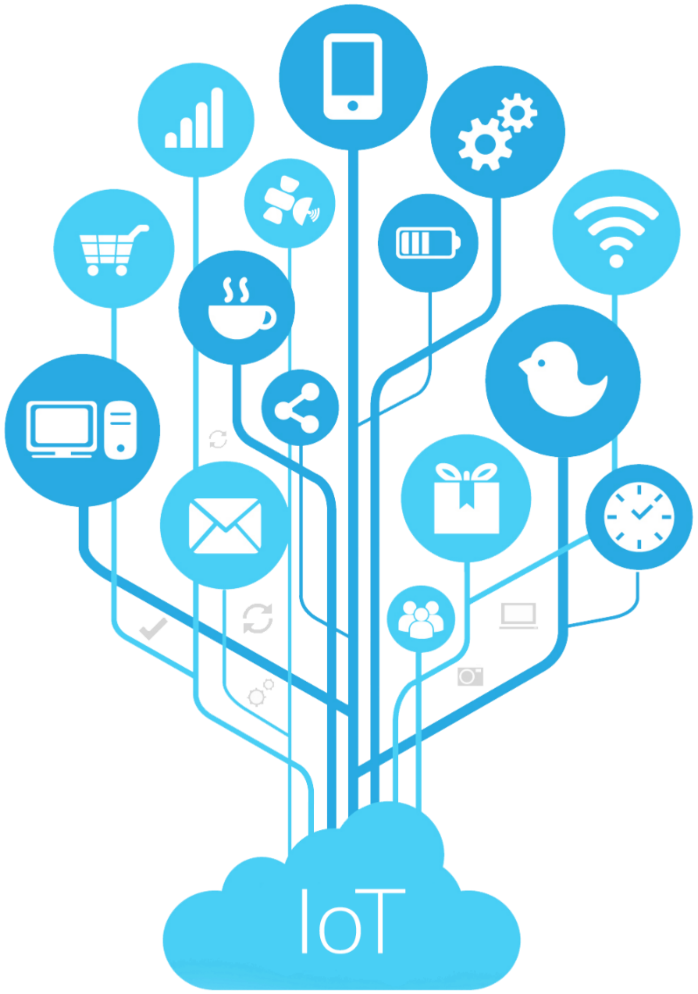
How Voice Service Threatens Cellular-Connected IoT Devices in the Operational 4G LTE Networks

Tian Xie[1], Chi-Yu Li[2], Jiliang Tang[1], Guan-Hua Tu[1]

[1]Michigan State University

[2]National Chiao Tung University

Internet-of-Things (IoT) Era



‘Things’ include a wide variety of devices

- House appliances
- Hotspot on vehicles
- Wearable devices
- Heart monitoring implants
- Cameras streaming live feed of wild animals
- Biochip transponders on farm animals
- Etc.

https://appsec-labs.com/iot-security/

Cellular IoT

- Rel-8/ Cat. 4, Rel-8/Cat. 1, etc.
- Providing wide range data rates (0.2 Mbps to 150 Mbps) with low-power consumption for IoT devices.
- Already being proposed in 4G LTE networks and can be merged with existing networks

Non-Cellular IoT

- LoRA, SigFox, etc.
- Only for low-speed transmission (<= 50 Kbps) and low-power consumption IoT services.

Key Problem for Cellular IoT Services

- Does the existing network infrastructure support IoT services well?

Glance of Cellular IoT

1. Cellular IoT devices share the similar network architecture with non-IoT devices (smartphones).
2. Specific IoT cellular network specification.

