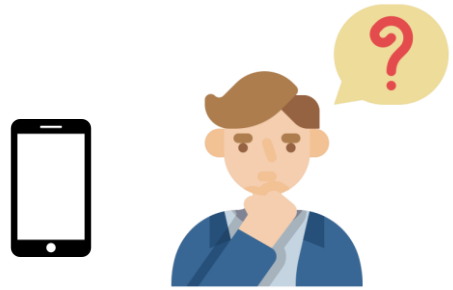
Small Cell, Big Risk: A Security Assessment of 4G LTE Femtocells in the Wild

Yaru Yang[1], **Yiming Zhang**[1], Tao Wan[2], Haixin Duan[1 3], Deliang Chang[4], Yishen Li[1], Shujun Tang[1 4]

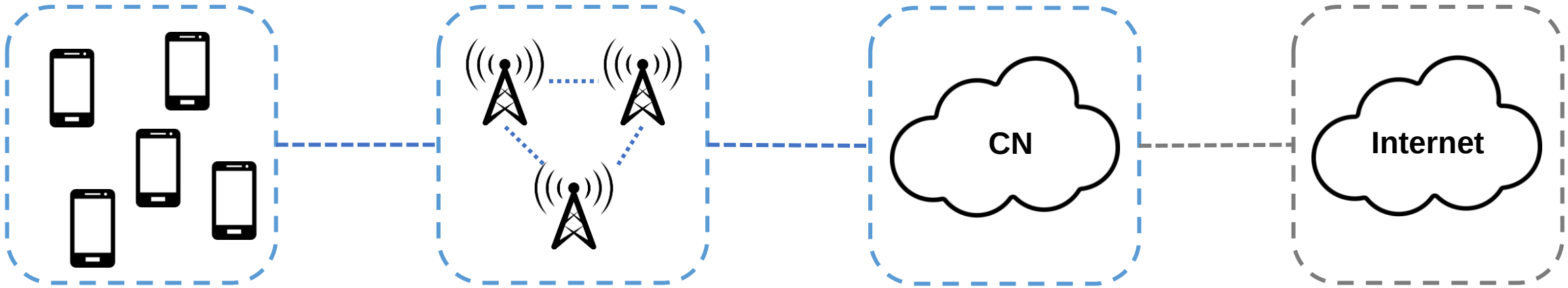
[1]Tsinghua University
[3]Quancheng Laboratory
[2]CableLabs & Carleton University
[4]QI-ANXIN Technology Research Institute

Email: yyr22@mails.tsinghua.edu.cn



Is your cellular communication truly secure?

Cellular Architecture Overview



UEs (User Equipment)

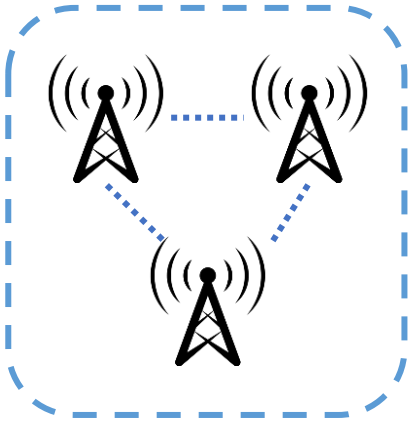
Base Stations

Core Network

External Network

Femtocells

- Deploy miniaturized base stations to improve coverage → femtocells
- In 3GPP terminology:
  - HNB[1] (3G)
  - HeNB[1] (4G)
  - 5G NR Femto[2]



