SUGISAKA MASANORI

Journal of Robotics, Networking and Artificial Life
Vol. 10(2); September (2023), pp. 156–159
ISSN (Online): 2352-6386; ISSN (Print): 2405-9021
https://alife-robotics.org/jrnal.html

Research Article

Securing 5G Non-Public Networks Against Fake Base Station

I-Hsien Liu, Meng-Huan Lee, 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

ARTICLE INFO

Article History

Received 09 October 2022
Accepted 12 October 2023

Keywords

5G
Non-public network
Cybersecurity
Fake base station

ABSTRACT

Various industries have adopted 5G Non-Public Networks to take advantage of improved connectivity while remaining separate from public networks. As these networks support private operations, they demand stringent security measures to prevent potential harm. This research paper focuses on securing 5G non-public networks against fake base station attacks, which pose a significant threat to the security of mobile networking. The study analyzes the risks associated with fake base stations and reviews various protection methods. Our findings underscore the importance of deploying effective countermeasures to mitigate the threats posed by fake base stations in 5G Non-Public Networks.

1. Introduction

The advent of Industry 4.0 and the Industrial Internet has made 5G technology an essential enabler for many use cases, thanks to its higher bandwidth and reliable communication capabilities. In particular, 5G is well-suited to support a larger number of devices and enable autonomous robots to cover wider areas in industrial settings [1]. However, as 5G usage expands, so do the attack surfaces compared to traditional wired or wireless LAN technology. One key area of concern is the Radio Access Network (RAN), which is vulnerable to radio-layer attacks, especially those carried out using fake base stations, which have been disrupting mobile networking since the 2G era. With the increasing availability of low-cost Software-Defined Radio (SDR) and open-sourced radio software, the likelihood of such attacks is on the rise. Despite ongoing improvements in security standards, these risks remain a pertinent issue. For companies and organizations to safely deploy 5G technology in critical operations, such as industrial facilities or utility infrastructure, it is crucial to understand these attacks. This paper aims to provide insight into the security risks posed by fake base stations in 5G Non-Public Networks (NPNs) and to review different countermeasures and challenges they face.

2. Background

This section provides an overview of 5G Non-Public Networks (NPNs) and the vulnerabilities associated with the authentication procedure in the 5G system.

2.1. *5G Non-Public Network*

5G Non-Public Networks (NPNs) offer a secure and exclusive network infrastructure for organizations to control their connectivity. Unlike Public Land Mobile Networks (PLMNs), which provide mobile network services to the public, NPNs are tailored to the specific needs of the enterprise or organization [2].

Third-party suppliers or Mobile Network Operators (MNOs) can provide assistance with configuring, optimizing, and managing the NPN. With the option to isolate the NPN from external networks and reside behind corporate firewalls, organizations can deploy 5G in industrial scenarios with confidence.

2.2. *Authentication and registration of 5G System*

The 5G system consists of three main components [3]. User Equipment (UE), Base Stations, and Core Network.

Corresponding author E-mail: jsli@mail.ncku.edu.tw, mhlee@cans.ee.ncku.edu.tw, ihliu@cans.ee.ncku.edu.tw URL: www.ncku.edu.tw

The UE stores a permanent identifier and key on a Universal Subscriber Identity Module (USIM) card, which is used for mutual authentication between the user and the network. The Base Stations act as access points for the UE to attach to the Radio Access Network (RAN), connecting it to the mobile network. The Core Network performs all management tasks and traffic routing.

The 5G system comprises the gNB (Next Generation Node B) and NGC (Next Generation Core) as the base station and core network, respectively.

To initiate registration to the mobile network, the Authentication and Key Agreement (AKA) procedure takes place between the UE and the Core via the Base Station. However, certain user information such as the identifier IMSI in 4G or SUCI in 5G may be transmitted in plain text before completion of the AKA procedure. This occurs because encryption is only enabled after a session key is agreed upon by both parties, as illustrated in Fig. 1. This vulnerability presents a significant avenue of attack for Fake Base Station (FBS) attacks, and warrants attention.