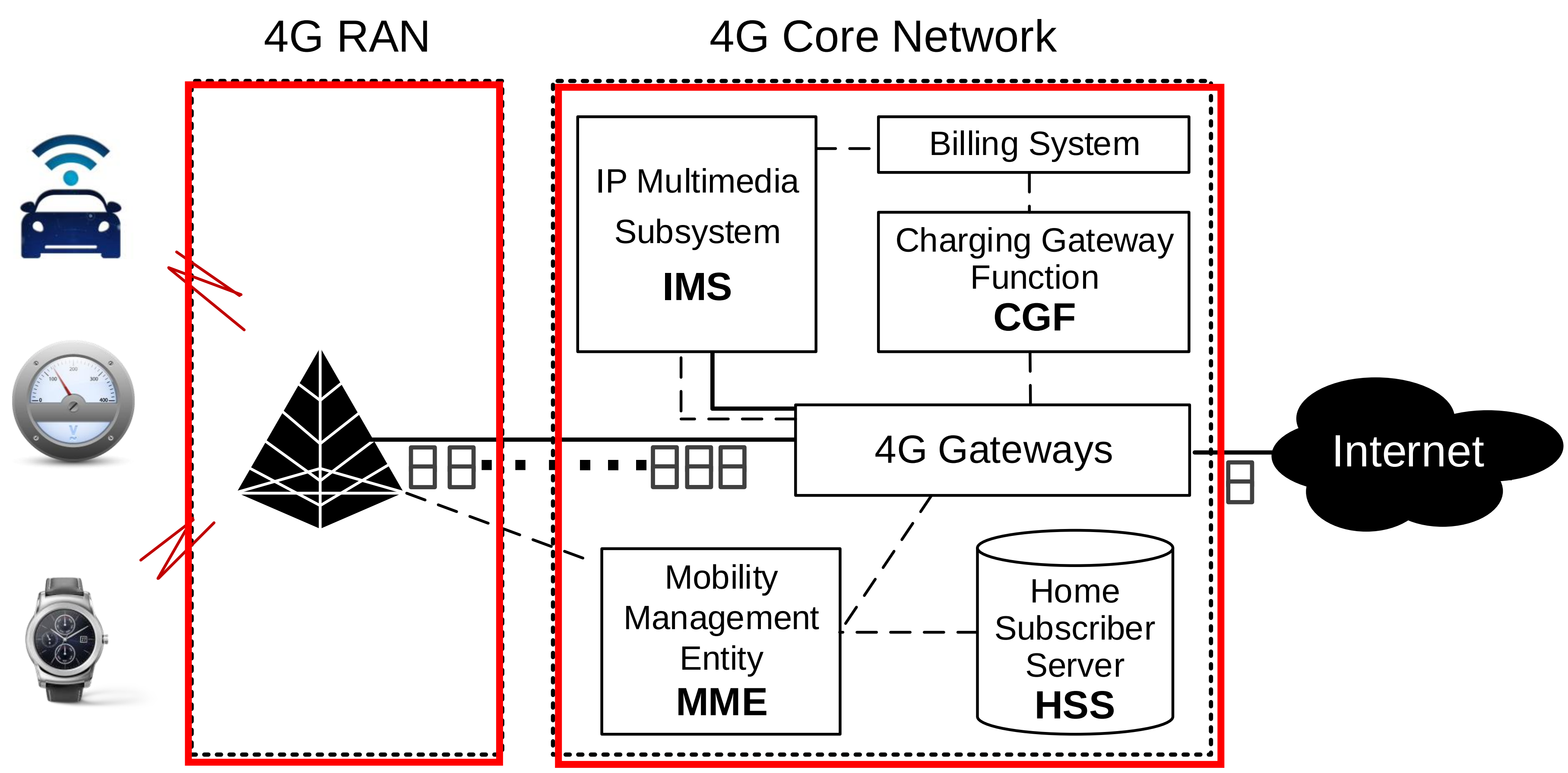
AT&T T Mobile verizon

Study of IoT Support in Cellular Networks

- **Cellular IoT Primer**
  - Cellular IoT Architecture
  - IoT Specifications
- **Vulnerability**
- **Proof-of-concept Attack**
- **Solution**

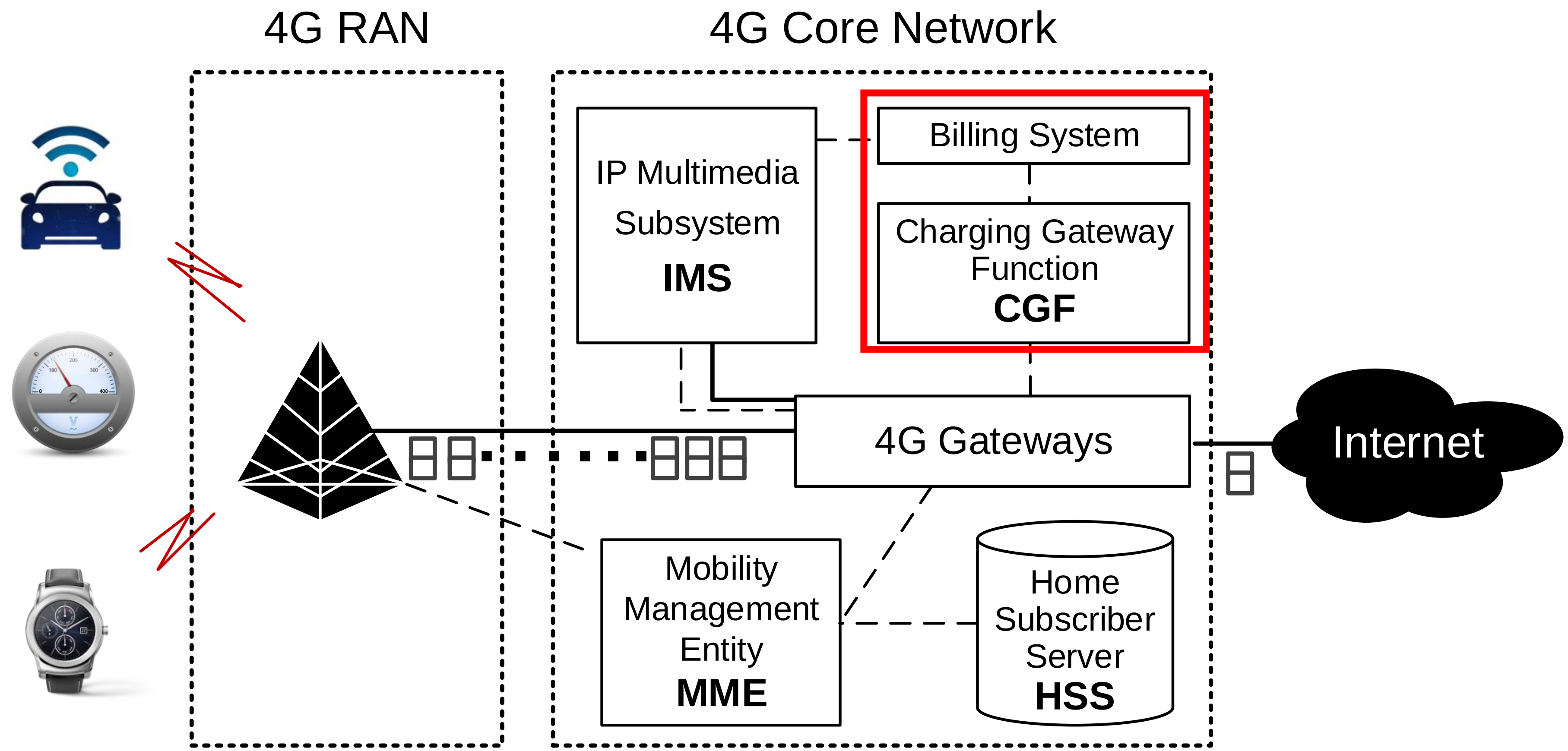
4G LTE Network Architecture for Cellular IoT