Base Stations

Operator-controlled sites

Traditional BS

Femtocell

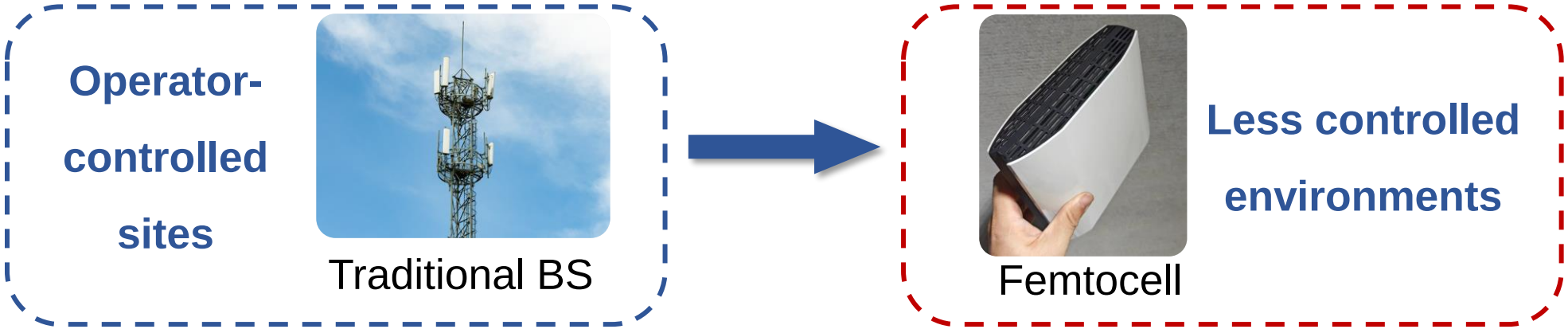
Less controlled environments

[1] 3GPP TS 22.220, "Service requirements for Home Node B (HNB) and Home eNodeB (HeNB)"

[2] 3GPP Work Item 1060048, "5G NR Femto (5G_Femto) Work Item"

Motivation

- Large and growing global deployment
  - Femtocell market size reached $6.49B in 2024[3]
- Critical cellular infrastructure directly connected to carrier core networks
- Shifted trust boundaries:
  - From operator-controlled sites
  - To less controlled environments with high physical accessibility
  - Adversaries can obtain and deploy femtocells within environments under their control



[3] Femtocell Global Market Report 2025, https://www.thebusinessresearchcompany.com/report/femtocell-global-market-report

Research Questions

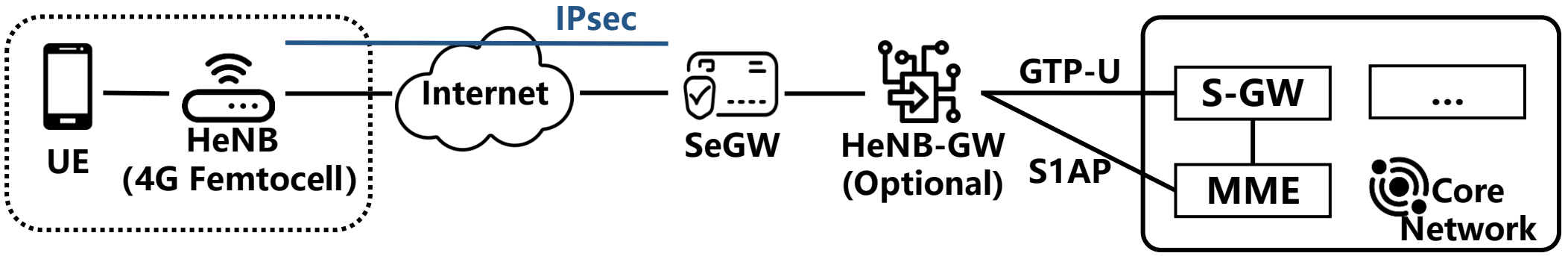


Figure 1. Femtocell Access Architecture in 4G Networks

- **Q1 Vulnerability**
  - Are common vulnerabilities enabling compromise present in 4G femtocells?
- **Q2 Impact**
  - If compromised, femtocells threaten users and the core network?
- **Q3 Exposure**
  - How many femtocells are accessible from the public Internet?

Q1 Common Vulnerabilities in 4G Femtocells

- **Scope**
  - 6 commercial 4G femtocells
  - Corresponding to 20+ OEM variants
  - 2 major operators
- **Methodology**
  - Specification compliance analysis
  - Service analysis
  - Firmware & hardware testing

Table 1. Summary of identified vulnerabilities

Vulnerability	FT-I	FT-II	FT-III	FT-IV	FT-V	FT-VI
V1. Accessible Debug Interfaces	✓		✓	✓		✓
V2. Credentials Extraction	✓	✓	✓	✓	✓	✓
V3. Predictable Credentials	✓	✓	✓	✓	✓	✓
V4. Management Services Exposure	✓	✓		✓		✓
V5. TR-069 Authentication Weakness	✓	✓	✓			

→ Local compromise

→ Remote compromise

Example: Predictable Credentials

Table 2. Credential Predictability in Tested Femtocells

Device	SSH	Web	Telnet
FT-I	root, admin, anonymous	admin, user	-
FT-II	root	user, admin	Omu…
FT-III	root, admin, anonymous	admin	-
FT-IV	root	femtodebug, admin	Omu…
FT-V	root	admin	-
FT-VI	root	admin	-

