Fake Base Station Threats in 5G Non-Public Networks

Meng-Huan Lee
Department of Electrical Engineering / Institute of Computer and Communication Engineering,
National Cheng Kung University, No.1, University Rd., East Dist.
Tainan City, 701401, Taiwan.

I-Hsien Liu
Department of Electrical Engineering / Institute of Computer and Communication Engineering,
National Cheng Kung University, No.1, University Rd., East Dist.
Tainan City, 701401, Taiwan.

Jung-Shian Li*
Department of Electrical Engineering / Institute of Computer and Communication Engineering,
National Cheng Kung University, No.1, University Rd., East Dist.
Tainan City, 701401, Taiwan.
*E-mail: mhlee@cans.ee.ncku.edu.tw, ihliu@cans.ee.ncku.edu.tw, jsli@mail.ncku.edu.tw**
www.ncku.edu.tw

Abstract

With 5G technology, traditional industrial and business equipment can now be connected wirelessly in a non-public network separated from public mobile services. Benefit from features such as high bandwidth and massive machine-type communications, while being able to control their own private 5G networks. But fake base stations used by law enforcement and hackers may collect private information and cause disruptions in cell services, thus compromising the security. In this research, we will analyze existing attack methods and detection mechanisms. And look at how those threats can affect the devices and operations in 5G non-public network.

Keywords: 5G, Non-public network, Fake base station, Industrial Internet

1. Introduction

Driven by Industry 4.0 and Industrial Internet initiatives, 5G has gained popularity for being a key enabler of such use cases. 5G provides higher bandwidth and more reliable communication compared to previous generations. Allowing more devices, like autonomous robots in a factory, to cover larger areas. These kinds of industrial scenarios are the most common use of 5G NPNs [1]. But more 5G usage may expose more attack surfaces compared to traditional wired or wireless LAN technology.

One of the big concerns regarding the security of mobile networking is in the Radio Access Network (RAN). And fake base stations are the most popular radio-layer attacks, being known for their disruptive capability since the 2G era. With the rise of low-cost Software-Defined Radio (SDR) and open-sourced radio software, the possibility of fake base station attacks is increasing. Although security standards have improved over the years, these risks are still relevant to this day. For companies and organizations to safely deploy 5G in crucial operations such as industrial facilities or utility infrastructure, stakeholders need to understand such attacks. So, in our research, we categorized several ways

* Corresponding author's E-mail: jsli@mail.ncku.edu.tw

of fake base station attacks, and identify their threats to 5G NPNs.

2. Backgrounds

We briefly introduce the basics of mobile networks, with a focus on 5G NPN in an industrial scenario. And the security measures in the 5G System that are related to fake base stations.

2.1. *5G Non-Public Network*

5G Non-Public Networks (also called private mobile networks) are purpose-built, independent networks. In contrast to Public Land Mobile Networks (PLMNs) that offer mobile network services to public subscribers, NPNs are intended for the exclusive use of an enterprise or an organization. According to 3GPP Release-16 [2], NPNs are categorized into SNPNs and PNI-NPNs.

NPNs give organizations control over the quality of their own connectivity although it could be beneficial to have support from a third-party supplier or Mobile Network Operator (MNO) to help configure, optimize, and operationally manage the NPN. An NPN can be isolated from external networks and reside behind corporate firewalls. This is the most common way for companies and organizations to deploy 5G in industrial scenarios.

2.2. *5G System, Authentication and registration*

A 5G system mainly consists of three parts [3]:

- *User Equipment (UE).* The UE (essentially the modem) stores a permanent identifier and permanent key on a Universal Subscriber Identity Module (USIM) card. With these credentials, user and network establish mutual authentication. Three identifiers are important: the permanent identifier SUPI (4G: IMSI), the concealed identifier SUCI, and the temporary identifier 5G-GUTI.
- *Base Stations.* Base Stations create the wireless network. They act as access points for user equipment to attach to the Radio Access Network (RAN), thus connecting to the mobile network.
- *Core Network.* The back-end core network performs all management tasks and traffic routing.

In 4G, the base station and core network are called eNB (Evolved Node B) and EPC (Evolved Packet Core). In 5G system, they are called gNB (Next Generation Node B) and NGC (Next Generation Core). For a UE to register to the mobile network, the Authentication and Key Agreement (AKA) procedure are performed between the UE and the Core via BS. But some user information may still be transmitted in plain text before the AKA finished the authentication, like IMSI in 4G or SUCI in 5G. Because encryption is only activated *after* both parties agree on a session key. As shown in Fig.1. This is one of the important attack vectors for FBS.