- Radio Access Network (RAN)
- Core Network (CN)
  - Management
  - Control
  - Data



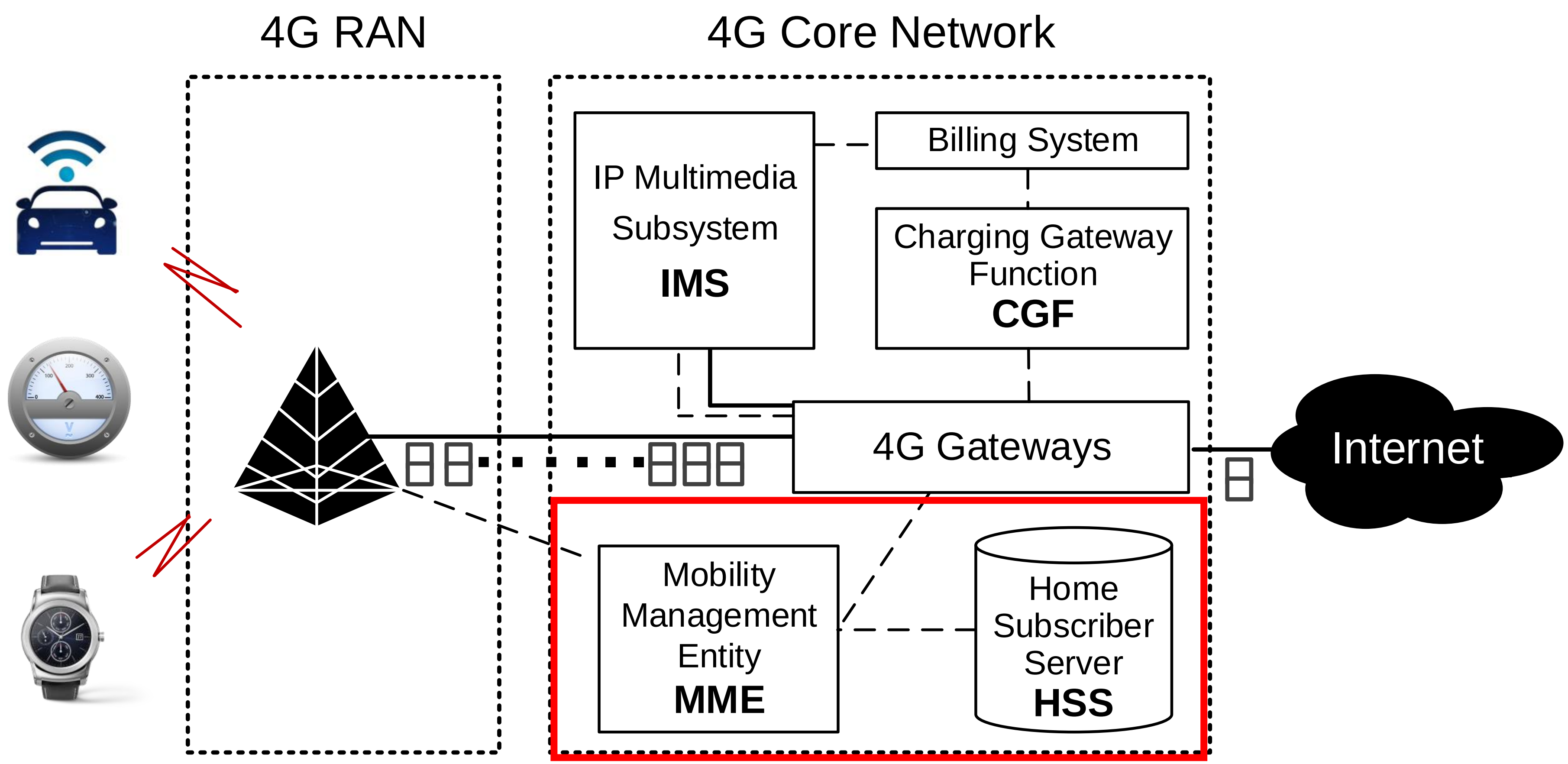
4G LTE Network Architecture for Cellular IoT