Static and recoverable Dynamic but derivable

- Observed across all tested femtocell models
- Credentials are either static or derivable

Example: Predictable Credentials

Table 2. Credential Predictability in Tested Femtocells

Device	SSH	Web	Telnet
FT-I	root, admin, anonymous	admin, user	-
FT-II	root	user, admin	Omu…
FT-III	root, admin, anonymous	admin	-
FT-IV	root	femtodebug, admin	Omu…
FT-V	root	admin	-
FT-VI	root	admin	-

Static and recoverable Dynamic but derivable

Derivation Mechanism

- Password-generation logic embedded in firmware
- Devices running the same firmware share identical generation logic
- Last four digits of the serial number derive the *admin* credential
- Full serial number + firmware version derive the *root* credential

Q2 Compromised Femtocells Impact on Subscribers

- **Experimental Setup**
  - Commercial deployment environment
  - Compromised femtocell under attacker control

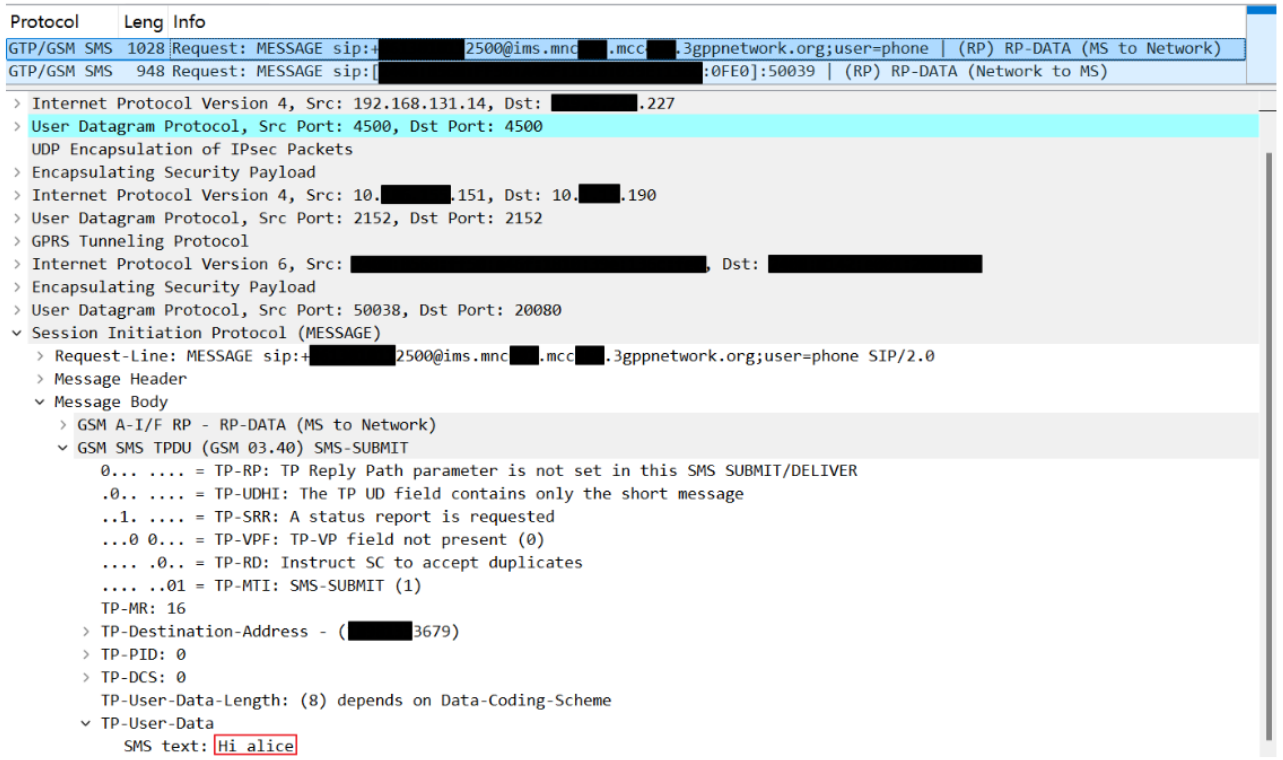


Figure 2. Eavesdropping on Subscriber SMS.

