Master's thesis

NTNU
Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

Sigurd Varhaugvik

Privacy Analysis of Next Generation Emergency Communication Network Devices in Norway

Master's thesis in Communication Technology and Digital Security
Supervisor: Stig Frode Mjølsnes, IIK
Co-supervisor: Ravishankar Borgaonkar, SINTEF IKT
June 2022

NTNU
Norwegian University of Science and Technology

Sigurd Varhaugvik

Privacy Analysis of Next Generation Emergency Communication Network Devices in Norway

Master's thesis in Communication Technology and Digital Security
Supervisor: Stig Frode Mjølsnes, IIK
Co-supervisor: Ravishankar Borgaonkar, SINTEF IKT
June 2022

Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

NTNU
Norwegian University of
Science and Technology

Title: Privacy Analysis of Next Generation Emergency Communication Network Devices in Norway

Student: Sigurd Varhaugvik

Problem description:

The Norwegian nationwide emergency wireless communication network is named "Nødnett". Nødnett has about 60 000 users, all members of first responder emergency organisations, both public and private. The existing Nødnett is based on the dated ETSI TETRA standard, and the next generation Nødnett (NGN) is planned to be based on 4G/5G cellular network technology, or even become an operational part of commercial mobile networks. This upgrade will enable a variety of new high-speed digital communication services, but will certainly also introduce new security threats to the NGN operation and the communication services provided.

This master thesis work will assess the practical significance of maintaining user terminal *location and tracking confidentiality* in the NGN environment, and specify a model for this security requirement. The work will investigate whether it is technical feasible to satisfy the specified tracking security in NGN, when existing smartphone user terminals equipped with both 4G/5G, WiFi, and Bluetooth communication are used. If practical attacks are identified, then the student will attempt to describe relevant technical mitigation techniques that can be applied. The investigation may be limited to the wireless communication layers. Important findings or claims should be sought to be supported by experimental validation.

Approved on: 2022-01-26

Main supervisor: Stig Frode Mjølsnes, NTNU IIK

Co-supervisor: Ravishankar Borgaonkar, SINTEF IKT

Abstract

The Norwegian Public Protection and Disaster Relief (PPDR) services such as ambulance, firefighters, and police are essential to maintaining a safe and secure society. Collaboration is essential to operate efficiently and requires a reliable wireless communication network. TErrestrial Trunked RAdio (TETRA) is the current emergency communication network used in Norway, called Nødnett. However, taking advantage of new technologies in the TETRA solution has proven difficult due to the low data rates it provides. Therefore a new solution for the Norwegian emergency communication, called Next Generation Nødnett (NGN), is required. Integrating NGN into the 4G and 5G mobile communication networks is one viable option. The 5G technology is developed with emergency communication needs in mind and hence, is a good fit for the NGN solution. Furthermore, a 5G enabled NGN adds support for technologies that can improve the work of the PPDR services and save lives.

However, adopting a new technology for emergency communication, requires changing all utilized equipment including the mobile handsets used in communication. Commercial mobile phones are a possible solution for replacing the handsets, and as they support other wireless communication technologies such as WiFi and Bluetooth, NGN has the possibility to take advantage of them, which can introduce new possibilities in the PPDR services work. However, new technologies also introduce new unique identifiers that can be used to track PPDR personnel's location.

This thesis, through a systematic method, aims at identifying location-privacy-related vulnerabilities and relevant mitigation techniques for the wireless communication technologies 4G, 5G, and WiFi. We identify and categorize ten vulnerabilities for WiFi and fifteen for 4G/5G and discuss how they can be exploited in the context of NGN to track PPDR service personnel with commercial mobile devices over time. We aim to provide the relevant stakeholders of NGN with information that will assist in designing a secure infrastructure for NGN.

We experiment with an attack on one of the identified vulnerabilities for WiFi to determine its effect on modern devices using Medium Access Control (MAC) address randomization. We also propose a new technique taking advantage of the same vulnerability that can track devices over time regardless of the device's randomized MAC address. We show that it can be used in low-traffic scenarios to track devices and discuss how its effect can be improved to work in high-traffic scenarios.

Sammendrag

Beredskapstjenester som ambulanse, brannmenn og politi er avgjørende for å opprettholde et trygt og sikkert samfunn. Samarbeid er essensielt for arbeidet og krever et pålitelig trådløst kommunikasjonsnettverk. Terrestrial Trunked RAdio (TETRA) er det nåværende nødkommunikasjonsnettverket som brukes i Norge, kalt Nødnett. Det har imidlertid vist seg vanskelig å dra nytte av nye teknologier i TETRA-løsningen på grunn av de lave datahastigheter den gir. Derfor kreves en ny løsning for norsk nødkommunikasjon, kalt Neste Generasjons Nødnett (NGN). Integrering av Nødnett i 4G- og 5G-mobilkommunikasjonsnettverket er et levedyktig alternativ. 5G-teknologien er utviklet med tanke på nødkommunikasjonsbehov og passer derfor godt til NGN-løsningen. Videre vil et 5G-aktivert NGN muliggjøre teknologier som kan forbedre arbeidet til beredskapstjenestene og redde liv.

Men å endre teknologien som brukes for nødkommunikasjon krever også endring av alt kommunikasjonsutstyr, inkludert de mobile enhetene brukt i kommunikasjon. Kommersielle mobiltelefoner er en mulig løsning for å bytte ut håndsettene, og siden de støtter andre trådløse kommunikasjonsteknologier som WiFi og Bluetooth, har NGN muligheten til å dra nytte av dem, noe som kan introdusere nye muligheter i beredskapsarbeidet. Nye teknologier introduserer imidlertid også nye unike identifikatorer som kan brukes til å spore plasseringen til brukeren av enhetene.

Denne oppgaven, gjennom en systematisk metode, tar sikte på å identifisere lokasjons-personverns-relaterte sårbarheter og relevante motvirkende teknikker for de trådløse kommunikasjonsteknologiene 4G, 5G og WiFi. Vi identifiserer og kategoriserer ti sårbarheter for WiFi og femten for 4G/5G og diskuterer hvordan de kan utnyttes i NGN for å spore beredskapspersonell med kommersielle mobile enheter over tid. Vi tar sikte på å gi de relevante interessentene i NGN informasjon som vil hjelpe til med å designe en sikker infrastruktur for NGN.

Vi eksperimenterer med et angrep på en av de identifiserte sårbarhetene for WiFi for å bestemme effekten på modern enheter med Medium Access Control (MAC) adresserandomisering. Vi foreslår også en ny teknikk som utnytter den samme sårbarheten som kan spore enheter over tid uavhengig av enhetens randomiserte MAC-adresse. Vi viser at den kan brukes i scenarier med lite trafikk for å oppdage og spore enheter og diskutere hvordan effekten kan forbedres for å fungere i scenarier med høy trafikk.

Preface

This Master's thesis results from a five-year Master's degree in Communication technology and Digital Security at the Department of Information Security and Communication Technology (IIK) at the Norwegian University of Science and Technology (NTNU). The research presented in this thesis was conducted between January 2022 and June 2022.

I would first like to thank my supervisor, Ravishankar Borganokar, and responsible professor Stig Frode Mjølsnes, for their time and valuable feedback throughout this time. Second, I have to give a special thanks to Molly Gibson for her help with the experiment.

I would also like to thank my family and friends for your support this semester.

Contents

List of Figures

List of Tables

List of Acronyms

3GPP 3rd Generation Partnership Project.

4G 4th generation of mobile architecture.

5G 5th generation of mobile architecture.

5G HE AV 5G Home Environment Authentication Vector.

5G SE AV 5G Serving Environment Authentication Vector.

5G-AKA 5G Authentication and Key Agreement.

5GC 5G Core Network.

5GS 5G System.

AK Anonymity Key.

AKA Authentication and Key Agreement.

AMF Access and Mobility Management Function.

AP Access Point.

ARPF Authentication credential Repository and Processing Function.

AUSF Authentication Server Function.

AUTN AUthentication TokeN.

AV Authentication Vector.

BLE Bluetooth Low Energy.

BSSID Basic Services Set IDentifier.

CI-RNTI Cancellation Indication RNTI.

C-RNTI Cell RNTI.

CSMA/CA Carrier-Sense Multiple Access with Collision Avoidance.

CS-RNTI Configured Scheduling RNTI.

CTS Clear To Send.

D2D Device-to-Device.

DSB Norwegian Directorate for Civil Protection.

EAP Extensible Authentication Protocol.

EAP-AKA Extensible Authentication Protocol Authentication and Key Agreement.

EAP-AKA' Improved Extensible Authentication Protocol Authentication and Key Agreement.

EAP-TLS Extensible Authentication Protocol Transport Layer Security.

ECIES Elliptic Curve Integrated Encryption Scheme.

EIR Equipment Identity Register.

eNB evolved-NodeB.

EPC Evolved Packet Core.

EPS-AKA Extensible Authentication Protocol Authentication and Key Agreement.

ESI Encrypted Short Identity.

e-SIM Embedded-SIM.

EUI-48 Extended Unique Identifier-48.

EUI-64 Extended Unique Identifier-64.

E-UTRAN Evolved Universal Terrestrial Radio Access Network.

GPSI Generic Public Subscription Identifier.

GUAMI Globally Unique AMF Identifier.

GUMMEI Globally Unique Mobility Management Entity Identifier.

GUTI Globally Unique Temporary UE Identity.

HRES Hash RESponse.

HSS Home Subscriber Server.

HXRES Hash eXpected RESponse.

IE Information Element.

IMEI International Mobile station Equipment Identity.

IMEISV International Mobile station Equipment Identity and Software Version number.

IMSI International Mobile Subscriber Identity.

INT-RNTI Interruption RNTI.

IOI Items Of Interest.

IOPS Isolated Operation for Public Safety.

IoT Internet of Things.

ISSI Individual Short Subscriber Identity.

ITSI Individual TETRA Subscriber Identity.

LTE Long Term Evolution.

MAC Medium Access Control.

MCC Mobile Country Code.

MCS-C-RNTI Modulation Coding Scheme Cell RNTI.

MITM Man-In-The-Middle.

MME Mobility Management Entity.

mmW millimeter Wave.

MNC Mobile Network Code.

MNMap Mobile Network Mapping.

MSIN Mobile Subscriber Identification Number.

MSISDN Moblie Station International Subscriber Directory Number.

NAI Network Access Identifier.

NAS Non-Access-Stratum.

NB-IoT Narrow Band IoT.

NFC Near-Field Communication.

NFV Network Function Virtualization.

NGN Next Generation Nødnett.

NG-RAN 5G Radio Access Network.

NIC Network Interface Controller.

NR New Radio.

NSA Non-StandAlone.

NSI-ID Network Slice Instance IDentifier.

NTNU Norwegian University of Science and Technology.

OUI Organizationally Unique Identifier.

PEI Permanent Equipment Identifier.

PIERCER Persistent Information ExposuRe by the CorE netwoRk.

PLMN Public Land Mobile Network.

PO Paging Occasion.

PPDR Public Protection and Disaster Relief.

P-RNTI Paging RNTI.

PS-RNTI Power Saving RNTI.

PUCCH Physical Uplink Control CHannel.

PUSCH Physical Uplink Shared CHannel.

RAND Random Challenge.

RA-RNTI Random Access RNTI.

RES RESponse.

RLF Radio Link Failure.

RNTI Radio Network Temporary Identifier.

RQ Research Questions.

RRC Radio Resource Control.

RTS Request To Send.

SA StandAlone.

SDN Software-Defined Networking.

SDR Software-Defined Radio.

SEAF SEcurity Anchor Function.

SFI-RNTI Slot Format Indication RNTI.

SIDF Subscription Identifier De-concealing Function.

SIM Subscriber Identity Module.

SI-RNTI System Information RNTI.

SLR Systematic Literature Review.

SL-RNTI Sidelink RNTI.

SN ID Serving Network Identifier.

SP-CSI-RNTI Semi-Persistent Channel State Information RNTI.

SPS-C-RNTI Semi-Persistent Scheduling Cell RNTI.

SQN Sequence number.

SSID Service Set IDentifier.

S-TMSI Serving Temporary Mobile Subscription Identifier.

SUCI Subscription Concealed Identifier.

SUPI Subscription Permanent Identifier.

SVN Software Version Number.

TA Tracking Area.

TAC Type Allocation Code.

TAU Tracking Area Update.

TC-RNTI Temporary Cell RNTI.

TETRA TErrestrial Trunked RAdio.

TMSI Temporary Mobile Subscription Identifier.

ToRPEDO TRacking via Paging mEssage DistributiOn.

TPC-PUCCH-RNTI Transmit Power Control-PUCCH RNTI.

TPC-PUSCH-RNTI Transmit Power Control-PUSCH RNTI.

TPC-SRS-RNTI Transmit Power Control-Sounding Reference Signal-RNTI.

UDM Unified Data Management.

UE User Equipment.

USIM Universal Subscriber Identity Module.

UUID Universally Unique IDentifier.

WEP Wired Equivalent Privacy.

WPA Wi-Fi Protected Access.

WPS WiFi Protected Setup.

WPS UUID WiFi Protected Setup UUID.

XRES eXpected RESponse.

Chapter 1
Introduction

Over the last few years, the rapid development of new technologies has pushed the Norwegian PPDR service to reevaluate the emergency wireless communication network solution, as the current solution does not support the required data rates to take advantage of these technologies. One of the proposed solutions is to integrate the network into the 4G and 5G mobile networks, which is not a new idea as it already has been deployed/is under development in other countries in the world [Sou; Fira; UK 22].

This chapter introduces the thesis and justifies the topic's relevance for the literature review on existing vulnerabilities and the experiment on one of the identified vulnerabilities.

1.1 Motivation

The PPDR services, including police, firefighters, and ambulances, play a critical role in maintaining a safe and secure society by responding to emergencies and disasters. They require a secure and reliable way of communicating with high availability to operate normally. In Norway, Nødnett is the public safety network used to deliver mission-critical communication [DSBc]. Nødnett, which means emergency network in Norwegian, is an isolated TETRA network. The fact that it is isolated means that it is physically separated from other networks (e.g., commercial networks) and hence uses its own frequency band. The defined TETRA standard has a maximum transmission speed of 12 kbit/s [DSB20], and in order for the PPDR services to access and use the network, they require specially made devices. These are devices like MPT3550, and they only have the communication hardware required to connect to the network and necessary equipment [MOT20].

Over the last couple of years, many new technologies like video streaming, augmented reality, Internet of Things (IoT), and many more have been introduced commercially. Taking advantage of these new technologies could be highly beneficial

for the PPDR service in their everyday work by reducing the response time and time spent on other tasks, leading to a safer society. However, the current Nødnett does not support the required data rates to take advantage of these technologies. Additionally, the current isolated solution for Nødnett is costly to maintain, and the Norwegian government has decided that the 700 MHz frequency band used currently by Nødnett should be available commercially [DSB18]. Therefore, the Norwegian government is looking at alternatives for the Next Generation Nødnett (NGN).

One of the proposed ways of implementing NGN is to have it as a part of the mobile network. Hence, the Norwegian Directorate for Civil Protection (DSB) has proposed solutions for running NGN within the commercial 4G and 5G mobile networks [DSB18]. With a switch to 5G based Nødnett, the transmission rate could be as high as 1 Gbit/s with a latency of 10ms, hence allowing for mission-critical real-time communication. This will make it possible to take advantage of new technologies, which will improve the efficiency of the PPDR services, leading to a safer and more secure society.

However, to adapt Nødnett to the mobile network, all or most existing end-user equipment will have to be replaced. Including the currently used Motorola [Mot] devices. An alternative is commercial mobile phones since they already work in the mobile networks, and upgrading them to take advantage of new technology features (e.g., high data rates) is beneficial to improve emergency responses. Therefore, commercial mobile phones are a candidate for future NGN devices. These devices also bring new wireless communication technologies like WiFi, Near-Field Communication (NFC), Bluetooth, 4G, and 5G into NGN. However, new communication technology also introduces new metadata and unique identifiers related to the device. The new metadata and identifiers will be transmitted over the radio interface by the device during wireless communication, increasing the risk of adversaries identifying the NGN device and exposing the PPDR user location[1].

Currently, in Norway, Nødnett is used by multiple government and private organizations, and anyone can apply to use it [DSBa]. However, the core users of Nødnett are the PPDR services. Therefore, having the location exposed could primarily be a threat for the police service personnel due to the nature of their work. It might disrupt an ongoing or covert criminal investigation and even threaten the safety of police service personnel, leading to casualties. Furthermore, by increasing the communication capabilities of the devices used by PPDR personnel, the attack surface of identifying and localizing (i.e., tracking[2]) a device is also increasing. This is

[1] In this thesis, the term "location" will refer to the physical geographical location of the PPDR user's device. Detecting a device's location is determined by sniffing the wireless signals transmitted on the air interface and obtaining identifiers that partially or uniquely identify the devices.

[2] The term "tracking" will refer to actively determining the location of a device belonging to PPDR personnel or someone within a group of PPDR personnel's.

because wireless communication signals are available to everyone within the device's transmission range. Therefore, not exposing the unique identifiers and metadata through the wireless signals is crucial for the safety of PPDR personnel (primarily police) and the secrecy of their sensitive operations.

The authors in [Syv20] identify the PPDR user location as a key asset in NGN and states the use of non-NGN wireless communication such as WiFi, NFC, and Bluetooth as a threat. Additionally, DSB and the police force have raised concerns about exposing the PPDR location to adversaries.

1.1.1 Exploiting modern WiFi enabled devices

Many existing attacks exploiting vulnerabilities in the WiFi protocol take advantage of using a persistent unique address to track devices over time. However, as MAC address randomization is becoming more and more common in commercial mobile devices, many straightforward tracking techniques are no longer applicable for tracking devices over time. Therefore, the practical experiment in this thesis will investigate whether one of the identified WiFi vulnerabilities is still applicable for tracking modern devices and investigate a new technique exploiting the same vulnerability that can track devices regardless of MAC address randomization.

1.2 Related Work

The authors in [Syv20] present a possible way of integrating Nødnett as part of the 5G network and an associated risk assessment. The risk assessment identifies the privacy concern by leaking subscribers' location data through communication technologies like WiFi, Bluetooth, and NFC and locating users through International Mobile Subscriber Identity (IMSI) catchers in 4G. However, their work considers abstract privacy concerns and does not go into the privacy concerns in any more detail. This thesis will present an overview and classification of privacy-related vulnerabilities in WiFi, 4G, and 5G and provide relevant mitigation techniques.

A location privacy analysis of the TETRA network is presented by Classen et al. [CPK+14]. It describes a way of localizing TETRA devices using antennas and direction-finding techniques on the physical layer. However, their research concerns the current TETRA network used by Nødnett. This thesis will look into NGN based on public 4G and 5G networks.

The authors in [Mat17] present many known privacy vulnerabilities for WiFi. However, we show that the list is incomplete and identify more vulnerabilities in this thesis. Additionally, many of the referenced vulnerabilities are old, and whether they are still relevant is not discussed. We will also provide a classification of the

vulnerabilities discovered. The authors in [Fon20] list known vulnerabilities for 5G. However, they do not look specifically at privacy threats or cover all.

Research done in both [VMC+16; Cun14] describes and test the vulnerability used in our experiment. However, they only show that the technique can trigger a response from the device, but do not investigate how it can be used to track devices over time. Additionally, the papers do not consider the commonness of randomization in modern devices as that was not common when the papers where released. Neither do they investigate how different devices respond when exposed to the vulnerability.

1.3 Goals and research questions:

This thesis will investigate how NGN devices can be identified and localized by exploiting wireless radio signals. The primary focus is to identify possible ways of tracking NGN devices used by the PPDR users, such as the police. More specifically, we aim to perform a systematic study and investigate how unique identifiers and metadata in layers 1, 2, and 3 of WiFi, 4G, and 5G communication technology can lead to the identification of a device. Additionally, identification and discussion of relevant mitigation techniques and their effect in practice on open issues will be conducted.

We aim to answer the following Research Questions (RQ) in the context of location preservation in 4G and 5G enabled NGN with an assumption of commercial devices.

RQ1: What are the primary location tracking concerns for commercial mobile phones regarding technologies like WiFi, 4G, and 5G in the context of NGN?

RQ2: How can tracking a device lead to tracking emergency security personnel in the context of NGN?

RQ3: Which communication technology is the most vulnerable to location tracking attacks on today's commercial mobile phones?

RQ4: What are the effective mitigation techniques to protect location tracking for commercial phones in the context of NGN?

RQ5: Do modern commercial devices in practice follow technical standards and implementation specifications defined for WiFi?

1.4 Work method

This section will describe and justify the research methodology adopted for this thesis. The methodology is divided into three main parts. The first part is a form of

a Systematic Literature Review (SLR) to obtain existing privacy vulnerabilities in WiFi, 4G, and 5G technologies and relevant mitigation techniques. The second part concerns a practical experiment with one of the identified vulnerabilities from the literature review. Finally, the third part consists of an analysis and discussion in the context of the NGN network with commercial devices of the identified vulnerabilities and results from the experiment.

1.4.1 Systematic literature review

A SLR described in [RM16] is too comprehensive for this thesis. Instead, a literature review will be conducted with a systematic form at its base. The literature review identifies the privacy-sensitive identifiers used by the technologies in Chapter 3. Existing privacy-related vulnerabilities that can identify the presence of a device and mitigation techniques will be presented and categorized in Chapter 4. In order to avoid biased papers and papers that are not peer-reviewed, a set of search keywords, databases, and inclusion and exclusion criteria are defined. They are inspired by the pre-project [Var21], but a few adjustments are made.

