From 5G to 6G: It is Time to Sniff the Communications between a Base Station and Core Networks

Ruoting Xiong
University of East Anglia
Norwich, UK

Kit-Lun Tong
University of East Anglia
Norwich, UK

Yi Ren
University of East Anglia
Norwich, UK

Wei Ren
China University of Geosciences
Wuhan, China

Gerard Parr
University of East Anglia
Norwich, UK

ABSTRACT

Thanks to mobility and large coverage, 6G mobile networks introduce satellites and unmanned aerial vehicles as aerial base stations (ABS) in the 6G era. Instead of using a wired backhaul in 5G and its predecessor, an ABS leverages a wireless channel to a core network (CN). However, such a wireless channel design introduces new security challenges. In this paper, we present that passive attackers could sniff the ABS-CN wireless channel and identify what users are doing based on deep learning methods. We collect GTP protocol data on our testbed and use convolutional neural networks to classify 5 types of encrypted App traffic, like IG and TikTok. Experiment results proved the effectiveness of the proposed method, revealing the confidential data leakage problem on the 6G wireless ABS-CN channel.

CCS CONCEPTS

• **Security and privacy → Mobile and wireless security**.

KEYWORDS

6G, Wireless Channel, Sniffing Attack, Encrypted Data Analysis, Deep Learning

ACM Reference Format:
Ruoting Xiong, Kit-Lun Tong, Yi Ren, Wei Ren, and Gerard Parr. 2023. From 5G to 6G: It is Time to Sniff the Communications between a Base Station and Core Networks. In *The 29th Annual International Conference on Mobile Computing and Networking (ACM MobiCom '23), October 2–6, 2023, Madrid, Spain.* ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/3570361.3614085

ACM MobiCom '23, October 2–6, 2023, Madrid, Spain

ACM ISBN 978-1-4503-9990-6/23/10.
https://doi.org/10.1145/3570361.3614085

1 INTRODUCTION

Although 5G is still under commercial development, the 6G mobile network is believed to be equipped somewhere in the range of 2027 and 2030 [4]. Unmanned aerial vehicles and satellites could carry terrestrial base stations as aerial base stations (ABS), enlarging the serving area and achieving greater signal coverage. ABS has enabled a variety of applications, e.g., smart farming, sports event, and emergency rescue. Therefore, the usage of ABS is an unstoppable trend in 6G [1].

However, the wireless channel between ABS and the core network (CN) brings new security issues. There is evidence that information on encrypted payloads can still leak through traffic analysis methods. Passive attackers could collect data from wireless channels and infer personal information like App types, browser types, or mobile operating systems without decryption [6]. From 1G to 5G, intensive studies focus on the attack and protection of wireless channels between user equipment (UE) and basestations [2]. However, there is no research on encrypted data analysis of ABS-CN wireless channels, where data are encapsulated by GPRS tunnelling protocol (GTP).

In this paper, we argue that attackers could sniff GTP data between ABS and CN in 6G, and identify App types based on deep learning methods, leading to personal information leakage. Firstly, we set up the 5G CN and collect data on the Ethernet interface where the user plane function (UPF) sends the data to a base station. Both UPF and the base station run the GTP protocol. Next, we process the .pcap files of different mobile applications into one-channel figure dataset and then deploy Resnet, Googlenet and Densenet models to do Apps classification. Finally, we show that personal information like App types is leaked through analysis of encrypted data even without decryption.

2 APP IDENTIFICATION FRAMEWORK

Our App identification framework consists of network testbed, data collection and processing, and deep learning models.

2.1 Network Testbed

In the 5G mobile network, there are three components: CN, base station, and UEs. We use free5GC [3] as CN, which is an open-source software 5G CN. We set up the CN in an x86 computer and connected it to the commercial basestation using an Ethernet cable. We use commercial cell phones as UEs.

2.2 Data Collection and Processing

In this experiment, we collect and process data on the user plane (UP). 5G CN decouples the control plane (CP) and the UP in order to provide users with low-latency network service. Specifically, CP deals with UE signalling data and control data when UE requests to get access to CN, or updates their sessions. After UEs get access to the network, they only communicate with UP in CN, or UP function, i.e., UPF. Here, both UPF and basestation run GTP protocols to encapsulate the data.

We capture data on CN Ethernet interface using WireShark. We collected 30,000 rows of packets for each App. All packets are encapsulated by GTP protocol. We observe that these applications rely on different protocols, such as QUIC, UDP, and TCP. Also, it is interesting to see that the brands of mobile devices, e.g., Samsung, Huawei, Apple, etc, have no impact on using protocols.