- Management Plane
  - Charging Gateway Function (CGF)
  - Billing System



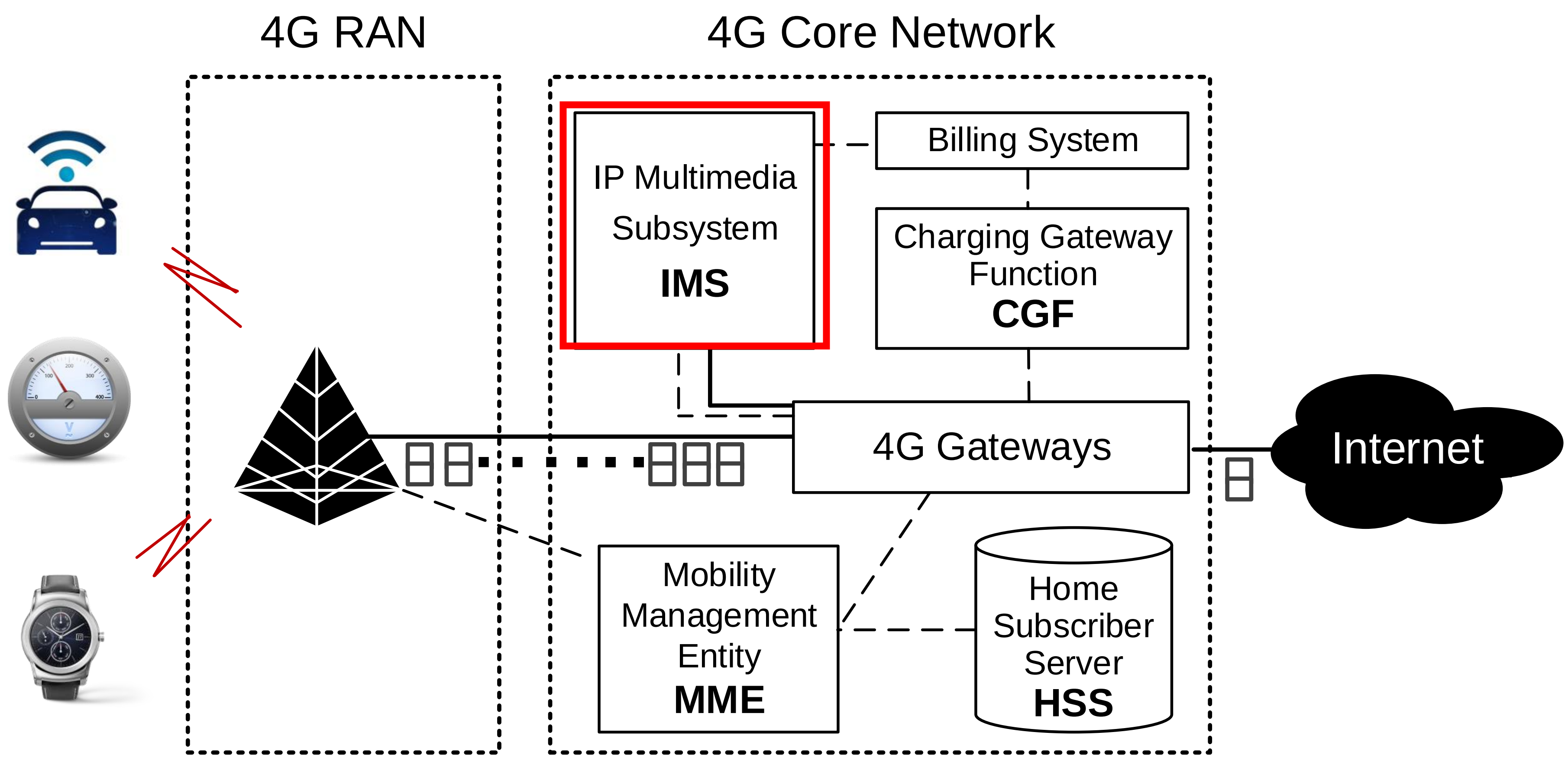
4G LTE Network Architecture for Cellular IoT

- Control plane
  - Home Subscriber Server (HSS)
  - Mobility Management Entity (MME)



4G LTE Network Architecture for Cellular IoT

- Data plane
  - CN connects RAN, IMS, and Internet



Cellular IoT Technologies in 4G LTE

- Various network specifications in the 4G LTE network for diverse demands from IoT services

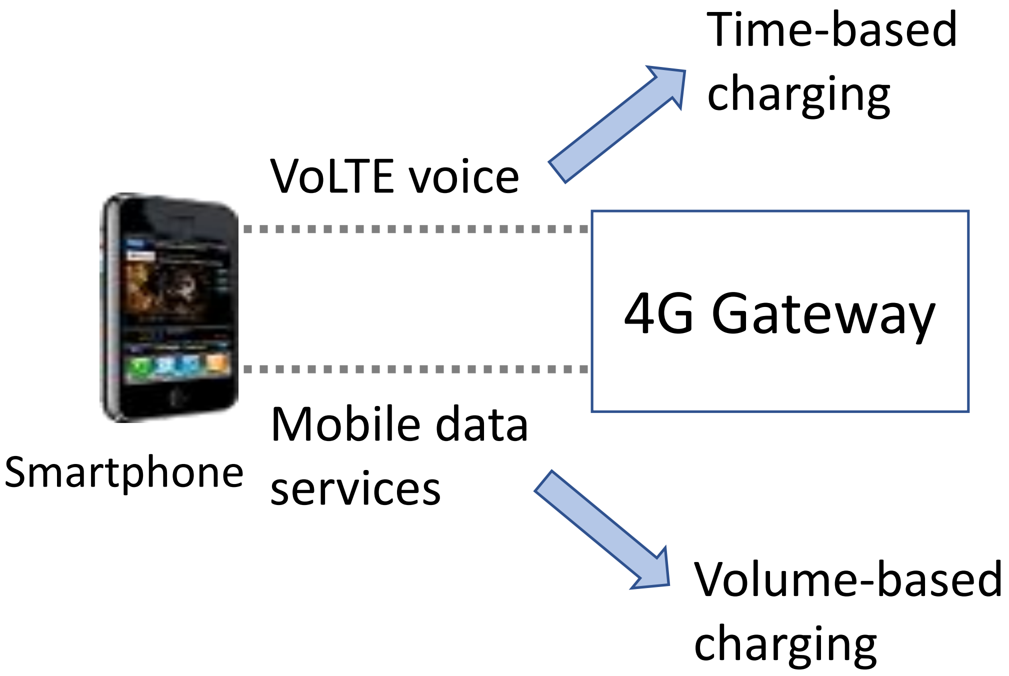
Technologies	Rel-8/Cat.4	Rel-8/Cat.1	Rel-12/Cat.0	Rel-13/Cat.M1	Rel-13/NB-IoT
IoT types	Critical	Critical/Massive	Massive	Massive	Massive
Downlink peak rate	150 Mbps	10 Mbps	1 Mbps	1 Mbps	0.2 Mbps
Uplink peak rate	50 Mbps	5 Mbps	1 Mbps	1 Mbps	0.2 Mbps
Duplex mode	Full	Full	Half/Full	Half/Full	Half
UE bandwidth	20 Mhz	20 Mhz	20 Mhz	1.4 MHz	180 KHz
UE max transmission power	23dBm	23dBm	23dBm	20 or 23dBm	23dBm
Complexity vs. Cat.1	125%	100%	50%	20-25%	10%
Voice over LTE	Yes	Yes	Yes	Yes	NA
Battery life	day(s)	year(s) [7]	>10 years [20]	>10 years [20]	>10 years [20]