Search keywords

The search terms were chosen to obtain the most relevant studies for the topics of the thesis. In addition to the search terms, papers were discovered through references from other papers describing vulnerabilities or mitigation techniques. The following search terms were used to search for papers in the academic archives listed in Table 1.1: “NETWORK location tracking”, “NETWORK tracking attack”, “NETWORK tracking android”, “NETWORK tracking iOS”, and “device location exposure in NETWORK”. “NETWORK” is one of the network technologies WiFi, 4G or 5G. Searches based on relevant discoveries from the result are conducted if necessary.

Search engines/literature databases

Different academic search engines and literature databases were used to ensure the credibility of the identified relevant papers for vulnerabilities and mitigation techniques. Table 1.1 presents the complete list of search engines and databases used. In addition, using standard documents or papers released by governments is done regardless of being in the databases.

Inclusion and exclusion criteria

We define inclusion and exclusion criteria to obtain the most relevant papers and avoid biases.
The inclusion criteria:

Database	URL
IEEE explore	http://ieeexplore.ieee.org/
Google scholar	https://scholar.google.com/
ACM digital library	http://dl.acm.org/
Science direct	http://www.sciencedirect.com/
Springer	http://www.springer.com/
arxiv	https://arxiv.org/
NTNU University Library	https://www.ntnu.edu/ub
IETF	https://www.ietf.org
Sciendo	https://www.sciendo.com/

Table 1.1: Search database sources

- The study focuses on vulnerabilities that can expose the location or identify the presence of a device through emitted signals or techniques that can increase the impact of other identified vulnerabilities.
- The study should not be published earlier than 2010 for WiFi and 2015 for 4G and 5G.
- The articles should be published as either surveys or research papers.
- The study should be written in English.

The exclusion criteria:

- The study has not been peer-reviewed
- The study is not published in any of the listed search databases, except for previous master thesis at the Norwegian University of Science and Technology (NTNU).

Standards and government papers are excluded from the criteria due to being relevant even when not published in an academic database or peer-reviewed.

Study selection

The first part of the study selection is by the filters at the search engines used with the keywords given. The keywords assure us that papers not relevant to this thesis will be filtered out. Then the exclusion and inclusion criteria are used to filter more papers. Finally, articles will be excluded based on unrelated titles, abstracts, and vulnerabilities unrelated to this thesis.

1.4.2 Practical experiment

The second part of the methodology is a practical experiment on one of the vulnerabilities discovered. The vulnerability will be tested in a controlled environment on commercial mobile devices to observe their behavior and in a real-world scenario to see if the vulnerability can be used in practice. A Python program with Scapy [Sca] taking advantage of the vulnerabilities is developed. The implementation of the experiment and results are presented in Chapter 5.

1.4.3 Analysis of results and vulnerabilities

The third part consists of a discussion and analysis of how the identified vulnerabilities can track emergency personnel in the context of NGN. Additionally, we will analyze the results of the experiment. We will focus on the police force and not limit ourselves to uniquely identifying the personnel. Techniques that can identify that the device belongs to a group of people, for example, the police force will also be discussed.

1.5 Contributions

The main contribution of this paper is a classification of location exposing vulnerabilities that are present in the network communication technologies WiFi, 4G, and 5G, and a presentation of how they can be taken advantage of in the context of NGN. Additionally, we will give a set of guidelines, in the form of mitigation techniques, on how the NGN infrastructure (network and devices) should be maintained and operated to mitigate identified threats. We also present a recommendation on selecting devices for NGN. RQ2 addresses different techniques that can correlate a unique identifier of a device to the emergency security personnel carrying the device. RQ3 provides an discussion on which communication technologies WiFi, 4G, and 5G pose the most location exposure risk in commercial mobile devices.

Additionally, Chapter 5 analyzes the effect of one of the vulnerabilities on modern devices in a controlled environment as well as in a real-world scenario. We also propose a new technique exploiting the same vulnerability and evaluate if it can track devices over time regardless of MAC address randomization.

We believe our results will assist the relevant stakeholders in deciding which commercial mobile devices can be used within NGN in context of location privacy. As well as provide helpful input when deciding which and how the wireless communication technologies can be taken advantage of by the PPDR services in NGN while maintaining the privacy of the PPDR personnel.

1.6 Outline

This thesis is divided into seven chapters. Following is a brief description of the content in each chapter.

Chapter 1 - Introduction presents and gives a motivation for the project. The RQs are also formulated.

Chapter 2 - Background provides the necessary background theory for the topics in this thesis. Essential information for WiFi, 4G, and 5G, as well as for Nødnett and NGN is also presented.

Chapter 3 - Identifiers provides the identifiers used during communication associated with one of the communicating parties.

Chapter 4 - Vulnerabilities and Mitigation Techniques presents the identified vulnerabilities through the literature study and relevant mitigation techniques.

Chapter 5 - Experiment presents the implementation and execution details of the experiment and the obtained results.

Chapter 6 - Discussion will discuss the discovered vulnerabilities and mitigation techniques in the context of NGN network. Additionally, the results of the experiment will be discussed.

Chapter 7 - Conclusion and Recommendation conclude the thesis and gives a recommendation on design for a secure infrastructure for NGN. The results of the experiment will also be discussed.

Chapter 2
Background

This Chapter will provide relevant background information for the topic of this thesis and introduce concepts required to explain the identified vulnerabilities and the technique used in the experiment.

2.1 Nødnett

Communication is essential for collaboration between the PPDR services. Therefore, the Norwegian PPDR services decided in 1995 to create a joint nationwide radio system called Nødnett, which is currently based on the TETRA standard. TETRA is a mobile radio standard meant for professional mobile radio such as military and public safety services [ETS]. It is used for critical communication in many countries in the world and is therefore also a good fit for the Norwegian Nødnett [DSBa]. Nødnett officially opened in 2015, and with its 2100 base stations, it covers 86% of the Norwegian mainland and almost 100% of the population [DSBb].

However, even though TETRA is used in many countries today, it is not widely used commercially, and hence not much research has been conducted on it. The current solution for Nødnett has multiple security mechanisms in place. For instance, it supports end-to-end encryption, which is a service only available to the PPDR and not to other users of Nødnett [DSB20]. The TETRA unique identifier is called Individual TETRA Subscriber Identity (ITSI) and it contains Individual Short Subscriber Identity (ISSI) which is essentially a phone number. For a devices to identify and authenticate itself, it first sends its identity to the base station before it receives a challenge from the base station. The device needs to possess the same symmetric key as the central server to answer the challenge correctly. The authors in [PKR10] provide an analysis of the authentication procedure and state that with knowledge of the symmetric key, an adversary can eavesdrop on the communication.

Additionally, due to the use of encryption in Nødnett, the device will never transmit its unique identifiers in the clear on the air interface. Instead, it will

generate and transmit an Encrypted Short Identity (ESI) temporary value to identify itself to the network [3GPj]. Hence, an adversary can not passively listen to the air interface and detect unique identifiers to track PPDR personnel. Additionally, S. Duan presents attacks that can reduce the availability of Nødnett [Dua13].

Devices currently used in Nødnett, such as the MPT3550, only have the necessary hardware to connect to the network and other Bluetooth devices [MOT20]. Furthermore, with the limited transmission speed of TETRA, taking advantage of new technologies has proven to be difficult. Hence, alternative devices and Nødnett solutions could be beneficial. Since TETRA is a not widely adapted network, not much research has been put into identifying its vulnerabilities. However, some vulnerabilities exist. For example, Classen et al. [CPK+14] describes an attack that detects nearby devices using the TETRA frequency. However, this is not a large concern in Norway since the network is available to many organizations, and hence detecting usage of the frequency band could originate from many entities. Therefore, TETRA is believed to be a secure communication technology.

The Nødnett is currently operated by MOTOROLA [Mot], but the contract between Motorola and DSB expires in 2026. This means that the Norwegian government can either re-negotiate the contract or look for other solutions for Nødnett. Since Nødnett is physically separated from the mobile network, it consists of its own infrastructure that requires its own power, which is a costly way of running a network. It also requires a separate frequency band to operate. It has already been decided that the 700MHz band Nødnett uses should be available commercially [DSB17] and hence, the Norwegian government has decided that after the contract expires in 2026, a new and more sustainable solution for Nødnett is required.

2.1.1 5G enabled Nødnett

5G is the newest standard within mobile networks, and it is created with critical communication in mind. High-priority data links and real-time communication is expected from the critical communication networks. This is provided in 5G through Network Function Virtualization (NFV) and the expected low latency. The 5G network can also be the foundation for other applications and services with different performance requirements, such as artificial intelligence, big data, and mission-critical IoT [MP18]. Additionally, 5G provides two important features for NGN: Device-to-Device (D2D) communication and Isolated Operation for Public Safety (IOPS). D2D is two devices communicating directly with each other without a middle man, and in the context of NGN it is mainly used when a device does not have access to the base-station [KS19]. The IOPS decreases the system's dependability on the core network by enabling the base stations to deploy their own core network in case it loses connection to the core [OCL+17]. If the base stations can connect to each

other, then one can be the core, and the others can act as usual [OCL+17]. The new core network is provided for public safety users and will have a limited set of functionality [OCL+17].

Many countries around the world are considering mobile networks as their following emergency communication network, and some countries are already testing the solution [UK 22; Sou]. In the United States of America, the emergency network known as Firstnet [Fira] is already built on commercial cellular networks (primarily 4G). Hence, deploying a 5G enabled emergency communication network is not just a theoretical possibility but a realistic option.

2.2 Use cases and technology selection

The different wireless communication technologies such as WiFi, 4G, and 5G all work towards accomplishing the same goal in NGN. These technologies assist in increasing the efficiency of the work of PPDR services. In this section, we will give examples of use cases for the different technologies to show why they are needed in NGN.

5G is the newest wireless commercial mobile network and will make it possible for the PPDR service to take advantage of many new applications and services. However, the 5G development in Norway only started commercially in 2020[NKO21] and the coverage of 5G will probably never be as high as for 4G in the early days. Hence, it is also important to include 4G in this thesis since it already has an 85% coverage of the Norwegian geographical area. Therefore, 4G combined with 5G can provide on-field high-speed Internet to the PPDR services. Furthermore, the 4G network is also vital for the study in this thesis due to downgrading attacks. However, older technologies such as 2G and 3G are not essential to analyze since the Subscriber Identity Module (SIM) cards can block them in a similar way as the Norwegian defense military describes in [Nom].

A secure WiFi network can act as an alternative for mobile network solutions in the office, which could be more cost-efficient and easier to manage security-wise. Additionally, having multiple communication capabilities is very beneficial because they can act as fallbacks for each other. For example, if one communication technology stops working for a device, the other could take over the communication and act as a fallback. However, this is currently not a feature in the TETRA Nødnett, where if the network stops working, no alternative to the Nødnett solution exists.

Bluetooth can assist the PPDR service in everyday work by connecting them to commercially available devices, like headsets. Furthermore, many smaller tasks could be automated by using Bluetooth Low Energy (BLE), like authentication between devices or unlocking cars, which again will reduce the response time of the

PPDR services. However, due to time restrictions, Bluetooth will not be discussed in this thesis. Furthermore, NFC is also a common communication technology on commercial mobile devices. However, due to the low range of the technology NFC will not be evaluated in this thesis.

2.3 Terminology

This thesis will use the terms anonymity and unlinkability when describing and discussing vulnerabilities. They are described in this section and are similar to those described in [PHT11].

2.3.1 Anonymity

Anonymity of a subject means that the subject is not identifiable within a set of subjects, the anonymity set [PHT11]. This means that an adversary can not identify the individual to whom the information it has at hand belongs. In the context of NGN, we will distinguish between two different types of anonymity. Individual anonymity refers to a subject not identified as a specific individual. In contrast, group anonymity refers to a subject not being identified to be part of a predefined group, such as PPDR personnel or the police force. The distinction is necessary since determining a subject to be part of the police force is very valuable to an adversary.

2.3.2 Unlinkability

Unlinkability of two or more Items Of Interest (IOI) from an attacker's perspective means that within the system, the attacker cannot sufficiently distinguish whether these IOIs are related or not [PHT11]. In the context of NGN, similar to anonymity, we distinguish between two types of unlinkability: Individual unlinkability and Group unlinkability. Breaking the unlinkability of two IOIs does not imply breaking the anonymity of a user. However, breaking the anonymity means breaking the unlinkability of a subject and an IOI. Additionally, by breaking the unlinkability an adversary will have more information on a subject which might reduce the anonymity set of the subject.

2.4 WiFi

WiFi was first released in 1997 and has since grown to be one of the most popular wireless networks used in the world. It is maintained by the WiFi Alliance [Wi-b] and consists of multiple network protocols based on the IEEE802.11 standard. WiFi is deployed mainly in stationary locations such as work offices or homes and aims at being a wireless alternative for fast cabled Internet. The technology consists of two parts. The network router, often referred to as the AP, and a WiFi-capable

device. The communication happens between the two entities where the AP is responsible for maintaining a connection to the Internet. The surrounding area and the hardware used on the WiFi router is the central part that determines the range of the signals, but for private use, which is mostly indoors, it has a range of around 30 meters [Ele]. However, this can be extended with the mesh networks [Wi-c]. Additionally, with WiFi Enterprise [Wi-a], it is possible to deploy the same network in multiple geographical locations, which corporations often use to make it simpler for employees to use the network.

The standard is old, and there are many examples of exposing a user's location through the use of WiFi signals [Mil]. The standard has been updated many times to provide more and new functionality and improve the security features of the protocol. For example, many early implementation vulnerabilities have also been mitigated in newer devices by taking advantage of randomized MAC addresses and not advertising which network SSID it wants to connect to. In addition, the security measures in WiFi have improved from the seriously flawed Wired Equivalent Privacy (WEP) to the much stronger Wi-Fi Protected Access (WPA)3 protocol, which is the newest security standard for WiFi. However, even with the security enhancements, attacks that violate the location privacy of the user still exists [VMC+16; Fre15].

2.4.1 Network channels

WiFi operates at the two open (i.e., unlicensed) frequency bands, 2.4GHz and 5GHz [IEE21]. The main difference between the two bands is that while the 5GHz band has a higher data capacity, it also has less range than the 2.4GHz band. If two APs on separate bands have the same name and security context, a device will see the two as the same network and can switch between them. The frequency bands are further separated into channels. The standard defines 11 channels for the 2.4GHz band and 45 for 5GHz. However, due to transmitter variation, the channels overlap with each other. For 2.4 GHz, there are three non-overlapping channels, while for 5GHz, it is 24 non-overlapping.

2.4.2 Information element (IE)

An Information Element (IE) is a field in an 802.11 packet. The IE is usually provided to inform the router of capabilities, preferences and needs of the device in the wireless communication. Many different types of IE exist and some are optional and some required in certain packages. The IEs consists of three values: a type, length and value. The type indicates what the IE contains, the length is the total length of the IE and the value indicates the content.

2.4.3 Network discovery

Network discovery is the process in which a device detects the presence of a nearby network. In WiFi, this can happen in two different ways, one by the device sending out a probe request to nearby APs and the other where the AP sends out a beacon frame to advertise its presence [IEE21]. Once a device detects an available network present, it can attempt to connect to it.

Probe request

A device emits probe requests regularly to trigger responses from nearby APs. The probe request contains an address the device wants to receive responses to (which might be randomly generated), optionally the identifier of the AP it wants to connect to, and optionally a set of IEs the device wants to inform the networks about. If the identifier of the AP is empty (not set), then all APs in the proximity will respond to the request. However, only the AP with that identifier will respond if it is set. The probe request triggers a probe response from the AP, and when the device receives the responses, it knows which networks are available in the proximity. Since a AP only listen to one channel, the device needs to iterate over the channels and send probe requests in order to be sure the AP receives the request.

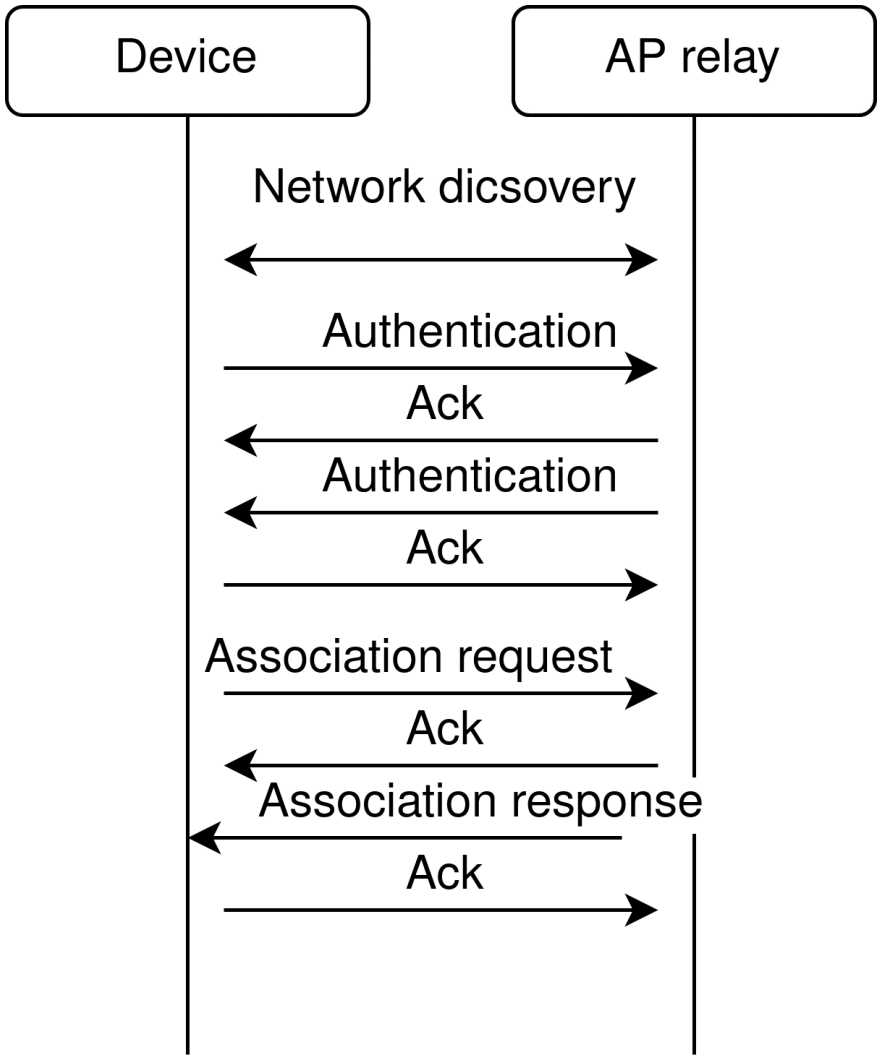
Beacon frame

The AP regularly sends beacon frames to advertise its presence to all the devices in the proximity. The beacon contains, amongst others, the identifier of the AP. Devices will need to detect the beacon to know of the presence of the AP. The AP only operates at one network channel and hence only emits beacons at one channel. Therefore the device needs to iterate over all channels and listen for beacons to identify all APs. The beacon frame will be detected by a device that is both connected and not connected to a network. Devices connected to a network can decide to connect to the discovered network if preferred.

2.4.4 Network attachment

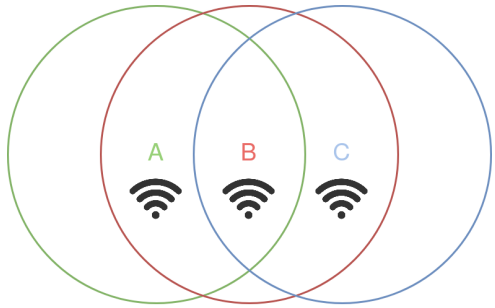
After a device discovers a network, it will initiate the attachment procedure with the network. The procedure starts with the device sending an authentication message to the network and is defined in [IEE21]. The authentication is done by the device to provide proof of identity and can be done with multiple different protocols. Which protocol depends on the security features of the AP router and the version of WiFi used. If the network approves the authentication of a device, it will respond with an authentication message. Once the device is authenticated, it will try to associate with the network. Association is necessary to establish before the network and device can communicate. This is because the network needs to know to which AP it should route

Figure 2.1: Network attachment in WiFi



the data for the device. The device initiates the association by sending an association response to the network AP, and once a logical link has been established, the network will respond with an association response. Both association and authentication messages require acknowledgment messages. After the network attachment procedure is complete, the device and network will negotiate keying material for the session. Figure 2.1 present the entire sequence.

Figure 2.2: Hidden terminal problem



2.4.5 Hidden network

Hidden networks are networks that do not emit beacon frames and hence do advertise their presence to nearby devices. This is done so that people that do not know that the network is present will not try to connect to the network. For the device to discover this network, the device needs to transmit a probe request with the identifier name of the AP. Once the AP detects the message, it will respond, and the device has detected the network. Since the network never advertises its presence, the first time a user connects to the network, the network name and password need to be entered manually before the device can send the probe requests.

2.4.6 RTS/CTS

WiFi uses the Carrier-Sense Multiple Access with Collision Avoidance (CSMA/CA) technique for the channel access control. A device that wants to transmit on the channel will listen for data traffic, and if it detects another device transmitting, it will wait a random amount of time before trying again. On the other hand, if no data transmission is detected, the device will attempt to transmit. However, this introduces the hidden terminal problem, which can be seen in in Figure 2.2. Both devices A and C can see the AP B but not each other, which can result in both A and C transmitting at the same time, creating interference at the AP. In order to mitigate this problem, WiFi introduces Request To Send (RTS)/Clear To Send (CTS) scheme [IEE21]. Before it transmits data, a device will send an RTS message with its own MAC address and the address of the receiver. If it is clear to send, the receiver device will respond with a CTS message containing the device's address. Once the device receives the message with its address, it will transmit data. If a device receives a CTS message with a MAC address different from its own MAC address, it has not been allowed to transmit and will have to wait.