- **Verified Threats**
  - SMS eavesdropping
  - Call eavesdropping
  - Data service hijacking
  - Overbilling attack

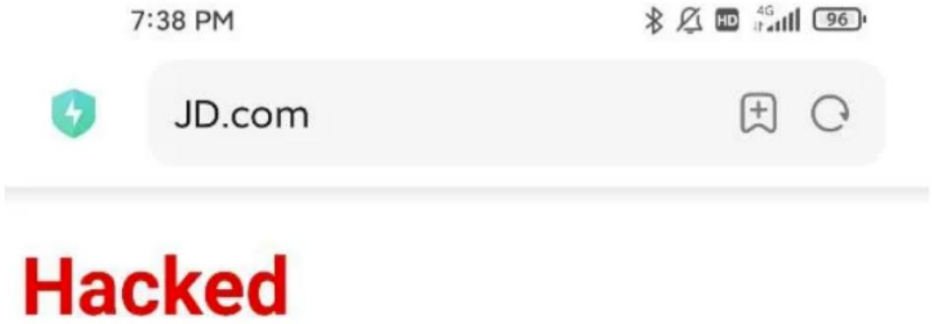


Figure 3. Data Service Hijacking

Q2 Compromised Femtocells Impact on Core Networks

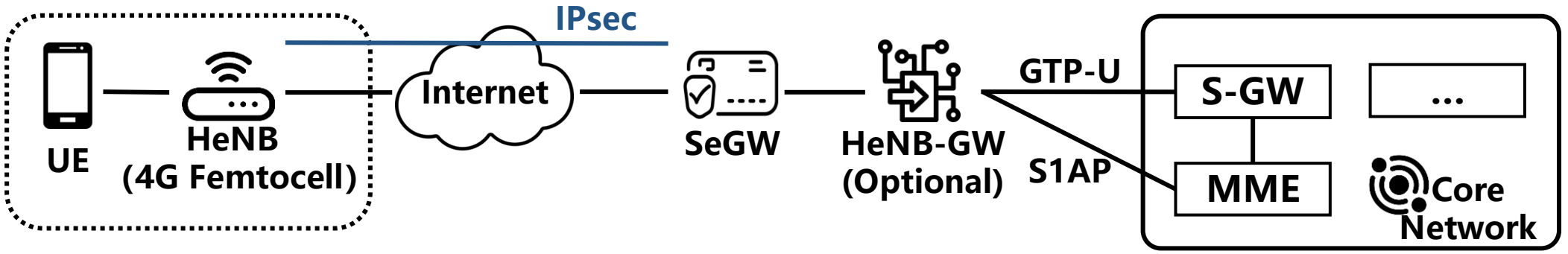


Figure 1. Femtocell Access Architecture in 4G Networks

Method

- Control-plane and user-plane traffic analysis
- Theoretical analysis without impacting live carrier networks

Potential Threats

- GTP-U & S1AP protocol abuse
- Unauthorized interaction with other core interfaces

Q2 Compromised Femtocells Bypassing Security Mechanisms

Vulnerability

- Weak IPsec authentication between femtocell and SeGW (Security Gateway)
- Authentication materials retrievable from the device

Security Implications

- Requires only extraction of stored authentication materials, without full privilege escalation
- Results in IPsec tunnel hijacking
- Allows traffic injection toward the core network without being constrained by femtocell hardware limitations

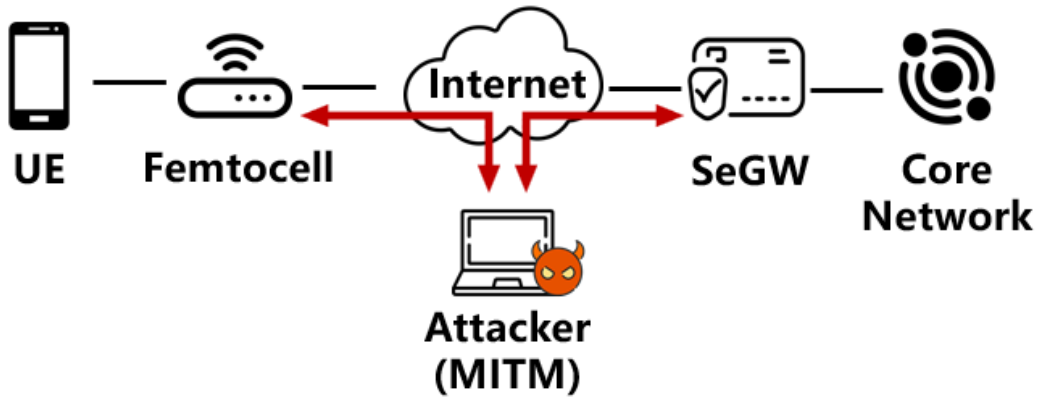


Figure 4. IPsec Hijacking

Q2 Compromised Femtocells Bypassing Security Mechanisms

CSG (Closed Subscriber Group) Bypass

- Restricts access to authorized subscribers only
- Web interfaces allow modifying CSG configuration