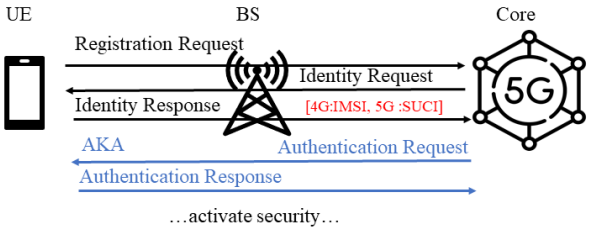

Fig.1. Part of the registration process and the Authentication and Key Agreement (AKA) procedure.

3. Fake base station attacks

Fake base stations are malicious radio devices that disguise themselves as legitimate ones to attract nearby signals. Fig.2 illustrates an FBS attack in NPN, the FBS can try to trick UEs to connect to them and/or listen to the messages broadcasted by legitimate BS to obtain information about the network. They are mainly used for two purposes: 1) to identify or track users, 2) to perform Denial of Services.

User tracking is the most common use of fake base stations. By exploiting the vulnerability in the authentication procedure when the messages aren't yet encrypted (see 2.2), attackers obtain identifiers and track

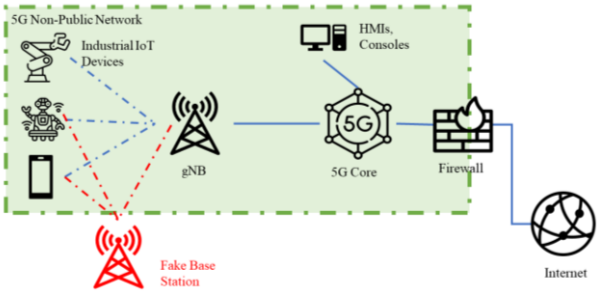

Fig. 2. Fake base station attack in NPN

the target of interest. "SUCI(IMSI)-catcher" is the collective name given to devices used to eavesdrop and track mobile network subscribers [4]. In public networks, the target is usually a person's phone or personal device. There are several reports of such devices (branded "Stingray") being used by law enforcement or appearing in cities [4], [5]. Which compromised users' privacy and leaked their locations. Another use of FBSs is to trick UEs into downgrading their connections to older generations (2G/3G/4G) by sending them reject messages during the registration phase [6].

4. Fake base stations threats in NPN

Here we identify how the above-mentioned attacks can affect the NPN in an industrial scenario. In this scenario, the UEs in the network are mostly industrial devices such as robotic arms, sensors, or mobile robots instead of usual smartphones. So, the goals of the attack and the impact would be different.

4.1. *Impacts of fake base stations attacks in NPN*

In industrial NPN, low-latency and reliable services are key. The threats posed by FBSs in an NPN are mostly similar to public networks, but the impact can be more severe.

- *SUCI(IMSI)-Catchers:*
  Just like public networks, attackers can use FBS to track the movement of a particular UE in an NPN. This is especially dangerous in an industrial setting. As it can be used to track and monitor the activities of personnel or industrial devices. Though tracking a stationary target (like a static robotic arm) may not have much use, tracking Autonomous Mobile Robots could let the attackers learn more about the physical environment like the factories' layout and route of the robots. And if the attacker can track certain employees via "SUCI-Catching" their company phones, it could pose big security risks.
- *Downgrade or Denial of Services:*
  By downgrading the connection of UEs in an NPN, attackers can exploit the vulnerabilities of older communication standards and redirect them to an unsafe network controlled by the attackers. Or they can force UEs to temporarily lose mobile service, causing higher latencies or unreliable connections. Which leads to disruption in production lines or other operations.

The different types of FBS attacks and their key aspects are shown in Table 1.

4.2. *Countermeasures*

In order for NPN operators to combat these threats, there are some existing measures from public networks that can be used in NPN. One way is to monitor nearby BSs and check the presence of unknown or malicious BSs. So operators can then respond to possible FBSs or warn the users of incoming dangers. This can be done by special apps[7] or network-side detection mechanisms.

By measuring physical parameters like signal strengths, or detecting abnormal behaviors like duplicate requests or registration procedures that are out-of-order[8]. And rate-limit attach requests like some MNOs do in public networks [3].

4.3. *Challenges*

While 3GPP is aware of the FBS attacks and putting effort to remedy the issues in newer standards, lots of mobile services may not keep up with those updates. One example is the previously mentioned downgrade attacks, where it's still common for 4G and 5G devices to coexist in a network. New security standards may not be

Table 1. Different types of fake base station attacks.