2.5 4G/5G

The 3rd Generation Partnership Project (3GPP) is responsible for the development of both the fourth and the fifth-generation mobile network, and the two mobile network generations are similar in their overall structure. Figure 2.3 represents the main parts of the fourth and fifth-generation mobile networks. The User Equipment (UE) is similar for both generations and represents all devices that can connect to the network through a SIM card. The access network is the bridge between the UE and the core network and is responsible for transporting data between the UE and the core network and vice versa. The access network, named Evolved Universal Terrestrial Radio Access Network (E-UTRAN) in 4G and 5G Radio Access Network (NG-RAN) in 5G, consists mainly of base stations. The core network is responsible for many functions, including authenticating and authorizing users, connecting the users to outside networks, routing calls, and billing the customer. Hence the core consists of many different entities with different interfaces and responsibilities. The list below summarizes the most important entities in the context of this thesis.

4G [3GPe]:

- Mobility Management Entity (MME) is responsible for tracking the UE within the network and providing access to authentication of the UE.
- Home Subscriber Server (HSS) contains subscriber information of the user in the network and is located in the subscriber's home network.

5G [3GPi]:

- Access and Mobility Management Function (AMF) is located between the administrative core functions and the UE and is responsible for, amongst others, access to authentication and authorization functions.
- Authentication Server Function (AUSF) is responsible for authentication of both 3GPP and non-3GPP access.
- Unified Data Management (UDM) manages the subscriber identification material and generates the authentication material.

The 4th generation mobile network was first deployed in Oslo, Norway in 2009 [Val] and had in 2020 grown to have a population coverage of 99,9% in Norway [Tel]. The 4G network brought an all-IP service to the mobile network, which improved the broadband capacity and increased the number of technologies that mobile devices

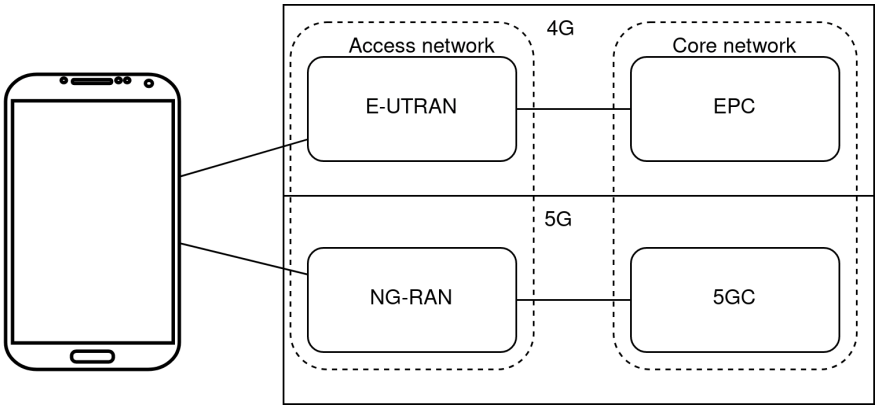


Figure 2.3: Overall 4G and 5G network structure.

could use. In addition, it improved the security of its predecessors by using temporary identifiers and further abstractions of the identifiers to reduce the window where a device used the same identification. Secure signaling between the UE and the MME in Evolved Packet Core (EPC) is also a feature of 4G and the Extensible Authentication Protocol Authentication and Key Agreement (EAP-AKA) protocol provides secure inter-working between the 3GPP and non-3GPP networks [SNMB10]. Even though 4G introduces new security features, many attacks are still possible [HCMB18], including IMSI catchers attacks that are provided by Christian Sørseth in [Sør17] and by Mjølsnes et al. in [MO17].

The fifth-generation mobile network is the technology that aims at improving the broadband speed in mobile networks and improves its predecessor 4G in many areas. The 5G is currently being rolled out in many countries worldwide as the newest mobile network. The main improvements from 4G are the increased throughput and reduced delay. This comes from improving previously used technologies like NFV and Software-Defined Networking (SDN) in the core and taking advantage of new technologies like millimeter Wave (mmW) frequencies in the access network [Qua; BKP17]. The newest generation mobile network is expected to give opportunities for new use cases in the mobile network like IoT, smart city, and gaming services. The 5G also aims at improving the security by, amongst others, minimizing IMSI catcher attacks. However, other attacks to identify user location also apply, such as the TRacking via Paging mEssage DistributiOn (ToRPEDO) attack [HEC+; NND16].

2.5.1 5G standalone (SA) vs. non-standalone (NSA)

The 5G is currently under deployment in many countries in the world. However, due to the expenses related to deploying a large-scale 5G network, the 3GPP has created five network architectures for 5G, which describes inter-working with 4G. These

five architectures fall into two categories, StandAlone (SA) New Radio (NR) and Non-StandAlone (NSA) NR. Standalone NR refers to an architecture where the 5G System (5GS) consists of NR and the 5G Core Network (5GC) with NR as the control plane anchor, while in non-standalone Long Term Evolution (LTE)/evolved LTE will be the control plane for NR [LHC+20]. The two most supported architectures are option 2 for SA and option 3 for NSA as described in [3GPg]. For these two types, a more clear separation is made. Both the options will use NR as the access network. However, the SA version will use the 5GC as the core while NSA will use EPC as the core network. First, deploying a NSA 5G network and then evolving it to be a SA network seems like the most natural development due to dividing the cost of 5G deployment over time. However, this will also increase the time it takes to have a complete 5G SA network. It is also important to note that, with the use of 5G NSA, the technology improvements and changes in the core are not taken advantage of. This includes the security techniques to protect against IMSI catchers, and hence, 5G NSA does not provide any protection against IMSI catchers.

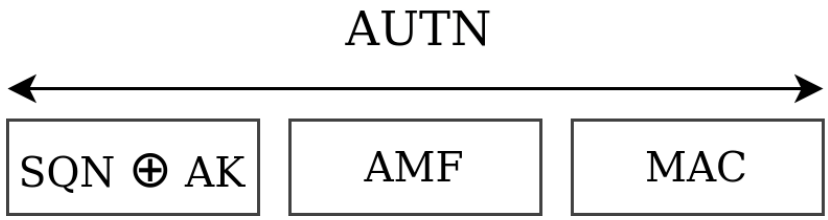
2.5.2 Authentication and connection establishment

In the following, the authentication procedure during connection establishment will be described for both 4G and 5G [3GPc]. Universal Subscriber Identity Modules (USIMs) for both 4G and 5G use the AUTN to ensure freshness of the authentication request and to protect against replay attacks. The structure of the AUTN can be seen in Figure 2.4. It consists of a SQN, a Authentication and key Management Field (AMF) and a message authentication code (MAC). The SQN is XORed with a Anonymity Key (AK) computed from a Random Challenge (RAND) and the permanent key stored in the USIM and is used to protect the SQN in transmission. The AMF can be used to specify the key and algorithm used to generate the AUTN and the MAC is used to authenticate the AUTN. In order for the UE to verify the freshness of the authentication request it will first generate the AK from the same RAND and XOR it with the protected SQN to reproduce the SQN. The UE will verify that the SQN is within a given range before it will compute a hash value from the permanent key at the USIM, the SQN, AMF and RAND. If the computed hash equals the MAC in the AUTN and the SQN is within a given range, the UE can assume the AUTN to be fresh.

4G EPS-AKA

The 4G defines the Extensible Authentication Protocol Authentication and Key Agreement (EPS-AKA) [3GPd] procedure to authenticate a UE as well as to establish the keying material for privacy protection. The EPS-AKA procedure is part of the

Figure 2.4: AUthentication TokeN (AUTN) structure.

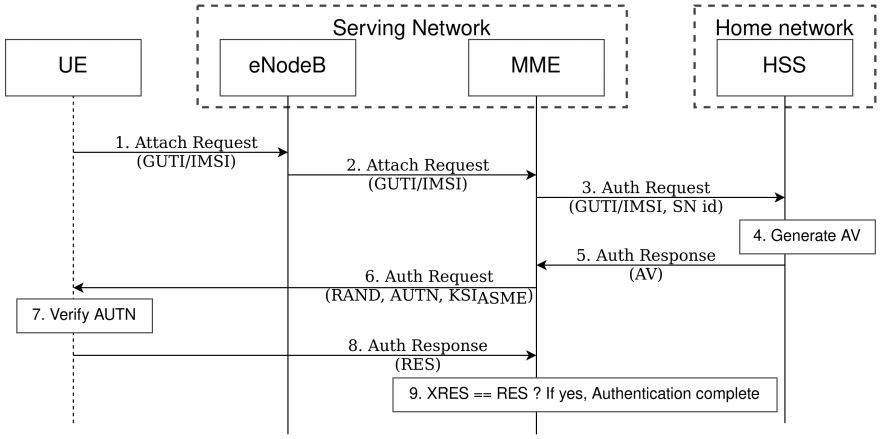


attach procedure[1] and is an important part of the security in 4G. Figure 2.5 shows the EPS-AKA procedure which is is initiated by the UE sending an attach request (1) to the access network with its identity. The identity will then be passed on to the MME (2) and further to the HSS in the home network of the UE with the Serving Network Identifier (SN ID) (3). If the home network can identify the UE based on the identifiers it will generate an Authentication Vector (AV) (4). In 4G EPS-AKA the AV consists of a RAND, a AUTN, an eXpected RESponse (XRES) and the key: K_{ASME}. The AV will then be sent to the MME (5). The AUTN and RAND is then forwarded to the UE (6) along with the KSI_{ASME} which the UE will use to identify the K_{ASME}. The UE will then verify the freshness of the authentication request (7), as described in 2.5.2. If the AUTN is verified, the UE will produce a RESponse (RES) from the AUTN as well as keying material. The result value will be transmitted back to the MME (8) so that it can verify that the XRES from the HSS through the AV and RES from UE are the same. If the two values are equal (9), then the authentication is successful and UE has authenticated the serving network and vice versa. After the authentication, both parties will have the similar keying material and hence can set up secure communication. First Non-Access-Stratum (NAS) security is set up between the MME and the UE to protect NAS messages. Then Radio Resource Control (RRC) security is set up between the UE and the evolved-NodeB (eNB) to protect RRC messages.

The 4G EPS-AKA procedure has two main weaknesses. First, the home network of the UE is not part of the authentication decision. It only produces the key and authentication material, and then the serving network decides if the authentication is valid. Second, the IMSI value might be sent over the air unencrypted. Even though a temporary identifier might be used instead of the permanent one if available. A simple identity request message by the core will reveal the IMSI, and the use of IMSI in UE identification lays the foundation for IMSI catchers attacks. Therefore, other choices for authentication are available in 5G.

[1] Attach procedure is the procedure in which a device attaches to a network by establishes a connection with the core network.

Figure 2.5: 4G EPS-AKA procedure.



5G-AKA

5G provides three choices for authentication of a user, which are 5G Authentication and Key Agreement (5G-AKA), Improved Extensible Authentication Protocol Authentication and Key Agreement (EAP-AKA') and Extensible Authentication Protocol Transport Layer Security (EAP-TLS). The 5G-AKA [3GPh] is a new authentication method not based on Extensible Authentication Protocol (EAP) and will be described in detail here. The EAP-AKA' is similar to the 5G-AKA; however, the serving network does not authenticate the user and hence has to trust the home network's decision. EAP-TLS trust model is different from the two other options since it is based on public keys instead of symmetric keys. EAP-TLS is defined for IoT environments, and private networks and hence is not described in this section.

The 5G-AKA procedure is an improvement over the 4G EPS-AKA since it removes the two of the vulnerabilities. The procedure can be seen in Figure 2.7 and is described in the following.

1. The UE transmits its identity to the SEcurity Anchor Function (SEAF) which is part of the AMF [3GPh] in the access network.

2. The attach request will be forwarded to the AUSFin the home network of the UE along with the SN ID of the SEAF.

3. After verifying the serving network, the AUSF will further pass the request to the UDM.

4. If the UDM receives a SUCI value, it will use the Subscription Identifier Deconcealing Function (SIDF) to obtain the Subscription Permanent Identifier (SUPI) value from the SUCI.
5. Based on the SUPI value, an authentication method is selected.
6. The 5G HE AV is generated.
7. The UDM transmits the 5G HE AV to the AUSF. Additionally, if a SUCI value was received, it will also transfer the SUPI.
8. The AUSF will then calculate the Hash eXpected RESponse (HXRES) from the XRES in the 5G HE AV and temporary store the key K_{AUSF}.
9. 5G SE AV is transmitted to the SEAF in the serving network.
10. AUTN and RAND will be transmitted to the USIM.
11. The USIM verifies the AUTN in the same way as for 4G. If the verification fails, an error message will be transmitted.
12. If the verification is successful, the USIM will generate a RES and send it to the serving network.
13. The serving network validates the RES by hashing it and comparing the result with the HXRES.
14. Then the RES will be sent to the AUSF in the home network of the UE.
15. Now, the home network verifies the RES and, if successful, approves the authentication.
16. If it is approved, AUSF will generate a new key, K_{SEAF}, and send it to the SEAF. If the original request was made with SUCI, the response will also contain the SUCI of the user.
17. The UDM in the home network will be notified that the authentication was successful. To, for example, log the instance.

The 5G-AKA fixes the two vulnerabilities compared to the 4G EPS-AKA by leaving the final authentication decision up to the home network of the UE and by never transmitting the SUPI on the air interface.

Figure 2.6: 5G Home Environment Authentication Vector (5G HE AV) and 5G Serving Environment Authentication Vector (5G SE AV) structure.

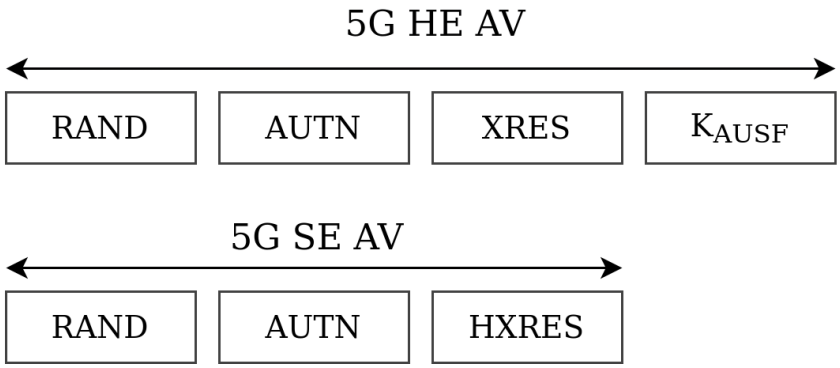
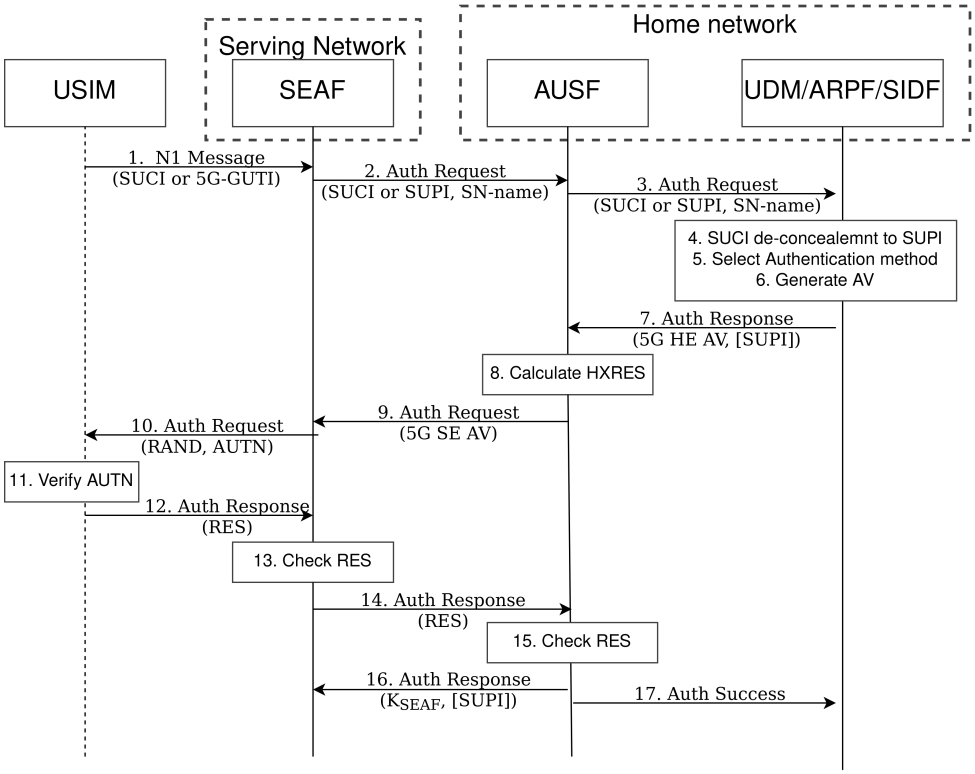


Figure 2.7: 5G Authentication and Key Agreement (5G-AKA) procedure.



Chapter 3
Privacy-Sensitive Identifiers

The wireless communication technologies discussed in this thesis use unique identifiers to identify the network and the device. Some are permanently used, and others are temporary and chosen at random. Additionally, some identifiers are not necessarily unique but can be used for identification or reduce the number of possible identities. This chapter presents the relevant privacy-sensitive identifiers for WiFi, 4G, and 5G.

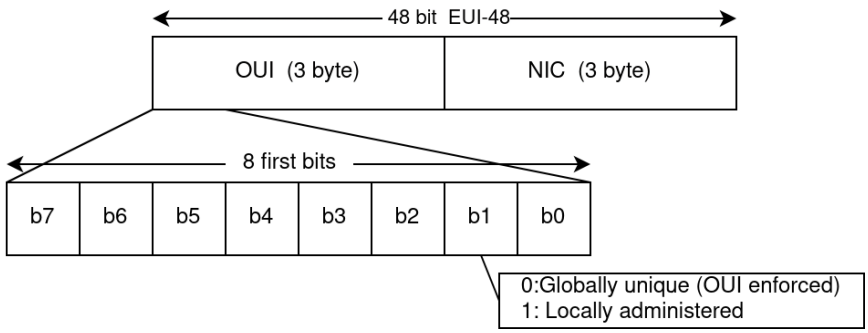
3.1 WiFi

In this section we present and describe privacy-sensitive identifiers in WiFi and their use cases. Exposing the identifiers may compromise privacy aspects of PPDR personnel. All the identifiers and information is from the WiFi standard [IEE21].

3.1.1 MAC

The Medium Access Control (MAC) address is a unique identifier assigned to every network interface. Hence, every device that supports WiFi has a MAC address. The address is 48 bits, and its structure is defined by ISE/IEC 10039 [ISO91] and can be seen in Figure 3.1 [IEE]. The first part is the OUI which identifies the manufacturer that distributes the address. The second part is the Network Interface Controller (NIC), which is unique within that organization. Networks can use the MAC address to block access to unauthorized or stolen devices. In WiFi, it is used to determine if a packet is meant for the device or not. The address can either be globally or locally administered (the bit is marked in Figure 3.1). If it is globally administered, it is globally unique, and the OUI value belongs to a manufacturing company. However, no such guarantee is given for locally administered, and it could indicate a random MAC address.

Figure 3.1: EUI-48 MAC address.



3.1.2 SSID

The Service Set IDentifier (SSID) is not an identifier on the UE but rather the name that identifies the network AP. The operator of the AP determines its SSID and hence, is not a unique identifier. However, since an unlimited number of names exist in a limited geographical area, it is a low chance that two different networks have the same SSID. A WiFi-enabled device uses the SSID to determine which network it wants to connect to. The SSID and the security context of the AP determine if the device recognizes the network and whether it will connect to it. AP's usually advertise their presence through a beacon frame. The beacon frame will contain the SSID of the network.

3.1.3 BSSID

The Basic Services Set IDentifier (BSSID) is, in the same way as the SSID, an identifier of the network AP. In contrast to the SSID, it is the layer 2 MAC address of the network card on the AP and is used to identify the network card of the router. Therefore, two routers with the same SSID will have different BSSID values. Hence, the BSSID addresses the packet to that AP and distinguishes two network AP with the same SSID.

3.1.4 WPS UUID

The WiFi Protected Setup UUID (WPS UUID) is the information inside the optional WiFi Protected Setup (WPS) IE, and it is used to establish a WPS connection. The Universally Unique IDentifier (UUID) is a 16-byte long identifier. However, the generation of it is not specified. Nevertheless, it is recommended to use the RFC 4122 specification with a MAC address from one of the device's network cards [Wi-20]. Since it is an identifier for WPS, and not all devices use WPS, not all devices have this identifier.

3.2 4G and 5G

In 4G and 5G many identifiers exist that can uniquely or partially identify a device. Many of these identifiers are equal for 4G and 5G, some are new in 5G and some are used differently. This section will describe the identifiers for 4G and 5G and how they are used. The identifiers are retrieved from various 4G and 5G standards.

3.2.1 IMSI

Each mobile device in a 2G/3G/4G system needs a unique International Mobile Subscriber Identity (IMSI) [3GPe]. Similarly, 5G devices that want to connect to the public network will also need an IMSI [3GPf]. The IMSI consists of three parts and is no longer than 15 digits. The first part is the three-digit Mobile Country Code (MCC) which identifies the country of the mobile subscription. The second is Mobile Network Code (MNC), which identifies the subscriber's Public Land Mobile Network (PLMN) within the MCC in public networks. The MNC is 2 or 3 digits depending on the value of MCC. The third and last part of the IMSI is the Mobile Subscriber Identification Number (MSIN) which identifies the subscriber within the PLMN in public networks. The IMSI is stored in the subscriber's home network (HSS for 4G and UDM for 5G) and USIM. In 4G networks, the UE will send the IMSI in the clear to the serving network (eNB) when no valid temporary identifier is available at the UE. The IMSI will also be sent if the UE is accessing a new PLMN and is configured to perform attach with IMSI at PLMN change. Additionally, when the serving network cannot identify the subscriber based on the temporary identity. It will send an identity request to the UE, which will respond with its IMSI. In 5G, however, additional protection has been added, and the IMSI will never be transmitted; instead, a concealed version will be transmitted, which is described later.