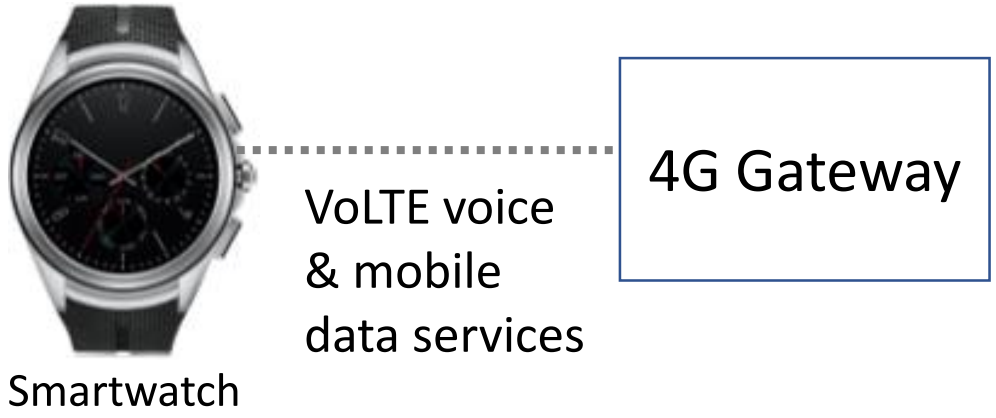
Widely used

Newly launched

Vulnerability

- Conventional charging function operates on a per-bearer basis.