3. Security risks posed by the fake base station

In the context of 5G networks, fake base stations (FBSs) pose a significant threat as they can easily deceive nearby mobile devices by impersonating legitimate base stations.

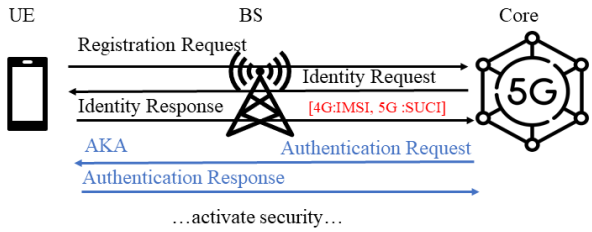

Fig.1. Request and response in the Authentication and Key Agreement (AKA) procedure.

As depicted in Fig. 2, FBS attacks in NPN can lead to a host of malicious activities, including but not limited to user tracking and denial of services.

The former, in particular, is a widely adopted tactic used by attackers to exploit the vulnerability in the authentication procedure during which messages remain unencrypted (see2.2), enabling them to obtain crucial user information and track the target. These malicious devices, also known as "SUCI(IMSI)-catchers," have been used by law enforcement and have caused significant concerns over privacy infringement and location leakages [4], [5].

Additionally, FBSs can force mobile devices to downgrade their connections by sending reject messages during registration, leading to a downgrade in network performance [6]. Therefore, it is imperative for NPN operators and stakeholders to be aware of these threats

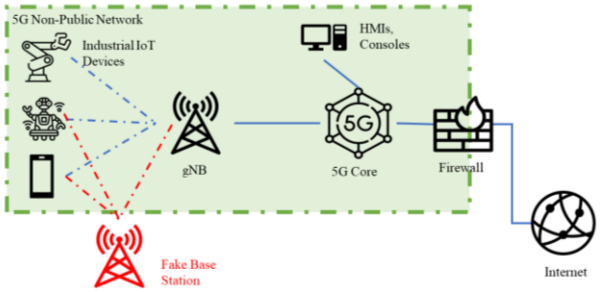

Fig. 2. Fake base station attack in NPN

and deploy robust countermeasures to ensure the security and integrity of their 5G networks.

4. Countering fake base station in 5G NPN

Here we discuss the different aspect of countering fake base station attacks. We start by identifying how the attacks can affect the NPN. The goals of the attacker and the impact of attacks would be different from public networks [7].

4.1. *Fake base stations threats in NPN*

In an industrial NPN, reliability and low latency are crucial factors. While the threats posed by FBSs are similar to those in public networks, the impact can be more severe in industrial settings.

- *SUCI(IMSI)-Catchers:*
  Attackers can exploit FBSs to track the movement of a particular UE in an NPN, just like in public networks. This is especially dangerous in an industrial environment as it can enable attackers to monitor the activities of personnel or industrial devices.
- *Downgrade or Denial of Services:*
  Attackers can exploit the vulnerabilities of older communication standards by downgrading the connection of UEs in an NPN, redirecting them to an unsafe network controlled by attackers. Alternatively, attackers can cause UEs to temporarily lose mobile service, resulting in higher latencies or unreliable connections disrupting production lines and other operations.

Table 1 summarizes the different types of FBS attacks and their key aspects. To protect against these attacks, effective countermeasures must be implemented in the 5G NPN to ensure security and minimize the risks posed by FBSs.

To show how simple that a fake base station attack can be used in modern network. We set up a fake base station to imitate operators in Taiwan. Table 2 shows the result of spoofing different public network operators. The experiment ran successfully with two subscriptions from Operator A (466-01) and Operator B (466-89). Showing that there is not enough security mechanism in place to prevent this kind of attack.