3.2.2 NAI

Network Slice Instance IDentifier (NSI-ID) [3GPi] is a unique identifier of a UE which is based on the Network Access Identifier (NAI) format as defined in IETF RFC 7542 [IET]. It consists of a username and a realm. The realm part is used for routing when the UE is roaming, and the username uniquely identifies the UE within the realm. Both the username and the realm are variable-length strings. The identifier is used for private networks [1].

[1] A private 5G network is a non-public network that aims at supporting services that are not supported in other systems.

3.2.3 SUPI

The Subscription Permanent Identifier (SUPI) [3GPi] is the globally unique identifier in the 5GS, and every subscriber in the 5GS shall be allocated a SUPI. The SUPI is stored at the USIM of the subscriber and in the UDM of the home network, and it can take different forms. For a user device, the two most important are an IMSI, as presented in 3.2.1, and an NAI described in 3.2.2. In order to provide subscriber confidentiality in 5G, when a UE needs to transmit the SUPI to the network to be identified, it will do so in a concealed form. Therefore, all 3GPP UE allocated SUPIs should be based on the IMSI to provide interworking with the 4G.

3.2.4 SUCI

The concealed SUPI is called Subscription Concealed Identifier (SUCI) [3GPh] and is a privacy-preserving identity. The structure of SUCI can be seen in Figure 3.2. It contains, amongst others, the identifier of the home network, the protection scheme identifier, the home network public key identifier, and the scheme output. The home network identifier is used for routing purposes and is the MCC and MNC for IMSI SUPI and the realm for NAI SUPI. The protection scheme identifier identifies the protection scheme, and the home network key identifier identifies what key is used with the protection scheme to produce the scheme output. The scheme output is what will be used to de-conceal the SUCI. It consists of the public key of the UE, the cipher text, and a MAC. The standard provides three options for the protection scheme, one null scheme and two Elliptic Curve Integrated Encryption Scheme (ECIES). Additionally, the home operator can define their own schemes.

The output of the null scheme will be the same as the input, and hence once it is used, the SUPI will be transmitted in the clear, and the SUCI will then provide no privacy protection. The null scheme will only be used in three cases. First, if the UE makes an unauthenticated emergency session and no temporary identifier is available. Second, if the home network is configured to use the null scheme, and third if the home network key is not provided to the USIM when generating the SUCI.

As stated earlier, the SUPI is never transmitted from the USIM (or device) in 5G. Instead, the SUCI is used to identify the device. It is only transmitted if the temporary identifier (5G-Globally Unique Temporary UE Identity (GUTI), described in Section 3.2.6) is unavailable at the USIM or the network can not identify the subscriber based on it.

3.2.5 TMSI

The Temporary Mobile Subscription Identifier (TMSI) [3GPf] is an identity issued to provide confidentiality to the subscriber. It is a 32-bit long value and only a

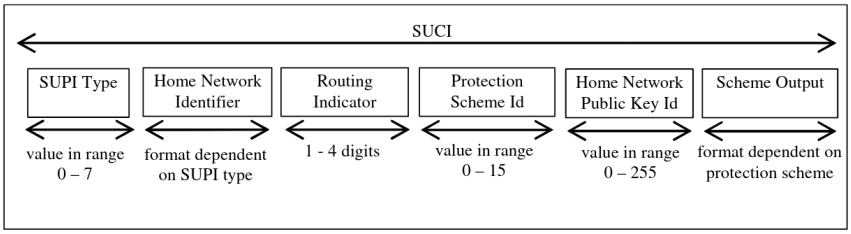


Figure 3.2: SUCI structure.

temporary identity. The TMSI only has local significance to the entity that issued the temporary identity. For 4G, the MME is responsible for assigning a TMSI to the subscriber. For 5G, the temporary identifier is denoted 5G-TMSI and is distributed and maintained by the AMF. In this thesis, TMSI will refer to both 5G-TMSI and TMSI. Due to the local significance of the TMSI, only the MME or the AMF, depending on 4G or 5G, can map them back to the subscriber's permanent identity. The temporary-permanent identity mapping shall only be known to the subscriber and issuing entity. The temporary identity will only be transmitted to the subscriber when a security context is established, and the transmitted data is encrypted.

The TMSI is used when a device wants to connect to the network, and the value is available. As a result, it will reduce the use of permanent identifiers (IMSI/SUPI), which improves the user's privacy. Moreover, it can reduce the connection time to a network by faster identification.

3.2.6 GUTI

Due to the local significance of the TMSI, if the subscriber changes its location and connects to a new MME or AMF, the TMSI value would no longer identify the device and a new authentication procedure with the core have to be conducted. Therefore Globally Unique Temporary UE Identity (GUTI) [3GPf] is provided to the subscriber to support identity confidentiality to the subscriber outside the serving network of the MME or AMF. The GUTI is available in both 4G and 5G (named 5G-GUTI for 5G) and is composed of two parts. The first part is the routing information of the entity that issued the TMSI and can map it to the permanent identity. For 4G, this is called GUMMEI, and for 5G, it is called GUAMI. The routing information consists of a MCC and MNC that routes to the correct PLMN, as well as the identifier of the entity (MME or AMF) that issued the TMSI within the PLMN. The structure of GUMMEI and GUAMI can be seen in Figure 3.3. The second part is the TMSI of the subscriber.

In order to have more efficient radio signaling (e.g., paging), a shorthand version of the GUTI is provided for both 4G and 5G. For 4G, it is called Serving Temporary

<GUMMEI> = <MCC><MNC><MME Identifier>
<GUAMI> = <MCC><MNC><AMF Identifier>

Figure 3.3: Globally Unique Mobility Management Entity Identifier (GUMMEI) and Globally Unique AMF Identifier (GUAMI) structure.

Mobile Subscription Identifier (S-TMSI), and for 5G, it is called 5G-S-TMSI. They both still contain the TMSI for the subscriber but reduce the part that identifies the issuing entity. More specifically, the MCC and MNC that identifies the PLMN are no longer part of the GUTI. For 5G, the truncated 5G-S-TMSI further reduces the length of the 5G-S-TMSI but can still uniquely identify the subscriber within the AMF. The truncated 5G-S-TMSI is used in RRC connection re-establishment for Narrow Band IoT (NB-IoT) devices.

3.2.7 IMEI and IMEISV

The International Mobile station Equipment Identity (IMEI) or the International Mobile station Equipment Identity and Software Version number (IMEISV) can both uniquely identify the mobile station equipment. The two most important parts of the IMEI are the eight-digit Type Allocation Code (TAC) and the six-digit serial number. The TAC is distributed by the GSM Association [GSM], and the serial number is allocated by the manufacturer (in sequential order). It will uniquely identify the device within the TAC. The IMEISV also have the TAC and serial number. However, it has a two-digit Software Version Number (SVN) that identifies the software version on the mobile device that the manufacturer allocates. For a device, the TAC and serial number in IMEI and IMEISV is identical [3GPf]. During the attach procedure, the identity of the mobile entity shall be retrieved by the serving network from the UE in an encrypted way (unless it is an emergency connection and no IMSI is available) [3GPe]. The serving network can then verify with Equipment Identity Register (EIR) if the device should be allowed to access the network or not (i.e., if it is blacklisted or not) and continue the connection establishment with the UE. Hence, the purpose of the IMEI is to identify the mobile equipment for tracing and blacklisting when necessary (e.g., a stolen device).

3.2.8 PEI

In the 5GS, it is the Permanent Equipment Identifier (PEI) [3GPh] that identifies the mobile device. The PEI consists of a type and a value which can be on IMEI, IMEISV, MAC address, or Extended Unique Identifier-64 (EUI-64) format. However, for a device supporting any 3GPP access technology, the PEI must be allocated in the IMEI or IMEISV format and hence is the same as the IMEI or IMEISV for previous 3GPP systems such as 4G. The AMF can optionally request the PEI of

a UE when establishing a security context with a security mode command. The reply will be ciphered, integrity protected, and contain the PEI if it was requested. The PEI shall only be transmitted after establishing a security context except for emergency registrations.

3.2.9 MSISDN

One or more Moblie Station International Subscriber Directory Number (MSISDN) [3GPf] values should be allocated to the mobile device to use for all calls to that device. The MSISDNs is also known as the phone number of a device and comes from the E.164 numbering plan [ITU]. The MSISDN consists of a country code and a national significance number and needs to be globally unique. The number is used to route the call to the subscriber's home network, which is aware of the subscriber's location and can route the call to the subscriber.

3.2.10 RNTI

Radio Network Temporary Identifier (RNTI) [3GPa] values are assigned as an identity to a connected user in a cell. In 4G eight different RNTI values are used (Paging RNTI (P-RNTI), System Information RNTI (SI-RNTI), Random Access RNTI (RA-RNTI), Temporary Cell RNTI (TC-RNTI), Cell RNTI (C-RNTI), Semi-Persistent Scheduling Cell RNTI (SPS-C-RNTI), Transmit Power Control-PUSCH RNTI (TPC-PUSCH-RNTI), Transmit Power Control-PUCCH RNTI (TPC-PUCCH-RNTI)). In 5G, it is 13 (P-RNTI, SI-RNTI, RA-RNTI, TC-RNTI, C-RNTI, Modulation Coding Scheme Cell RNTI (MCS-C-RNTI), Configured Scheduling RNTI (CS-RNTI), TPC-PUSCH-RNTI, TPC-PUCCH-RNTI, Transmit Power Control-Sounding Reference Signal-RNTI (TPC-SRS-RNTI), Interruption RNTI (INT-RNTI), Slot Format Indication RNTI (SFI-RNTI), Semi-Persistent Channel State Information RNTI (SP-CSI-RNTI)). The most critical value for location exposure is the C-RNTI. It is used to identify RRC connection and scheduling for the UE and UE uplink transmissions.

3.2.11 GPSI

The Generic Public Subscription Identifier (GPSI) [3GPf] identifies 3GPP subscriptions in data networks outside of the 3GPP system. The association between the GPSI and the SUPI is stored in the 3GPP system, and hence, the GPSI can be used both inside and outside the 3GPP system. The GPSI number can be either an MSISDN or an external identifier, and the MSISDN value may supported both in 5GS and in 4G network systems.

Chapter 4
Vulnerabilities and Mitigation Techniques

The following chapter presents vulnerabilities and mitigation techniques for WiFi, 4G, and 5G. The vulnerabilities will be classified as either an implementation vulnerability or a standard vulnerability. The standard vulnerability classification means that the vulnerability is in the technology's standard protocol or design architecture. Hence, all commercial devices with 4G, 5G, or WiFi are vulnerable. An implementation vulnerability is a vulnerability present in either the software or hardware of the device that follows the standard.

4.1 WiFi

This section will present the vulnerabilities in WiFi found in the literature study. Since it is an old standard, some of the known vulnerabilities have efficient mitigation techniques that are widely adopted. However, this section will mention them since they are still valid vulnerabilities concerning the WiFi standard. Table 4.1 presents a summary of the identified vulnerabilities.

4.1.1 Attacker model

For WiFi, we consider two different attacker models for exploiting the vulnerabilities. The passive attacker can passively monitor the air interface to capture radio layer information within the proximity of its monitoring device. The passive attacker does not interrupt any traffic and hence, goes unnoticed. In addition to the passive attackers' capabilities, the active attacker is capable of fabricating and transmitting packets to trigger a response from the target. Both models use off-the-shelf hardware (network card) and software (such as Wireshark [Wir] and TCPDump [The]), resulting in a low-cost hardware and software setup. The two models are represented in Table 4.1 as *Passive* and *Active* under the *Attacker model*.

The attacker's primary goal is to determine that a particular signal from the set of all signals belongs to a target individual or an individual from a group of targets

(a group can, for instance, be all PPDR personnel). In other words, the attacker attempts to break the anonymity or group anonymity of a target. The attacker's second goal is to break the unlinkability of two signals and determine if their origin is the same device. This might reduce the anonymity set or correlate previously detected signals to a target.

Extending the attacker models can be done by using multiple passive and active devices to generate and obtain signals in different locations to retrieve more location-exposing data. However, the attacker needs to be local and have hardware installed in the range of the target device. We also assume that only the information transmitted on the radio interface is available to the attacker and that no encryption keying material is available.

4.1.2 Vulnerabilities

V-1 SSID of previous network
WiFi devices store information (SSID and security features) on which networks it has been attached previously to connect to the network automatically the next time. The devices send probe requests when they want to detect APs in their proximity. Since these requests can contain the SSID of previously connected networks, an adversary can listen to the probe request to detect the previously connected networks of the device [DPČ19]. Furthermore, tools like Wigle [Wig] can identify the physical geographical location of the network through its SSID and hence, can reveal a device's previous whereabouts. The authors in [CKB12; VMC+16] suggests that knowledge of previously connected network SSIDs is enough to identify and track a device over time.

However, the SSID field is not required, and when not set, all APs in the proximity will respond to the probe request with their SSID. Since this is an option in WiFi standard, it can be seen as an implementation vulnerability. However, hidden WiFi APs never announce their presence as regular WiFi APs do. Hence, the probe request needs to contain the SSID of the network. Therefore, if the PPDR services deploy hidden networks, the adversary can assume any device sending a probe request with the SSID of the PPDR WiFi network to be part of the PPDR service.

V-2 Information Element (IE)
The 802.11 standard defines optional IEs in the probe request. The IEs inform the network of various functionalities such as throughput and supported rates. Since they are not mandatory, which fields a device includes and their length depends on the capabilities and configurations of the device. Additionally, the order of the elements can provide more information since they are, contrary to the 802.11 standard recommendation, not always sorted in ascending order [VMC+16]. An analysis of the different IEs is done in [VMC+16] and shows how a device can be fingerprinted based

on the different IEs used. The authors in [UCF+20] also show that this can track a device over time since the fingerprints do not change frequently. In non-crowded areas, the technique can have an accuracy of up to 91.3%. However, it is necessary to conduct experiments on the vulnerability in crowded areas to determine its effect on large-scale tracking.

V-3 Probing frequency
Devices emit probe requests when they wish to identify nearby networks. Research in [WK16] proposes to look at the transmission frequency of probe requests to classify the device type and model. They discover that specific devices can be identified based on their transmission frequency. However, in a high traffic scenario, the probes need to be transmitted with the same MAC address in order for the adversary to relate them. They also discovered that most devices use some degree of randomness in the probing frequency and hence can not be fingerprinted with this technique. This vulnerability will be classified as an implementation vulnerability since the probing frequency is not standardized.

V-4 Interframe transmission time
A WiFi device might send out probe requests in bursts when trying to connect to a network. The authors in [MCRV16; Fre15] propose to use the time between the arrival of probe requests in a burst to map distinct bursts over time to each other. The inter-frame burst arrival time is based on the driver of the device and the number of known networks and is similar over time for one device [MCRV16]. The results from the research are that identifying devices with the inter-frame arrival time can have an accuracy of 77%, and two bursts could be traced back to the same device even when 50 days had passed between the two bursts in a lab setting. However, a test to see if this technique could correctly classify the burst in real-time gave a true positive rate of 0. Hence, the attack is not applicable for real-time tracking, where only a small timeframe of information is available. Nevertheless, it provides good results for analysis after data collection (i.e., offline algorithm). The attack also requires that the device's MAC is the same for all frames in the burst.

V-5 Sequence numbers
Each 802.11 packet transmitted contains an increasing SQN to provide replay protection and for devices to identify packets that are detected multiple times. The researchers in [Fre15] suggest using the SQN to map sequential probe requests from the same devices using MAC address randomization. However, this requires that the devices use and increase the same SQN value even when generating a new MAC address. Since the SQN should be associated with the MAC address, when a new random MAC is generated, a new random SQN should also be generated. Therefore, we classify this as an implementation vulnerability. However, with the technique, the researchers could link probe requests with randomized MAC addresses to the same

device. This vulnerability can also be combined with V-2 and V-3 to distinguish devices in crowded areas better.

V-6 WiFi Protected Setup (WPS)
WiFi protected setup is an optional IE in the probe request and indicates the device's support for the protocol. The IE contains the WPS UUID which is meant to identify the device. The authors in [VMC+16] perform an analysis of the generation of the UUID for some devices and provide two vulnerabilities taking advantage of how the identifier is generated.

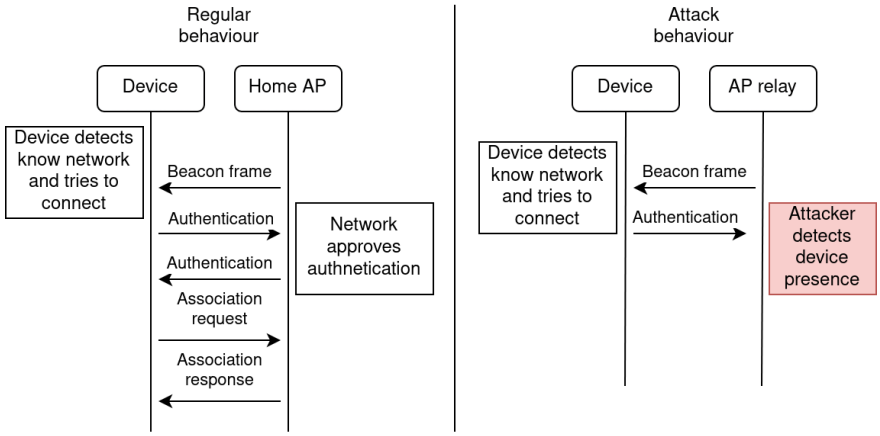
(1) The UUID value is generated from a MAC address and has a larger value space than the MAC address. Therefore, the UUID will also be unique and can be used to track the device. However, the analysis also showed that only 5.5% of the devices used the WPS IE, and hence, most devices could not be tracked this way. Newer research from 2017 in Jeremy et al. [MMD+17] shows that around 30% of Android devices had the WPS IE.

(2) The recommendation for the UUID generation is that the device uses the MAC addresses from one of its network cards. By generating all possible UUIDs from the set of possible MAC addresses of a device, an adversary can reverse the UUID to the MAC address. Therefore, by detecting a probe request with the WPS IE, an adversary can determine the MAC of the target. Jeremy et al. [MMD+17] experimented on reproducing the MAC address from the WPS UUID value. Their experiment was done with the ground truth[1] and gave a 100% success rate.

V-7 Unprotected AP broadcasting
If a device detects a beacon frame with an SSID and a security context it recognizes, it will respond with a MAC address and attempt to establish a connection. Cunche et al. [Cun14] presents a vulnerability in which the adversary impersonates a known network of the target device through a WiFi AP-relay. The relay replays beacons from the legitimate AP to impersonate it. To which devices will respond by attempting to authenticate with the network using a MAC address. If the adversary detects an authentication attempt to the network, it knows that someone in the proximity has previously been connected to the impersonated network. Additionally, the adversary can track the device over time if the device uses a persistent MAC address in the authentication. A random MAC address is associated with a network the first time the device connects to the network for Android (version 10 and higher) and iOS (version 14 and higher) [IET22]. However, the same random address is used persistently. To break the user's anonymity, the adversary would need to know the address associated with that network to identify the user behind the device.

[1]Research with the ground truth, can verify the results against the true values to determine its effect.

Figure 4.1: AP relay attack



Additionally, for iOS devices, the MAC address is associated with the BSSID, so the adversary would also have to spoof the MAC address of the AP [IET22]. The flow of the attack compared to normal behavior can be seen in Figure 4.1.

V-8 RTS/CTS

The purpose of Request To Send (RTS)/Clear To Send (CTS) messages in WiFi is to avoid collisions of transmission of packets from two different devices. The authors in [MMD+17] present a vulnerability in which a device will respond to an RTS message if it detects its own MAC address as the receiver address. An adversary can take advantage of this by sending RTS messages with the target MAC address as the receiver and a random address as the transmitter address. If it detects a CTS with the same random address, the adversary can assume the device is in proximity. The results from [MMD+17] shows that all device tested were vulnerable to this attack, which includes up to iOS version 10.1 and android 7.1. However, as the devices needs to detect its own MAC address, this technique can not be used for large scale tracking as it requires looking for many MAC addresses.

V-9 MAC address in clear

The MAC address uniquely identifies a device and hence, many device choose to use a random value. However, in different scenarios the MAC address can be sent in the clear. Three of them are presented here.

(1) The WiFi probe request contains a MAC address field, which means an adversary listening can obtain the MAC addresses. If a device uses its actual MAC address, it is simple to track it over time. Hence, it could be the basis for a large-scale tracking system (as in Probr [SMS+16]). However, it has become more and more common to use a randomized MAC address, as shown in [DPČ19] with a decrease

from 29.2 probe requests per MAC address in 2015 to only 2.6 in 2018. Even though randomization is common, it is not guaranteed since the 802.11 standard allows it, and poor implementation could result in a vulnerability for some devices.

(2) The authors in [VMC+16] presents another implementation vulnerability where the device would, after detecting a hotspot 2.0 advertisement, query more information from the hotspot and reveal its actual MAC address. This vulnerability could be used in the same way as the AP relay in V-7 to detect user presence. However, as of 2016, only 16% of devices would respond to a hotspot advertisement.

(3) When a device has established a connection with a network, it will use its MAC address to receive packets meant for it. Whether the MAC is unique, random, or random for that network depends on the implementation of the device, but it affects the information retrieved by the adversary. The attacker can track which devices are connected to a network in the proximity by passively listening. The adversary either needs to know the MAC address of the target devices or the MAC address of the AP since the communication goes both ways.

V-10 Improper usage of randomized MAC
The MAC address randomization protects the privacy of the user. However, if it is not updated often enough, an adversary can still track a device over a smaller period. The authors in [MCRV16] analyze different MAC address randomization implementations. They conclude that Windows and Linux device does not update their addresses during network discovery and some iOS devices had limited use of the randomization. However, the analysis done is from 2016 and hence, does not concern with newer operating systems and devices.