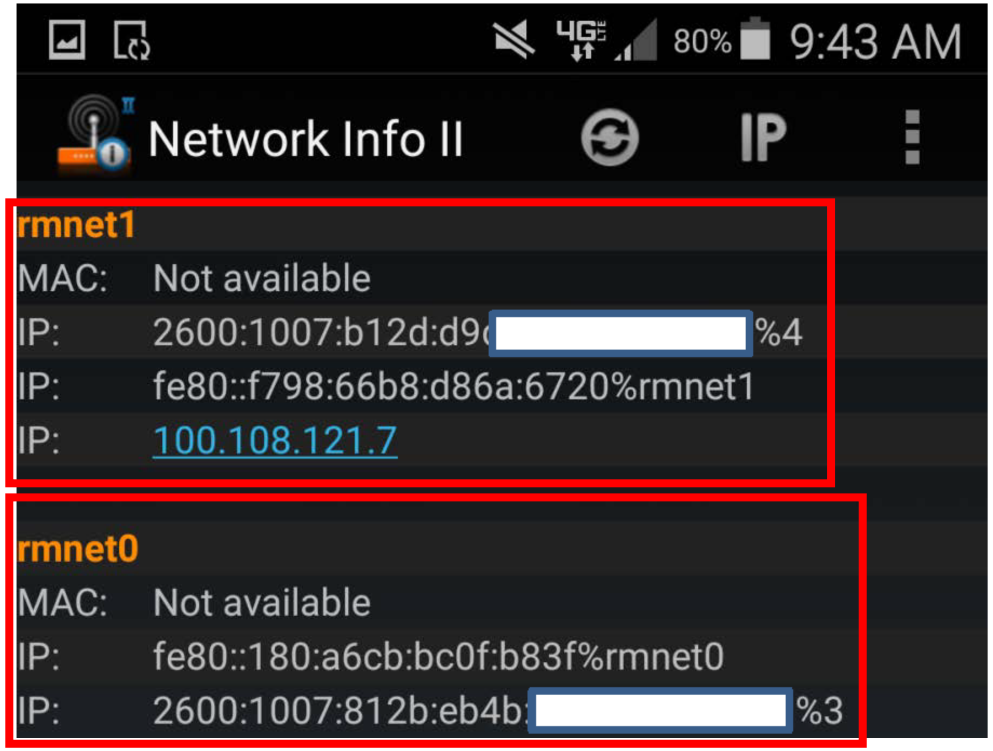
Improper IoT Service Charging Function

- Network Interface

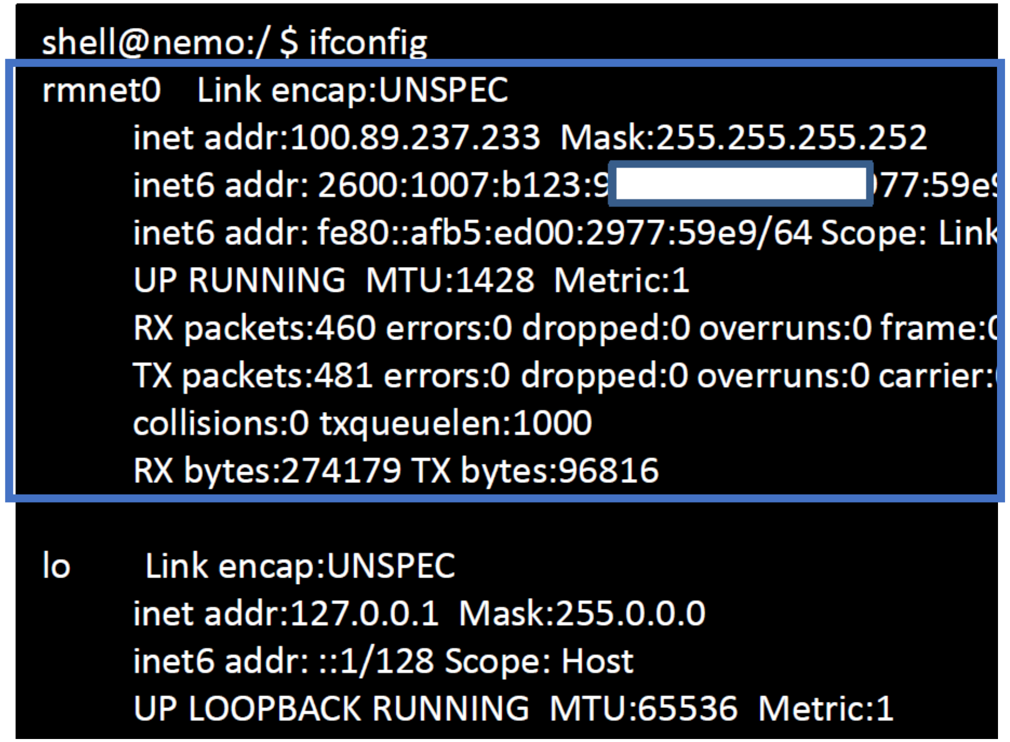
Same experiment location

Phone: enable VoLTE and mobile data

Two network interfaces



Watch: enable VoLTE and mobile data



Only one network interface

Improper IoT Service Charging Function

Question: Which charging function is used on the smartwatch?

Currently, the service plan for IoT devices provided by operators is volume-based charging.

This bearer's charging method is volume-based. Thus, the VoLTE service will be charged too. (VoLTE signaling is not free!)

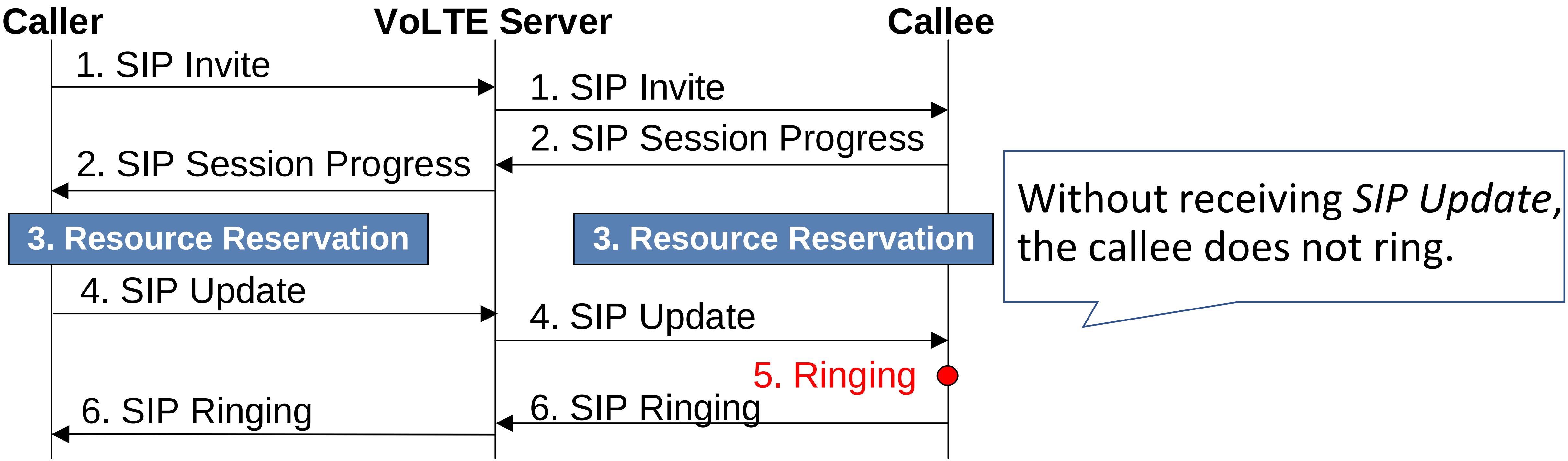
Watch: enable VoLTE and mobile data

```
shell@nemo:/ $ ifconfig
rmnet0   Link encap:UNSPEC
         inet addr:100.89.237.233  Mask:255.255.255.252
         inet6 addr: 2600:1007:b123:9[redacted]77:59e
         inet6 addr: fe80::afb5:ed00:2977:59e9/64 Scope: Link
         UP RUNNING  MTU:1428  Metric:1
         RX packets:460 errors:0 dropped:0 overruns:0 frame:
         TX packets:481 errors:0 dropped:0 overruns:0 carrier:
         collisions:0 txqueuelen:1000
         RX bytes:274179 TX bytes:96816

lo       Link encap:UNSPEC
         inet addr:127.0.0.1  Mask:255.0.0.0
         inet6 addr: ::1/128 Scope: Host
         UP LOOPBACK RUNNING  MTU:65536  Metric:1
```