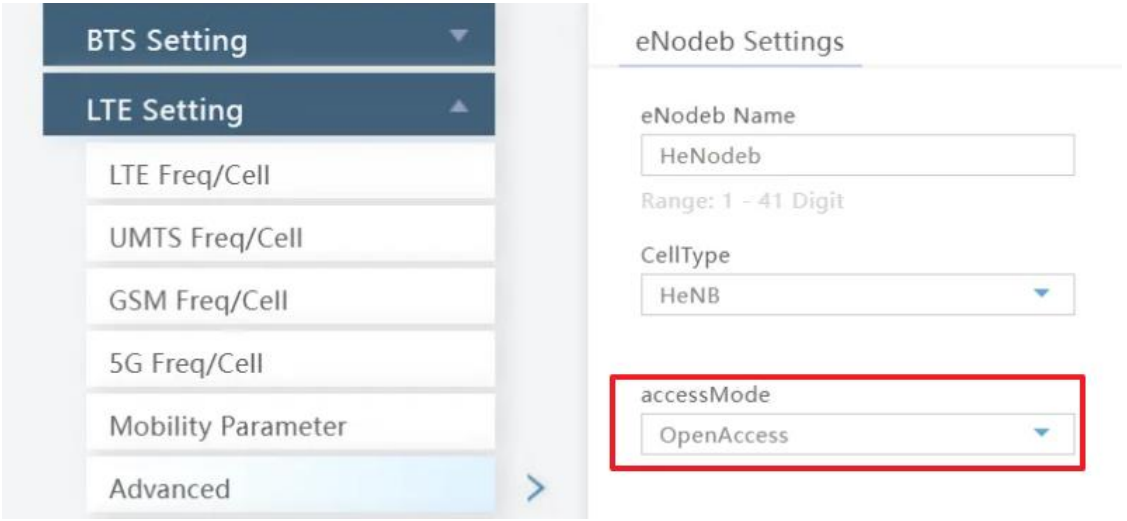


Figure 5. Example of CSG Configuration Interface

Location Verification Bypass

- Restricts femtocell access to specific geographic regions
- In evaluated devices, verification relies on IP-based geolocation
- Use of an IP proxy enables bypassing

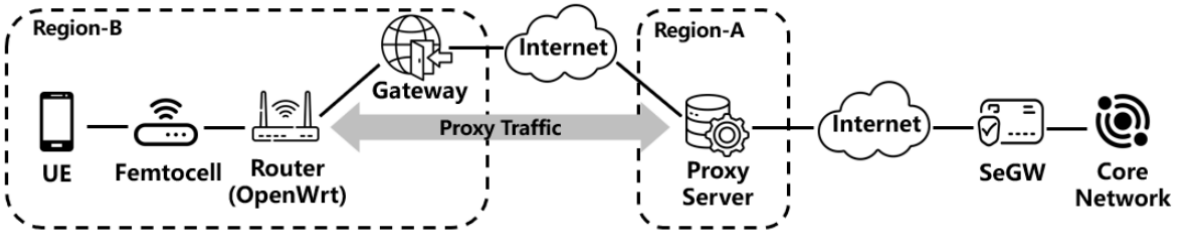
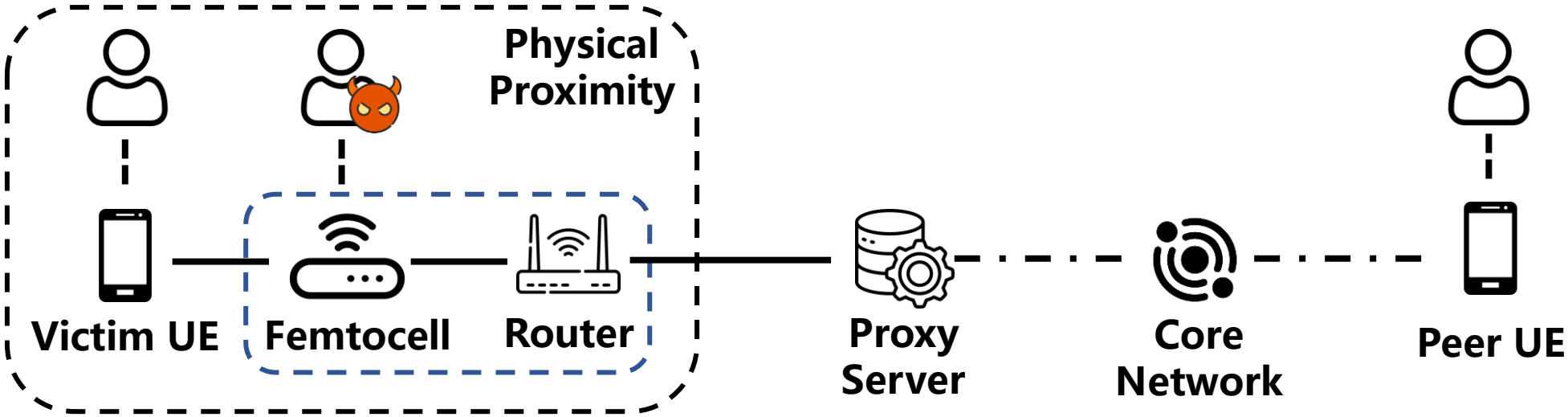