4.1.3 Detection area

The vulnerabilities described above are all limited to detecting devices within the range of the listening device, which is small for WiFi. However, multiple listening devices can detect targets in a larger area. The authors in [PCB+17] propose a solution for how this can be done by combining results from different listening devices at a central server. By having multiple detection devices, tracking is not just limited to detecting a user's presence. An adversary can also determine a target's movements based on detections at multiple tracking locations.

4.1.4 Mitigation techniques

The mitigation techniques presented can completely or partially mitigate one or more of the presented vulnerabilities. They can be seen as a set of guidelines on how to implement NGN in context of device privacy.

M-1 Implementation vulnerabilities
Verifying that the devices in use do not have any implementation vulnerabilities an adversary can take advantage of is important to protect the privacy of the devices. Testing the devices in an isolated room by listening to the traffic it transmits can reveal different vulnerabilities. The most important vulnerabilities to test are MAC and SSID in probe requests since they are the simplest to take advantage of. For iOS (version >= 14) and Android (version >= 10) MAC address randomization is used for scanning and a random addresses is used per network [IET22]. Testing V-1, V-2, V-5, V-9 (1), and V-10 is also important. For V-9 (1), android devices have a developer option to use a random MAC for every connection which should be turned on. Additionally, Apple devices mitigate V-5 by producing a new random SQN every time the MAC is switched [App21b].

M-2 Visible network
If NGN takes advantage of the WiFi technology, they can deploy their APs as either visible or hidden networks. The main difference between the options is that visible networks transmit the SSID in every beacon frame from the AP. While for hidden networks, the AP will never transmit or advertise its presence. Hence, a device wanting to connect to a hidden network needs to send probe requests with the target AP's SSID. Even though the AP never transmits the SSID, it is simple to obtain by listening to a successful connection establishment between the AP and the device. Hence, an adversary can obtain the SSID regardless of whether it is hidden or visible. For example, suppose only the PPDR service has access to the NGN WiFi APs and that they are hidden. In that case, an adversary can take advantage of vulnerability V-1 to detect the presence of NGN devices (PPDR personnel). Therefore, it's recommended to implement visible networks for better privacy.

M-3 Turn off WiFi
Most phones have WiFi turned on most of the time, and hence, the device will send out many probes to see if it can connect to a nearby APs. On the other hand, when WiFi is turned off, the device will not send probe requests or connect to networks. Therefore, regarding location privacy, it is optimal only to have WiFi turned on when the device is in a physical area where it is expected to find a known network. *Geofencing* is a technique that automatically turns on WiFi when in certain geographical areas and can be implemented through mobile applications. This technique will mitigate all the vulnerabilities described to only work in areas where the device expects to have a WiFi connection. Furthermore, since most vulnerabilities only work when a device is not connected to a network, it will drastically reduce the threat of location exposure. However, it might be time-consuming to implement and maintain if the NGN devices also need to be used in other networks, such as private home networks of PPDR personnel.

M-4 Limit network connections
The more networks a device is connected to, the more unique it can be identified with the V-7 vulnerability. Additionally, it might connect to hidden networks that can reveal a device's location with V-1. Some networks might also have poor security features and be vulnerable to other attacks. Hence, restricting which networks a device can connect to or who can control the network settings could improve the security.

M-5 Establish same network in different locations
Assume that NGN WiFi APs are independently deployed in all police stations. First, device connections would be more challenging to manage security-wise if devices need connections to different networks. Second, the amount of devices connected to a unique NGN AP is lower. Hence, an adversary using the AP relay attack described in V-7 is able to track the device back to the station the device belongs to. Therefore, deploying different networks in different locations can reveal the users work station. However, there is also a downside. An adversary only needs to impersonate the one network used by all stations to detect PPDR personnel. However, this provides the PPDR personnel with the largest anonymity set detecting and generally tracking PPDR devices is possible with other technologies as well. Therefore, protecting the user behind the device is more important and the same network should be deployed in multiple location.

M-6 Re-connect to networks
For iOS devices with version 15 or higher, forgetting the network the device is connected to and then later reconnecting to the network generates a new random MAC address the device associates with the network [App21a]. However, the duration between forgetting and reconnecting needs to be at least two weeks for the MAC to be reset [App21a]. Which makes the WiFi network unavailable for the device for two weeks.

M-7 Erase content or reset network settings
For iOS 14 and higher, a random MAC is used for every network the device is connected to. However, the same random address will be used every time for the same network. According to Apple documentation [App21a], erasing all data and settings or resetting the network settings on the device forces the device to connect with a new address the next time it connects to the network. Hence, by regularly resetting the network settings, the device's MAC address to the network will also be reset and mitigates the risk of having the device tracked over time. However, this requires an easy or automated way of resetting and reconnecting to the network.

M-8 Do not add networks manually
Adding a network by manually inputting the SSID and security context will trick the

device into believing the network is hidden and will therefore advertise the network SSID in probe requests. Hence, networks should not be manually added unless they are hidden networks to mitigate V-1.

M-9 Updating SSID of network
Knowledge of the network SSID of a target enables an adversary to track the device through V-7. Therefore, frequently updating the value makes tracking more cumbersome for an adversary. Furthermore, this technique will, for iOS 14 and higher and Android 10 and higher, produce a new MAC for the device, which will force the adversary to perform the difficult task of correlating the addresses with each other to track the device over time. However, this technique requires the devices to forget the old network SSID connection every time the value is updated and hence, increases the maintance of the network.

Table 4.1: WiFi location exposing vulnerabilities.

Classification		**No.**	**Implication**	**Assumption**	**Attacker model**	**Vulnerability type**
Probe request	SSID	1	Detect previously connected networks		Passive	Standard and implementation
	Information element	2	Location exposure			Implementation
	Probing frequency	3				
	Interframe transmission time	4	Location exposure, not real-time			
	Sequence numbers	5	Temporary location exposure			
	WPS	6 (1)	Location exposure			Standard
		6 (2)	Reveal MAC address			
Beacon frame	Unprotected AP beacon	7	Location exposure	AP relay, SSID of target network	Active	
RTS/CTS	RTS/CTS	8		AP relay, MAC of target		
Identification exploits	MAC address in the clear	9 (1)	Location exposure and reveal MAC address		Passive	Implementation
		9 (2)		AP relay	Active	Standard
		9 (3)		MAC of target or AP	Passive	
	Infrequent update of MAC	10	Temporary location exposure			Implementation

4.2 4G and 5G

The 5G standard improves security issues from the previous 4G standard. For example, IMSI catchers are not theoretically possible in the 5G standard, and the paging protocol is also improved. However, 5G still possesses security vulnerabilities, and downgrading attacks can introduce many of the attacks applicable on the 4G network. Furthermore, the 5G NSA network does not have the 5GC and hence, does not implement many of the security fixes introduced in 5G SA. This section summarizes vulnerabilities in 4G and 5G that can reveal a user's location, reveal a user's permanent identifier, map between different identifiers or counter the refreshment of the temporary identifiers. The vulnerabilities for 5G and 4G identified through the literature study are summarized in Table 4.2.

4.2.1 Attacker model

For 4G and 5G, we will consider three different attacker models. The two first, passive and active, are similar to the ones described for WiFi networks. Where the passive attacker can listen to the air interface to capture radio packets with a monitoring device, and the active attacker can fabricate signals or, in other ways, trigger the network or UE to transmit signals. The third attacker model extends both the passive and active by also being able to act as a Man-In-The-Middle (MITM) relay between the network and the UE. The MITM relay can impersonate a UE towards the network and an eNB towards the UE, and alter, drop or add messages between the communicating parties. All the attacker models use commercially available Software-Defined Radio (SDR) equipment, and for deployment in one location, it is a low-cost setup. The three models are represented in Table 4.2 as *Passive*, *Active* and *MITM relay* under *Attacker model*.

The goals of the attacker are the same as for WiFi, i.e., breaking the anonymity of the user and unlinkability of two signals 4.1.1.

As for WiFi, The attacker models can be extended by deploying devices in multiple locations to obtain better tracking capabilities. And the same assumptions are made as in 4.1.1

4.2.2 Vulnerabilities

V-1 Authentication and Key Agreement (AKA) linkability
Even though the 5G-AKA procedure improves its predecessor, vulnerabilities are still present in 5G-AKA. The UE will, during authentication, first verify the integrity of the AUTN and then check if it is not a replayed message. If one of the checks fails, the UE will send a failure message to the network with the cause of the failure. Exploiting the failure message can be done in two different ways described below.

(1) The authors in [BDH+18] presents an attack taking advantage of the failure message. The adversary needs to listen to one successful AKA procedure for the target UE to obtain an AUTN with a valid MAC. The adversary then acts as a MITM relay and sends the AUTN of the target to a device during authentication. The adversary knows that it communicates with the target when it receives a synchronization failure and not a MAC failure. This strategy breaks the user's anonymity and can track a targeted individual over time. The attacker can use the same AUTN to identify the target multiple times. Chlosta et. al [CRPH21] discovered that after two failures at the UE during authentication, the UE would cancel the registration attempt. Hence, the attack described above can only have two targets, such as important personnel. However, it can not be used to track more than two individuals.

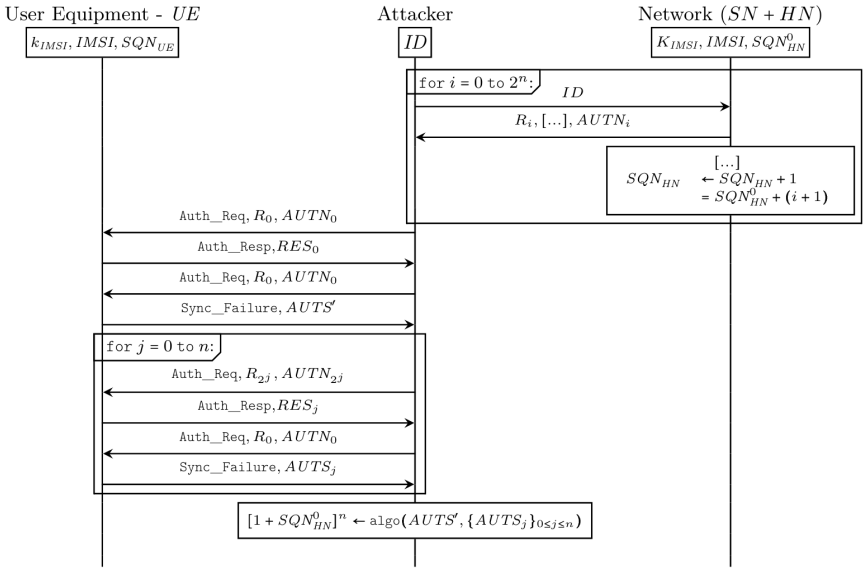
(2) The SUCI-catcher attack [CRPH21] extends the attack described above by adding a reset & sync procedure. This is simply a procedure that allows the UE to successfully connect to the network, i.e., the adversary acts as a MITM relay without interfering with the messages. The sync & reset procedure happens between the linkability attack and ensures that the UE is still connected to the network. The SUCI-catcher attack also uses a different technique to identify a target. Instead of using the AUTN, a valid SUCI is used to obtain authentication requests from the network. The adversary can now try SUCI values for as many targets as possible. However, due to the sync & reset procedure between each try, testing for many identities takes time, and results showed that testing 500 identities could take up to 16 minutes, which implies that it cannot be used for large-scale tracking. However, for smaller groups such as the police service, 500 identities could be the entire force in a limited area. Furthermore, the device will have little to no service during the SUCI-catcher attack since it is not connected. Hence the user of the UE might detect that something is happening and might reboot the phone which aborts the network connection attempt.

V-2 Exposure of SQN

The authors in [BHPS19] present a vulnerability in 4G and 5G AKA procedure taking advantage of the usage of Sequence number (SQN) to break the unlinkability of two messages sent at different times. More precisely, the way the SQN is concealed in transmission and how the UE notifies the network that the SQN value is out of sync. First, for the same RAND value, the UE will generate the same AK used to conceal the SQN. Hence an attacker can replay the same AUTN to force the UE to calculate the same AK as a previous message. Second, the UE will reply with an out-of-sync message containing the expected SQN when it receives an unexpected value. These two vulnerabilities result in two attacks [BHPS19] that both require the adversary to operate a MITM relay.

(1) First, an adversary can, by having an AUTN for a target user, replay it

Figure 4.2: Sequence number (SQN) exposure procedure (V-2 (2)) [BHPS19].



during AKA to obtain the expected SQN from the UE in the out of sync message. Since they are concealed with the same value, the adversary then calculates the difference between the two SQN values. If the difference is slight (less than 10-15), the adversary can assume the UE belong to the same USIM and hence is the same user. Note that this attack will already determine if it is the target UE when a sync failure is detected (which is the vulnerability described in V-1. It is mentioned here since even if the vulnerability in V-1 is fixed, this attack is still applicable).

(2) The second attack, seen in Figure 4.2, does not require the adversary to know an AUTN for the target. Instead, it will obtain a valid AUTN for the SUCI from the network and send it many times to the UE during connection to retrieve many sequential concealed expected SQNs from the UE. Together this reveals the last bits of the SQN to the adversary. Over time an adversary can obtain the SQN of the UEs in the network and correlate the SQN values to previous values. The same reset & sync procedure as for the SUCI-catcher is used, and hence not more than 9 bits (512 values) of the SQN can be retrieved within a reasonable time. This also puts a limitation on how many UEs can be in tracking.

V-3 ToRPEDO

The TRacking via Paging mEssage DistributiOn (ToRPEDO) [HEC+] attack takes advantage of the cellular paging protocol to identify the presence of a target UE within a location area. It establishes an association and breaks the unlinkability between the device's phone number and Paging Occasion (PO). The association

is achieved by listening for paging messages in the location area while triggering the network to send paging requests to a device (through SMS, calls, and Twitter notifications). If the device is in the listening area, the adversary will see a spike in the PO for the device. For 4G, the PO is calculated from the IMSI and is constant over all sessions. For 5G, however, the PO is calculated from the 5G-S-TMSI [3GPb]. Hence, if the TMSI value is not updated frequently enough (from [HEC+], between every 3 or 4 paging messages), the UE is vulnerable to the attack.

Additionally, the adversary needs the MSISDN of the device to send an SMS or call it. Taking advantage of the paging protocol requires the UE to be in idle mode, and with multiple calls required, the adversary will have to wait for about 35 seconds between every call. This results in an attack time of around 3-4 minutes which does not provide real-time tracking and limits the tracking of moving targets. Also, the adversary does not know when the UE is in idle mode and hence, might provide a false negative[2].

V-4 PIERCER

The Persistent Information ExposuRe by the CorE netwoRk (PIERCER) attack by Hussain et al. [HEC+] extends the ToRPEDO attack to retrieve the IMSI of a UE in 4G. First, it uses ToRPEDO to obtain the PO of the user, which is constant over all sessions since it is generated from the IMSI. Then the adversary will hijack the paging channel of the UE to block all paging messages to the UE. The adversary then triggers the network to page the UE. However, the UE will not receive the paging messages since they are blocked. After two paging messages are sent from the network, and no reply is received, the network might page with the IMSI of the user. From [HEC+] only paging messages that were time-sensitive (e.g., phone calls) would result in paging with IMSI. Hence, an adversary with knowledge of the UE's phone number could obtain its IMSI with the PIERCER attack.

V-5 Unprotected paging request

The authors in [HCMB18] present an attack in 4G where the adversary with knowledge of the target IMSI can detect a user presence. When the UE is in idle mode, it might receive a paging request from the network telling it to wake up. The request contains the identity of the UE, which can be IMSI for 4G. Since the paging request is not integrity protected, any device can fake the request with the target UE IMSI and send it. The adversary can then verify a user's presence if it detects an attach reply with the target IMSI. However, the adversary cannot ensure that the target is not within the listening area when no attach reply is detected. This is because the target needs to be in idle mode to reply to paging requests, and the adversary cannot be sure when the UE enters the mode. For 5G, the adversary would need the TMSI

[2] A false negative occurs when the device is in area but not detected by the attack.

of the UE to determine the location, but with knowledge of the TMSI the attack is similar.

V-6 Mapping of TMSI to C-RNTI
The authors in [RKHP19] present a vulnerability on the link layer of the 4G protocol stack. An adversary can obtain the C-RNTI of a user by knowing the TMSI and hence, break the unlinkability between them. In the RRC connection establishment, an adversary can map the target's TMSI value to the C-RNTI during its distribution. Since the C-RNTI is used to identify the device during active communication, it can localize a device while it is communicating, compared to the other vulnerabilities described that require special operations such as attach and handover. Exploiting the vulnerability can be done entirely passively since the adversary only needs to listen to the communication, making it simpler to conduct and harder to detect. However, it requires that the adversary knows the TMSI of the target and can listen during the C-RNTI distribution.

V-7 Mobile Network Mapping (MNmap)
The Mobile Network Mapping (MNMap) attack by Shaik et al. described in [SBPS19] takes advantage of the UE capability message sent unencrypted to the network in 4G. An adversary can trick the UE into sending a Tracking Area Update (TAU) message to the relay eNB by establishing a MITM relay with higher signal strength and different Tracking Area Code (TAC) than the other base stations nearby. The eNB can then send a UE capability inquiry message to obtain the UE capabilities. Once the adversary knows the capabilities of the UE, it can start the process of analyzing it to determine the device type. The device type can further lead to the identification of the device and the user.

V-8 Unprotected RRC messages
In 4G, the RRC[3] messages sent does not need to be protected. Shaik et al. describe two techniques taking advantage of this in [SBA+15] to obtain the fine graded location of the user.

(1) An adversary can operate a MITM relay base station with a different TAC than other base station in the proximity. When a UE connects to this relay and has established an RRC connection, it will see the new TAC and initiate a TAC procedure. During this procedure, the MITM relay can ask the UE, unprotected, to obtain and send the received signal strength for base stations by giving the UE their cell IDs. The UE will reply with an unprotected measurement report of the signal strengths of nearby base stations.

(2) An adversary can, by having two MITM relays in an area, retrieve an Radio

[3]RRC is used for, amongst other, connection handling, paging notifications, and connection procedures in layer 3 of 4G and 5G.

Link Failure (RLF)[4] from the UE. First, one relay will complete the RRC connection establishment with the UE before stopping the communication, which triggers the UE to create an RLF report. Second, the other relay will set up a new connection with the UE. Now the UE will indicate that it has a RLF report, and the relay can ask for the report in an unprotected message. The RLF report contains the signal strength of all the base stations in the proximity of the UE.

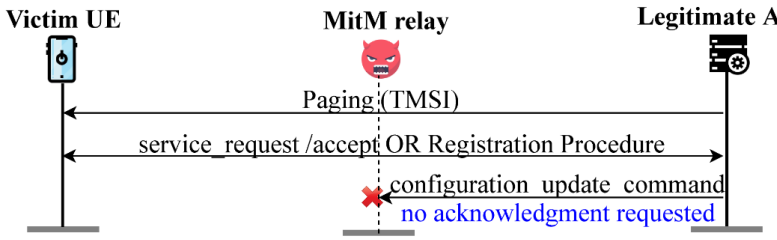
Both the attacks described above obtain the signal strength of nearby cell towers of the UE. The signal strengths combined can triangulate the position of the UE to get a more fine graded location estimate. Instead of knowing that the user is within the range of the listening device, the adversary gets a better position estimate of the UE. The techniques can more precisely determine the location and movement of PPDR personnel over time. In addition, these two vulnerabilities can be combined with others, such as V-1, V-3, or V-5, to provide a fine graded location of a specific target.

V-9 Neutralizing TMSI Refreshment
Hussain et al. [HEK+19] presents a vulnerability in both 4G and 5G in which the adversary can block the update of the TMSI as seen in Figure 4.3. With the knowledge of the target UE's C-RNTI value and acting as a MITM relay, the adversary can detect the transmission of the target config update message. This message contains a new TMSI, and if the message does not require an acknowledgment from the UE, the adversary can discard the message; hence, the UE will not know of the new TMSI. The attack blocks all messages to the target with the new TMSI, and with no response, the network will, after some time, cancel the TMSI update. Blocking the TMSI does not break the anonymity or the unlinkability, nor does it lead to location tracking; however, it forces the UE to have the same TMSI over time. Hence, the adversary can identify the UE's presence with the temporary identifier. The adversary can use the vulnerability in V-6 to obtain a mapping between the TMSI and the C-RNTI. The attack requires the adversary to know the old TMSI of the target to hijack its paging channel.

V-10 Blocking security mode update
The 5G SUCI protects the SUPI during transmission. However, the null scheme, an option for encryption, offers no protection. The authors in [HEK+19] presents an attack where an adversary uses a MITM relay to substitute the UEs *security mode complete* message with a *security mode failure* when establishing an RRC security context. Substituting the messages results in the network and the UE falling back to the protection scheme used prior to the security mode procedure. Devices that the AMF can not authenticate will enter the limited-service mode. In this mode, the

[4]RLF report is an RRC message containing measurement reports of present eNBs. The report is transmitted to the network when a device detects connection failures.

Figure 4.3: Blocking configuration update command [HEK+19].



device uses the null scheme until it establishes a security context with the network. Therefore, the attack can force a target device in limited service mode to use the null scheme. Furthermore, the adversary can ask for the UE identifier through an identity request, similar to the IMSI-catcher attack. The UE will then respond with the SUCI using null scheme protection(i.e., SUPI). This vulnerability can reveal the SUPI of a UE. However, NGN devices will never naturally be in limited service mode. Hence, exploiting this vulnerability can be cumbersome for an adversary.