Proof-of-concept Attack

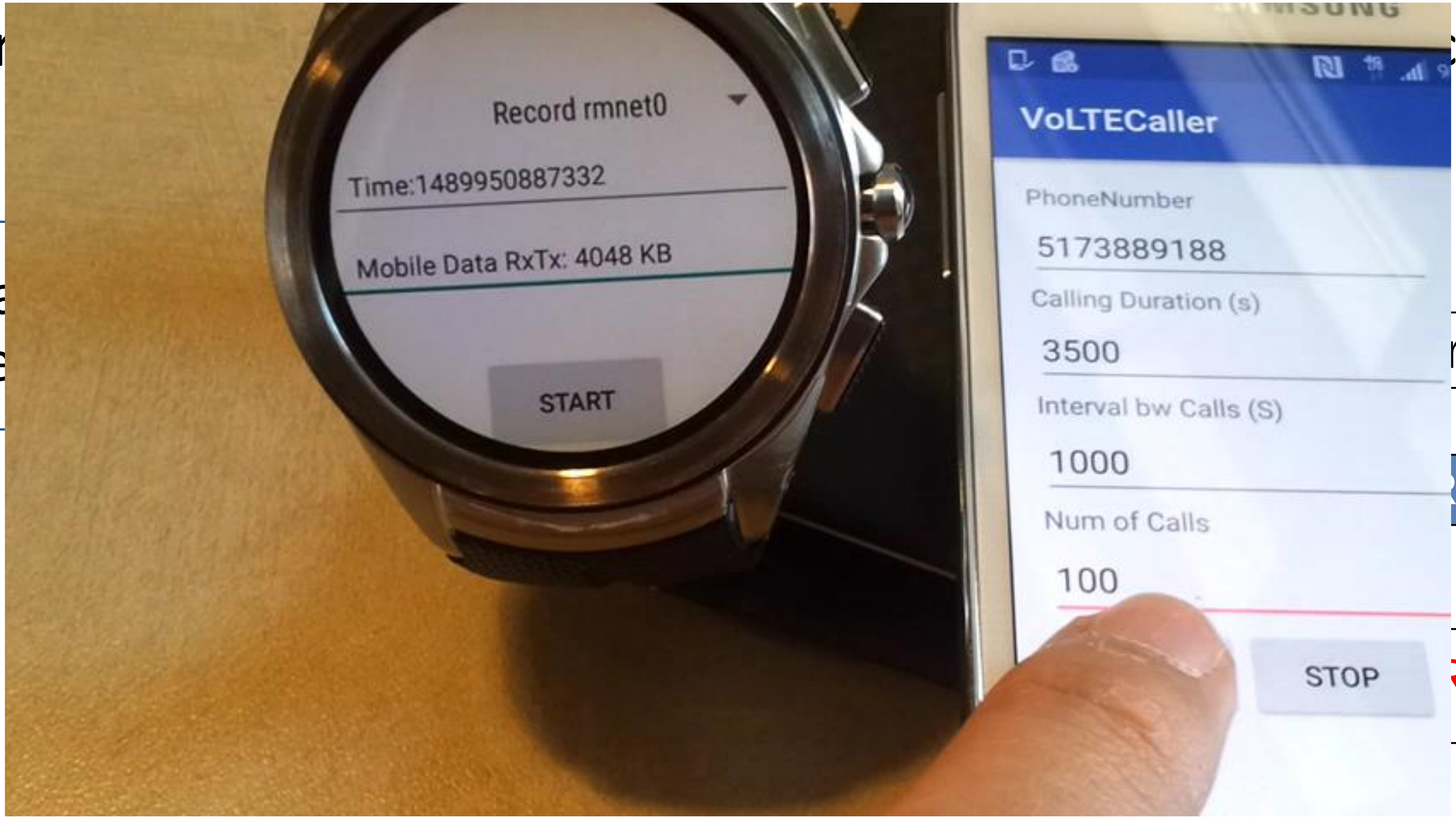
- Launch an IoT overcharging unaware attack by sending a large number of VoLTE call signaling spams



Proof-of-concept Attack

- Use our ... h the attack.

Interrupt the dia... observing SIP Se...