Figure 6. Illustration of IP-based Location Verification Bypass

An End-to-End Attacking Example



Targeted Eavesdropping: Attack Steps

- Obtain femtocell from operator or second-hand market
- Extract and recover SSH credentials
- Gain root access
- Bypass location verification (e.g., via IP proxying)
- Deploy the setup near the target
- Eavesdrop SMS messages and voice calls

Q3 Internet Exposure of Femtocells

- Identification Features
  - **IKEv2**
    - Femtocells establish IPsec tunnels with the SeGW using IKEv2
    - Peer-to-peer → also act as responders
  - **TR-069**
    - Remote management interface used by operators for device configuration and monitoring
    - Specification[4] requires devices to listen for management requests
  - **Web-Based Indicators**
    - HTTP and TLS responses may reveal device type
    - Positive indicators (e.g., *femto*) and negative indicators (e.g., *router*)

[4] Broadband Forum, "CPE WAN Management Protocol," Technical Report (TR) TR-069 Amendment 6 Corrigendum 1, 6 2020.

Q3 Internet Exposure of Femtocells

- Identification Features
  - IKEv2
  - TR-069
  - Web-Based Indicators

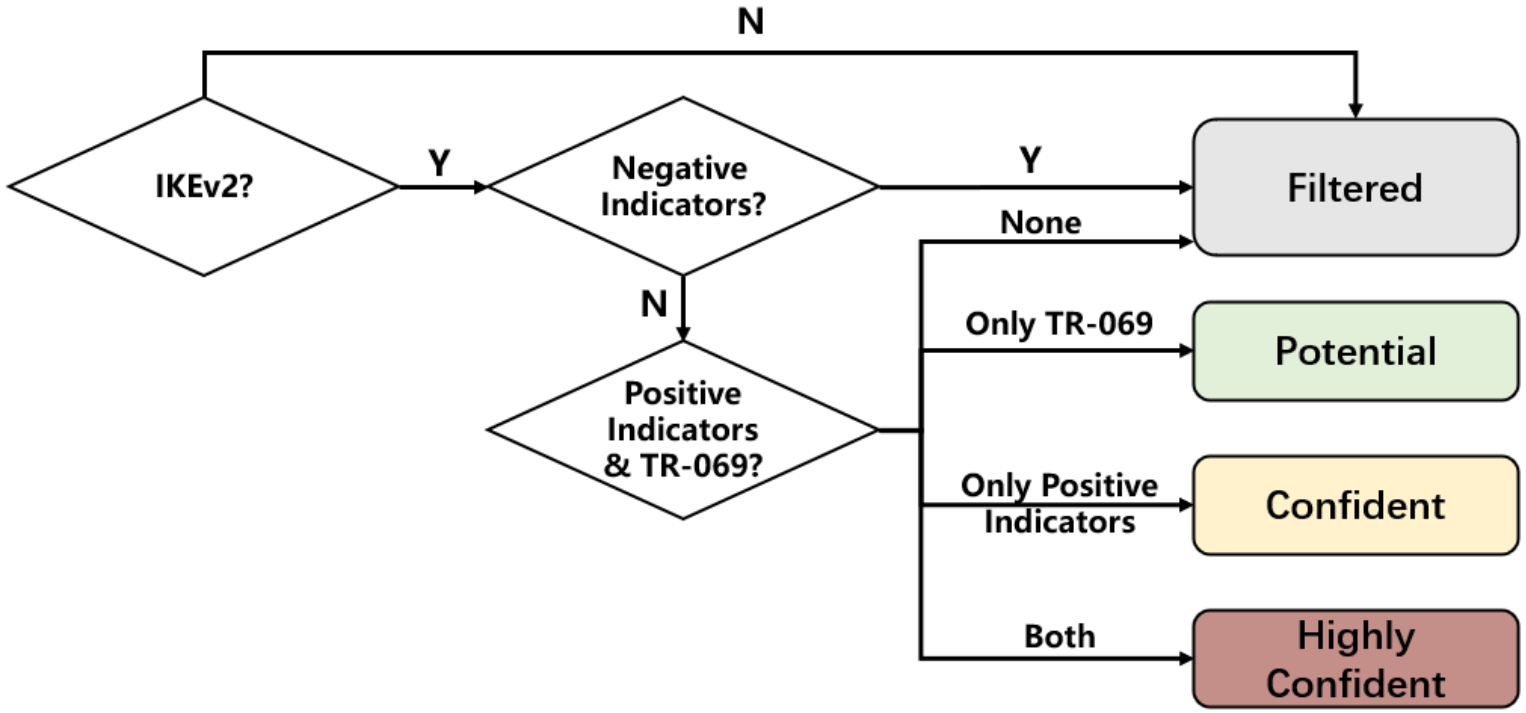


Figure 7. Classification Workflow

Q3 Internet Exposure of Femtocells

- 86,108 suspected femtocells identified, of which 52,768 were labeled as *highly confident*, 720 as *confident*, and 32,620 as *potential*
- Hundreds of devices matched fingerprints of analyzed vulnerable models