V-11 Security mode command message

The security mode command message is sent to the UE to establish a secure context between the network and the UE. It is recommended that this message is both integrity and replay protected. However, research in [HCMB18] suggests that this is not always the case. Hence, an adversary can listen to a valid authentication of the target and store the security mode command message. The adversary can then later act as a MITM with a rouge eNB and, after initial connection setup, replay the security mode command message captured earlier. Only the target will respond with a *security mode complete* message, at which point the adversary has broken the anonymity and detected its target. Other devices will respond with a *security mode reject* message. After the UE transmits the reject message, it shall abort the security context [3GPk]. Hence, the technique can only test for one individual before the device aborts the connection. Therefore, it is not applicable to track multiple targets over time. However, tracking one individual is possible.

V-12 IMSI-Catcher

In 4G, the UE might transmit the IMSI unprotected to the network to identify itself. IMSI-catchers [MO17; Sør17; PGBB21] takes advantage of the IMSI transmitted in the clear to break the anonymity of the UE. The UE will send its IMSI to the network in reply to an identity request or when no temporary identifier is available during the AKA procedure. IMSI-catchers can be both passive and active attacks. In the passive version, an adversary will install a listening device and wait for the IMSI to be transferred naturally. While in the active version, the adversary acts as a MITM relay, and when a UE connects, it sends an identity request to which the

UE will reply with its IMSI. The active version can obtain more IMSIs since it does not have to wait for the transmission to occur naturally (when the target makes or receives a call) and hence, is a more efficient attack. Since the IMSI is permanent for a USIM, this vulnerability can track individual USIMs (devices) over time.

V-13 SUCI NAI format
John Preuß Mattsson in [MN21] presents a vulnerability in the generation of the SUCI from the SUPI that results in the SUCI providing no privacy protection. The vulnerability exists because the SUCI calculation is done with a symmetric key the same length as the plaintext. Hence if the plaintext has a unique length, so will the SUCI. This is not a problem for SUPIs with IMSI values since the plaintext is the MSIN with a fixed length for all 4G and 5G subscribers. However, for NAI identifiers in private networks, it is the username that is encrypted which can have a variable length and hence be used to identify the presence of a target. Since this is part of the standard and occurs whenever a user wants to identify itself with the network, an adversary can exploit this vulnerability completely passive. Especially for very long or very short usernames, this vulnerability can break the user's anonymity. The researchers indicate that when the usernames are taken from large data sets of real-world names, the anonymity set is reduced to just three people. This vulnerability only applies to private networks and hence is only a concern for NGN if adopting private networks.

V-14 Predictable TMSI
The TMSI value assigned to a UE should be updated frequently to provide privacy. However, updating the identifier depends on the implementation, and research shows that this is not always as frequently as it should. The authors in [SBA+15; HBK18; HEC+] showed that multiple 4G operators reattaching to the network did not provide a new TMSI and that a UE could be connected to a network for seven straight days [HEC+] without having its TMSI updated. These implementation vulnerabilities allow adversaries to identify and track a device based on the temporary identifier over time. It can also enhance other vulnerabilities and attacks described in this section that requires the knowledge of the TMSI.

Additionally, research has proven that even when a new TMSI is assigned, it is not necessarily random [HBK18]. Fixed bytes and increasing TMSI values have been observed for different operators worldwide. Therefore, an adversary can learn the pattern used by an operator by placing many calls from a USIM and observing the assigned TMSI values. The learned pattern can later help map an old TMSI to a new TMSI in the wild for a target by seeing if the values match the pattern. In this way, an adversary can track a user over time, even with different TMSI values.

Since 5G-SA deployment is not yet widely deployed, determining if predictable

TMSI values are a vulnerability in 5G can not be determined yet. However, implementation vulnerabilities can happen in any technology, and if operators continue to use the same techniques or approaches, this may be expected in 5G.

V-15 MNC in the clear
The permanent identifiers in 5G are better protected than in 4G. However, the MCC and MNC values are still always transmitted in the clear to provide routing information in case of roaming [KM20]. An adversary can listen to all the traffic completely passively to obtain the used MCC and MNC values. The MCC and MNC will reveal the country and the network operator of the UE. In addition to the SUCI identifier, the 5G-GUTI also contains the MNC and MCC values. Therefore an adversary exploiting this vulnerability can obtain more location estimates on targets than other vulnerabilities since the 5G-GUTI is used more frequently than the SUCI in 5G. The same applies to 4G but for the identifiers IMSI and GUTI.

4.2.3 Location exposure detection area

Some of the vulnerabilities described above can reveal a UEs location. However, the size of the detection area can vary. The vulnerability described in V-8 can obtain a fine graded location of the user. V-1, V-2, V-5, V-6, V-9, V-11, and V-12 require direct communication with the UE or detection of signals from the UE. Hence, they can determine that the UE is within range of the listening device. The ToRPEDO attack in V-3 takes advantage of the paging signals from the network. Two types of paging exist, smart (only one base station broadcasts paging) and non-smart (all base stations in a Tracking Area (TA) broadcast paging) [HEC+]. In the case of non-smart, the UE could be within a 10+ km radius, while for smart, it can be within a micro cell with a radius of around 200-2000m [SBA+15]. The attacker also needs to know the physical geographical area covered by the TA dedicated to the base station transmitting the paging request to estimate the user's location. An adversary can deploy multiple listening devices in strategic locations to obtain multiple copies of the same signals and use triangulation to obtain a more accurate estimate of the UE location. However, this is more expensive and requires more attacking infrastructure and capabilities to operate. The triangulation method does not provide a more accurate estimate for V-3 since it only listens for data from the network.

4.2.4 Mitigation techniques

The following subsection presents mitigation techniques that can completely or partially mitigate one or more of the presented vulnerabilities. They can be seen as guidelines on how to implement a 5G-enabled NGN.

M-1 Allow access for non-PPDR personnel
The Current Nødnett solution is available for more people than just the PPDR

services. Hence, other companies and institutions can use the network to obtain reliable communication. If this also is possible for NGN, then more devices will have access to the core network of NGN. Hence, more devices will have the same MNC value, and detecting that value will provide less information to an adversary (i.e., mitigate V-15). However, allowing access for more people also increases the maintenance and network load of the system.

M-2 Limit consecutive paging
Vulnerabilities V-3 and V-4 trigger the network to send paging messages which can reveal the user's presence and retrieve its IMSI value. The network controls the paging, and hence the network can limit the paging request sent to a UE. The limitation can be on the device that triggered the paging (i.e., if one device sends many consecutive requests) or a set of predefined allow paging rules (i.e., only NGN devices can trigger paging to NGN device). An example could be that only a set of UEs can make a call to an NGN device phone number. However, this will not remove the vulnerability. It will only make it more difficult for the adversary to execute.

M-3 Limit authentication responses
The vulnerabilities V-1 and V-2 require an AUTN from the network in order to detect a target UE. However, the variant that tracks multiple individuals (V-1 (2)) requires that the UE authenticates with the network many times. This can be detected by the network and used to disconnect the UE. As a result, the UE will not establish a connection with the network and disconnect from the adversaries MITM relay. The same applies to V-2 (2). This will remove the possibility of tracking multiple targets. However, tracking one individual will still be possible through vulnerabilities V-1 (1) and V-2 (1).

M-4 Prioritize 5G networks over 4G networks
The 5G network is more secure than the 4G network, with fewer significant vulnerabilities. Therefore, prioritizing 5G networks, when both 4G and 5G are available, will reduce the attack possibilities for an adversary. The prioritization is done in the settings on the individual device or by the network.

M-5 Limit active IMSI time
Frequently updating the IMSI in order to prevent tracking of a UE over time can reduce many of the vulnerabilities presented. For example, if all NGN UEs get a new IMSI, an adversary without knowledge of the network and the distribution of the new IMSI can not track a UE over time with the techniques presented. Furthermore, for a device with Embedded-SIM (e-SIM), the distribution of the new IMSI does not require any hardware updates and hence can happen automatically.

M-6 Implementation vulnerabilities
Verifying that the implementation vulnerabilities described are not present in the

NGN network is essential. For example, for vulnerability V-11, it should be verified that the UE does not respond to a *Security mode command* message that is not integrity protected. This also requires that the network integrity protects all *Security mode command* messages. For V-13, TMSI value must frequently be updated with a random value. However, the management and distribution of the TMSI are up to the serving network, which will be networks not operated or controlled by NGN. Hence, verifying this for all the network operators in Norway is essential.

Table 4.2: 5G and 4G vulnerabilities.

Classification		No.	4G	5G-NSA	5G-SA	Implication	Assumption	Attacker model	Vulnerability type
AKA protocol exploits	AKA linkability	1 (1)			x	Location exposure (one target)	Valid AUTN for target	MTIM relay	Standard vulnerability
		(2)			x	Location exposure (multiple targets)	Knows SUCI		
	Exposure of SQN	2 (1)	x	x	x	Location movement over time	Valid AUTN for target		
		(2)	x	x	x		Knows SUCI		
Paging	ToRPEDO	3	x	x	x	Location exposure	Knows MSISDN	Active	
	PIERCER	4	x	x		Map MSISDN to ISMI	ToRPEDO, hijack paging channel		
	Unprotected paging request	5	x	x		Location exposure	Knows IMSI in 4G Knows TMSI in 5G		
RRC messages	Mapping of TMSI to C-RNTI	6	x	x		Map TMSI to C-RNTI	Knows TMSI	Passive	
	Mobile Network Mapping (MNmap)	7	x	x		Location exposure		MTIM relay	
	Unprotected RRC message	8 (1)	x	x		Fine graded location exposure			
		(2)	x	x					
	Neutralizing TMSI Refreshment	9	x	x	x	Stop TMSI update	Knows C-RNTI and TMSI Hijack paging channel		
	Blocking security mode update	10			x	Expose SUPI			
	Security mode command message	11	x	x		Location exposure (one target)	Valid security mode command for target		Implementation vulnerability
Identification exploits	IMSI-catcher	12	x	x		Location exposure		MTIM relay / passive	Standard vulnerability
	SUCI NAI format	13			x	Location exposure		Passive	
	Predictable TMSI	14	x			Predict user TMSI	Know operator TMSI pattern		Implementation vulnerability
	MNC in the clear	15	x	x	x	Improve other attacks	Knows MNC of NGN operator		Standard vulnerability

Chapter 5
Experiment - Exploiting WiFi vulnerability

The experiment is based on the AP relay attack, exploiting vulnerability V-7 for WiFi described in [Cun14]. The concept in [Cun14] is to implement a fake AP that impersonates a network the target device previously has been connected to by advertising the same SSID and security context. Once the target device detects the impersonated network, it will automatically attempt to authenticate to it with its MAC address. The adversary stores the MAC address of the device that tries to authenticate and, in that way, tracks the device over time. The paper [Cun14] shows that it manages to trick devices into authenticating with the fake AP and thereby detect MAC addresses of devices that have been connected to the network previously. Hence, breaking the unlinkability between the device and its MAC address. However, the paper does not analyze the attack's efficiency in a real-world tracking scenario nor investigate devices' behavior when exposed to the attack.

Additionally, the paper does not consider MAC address randomization, and since it was published in 2014, randomizing the MAC address has been taken advantage of at a much higher rate according to [DPČ19]. The authors in [VMC+16] test a similar attack in a train station for one hour to detect MAC addresses. However, they assume a device will use its actual MAC address when attempting to authenticate, which is not true for modern devices according to [IET22]. We also propose a new technique of exploiting vulnerability V-7 to track devices over time regardless of the randomized MAC address used.

This experiment aims to analyze how the AP relay attack (from vulnerability V-7) works in practice when deployed in a real-world scenario and how different devices behave when exposed to the fake AP. First, we present our preliminary investigation. Second, we describe the implementation of the experiment in the context of both the real-world scenario and the device behavior. Then we propose a new technique to track devices regardless of the MAC randomization. Lastly, we discuss the privacy concerns before presenting our results.

5.1 Preliminary investigation

This section presents our preliminary investigation into the WiFi authentication procedure for modern devices and the feasibility of collecting MAC addresses based on the attack described in vulnerability V-7. We propose an improved attack sequence from our investigation that we use in our experiment.

5.1.1 Initial attack

The initial attack was implemented and tested in a busy location by emitting legitimate beacon frames. Once a device attempted to authenticate with the network, the MAC address would be stored. Wireshark [Wir] was also run to detect all traffic to verify and analyze the attack efficiency. During 40 minutes, very few authentication attempts were made to the network. By inspecting the traffic of a device before it attempted to authenticate, we observed that the devices first emit a probe request with the SSID of the imitated network before authenticating. Therefore, some devices might have sent out a probe request but did not attempt to authenticate since no response was detected. Upon further inspection of the Wireshark trace, we observe that multiple devices transmitted probe requests with the imitated network SSID but did not try to authenticate to the network. Additionally, the devices that authenticated did not use MAC randomization, indicating that they could be older devices with fewer security features.

5.1.2 Legitimate connection establishment

From inspecting successful authentication attempts to the legitimate network, we confirmed that most devices would not directly authenticate with the network after detecting a beacon frame. Instead, they would send a probe request and expect a response before authenticating.

5.1.3 Improved attack sequence

From the observations made, we made an improved attack sequence that implements the probe request and response messages missing from the initial attack. Figure 5.1 displays the improved attack sequence. First, the device discovers the network through a probe request or beacon frame. Upon discovering the network, the device will send a probe request, possibly with a new MAC address or containing the SSID of the network. Then, the fake AP will reply with a probe response which the device will acknowledge. The acknowledgment triggers a new beacon frame from the fake AP. Finally, the device will authenticate to the network.

Detecting a probe request with the target SSID is enough to determine that the device has been connected to the network before. However, some devices were observed

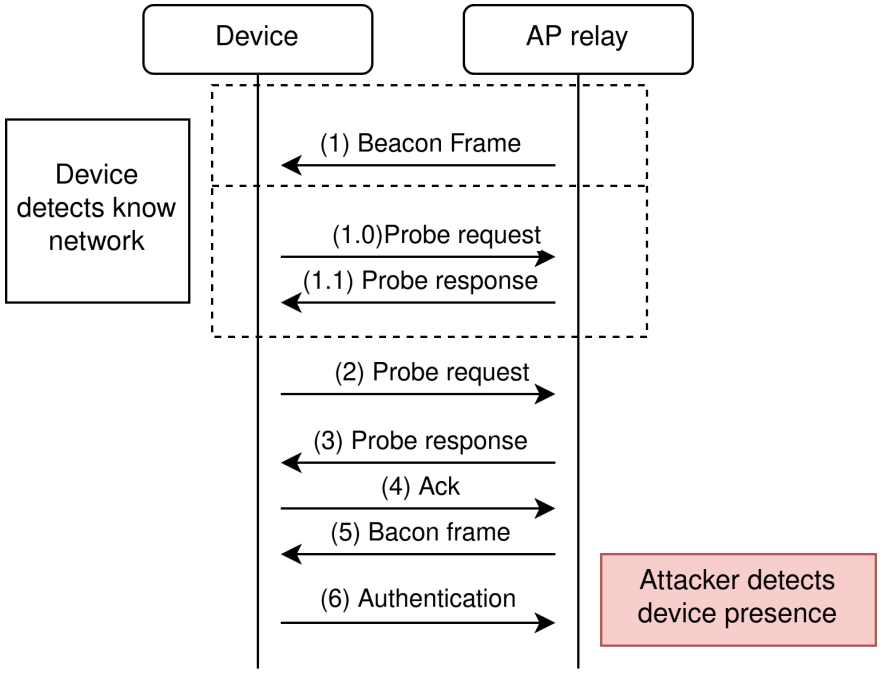


Figure 5.1: Improved AP relay attack.

using a random MAC until authentication. Therefore, obtaining a persistently used MAC address for these devices will require the authentication message. Additionally, some devices might be vulnerable to V-1 for WiFi and send probe requests with the target SSID even when not detecting the fake AP, which could affect the experiment results. Therefore we implemented the entire attack sequence.

5.2 Experiment description

The experiment is divided into two. First, we will observe and analyze different devices' behavior when exposed to the AP relay to determine how the attack can track devices. Second, we deploy the AP relay in a real-world scenario to see if it can detect and track devices over time.

This section first describes a new technique for tracking devices based on the AP relay attack. Then we describe the program implementation used in the experiment before describing how we will conduct the two experiments.

5.2.1 Tracking devices regardless of MAC randomization

Devices will attempt to authenticate to a known network when it is detected. However, the fake AP described above will not respond to a device's authentication attempt. Hence after some time, the device will stop the authentication attempt. Therefore, exposing a device to multiple known networks will trick the device into authenticating to a second fake AP after a failed authentication attempt to the first AP. Therefore, an attacker with a set of APs that are a unique pseudonym of the target can set up fake APs of all the networks and trigger the device to authenticate to all the networks to track the target over time.

The research in [IET22] suggest that most new device will associate a random MAC address with each network it establishes a connection. Hence, if a device attempts to connect to two different APs, it will do so with two different MAC addresses. Therefore, two consecutive authentication attempts from one device can not be correlated based on the MAC address. However, basing the correlation on time between and duration of the authentication attempt is possible. We will use the device behavior experiment to obtain timing information of different devices and later discuss whether this technique can work in practice.

5.2.2 Attack infrastructure and program implementation

The experiment was run from a Lenovo ThinkPad E14 laptop with Ubuntu 20.04 as the operating system and the network card in monitor mode to capture and transmit 802.11 packets. The network card must support monitor mode, otherwise the attack program would not run. The attack program on the laptop was implemented through a python script using Scapy [Sca] to transmit packages. The behavior of the program was simple and had three main parts. First, ten times every second, a beacon frame was emitted announcing the AP presence to nearby devices. Second, every time a probe request with an SSID field either empty or equal to the SSID of the imitated network was detected, a probe response would be transmitted. Last, it would emit a beacon frame whenever an acknowledgment packet destined for the AP was detected. The imitated network was the eduroam campus network. The network is an enterprise network that is available to many people. In order to imitate it in the best possible way, legitimate beacon frames and probe responses were captured and directly repeated with the same IEs and headers. The timestamp of the packets was set equal to the timestamp of APs in the proximity (if any, else 0), and the sequence number was increased for every packet. Whether all IEs and headers were necessary to imitate the network is out of the scope of this experiment.

Additionally, according to [IET22], iOS 14+ associates a random MAC address with the BSSID (MAC of AP) and not the SSID. Therefore, if the program is to

be deployed in multiple locations and impersonate the same network, they must all have the same BSSID.

5.2.3 Device behaviour

Different devices were tested in an isolated environment to observe their behavior. For each device, we observed their behavior to answer the following questions:

1. Idle: How often will a device try to authenticate to the fake AP when WiFi is turned on but the screen is turned off?
2. Screen turned on: How long does it take for the device to authenticate to the network after the user turns on the screen?
3. Already connected: Does the device try to establish a connection with a known network when already connected to a network with a different SSID?
4. Randomized MAC: Does the device authenticate with a randomized MAC address?
5. Persistent MAC: Does the device use the same MAC address in two authentication attempts one week apart to the same network?
6. Multiple SSID: When the device is in the proximity of multiple fake APs with known networks, how long will the device wait between failed connection attempts?

For testing question 1, the devices were left with the screen turned off, all applications closed, and not connected to a network for 45 minutes with the fake AP running. Question 6 is added to see if it is possible to track a device regardless of MAC randomization. For testing question 6, we used three different networks, the eduroam campus network and two hotspot networks. The devices were connected to the test networks by establishing a hotspot on a laptop, and when the device detected the network, connect it. This ensured that the device did not believe the network was a hidden network and hence, would not advertise the SSID in probe requests.

5.2.4 Real world experiment

The real-world experiment is conducted by spoofing only one network (eduroam) in a location where it is not usually deployed. Most devices will not continuously look for networks to connect to when the device is not in use to save power. Therefore, the attack will be placed close to a busy intersection and a bus stop. The attack will imitate one network. However, imitating multiple networks through one or more

Device Name	OS	Idle	Unlock screen	Random MAC	New MAC per session	Avg. duration of auth. attempt	Min time between auth.
Samsung Galaxy S21	Android 12	2 min 17 sec; 27 min 39 sec	∼4s	Yes	No	∼0.17s	∼0.6s
Samsung Galaxy A41	Android 11	20 min 28 sec	∼4s	Yes	No	∼0.2s	∼1s
Samsung Galaxy A71	Android 11	2 min 44 sec	∼4s	Yes	No	∼0.95s	∼1.6s
Samsung Galaxy A5	LineageOS 18 (Android 11)	N/A	∼2s	No	No	∼0.96s	∼1.4s
Nokia Android One	Android 11	10 min 4 sec	∼4s	Yes	No	∼0.96s	∼1.6s
iPhone 7	iOS 15.4.1	N/A	∼2s	Yes	No	∼0.45s	∼0.22s

Table 5.1: Summary of device behavior results.

devices would likely result in more detections since more devices would detect at least one known network and attempt to connect to it. The main goal is to determine if a device can be tracked over time through this vulnerability and to see how many devices use a random MAC when authenticating to the network.

5.3 Privacy concerns

For the real-world experiment, only the MAC address, location, and timestamp are collected to store the minimal amount of data related to a device. The MAC address is personal data; therefore, we will not register any other personal data with it. Additionally, the MAC will not be matched with the device user.

5.4 Results

This section presents the results of the experiment.

5.4.1 Device Behavior

The devices were tested individually in a controlled environment. Multiple tests were conducted to observe the behavior, and a similar behavior was detected for all devices tested. For two minutes, while the devices were idle (not in use), no connection attempts were detected. However, once the screen was turned on[1], the devices would immediately send out probe requests and, after 2-4 seconds, discover and attempt to connect to the network. Most devices used a random MAC to connect to the network. However, the same random MAC was used persistently over different sessions. The results are summarized in Table 5.1.

[1]The user powered on the screen, but the device was not unlocked.