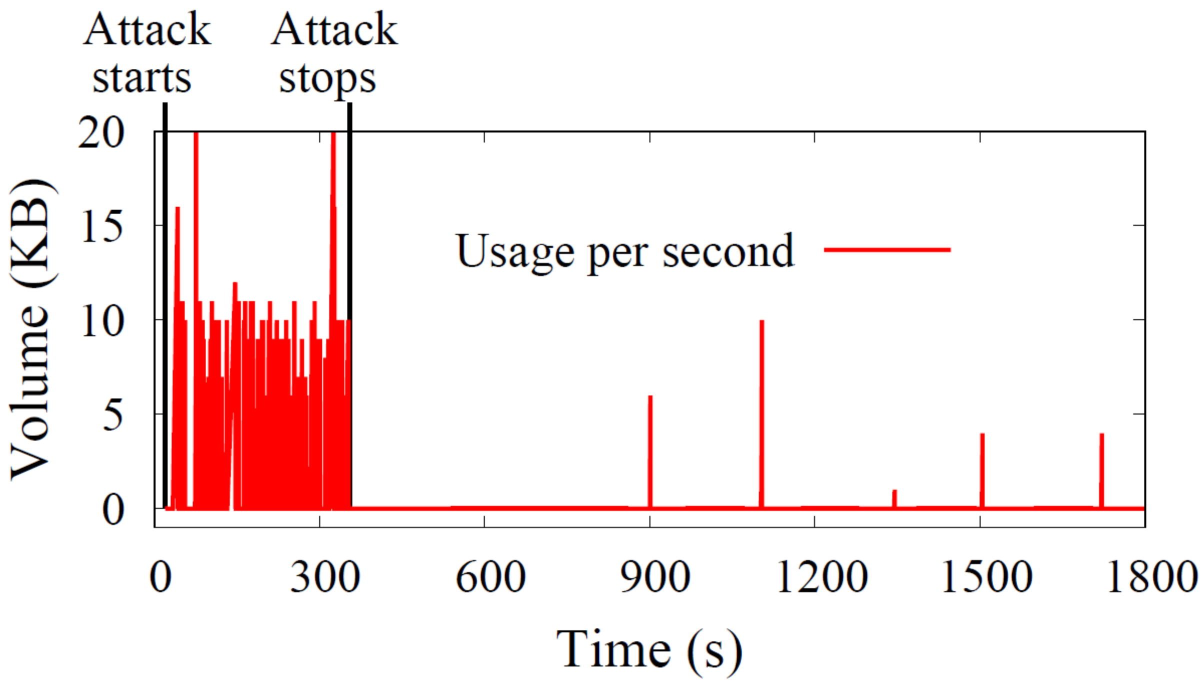
Callee

...rogress

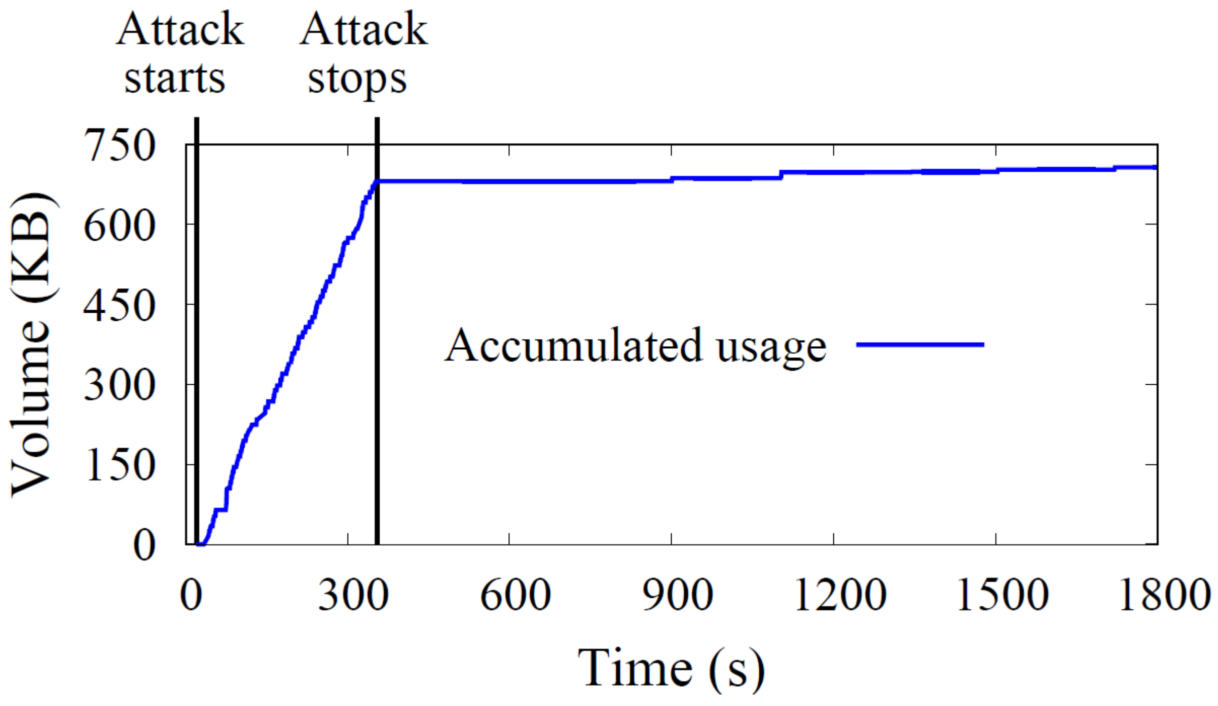
...eservation

Ringing

Attack Result



Data usage volume per second



Accumulated data usage volume per second

Each VoLTE call attempt: 3.24 seconds

Total data consumed: 681 KB

177 MB

Real World Impact?

- Verizon provides a cellular IoT charging plan for IoT users ($2 for one device with 200 KB data.
- The attack can consume 681 KB in 324 seconds, which means that 200KB data can be used in 100 seconds.
  - No automatically refill: Denial of service
  - Automatically refill: Non-negligible financial loss

$2 per 100 seconds = $1440 per day for a single IoT device!

Solution

- Flow-based service charging method for IoT devices.
- Service data flow is identified by the five-tuple information:

Source IP address or mask	Source port number	Destination IP address or mask	Destination port number	Protocol ID (TCO/UDP)

VoLTE signaling can be represented (*, *, VoLTE_Server_IP, 5060, TCP)

Solution

- Advantage of flow-based charging method
  - Compatible: Applying different charging methods to a single bearer for different services
  - Deployable: T-Mobile and Verizon provide users with free DNS services (packets over TCP/UDP destination port 53 are free of charge)

CONCLUSION

- Review the network architecture and specification for cellular IoT
- Vulnerability
  - The single bearer of IoT device servers both VoLTE services and data services.
- Proof-of-concept attack
- Solution
  - Flow-based service charging method

Thank you! Questions?