Attack type	Attack vectors	Result	Threats to NPNs
SUCI(IMSI)-Catchers [3], [4], [5]	Collect and track identifiers. Listen to paging messages.	Tracking and locating of specific users in an area. Compromising user privacy.	Keep track of static devices and moving robots. Track important employee's phones.
Downgrade or DoS [6]	Faking reject messages.	Redirect users to older standards or unsafe networks. Causing UEs to lose connection, lead to DoS.	Unreliable connections, higher latencies. Gaining access to devices via unsafe networks.

implemented for compatibility issues, or simply bypassed by attacking legacy devices.

Though detection-based countermeasures might be a good option, it requires additional apps or mechanisms to be put into UEs or Core. Which are added costs for NPN operators and could add unwanted latencies. Existing methods also generally aims for public network, not NPN in an industrial scenario.

And as S.Park et.al's research shows, detection apps have their own limitations[7], so one should not solely rely on apps.

5. Conclusions

In this reasearch, we analyzed the threats of fake base station attacks in a 5G Non-public network. We identified the two main attack vectors, user tracking and Denial of Services, and examined their effects in an industrial scenario. We also discussed some existing countermeasures and identified the challenges that NPN operators may face. As 5G NPNs starting to be widely deployed, further research is needed to understand the threats and develop more effective countermeasures for such scenarios. We hope to raise awareness and advise operators and organizations to take precautions when configuring their NPNs.

Acknowledgements

This work was supported by the National Science and Technology Council (NSTC) in Taiwan under contract number 111 - 2221 - E - 006 - 079 – .

References

1. A. Aijaz, "Private 5G: The Future of Industrial Wireless," in IEEE Industrial Electronics Magazine, vol. 14, no. 4, pp. 136-145, Dec. 2020, doi: 10.1109/MIE.2020.3004975.
2. ETSI, "System architecture for the 5G System (5GS); Release 16", 3GPP TS 23.501
3. M. Chlosta, D. Rupprecht, C. Pöpper, T. Holz, "5G SUCI-catchers: still catching them all?" the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '21). New York, NY, USA, Jun. 28-Jul. 2, 2021.
4. C. Cullen, B. Bureau, "Someone is spying on cellphones in the nation's capital", CBC News, April 2017
5. A. Ramirez, "ICE Records Confirm that Immigration Enforcement Agencies are Using Invasive Cell Phone Surveillance Devices", ACLU, 2020.
6. H. Lin, "LTE REDIRECTION: Forcing Targeted LTE Cell-phone into Unsafe Network", Hack in the Box Security Conference, Amsterdam, Netherlands, May 2016.
7. S. Park, A. Shaik, R. Borgaonkar, A. Martin, Jean-Pierre Seifert, "White-Stingray: Evaluating IMSI Catchers Detection Applications." In Workshop on Offensive Technologies (WOOT). USENIX Association, Aug. 14-15, 2017
8. M. Echeverria, Z. Ahmed, B. Wang, M. Fareed Arif, Syed R. Hussain, O. Chowdhury, "PHOENIX: Device-Centric Cellular Network Protocol Monitoring using Runtime Verification", Jan 2021.

Authors Introduction

Mr. Meng-Huan Lee

He is studying for his master's degree in Department of Electrical Engineering / Institute of Computer and Communication Engineering, National Cheng Kung University. He graduated from the Department of Communications Engeineering, National Chung Cheng University, Taiwan in 2021. His interests are Cyber-Security and Cellular Network Security.

Dr. I-Hsien Liu

He is a research fellow in the Taiwan Information Security Center @ National Cheng Kung University (TWISC@NCKU) and Department of Electrical Engineering, National Cheng Kung University, Taiwan. He obtained his PhD in 2015 in Computer and Communication Engineering from the National Cheng Kung University. His interests are Cyber-Security, Wireless Network, Group Communication and Reliable Transmission.

Prof. Jung-Shian Li

He is a full Professor in the Department of Electrical Engineering, National Cheng Kung University, Taiwan. He graduated from the National Taiwan University, Taiwan, with B.S. in 1990 and M.S. degrees in 1992 in Electrical Engineering. He obtained his PhD in 1999 in Computer Science from the Technical University of Berlin, Germany. He teaches communication courses and his research interests include wired and wireless network protocol design, network security, and network management. He is the director of Taiwan Information Security Center @ National Cheng Kung University. He serves on the editorial boards of the International Journal of Communication Systems.