No.	Time since reference or first frame	Source	Destination	Protocol	Length	Type/Subtype
9370	27.706683294	22:75:09:ca:18:be	Cisco_36:43:a0	802.11	102	Authentication
9449	27.869952075	22:75:09:ca:18:be	Cisco_36:43:a0	802.11	102	Authentication
9639	28.325715484	92:40:39:79:0b:50	IntelCor_14:19:c3	802.11	102	Authentication
9737	28.494780563	92:40:39:79:0b:50	IntelCor_14:19:c3	802.11	102	Authentication

Figure 5.2: Samsung Galaxy S21 attempting connect to two different APs.

No.	Time	Source	Destination	Protocol	Length	Type/Subtype	Sequence number
3092	41.683595244	de:82:d8:7f:eb:ee	4e:39:28:ba:b6:73	802.11	114	Authentication	3572
3199	42.146435471	de:82:d8:7f:eb:ee	4e:39:28:ba:b6:73	802.11	114	Authentication	3576
3225	42.368932809	a6:a1:d8:c2:e5:aa	IntelCor_14:19:c3	802.11	114	Authentication	3579
3333	42.780805311	a6:a1:d8:c2:e5:aa	IntelCor_14:19:c3	802.11	114	Authentication	3583
3417	43.982110710	16:6a:e9:05:98:31	Cisco_36:43:a0	802.11	114	Authentication	3587
3540	44.442050279	16:6a:e9:05:98:31	Cisco_36:43:a0	802.11	114	Authentication	3591

Figure 5.3: iPhone 7 attempting connect to three different APs.

No.	Time since reference or first frame	Source	Destination	Protocol	Length	Type/Subtype	SSID
9233	27.348175246	22:75:09:ca:18:be	Broadcast	802.11	241	Probe Request	eduroam
9359	27.652822871	22:75:09:ca:18:be	Broadcast	802.11	241	Probe Request	eduroam
9500	27.968395614	92:40:39:79:0b:50	Broadcast	802.11	245	Probe Request	RandomSSID1
9624	28.271934592	92:40:39:79:0b:50	Broadcast	802.11	245	Probe Request	RandomSSID1

Figure 5.4: Samsung Galaxy S21 probe requests to different APs with their SSID.

The "Idle" column indicates the device's authentication attempts to the fake AP during a 45-minute period where the WiFi on the device was turned on, and the screen locked just before the fake AP was started. The "Unlock screen" column indicates how long it took from when turning the screen on until an authentication attempt was detected. Since the fake AP did not respond to authentication messages, when a device made an authentication attempt, it would not get any response and, after some time, stop the authentication attempt. The column "Avg. duration of auth. attempt" indicates the average duration of an authentication attempt for the devices. When the devices were exposed to multiple fake APs, they all would attempt to connect to multiple different networks. The minimal detected time between the start of two authentication attempts to different networks is presented in the column "Min time between auth.". For Galaxy S21, a Wireshark trace showing the first and last message of two consecutive authentication attempts is shown in Figure 5.2. A similar Wireshark trace for the iPhone 7 is shown in Figure 5.3.

As with many devices in the preliminary investigation, all devices transmit a probe request with the SSID before attempting authentication to the network. The probe request uses the same MAC address as in the following authentication request, i.e., the MAC address used persistently for the network. Therefore, the minimal time between the start of two probe requests with different SSIDs is similar to the minimal time between two authentication attempts and is for Galaxy S21 shown in Figure 5.4.

The devices were exposed to the attack for 30 minutes while connected to a different network to answer question 3 from Section 5.2.3. During the 30 minutes, the devices were actively used, and the WiFi settings were opened multiple times. However, neither device attempted to connect to the fake AP.

Rank	OUI owner	No.	Percent
1	Apple, Inc.	694	51.9%
2	Huawei Technologies Co.,Ltd	151	11.3%
3	Samsung Electro-Mechanics(Thailand)	118	8.8%
4	Xiaomi Communications Co Ltd	94	7.0%
5	Intel Corporate	84	6.3%
6	Samsung Electronics Co.,Ltd	50	3.7%
8	Motorola Mobility LLC, a Lenovo Company	18	1.3%
10	Huawei Device Co., Ltd.	14	1.0%
12	Fairphone	7	0.5%
14	OnePlus Technology (Shenzhen) Co., Ltd	6	0.4%
19	Unknown	4	0.3%

Table 5.2: Some of the detected manufacturers from OUI (first 24 bits of MAC) lookup (not all are shown).

5.4.2 Real-world experiment

The experiment ran for eight days. However, during the first few days, the attack crashed multiple times due to technical difficulties; hence, the attack was only running consecutively for the last five days. During the entire experiment, 12775 authentication attempts were detected by the fake AP. Of the 12775 authentication attempts, 7298 unique MAC addresses were used. Of them, 2280 were detected in multiple periods[2]. Hence, 2280 devices were tracked over time.

Approximately 82% of the detected addresses were randomized, which leaves 18% not randomized. For the non-random addresses, the OUI value was extracted and looked up to determine the manufacturer. The results can be seen in Table 5.2.

The timestamp of each detection was logged along with the MAC address. The distribution of the duration between two consecutive authentication attempts (not necessarily from the same device) can be seen in Figure 5.5, from which we can see that the median value is around 18 seconds. We also observed that around 6% of the consecutive authentication attempts came less than 1 second apart. Additionally, the most authentication attempts detected during one second is never higher than three.

Figure 5.6 shows the detection pattern for a selection of the recurring devices during the five days the attack ran continuously. Each column represents all detection

[2]For two consecutive detections of the same MAC to be registered as different periods, the detections had to be at least 30 minutes apart.

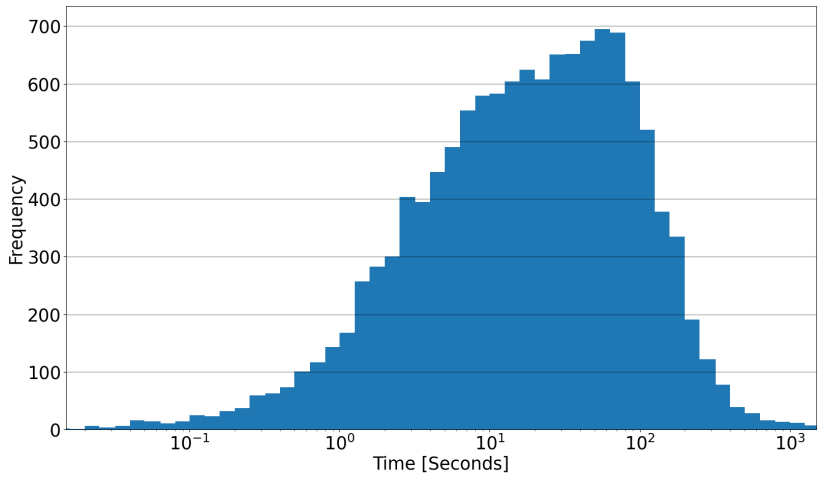


Figure 5.5: Frequency of the duration between consecutive authentication attempts. Note the logarithmic scale.

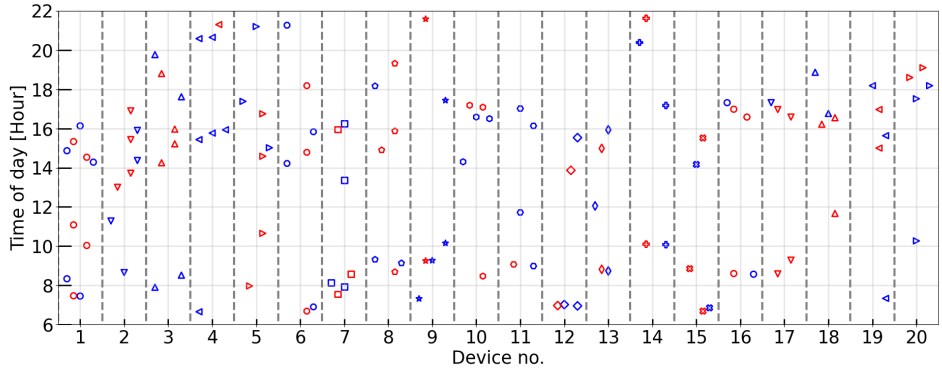


Figure 5.6: Detection patterns for 20 of the recurring devices during five days of capture. Alternating blue/red color on symbols to differentiate between days of capture.

for a device during the period, and consecutive days have alternating blue/red colors (blue: Monday, Wednesday, or Friday; red: Tuesday or Thursday).

Figure 5.7 shows a plot of all authentication attempts during the same period as above. The first time a device is detected, it will be assigned an increasing value (one higher than the previously detected device). The main line that forms in the plot shows the frequency of new MAC addresses detected over time.

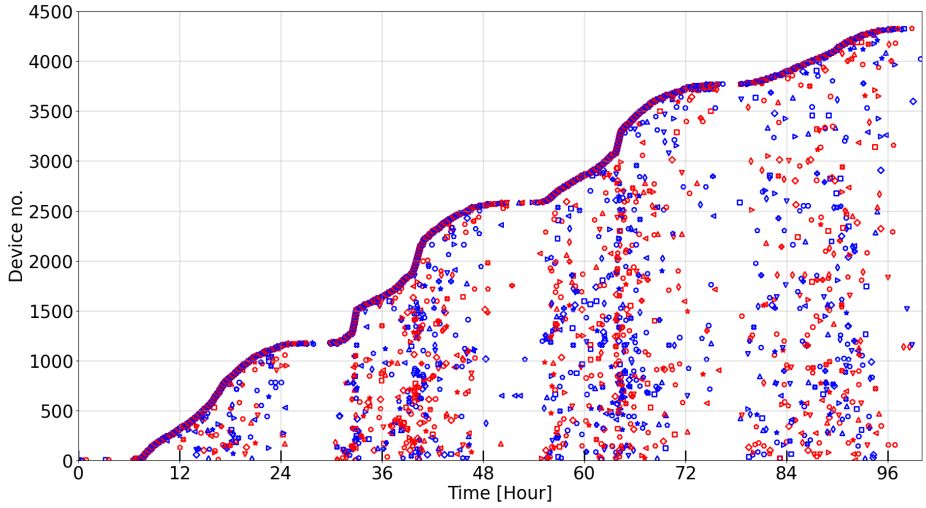


Figure 5.7: Plot of all MAC detections during a four day period. Time [Hour] 0 is Monday at 00:00. If a MAC is detected multiple times it is displayed on the same horizontal line.

Chapter 6
Discussion

This chapter discusses the finding of this thesis. First, we discuss the identified vulnerabilities and relevant mitigation techniques and their relevance to NGN. Then the results of the experiment will be discussed.

6.1 Undiscovered location exposing vulnerabilities

Chapter 4 presents the vulnerabilities discovered for WiFi, 4G, and 5G through the systematic literature review. However, as described in Section 1.4, the literature review done is not as comprehensive as the definition of a systematic literature review due to the limited time and scope of this thesis. A proper systematic literature review might have identified more vulnerabilities. Additionally, the vulnerabilities described in this thesis are not only applicable for tracking PPDR personnel but can be taken advantage of in other contexts as well.

The development of the 5G standard is a continuous process with regular updates of new features and security fixes. The updates provide new features and security fixes, but they might also introduce new vulnerabilities to the technology. These potential future vulnerabilities are not described here. Additionally, the current state of the 5G technology might include undiscovered vulnerabilities not described in the literature but, in the future, will pose a security threat to the network user, including NGN. If these are standard vulnerabilities and not discovered by anyone, they pose little threat, and not much can be done to protect against them. However, if there are implementation vulnerabilities, it might make it simpler for an adversary to detect a user's location. Hence, ensuring that the 5G implementation is consistent with the standard is essential and should be assured before NGN is taken into the deployment phase.

6.2 Exploiting vulnerabilities in the context of NGN

The vulnerabilities presented in Chapter 4 are known vulnerabilities that affect the technology. In the following section, we will describe scenarios on how an adversary can take advantage of the vulnerabilities in the context of NGN networks. We will also discuss how they can be prevented and what mitigation techniques can be relevant.

6.2.1 WiFi

For WiFi, we will assume that NGN deploys WiFi networks at locations where the PPDR personnel is frequently, such as police stations, hospitals, and fire stations. The scenarios will focus on tracking police personnel by detecting their presence.

Knowledge of police station location

An adversary with the knowledge of the location of a police station can quickly obtain the SSID of the WiFi network. It is trivial if it is a visible network, and for hidden networks, the adversary needs only to detect one successful authentication attempt to obtain the SSID. Once the SSID is known, vulnerability V-7 can be taken advantage of. The adversary can place AP relays that imitate the police station WiFi network in strategic locations[1] it wants to detect police presences. When it detects an authentication attempt, it can notify the adversary, which further can act on the information. The adversary will detect the MAC address of the NGN device, but it will not know which police officer it is related to without other information. The collection of MAC addresses can be used to create a database of police movements, driving routes, or hotspots. This yields important information to an adversary and can be used to target police officers or plan illegal activities. Suppose the adversary detects multiple NGN devices simultaneously in an area where it is conducting illegal activity. In that case, they can act on that and temporarily stop the criminal activity, cover up its tracks, or try to escape if they believe they are being targeted.

This attack is active, which means it can be detected and poses a risk to the adversary. The police can detect WiFi signals of a device impersonating their police station AP in a different location than their station and then assume that an adversary in the proximity is trying to track police devices. The detected signal information can indicate that some illegal activity is happening in that area. Furthermore, the police can, with scanners, try to locate the fake AP to confiscate and use it as evidence.

If NGN decides to use hidden WiFi networks, the adversary can, with knowledge of the SSID, take advantage of the vulnerability in V-1 to detect police officers. This

[1] If a fake AP is placed close to the legitimate AP, the devices might connect to the legitimate network and hence, not be detected by the fake AP.

can be done passively and can not be detected through wireless signals. However, it requires that the device transmits a probe request, and the time interval between such requests can be up to 6 minutes [Fre15], or 20 minutes from our results. With such a long duration between the probe request, this can not provide real-time detection when the device is not in use and has a low chance of detecting high-speed targets. However, it still poses a threat against stationary targets and users using their devices. NGN personnel is usually connected to a call when responding to incidents to provide real-time communication. However, how a device behaves when regarding the WiFi signals emitted when on a call is unknown, but it might reveal its location.

The main problem here that enables the adversary to obtain a user's location is that the WiFi on the device is always enabled, even when it is in a location where it is not expected to have a network connection. Therefore, taking advantage of the mitigation described in M-3 (turning off WiFi) will completely mitigate the location exposure vulnerability outside the police station. However, human errors can occur if the officers are responsible for turning the WiFi off. Therefore an automatic solution is more efficient, like an app that controls whether WiFi is turned on or off based on the geographical position.

An adversary with a network card in promiscuous mode[2] can passively listen to the network traffic at the police station. Furthermore, since the MAC address is used to address a connected device, as described in V-9 (3), the adversary can, over time, detect what devices and how many devices are connected to the station networks. The adversary can filter out the traffic that originates from other networks by only detecting packets with the MAC of the target network AP. The adversary can, over time, learn the work hours of devices and which devices are in the stations at a given time. It is hard to protect against this attack since the WiFi signals are transmitted in every direction, and turning WiFi off means the technology can not be taken advantage of. However, ensuring that the devices regularly use a new random MAC address when connecting to the station network will increase the user's privacy by making it more difficult to correlate MAC addresses over time.

Learning device WiFi behavior

An adversary can listen to probe requests and connection establishments near the police station WiFi network. Over time this can be analyzed to learn the IE and interframe transmission times for the devices used by the police officers. Suppose the IE, interframe transmission time, or a combination can uniquely or partially identify the device. In that case, it can later be used to track police devices outside of the

[2]A network card in promiscuous mode will capture all packets transmitted on the air interface rather than just the once addressed for it.

police stations. However, due to the low range of WiFi signals, it can be difficult for an adversary to get a listening device close enough to the station, which increases the risk of the attack. Using specially made devices might be an option for NGN. However, if the device has special network cards with unique characteristics (such as interframe transmission times and IE), this can be used to identify the presence of police personnel. For special-made devices, unique IE might also be used to track devices. Additionally, if all NGN users have the same device, it can be easy for an adversary to detect the presence of an NGN device. However, which officer the detected device belongs to is not revealed.

Learning MAC address of a device

The AP relay attack can be used to identify the MAC address of a target individual to break the anonymity through the Stalker attack [Cun14]. The adversary needs to know what the target looks like and its location. By following the target around with the AP relay attack, eventually, only one MAC address will have been constantly detected by the attack, which is the MAC of the target, and the attack is successful. The paper does not describe how this attack performs with random MAC addresses. However, according to [IET22], the randomization techniques in modern devices use the same MAC address every time for the same network. Hence, this attack should work for most modern devices using MAC randomization. With knowledge of the MAC address used for the station network, the adversary can identify the individual behind the device in previous and future WiFi network sniffing. The same strategy can be used for the hotspot vulnerability in V-9. With knowledge of the target's MAC address, other vulnerabilities such as V-6 and V-8 become easier to take advantage of for an adversary. This can be mitigated for NGN devices by turning off the WiFi on the device. Then the device will not respond to the beacons and can not have its MAC revealed. However, some devices have options to automatically turn WiFi on [App22; Sam20] so that device automatically connects to a known network when in the proximity to improve the user experience. These setting should be turned off as they require the device to always look for networks, even when the devices says the WiFi is turned "off".

6.2.2 4G and 5G

Compared to WiFi, the mobile networks have a more extensive area coverage; hence, location tracking can be done at a larger scale with less equipment. However, tracking in mobile networks also provides lower location accuracy, which reflects the vulnerabilities' practical exploits.

Learning device behavior

If NGN allows different types of devices to be used within the network, an adversary can physically observe what device target individuals use. Later, the adversary can use the vulnerability in V-7 for 4G and 5G to determine which devices are in the proximity of its MITM relay. If only one or a few people use the specific device detected within NGN, this can break the user's anonymity. Furthermore, this vulnerability can be used in combination with the IMSI-catcher attack (V-12) to obtain the IMSI of a user. However, this strategy requires the adversary to have a preexisting database of expected device behaviors, which can be costly to obtain. This strategy can also go the other way around, where if an adversary knows the IMSI of a target, it can use the information to learn which device the target is using. This can lead to further attacks on the device's software or hardware which are out of the scope of this thesis. If multiple NGN users are using the same devices, this strategy can not be used to identify targets uniquely. Instead, it will identify that an NGN device is present, but not which NGN personnel and, to some degree, preserve the user's anonymity. This also comes with a downside, such as all devices being vulnerable to the same hardware and software vulnerabilities.

MNC of NGN deployed core network

As stated in vulnerability V-15, an adversary can obtain the MCC and MNC value of a device by passive monitoring. This is not a concern for devices registered to large network operators since so many devices have the same MNC value that it provides little to no integrity breach and preserves anonymity. However, if the NGN solution implements its own core network (as is a possibility [DSB18]), it will be assigned its own MNC value. This makes it easier to detect the presence of an NGN device. Additionally, if the NGN network is to be restricted to only PPDR personnel, it will be trivial to track the general movements of PPDR personnel. Of course, the MNC value does not reveal the UE's identity. However, it can be used to identify movements and operations of the PPDR service.

Additionally, in smaller communities where few PPDR personnel is stationed, detecting an NGN device might reduce the number of possible identities to just a few people. Hence, increasing the risk of NGN devices being tracked in less populated areas. Even more concerning is that NGN personnel close to the national border can passively be tracked from the other side of the border. This enables other national actors to track NGN personnel close to the border without knowing the devices' permanent identifiers.

Knowledge of the MNC value used in NGN can also make it easier for an adversary to exploit other vulnerabilities. For example, for vulnerability V-1, V-2, V-7, V-11, and V-14, removing any device with a different MNC than the target MNC value will

drastically reduce the number of potential targets. Hence, improving the efficiency of the related attacks and increasing the threat of location exposure.

Temporary jamming
Most of the vulnerabilities described for 4G and 5G networks that identify a user's presence take advantage of the attach procedure in the network. However, a device will not reattach to the network in other situations than handover or when detecting a network with a stronger signal. This does not frequently happen for stationary devices, so an adversary can, over a short period, jam the mobile network, not with the intent to disrupt the service but to disconnect the device from the network. Once the device is disconnected, the jamming can stop, and the target UE will try to reconnect with the network. During the reconnection, the adversary can attack to detect user presence.

Criminal operations near 4G networks
Since 4G has more vulnerabilities than 5G, an attacker can set up a criminal operation in an area without 5G network coverage. The attacker can then take advantage of vulnerabilities in the 4G network, such as the IMSI-catcher, to detect when other devices enter the area. The attacker can then be notified if multiple police devices are detected and take necessary precautions. However, operating in a 4G environment also increases the risk for the crinimal.

Retrieving device SUPI
By temporarily having access to a target's device, an attacker can take advantage of vulnerability V-10 by placing an emergency call from the device before unlocking the SIM card. The device can then transmit its SUPI value in the clear, which the attacker can take advantage of by using a similar technique to the IMSI-catcher. The attack requires the attacker to know the target's location and access its device without being detected. It will not directly reveal the location of a device. However, it will provide helpful information to the attacker that can later assist in other attacks to obtain the target's location.

6.3 Communication technology location exposure

From the identified vulnerabilities in Chapter 4, we can see that even with the most modern mobile equipment, many vulnerabilities exist that could reveal a device's location. The vulnerabilities that originate from the technology standard are difficult to mitigate since they require changes in the standard. However, for the implementation vulnerabilities, the network deployer can ensure that no implementation vulnerabilities exist in the equipment used in the network. In the context of NGN, the devices selected can be chosen to mitigate as many vulnerabilities as possible. Especially for WiFi, this could remove most of the more straightforward passive tracking techniques

and leave an adversary only with resource-consuming techniques with lower efficiency. However, many of the vulnerabilities originate from the access network in mobile networks. Hence, if NGN takes advantage of existing access networks, they should verify that these networks do not possess any implementation vulnerabilities before deploying NGN. This can be both time-consuming and expensive.