4.2. *Countermeasures*

To thwart the nefarious attacks on NPN, operators can employ existing measures used in public networks. These measures include monitoring nearby BSs for any unfamiliar or malicious ones, which can be accomplished via specialized apps or
-side detection mechanisms [8].

Additionally, operators can utilize physical parameter measurements such as signal strengths or detection of abnormal behaviors like out-of-order registration procedures or duplicate requests [9]. Some MNOs in public networks also rate-limit attach requests [3].

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.	Location tracking of users. User privacy compromised.	Keep track of static devices and moving robots. Track important employee's phones.
Downgrade or DoS	Faking reject	Redirect users to older standards or unsafe	Unreliable connections, higher

Table 2. Fake base station test in Taiwan's network

Target Network	Target band	Physical Cell ID	IMSI Captured?
Operator A (466-01)	Band 3	180	YES
	Band 7	292	YES
Operator B (466-89)	Band 7	451	YES
	Band 8	451	YES

Attackers often employ low-cost SDR hardware and open-sourced radio software to conduct their attacks. However, these same tools can be used in reverse to detect potential threats, as demonstrated in the report by Threat Lab from Electronic Frontier Foundation (EFF) [10]. To aid in detecting fake base stations, the EFF has developed a project based on the srsLTE software suite and SDR hardware dubbed the "Crocodile Hunter" [11]. The tool works by listening for broadcast messages from all of the 4G stations in the area, inferring their location, and searching for any unusual activity.

4.3. *Challenges*

Despite efforts by 3GPP to address FBS attacks through newer standards, many mobile services may still struggle to keep up with these updates. For example, 4G and 5G devices still commonly coexist in a network, making it difficult to implement new security standards due to compatibility issues. In addition, attackers can bypass these new standards by targeting legacy devices using downgrade attacks.

While detection-based countermeasures are a viable option, they come with added costs for NPN operators and may cause unwanted latencies. Furthermore, existing methods are primarily designed for public networks and may not be suitable for NPN in an industrial scenario. Detection apps also have their limitations, as demonstrated by S.Park et al.'s research [8], so they should not be solely relied upon.

One should also have to keep in mind that we don't know how exactly commercial FBSs work. Instead, most of the research - including ours, relies on how we think they might work based on research findings and tests conducted by ethnic hackers.

However, open-source software tools like the Crocodile Hunter may be useful for operators and security researchers. These tools can help test different ountermeasures at lower costs, and operators can develop customized methods based on these tools to suit their specific needs.

5. Conclusions

In summary, this paper explored the risks posed by fake base stations in the context of 5G NPNs, focusing on user tracking and denial of services as two major concerns.

We reviewed various countermeasures and discussed their effectiveness in an industrial scenario.

While some existing solutions show promise, NPN operators face several challenges in implementing them effectively. As the deployment of 5G NPNs becomes more widespread, stakeholders must take proactive steps to secure their networks against these threats.

Acknowledgements

This work was supported by the National Science and Technology Council (NSTC) in Taiwan under contract numbers 111-2221-E-006-079- and 112-2634-F-006-001-MBK.

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. M.-H. Lee, I-H. Liu, J.-S. Li, "Fake Base Station Threats in 5G Non-Public Networks", ICAROB 2023, Oita, Japan, Feb. 9-12, 2023.
8. 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
9. 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.
10. Threat Lab, "Gotta Catch 'Em All: Understanding How IMSI-Catchers Exploit Cell Networks (Probably)", Electronic Frontier Foundation, 2019.
11. Electronic Frontier Foundation, "Crocodile Hunter", https://github.com/EFForg/crocodilehunter

Authors Introduction

Dr. I-Hsien Liu

He is an assistant professor in Department of Electrical Engineering, National Cheng Kung University, Taiwan. He obtained his Ph.D. 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. He is the deputy director of Taiwan Information Security Center @ National Cheng Kung University(TWISC@NCKU).

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.

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.