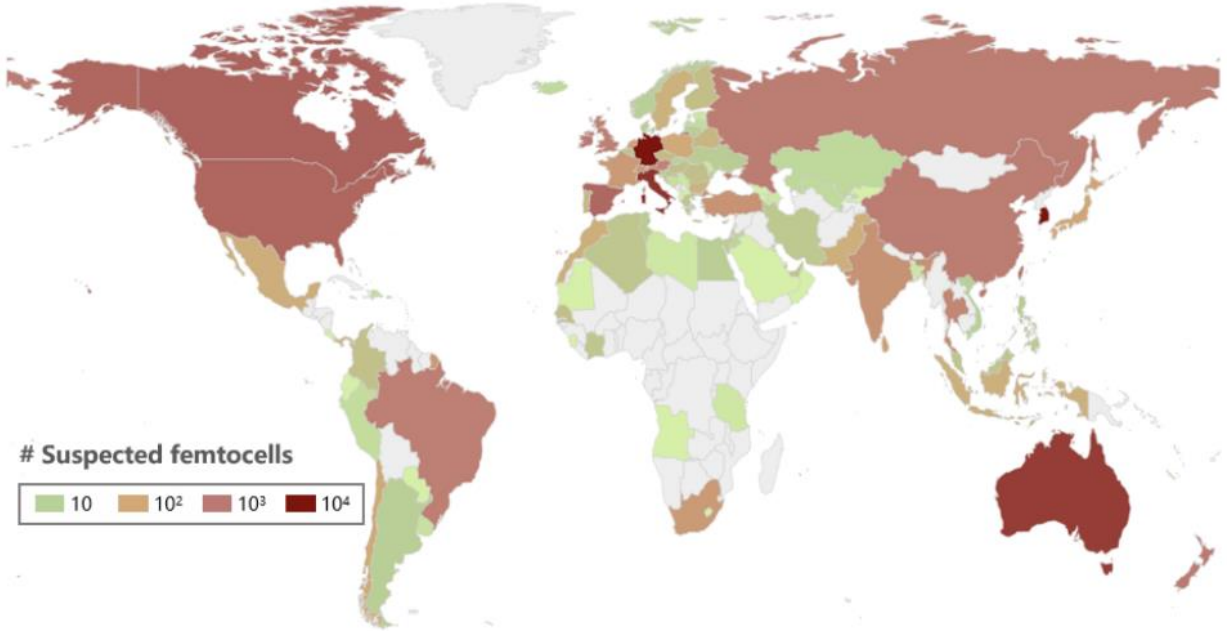


Figure 8. Global Distribution of Suspected Femtocells

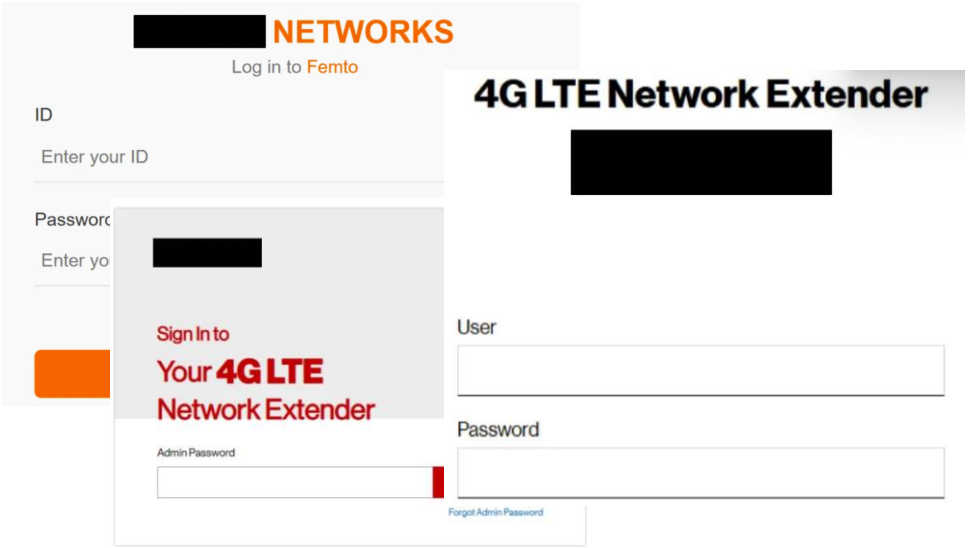


Figure 9. Examples of exposed web pages

Responsible Disclosure and Industry Impact

GSMA Coordinated Vulnerability Disclosure (CVD)

- CVD-2025-0106

National Vulnerability Disclosures

- CNVD-2025-23902
- CNVD-2025-29752
- CNVD-2025-29753
- CNVD-2026-03612
- CNVD-2026-03611
- 6 additional cases under review

Industry Coordination

- Multiple major operators
- Affected femtocell vendors

Recommendations

Enhancing Femtocell Security Standards

- Extend SCAS requirements to femtocells
- Mandate platform hardening (e.g., removal of debug interfaces, secure credential storage)

Mitigating Threats to Subscribers

- Strengthen UE-side verification of femtocell legitimacy
- Detect forged identities and abnormal CSG behavior
- Introduce authentication for broadcast messages

Mitigating Threats to Core Networks

- Strict filtering of femtocell-originated control traffic
- Mandate HeNB-GW deployment for traffic isolation
- Avoid unintended exposure of core network elements

3GPP Specification Impact

- 5G NR Femtocell Security Study[5]
- 5G NR Femtocell SCAS[6]

[5] 3GPP, “Study on security aspects for NR Femto phase2,” TR 33.746

[6] 3GPP, “Security Assurance Specification (SCAS) for NR Femto,” TS 33.546

Conclusion

A systematic security study spanning femtocell device analysis, impact evaluation, and Internet-scale measurement

- Identified and validated 5 common vulnerabilities across 6 commercial 4G femtocell models
- Highlighted significant security risks to users and potential implications for core networks.
- Designed an Internet-scale measurement pipeline and identified over 86,000 suspected exposed femtocells worldwide
- Coordinated responsible disclosure and contributed to ongoing 5G femtocell security standardization efforts

Small Cell, Big Risk: A Security Assessment of 4G LTE Femtocells in the Wild

Yaru Yang[1], **Yiming Zhang**[1], Tao Wan[2], Haixin Duan[1 3], Deliang Chang[4], Yishen Li[1], Shujun Tang[1 4]

[1]Tsinghua University
[3]Quancheng Laboratory
[2]CableLabs & Carleton University
[4]QI-ANXIN Technology Research Institute

Email: yyr22@mails.tsinghua.edu.cn