Next, we preprocessed the .pacp files to images using tools presented in [5]. We divided the dataset into smaller sizes by packet count. After processing, all data is converted to a one-channel figure and the sample size is 784 bytes. The training data occupies 80% and the test data is 20%. Now, our data is ready for model training and testing.

2.3 Deep Learning Model

Can attackers tell App types based on the GTP data sniffed? To answer this question, we choose three CNN models: Resnet, Googlenet and Densenet to classify the GTP data traffic with encrypted application payload.

3 PERFORMANCE RESULTS

We evaluate the accuracy of these three models in terms of different App types. Fig. 1 shows the accuracy of five Apps: IG, TikTok, Google Meeting, Youtube, and Twitter.

We observe that the classification accuracy results in terms of different models are all above 97%. The best model is Resnet, which achieves 99.8% accuracy on average. That is, attackers could identify what users are doing based on GTP data with high prediction accuracy. If the wireless channel of ABS-CN is exposed to attackers, it may leak the personal information. Therefore, the security issues of ABS-CN wireless channels in 6G should be further studied.

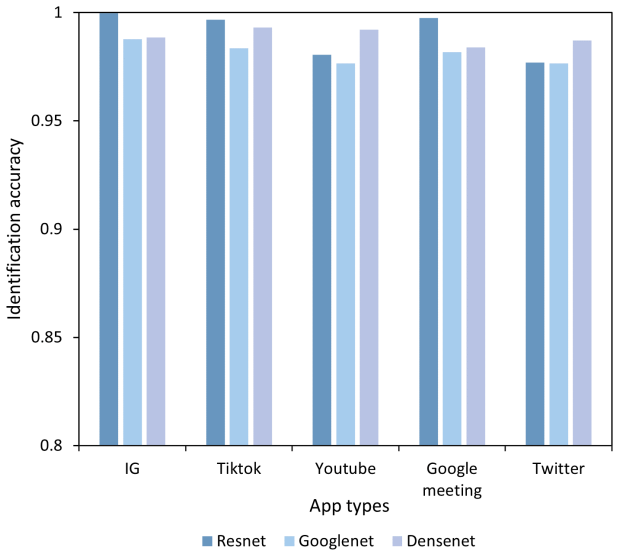

Figure 1: App identification accuracy in terms of different models.

4 CONCLUSION

In this demo, we show that a passive attacker could sniff on the wireless ABS-CN channel in 6G, and identify App types based on the GTP encrypted data by deep learning methods even without decryption. More research should focus on the wireless channels of CN and ABS.

As for future work, we are planning to identify other types of personal information in 6G, such as mobile operating systems. Also, we are going to simulate active attacks, e.g. fake base station and overshadowing.

REFERENCES

[1] Georgios Amponis, Thomas Lagkas, Maria Zevgara, Georgios Katsikas, Thanos Xirofotos, Ioannis Moscholios, and Panagiotis Sarigiannidis. 2022. Drones in B5G/6G networks as flying base stations. *Drones* 6, 2 (2022), 39–57.

[2] Simon Erni, Martin Kotuliak, Patrick Leu, Marc Roeschlin, and Srdjan Capkun. 2022. AdaptOver: adaptive overshadowing attacks in cellular networks. In *Proc. MobiCom '22*. 743–755.

[3] Cheng-Ying Hsieh, Yao-Wen Chang, Chien Chen, and Jyh-Cheng Chen. 2021. Design and implementation of a generic 5G user plane function development framework. In *Proc. MobiCom '21*. 846–848.

[4] Guangyi Liu, Na Li, Juan Deng, Yingying Wang, Junshuai Sun, and Yuhong Huang. 2022. The SOLIDS 6G mobile network architecture: driving forces, features, and functional topology. *Engineering* 8, 2095 (2022), 42–59.

[5] Zhuang Qiao, Liuqun Zhai, Shunliang Zhang, and Xiaohui Zhang. 2021. Encrypted 5G over-the-top voice traffic identification based on deep learning. In *Proc. ISCC '21*. 1–7.

[6] Liuqun Zhai, Zhuang Qiao, Zhongfang Wang, and Dong Wei. 2021. Identify what you are doing: Smartphone apps fingerprinting on cellular network traffic. In *Proc. ISCC '21*. 1–7.