Of the investigated wireless communication technologies in this thesis, only 5G matches the security level of the current TETRA solution for Nødnett when it comes to never transmitting the permanent identifiers in the clear. Transmission of the permanent identifiers in WiFi and 4G occurs when the device needs to identify itself to the network using IMSI for 4G and MAC for WiFi (even though it is random, a constant value is used). Hence, with a 5G enabled NGN with 4G and WiFi wireless technologies, the location privacy for the PPDR service is reduced. Additionally, with the use of multiple wireless technologies, many more unique identifiers need to be maintained when operating NGN compared to Nødnett. This increases the chance of human error in the maintenance of the identifiers and hence could in itself be a risk of device location exposure.

6.3.1 Location exposure in WiFi vs. mobile networks

Mobile networks and WiFi are two very different technologies. Tracking a device through WiFi provides a fine graded location of the device, while the area is more extensive for mobile networks. Which technologies are used for tracking depends on the attacker's needs and goals. However, combining the two would provide the best results in many cases. Then the adversary could track large-scale movements and detect when devices are in specific smaller areas. Another critical distinction between the mobile networks and WiFi is that the vulnerabilities in WiFi require the target device to scan for networks actively. However, for mobile networks, the device is always connected when powered on, and some vulnerabilities originate from the access network. Hence, an adversary can actively force the device to reveal its location in 4G and 5G through, e.g., the ToRPEDO attack, while for WiFi, the device is in control of when it can be tracked. Additionally, WiFi can be turned off when not needed to prevent tracking attacks. At the same time, it is problematic to disconnect the device from the mobile networks (it will not receive calls or messages). This results in the vulnerabilities of the mobile network always being a threat.

The WiFi and mobile network vulnerabilities can be exploited with off-the-shelf hardware and hence, are low-budget setups. However, due to the low range of WiFi, large-scale tracking in multiple locations requires more infrastructure and becomes more expensive than using 4G and 5G vulnerabilities in the same area. Hence, WiFi tracking in a large area might be unappealing to an adversary due to its cost, while in some locations, it might still be helpful as it provides a more accurate location.

6.3.2 Location exposure improvements in 5G

As expected, the 5G standard fixes many of the vulnerabilities present in 4G. Hence, 5G is still a more secure technology than its predecessor by mitigating many vulnerabilities, and the vulnerabilities that still are present require more resources from the adversary to achieve location tracking. However, many of the fixes rely on temporary identifiers to mitigate location tracking, and from 4G, some of the vulnerabilities originate from poor implementation of the temporary identifiers. Therefore, some security improvements rely on the implementation of the technology. Additionally, the increase of temporary identifiers and their use cases increases the consequence of poor implementation. Hence, ensuring proper implementation of the temporary identifiers is crucial for location privacy improvements.

6.3.3 Bluetooth

This thesis does not evaluate the location exposing vulnerabilities in the Bluetooth technology. This is not due to the lack of vulnerabilities but to time limitations. The technology is available in most commercial devices and has many practical use cases. The authors in [CGP+20] describe a technique that, within 4 seconds, can obtain the Bluetooth MAC address of any device with an active Bluetooth connection. In addition, Bluetooth is not a stationary network compared to WiFi, 4G, and 5G. Instead of being located in one geographical area, Bluetooth is deployed where the device is. This is because the Bluetooth device is usually the master in the communication and can connect to other devices in its proximity. Additionally, since it is deployed where the device is, it could be more challenging to manage in the context of NGN.

Due to the Covid-19 pandemic and contact tracing [Blu21], additional research has been done in the past years to research location exposing vulnerabilities in the Bluetooth technology [GSCC20; Bor20]. Additionally, Apple always on AirTag [App] can be used by adversaries to track devices over time [HBH22; MH21]. The low power consuming AirTag has a battery life of over a year and provides users with assurance that if they lose their belonging with an AirTag, they can identify its location. If NGN decides to take advantage of the Bluetooth technology, its vulnerabilities and mitigation techniques should be evaluated before deployment.

6.4 Mitigation techniques

The mitigation techniques described affect the vulnerabilities in different ways. However, the techniques also have downsides. For example, some of them limit the use cases of the devices and result in the PPDR personnel not being able to take full advantage of their phones. Other techniques increase the maintenance of both the devices and the network resulting in a higher cost of operating the network.

Therefore, the mitigation techniques should be valued against their downsides and negative effect on the network before NGN implementation.

We present the relevant mitigations that we identified during our research. However, other techniques may exist, and the ones presented in this thesis should not be considered a complete list of mitigation techniques for mobile location privacy. Additionally, devices and communication technologies are ever-changing. Hence, new techniques to mitigate vulnerabilities might arise, and some might become obsolete before NGN is to be deployed.

6.5 Experiment

The main purpose of the experiment was to see how a fake AP can be used to track WiFi enabled devices over time. The results show that the technique can be used to track devices over time with currently used devices. The results also show that newer devices tested will use randomized MAC addresses while older devices, such as the Galaxy A5, will not. This backs up the research in [IET22]. However, we also see that around 18% of the devices detected during the real-world experiment use a non-random MAC address when attempting to connect. This number could, in reality, be higher since some devices might use a random MAC address every time it attempts to connect and would be registered as different devices in the result data. Also, whether device manufacturers follow the practice of setting the MAC address to be locally administered[3] when using a random MAC has not been investigated. Hence, it could be a source of the number being lower. From Table 5.2 we see that four devices have used an unknown OUI value, which could indicate that some devices do, in fact, not produce the random MAC following the standard. Since the address area for MAC is so immense and relatively few connection attempts were detected, it can be safely assumed that two different devices will not use the same random MAC address.

In the following section, we discuss the results obtained from the conducted experiments and whether a fake AP can be used to track a device even when a random MAC is used for every message.

6.5.1 Network connection establishment

Our preliminary investigation observed that the network connection establishment procedure for modern devices was not as simple as expected from the initial attack taken from vulnerability V-7. Hence, we implemented a more extensive attack sequence where we expect a probe request/response before authentication. There can be many reasons why devices send a probe request and expect a response before

[3]By setting the second least significant bit of the first byte to one.

authenticating. For example, one could be that most devices have a unique MAC address for each network and want to use that address when establishing a connection. Another probable reason is that the network might have multiple APs in the proximity of the devices, and to detect all (not just the one detected by the beacon frame), the device needs to send a probe request. It can then determine which AP provides the best connection and connect to that one.

6.5.2 Device behavior

The results from the experiment show that most devices have a similar behavior when exposed to the fake AP. However, the tests are done on a limited number of devices, and many have similar operating systems and manufacturers. If more devices had been tested, the result might have been different. The limited testing was due to a lack of devices.

We can see from Table 5.1 that very few authentication attempts were made when the devices were exposed to the attack for 45 minutes. Most of the devices only attempted to authenticate once, while the Galaxy S21 attempted twice. However, the authentication attempts were 25 minutes apart. The low number of authentication attempts is probably due to the power management on the devices, limiting the frequency of the attempts when the device is not in use. However, this also reduces the effect of the attack on devices that are not in use. Especially for non-stationary devices that are only within the range of the fake AP for a short duration (e.g., people walking or driving). These devices will have a low chance of being detected by the attack. Therefore, the attack's efficiency depends on how much the target uses the device. An adversary could place the attack in a location where users usually use their devices to obtain the best results. When responding to an incident, PPDR personnel are consistently connected to a call to achieve real-time communication. This thesis has not investigated how often devices that are in use but not connected to a network will attempt to connect with an AP. However, we can assume the device will, at a higher frequency, attempt to connect with known networks when being in use.

It is also important to note that the devices did not have any applications installed or any accounts logged in to services. This might have reduced the frequency at which a device attempts to establish a network connection and hence, reduced the WiFi traffic emitted from the devices. Devices with network demanding applications installed might behave differently when exposed to the attack. This could especially increase the number of establishment attempts while in idle mode.

The test networks did not have the same security context. The eduroam network used WPA2/WPA3-Enterprise, while the two hotspot networks used WPA/WPA2-Personal. The security context difference did not result in any observed differences in

the authentication procedure. However, when the devices were exposed to multiple networks, all the devices except the iPhone7 first attempted to authenticate with the eduroam network (strongest security). This could be a coincident or indicate that the devices would actively attempt to connect to the network with the highest security first. However, this has to be investigated more.

During the testing, Wireshark only listened to one of the WiFi channels. Traffic transmitted by the device on other channels would not have been detected. Hence, a device might behave differently if the listening happened on all channels. However, since the device neither knows which channel to look for APs, it can be expected that the device will send probe requests on all channels when sending on one channel. Hence, we get a good picture of the device's behavior when listening to one channel.

6.5.3 Real world experiment

The experiment showed that around 1/3 of the devices detected were detected multiple times. This means that 2/3 of devices were not detected multiple times and were not tracked over time. This could be because many devices used a random address each time they attempted to connect to the network. However, a more reasonable explanation is that the experiment was not run for a long enough time for more devices to be detected multiple times. Either because they did not attempt a connection every time they were in the proximity or some devices only were in the proximity one time. Figure 5.7 backs up this argument, where we can see that after three days, the number of detected devices is approximately the same while the number of devices that attempts to connect for the first time is much lower.

The machine conducting the attack was placed by a window next to a road and two bus stops. However, the signals from the machine only reached the bus stop on one side of the road when testing the range of the signals emitted by the devices. Furthermore, when experimenting with other locations in the same area, we obtained five times more MAC addresses during a similar period. Hence, different placement of the attack machine would probably have resulted in more detections.

The duration of the experiment was only a little over a week. If many devices change their MAC addresses (e.g., every week), this technique would not be able to track devices over a long period. However, this was not detected in the test devices' behavior, nor is it indicated by other research papers [IET22]. Therefore, for the current state of MAC address randomization, with knowledge of the targets previously connected networks this technique provides an adversary the capability to track target devices over time.

From the distribution of devices using a non-random MAC in the data collected, over half of the distributed addresses are from Apple. This is way more than any

other vendor and can result from the fact that MAC randomization with Android 10 was released a year before randomization with iOS 14. However, Android devices are not just from one vendor, and we can assume that most detected devices are mobile phones. Therefore, as high as 48% of the addresses might be Android devices.

6.5.4 Tracking devices regardless or MAC randomization

From Table 5.1 we can see that the minimal time between the start of two consecutive authentication attempts combined with the duration of a authentication attempt will, for most devices, result in less than a second between two consecutive authentication attempts to two different networks. This means that if an adversary impersonates two different APs and, with less than one second apart, detects an authentication attempt to both the networks, it might be that the authentication attempts originated from the same device. However, from the distribution of the duration between two consecutive authentication attempts in Figure 5.5, around 6% of the detections are less than 1 second apart, with some even being less than 0.01 seconds apart. Therefore, the timing of the detected authentication attempts is not enough to determine with a high probability that they came from the same device in high traffic scenarios.

By analyzing the results obtained in the real-world experiment, we see that the highest number of authentication attempts made during one second is never higher than three. Even though the time between two consecutive authentication attempts can be very low, it is rare to see many authentication attempts within a second. Therefore, when using multiple fake APs and detecting multiple authentication attempts simultaneously, other information such as authentication duration, number of messages in the authentication burst, and IE can help correlate different authentication attempts and determine if they came from the same device. This might have a high probability of correctly correlating authentication attempts since the number of detected authentication attempts during one second was never higher than three. Therefore, even if a device uses a new randomized MAC address every time it authenticates with the network, it might still be identified based on the APs it authenticates to. This requires that the attacker can impersonate the previously connected networks of the target device and that the attacker knows that no other device has been connected to the same set of networks.

It is also important to note that most tested devices did not attempt to connect to all three networks in a row. After two failed connection attempts, some devices would not attempt a new connection for at least 20 seconds. At which point, it would not necessarily attempt to connect to the third network but might attempt one of the two already tried. This is true for all the devices except the iPhone 7, which attempted to connect to all three networks within three seconds. Therefore, to

identify a device uniquely with this technique, an adversary would, for most devices, need to have a set of two networks that only the target device has been connected to before. Research done in [GP09] on devices home/work network SSIDs prove a good pseudonym for a device. For PPDR services, this could make the AP at work (e.g., police station) the first target for an adversary and, in combination with the home network of the PPDR personnel, could uniquely identify the person. Allowing NGN devices to only connect to one network (station network) will mitigate the threat of being uniquely identified through this technique. However, a device will still reveal that it has been connected to the police station network previously and hence that the device most likely belongs to a police officer.

Most of the authentication attempts detected did not use IEs in the authentication request. However, it was observed for all individually tested devices that before authenticating, they would send a probe request with the SSID of the target network. Whereas the authentication message did not contain any IEs, the probe request contained as many as 13. This can be used as additional information when differentiating different devices that authenticate within the same interval. Some of the devices also used additional IEs when connecting to the eduroam AP compared to the hotspot AP. These were vendor-specific IEs and could even further be used to differentiate different devices. Taking the probe requests into account will help correlate different authentication attempts. However, it will also increase the computational power required by the attacker.

Since different devices have different timing information, an adversary can generate a database for a particular set of devices. Then when a target device is detected, look for similar timing information in the database and not just track a target but also determine what type of device the target has. This can also go the other way if the attacker knows the target device type (through physical observation), similar to vulnerability V-4 for WiFi, but can be used in combination with AP relay to provide better results.

Chapter 7
Conclusion and Recommendations

With 5G enabled NGN, the Norwegian PPDR service will be able to take advantage of many new technologies that can improve their everyday work. The wireless communication technologies discussed in this thesis will provide these new technologies. However, preserving the location privacy of the PPDR personnel is essential, and introducing new technologies also introduces new vulnerabilities. Therefore, it is vital to identify the location privacy concerning vulnerabilities and their relevant mitigation techniques so that the stakeholders can mitigate the risk when implementing NGN.

This thesis has identified privacy-sensitive identifiers used by the communication technologies and presented an overview of existing location-revealing vulnerabilities. Furthermore, the vulnerabilities are classified according to what they demand from adversaries and their origin within the technology. However, a literature study may never be enough to identify all vulnerabilities present in a system. Additionally, the 5G technology is still under development; hence, some vulnerabilities might be mitigated or even new ones introduced, which should also be considered when designing the NGN network. The thesis also identifies the ease of tracking devices over time if the same identifiers are used over long periods. Therefore, refreshing long-term identifiers increases the PPDR personnel's privacy and makes it more cumbersome for the adversary to map between identifier and user. The information regarding wireless location privacy in this thesis may be used to make decisions and prioritizations when designing NGN infrastructure and help plan for plausible scenarios.

Even though WiFi has many location-revealing vulnerabilities, mitigating them is simply by turning the WiFi off. Hence, with a properly implemented WiFi infrastructure within NGN where WiFi is turned off when in an area not expected to have a WiFi connection (e.g., *Geofencing*), the technology should be less of a location privacy concern to the PPDR personnel than mobile networks.

In addition to describing vulnerabilities, chapter 4 provides a set of mitigation techniques both for WiFi and the mobile networks that mitigate the location exposure vulnerability. These mitigation techniques can be seen as a set of guidelines for design NGN.

In Chapter 5, we implement one of the identified vulnerabilities and provide results from individual device testing and its effect in a real-world scenario. We can, from the results, conclude that with the current state of MAC address randomization, it is feasible to track many devices over time. Even though vendors randomize the address for each network, this is not enough to protect devices' privacy.

In Chapter 5, we also provide six questions regarding device behavior and perform tests on a selection of devices to observe the behavior and answer the questions:

1. Idle: Modern devices rarely (at least 20 minutes between) attempt to connect to networks when not in use.
2. Screen turned on: When turning on the screen, the device will immediately (max 4 seconds) attempt to connect.
3. Already connected: Modern devices will not attempt to connect a network when already connected.
4. Randomized MAC: Newer devices use a random MAC when connecting to a network.
5. Persistent MAC: Devices with default settings will use the same MAC address for connection attempts for the same network one week apart.
6. Multiple SSID: Modern devices will attempt to establish a connection with a network less than one second after failing to connect to a different network.

We also discuss the possibility of tracking WiFi-enabled devices over time, even when using MAC randomization for every new session. Our results show that it can be possible in low traffic scenarios if the adversary has a unique combination of previously connected network SSIDs using timing information. This technique might also be improved to work in high traffic scenarios with timing details, IEs, and probe requests.

Suppose other wireless communication technologies than the ones discussed in this thesis are to be taken advantage of in NGN, such as Bluetooth. Their identifiers and vulnerabilities should be identified to better understand the threat picture and implement mitigation techniques properly.

Regarding device selection, the devices applicable in FirstNet [Firb] can be used as a base. However, individual analysis of each device regarding the vulnerabilities and mitigation techniques described in this thesis should be done to enhance the users' privacy.

References

[3GPa] 3GPP, «5g; nr; medium access control (mac) protocol specification», *3GPP TS 38.321*, vol. V16.7.0 Release 16,

[3GPb] 3GPP, «5g; nr; user equipment (ue) procedures in idle mode and in rrc inactive state», *3GPP TS 38.304*, vol. V16.7.0 Release 16,

[3GPc] 3GPP, «Digital cellular telecommunications system (phase 2+) (gsm); universal mobile telecommunications system (umts); 3g security; security architecture», *3GPP TS 33.102*, vol. V16.0.0 Release 16,

[3GPd] 3GPP, «Digital cellular telecommunications system (phase 2+) (gsm); universal mobile telecommunications system(umts);lte;3gpp system architecture evolution (sae);security architecture», *3GPP TS 33.401*, vol. V14.5.0 Release 14,

[3GPe] 3GPP, «General packet radio service (gprs) enhancements for evolved universal terrestrial radio access network (e-utran) access», *3GPP TS 23.401*, vol. V16.12.0 Release 16,

[3GPf] 3GPP, «Numbering, addressing and identification», *3GPP TS 23.003*, vol. V16.4.0 Release 16,

[3GPg] 3GPP, «Radio access architecture and interfaces», *3GPP TS 38.801*, vol. V2.0.0 Release 14,

[3GPh] 3GPP, «Security architecture and procedures for 5g system», *3GPP TS 33.501*, vol. V15.12.0 Release 15,

[3GPi] 3GPP, «System architecture for the 5g system (5gs)», *3GPP TS 23.501*, vol. V16.11.0 Release 16,

[3GPj] 3GPP, «Terrestrial trunked radio (tetra); voice plus data (v+d); part 7: Security», *ETSI EN 300 392-7*, vol. V2.1.1,

[3GPk] 3GPP, «Universal mobile telecommunications system (umts); lte; 5g; non-access-stratum (nas) protocol for evolved packet system (eps); stage 3», *3GPP TS 24.301*, vol. V16.8.0 Release 16,

[App] Apple, *Lose your knack for losing things.* [Online]. Available: https://www.apple.com/airtag/ (last visited: Jun. 5, 2022).

[App21a] Apple, *Use private wi-fi addresses on iphone, ipad, ipod touch, and apple watch*, Nov. 2021. [Online]. Available: https://support.apple.com/en-us/HT211227.

[App21b] Apple, «Wi-fi privacy», Feb. 2021. [Online]. Available: https://support.apple.com/en-gb/guide/security/secb9cb3140c/web (last visited: Jun. 4, 2022).

[App22] Apple, «Use bluetooth and wi-fi in control center», Jan. 2022. [Online]. Available: https://support.apple.com/en-us/HT208086 (last visited: Jun. 1, 2022).

[BDH+18] D. Basin, J. Dreier, *et al.*, «A formal analysis of 5g authentication», pp. 1383–1396, 2018. [Online]. Available: https://doi.org/10.1145/3243734.3243846.

[BHPS19] R. Borgaonkar, L. Hirschi, *et al.*, «New privacy threat on 3g, 4g, and upcoming 5g aka protocols», *Proceedings on Privacy Enhancing Technologies*, vol. 2019, no. 3, pp. 108–127, 2019. [Online]. Available: https://doi.org/10.2478/popets-2019-0039.

[BKP17] C. Bouras, A. Kollia, and A. Papazois, «Sdn amp; nfv in 5g: Advancements and challenges», pp. 107–111, 2017. [Online]. Available: https://ieeexplore.ieee.org/document/7899398.

[Blu21] Bluetooth, *Bluetooth technology and the response to the covid-19 pandemic*, 2021. [Online]. Available: https://www.bluetooth.com/bluetooth-resources/bluetooth-technology-and-the-response-to-the-covid-19-pandemic/.

[Bor20] S. Borra, «Covid-19 apps: Privacy and security concerns», *Intelligent Systems and Methods to Combat Covid-19*, A. Joshi, N. Dey, and K. C. Santosh, Eds., pp. 11–17, 2020. [Online]. Available: https://doi.org/10.1007/978-981-15-6572-4_2.

[CGP+20] M. Cominelli, F. Gringoli, *et al.*, «Even black cats cannot stay hidden in the dark: Full-band de-anonymization of bluetooth classic devices», *2020 IEEE Symposium on Security and Privacy (SP)*, pp. 534–548, 2020. [Online]. Available: https://ieeexplore.ieee.org/document/9152700.

[CKB12] M. Cunche, M. A. Kaafar, and R. Boreli, «I know who you will meet this evening! linking wireless devices using wi-fi probe requests», pp. 1–9, 2012.

[CPK+14] J. Classen, M. Pfeiffer, *et al.*, «Analyzing tetra location privacy and network availability», *ACM*, pp. 117–122, Oct. 2014. [Online]. Available: https://dl.acm.org/doi/pdf/10.1145/2994459.2994463.

[CRPH21] M. Chlosta, D. Rupprecht, *et al.*, «5g suci-catchers: Still catching them all?», pp. 359–364, 2021. [Online]. Available: https://doi.org/10.1145/3448300.3467826.

[Cun14] M. Cunche, «I know your mac address: Targeted tracking of individual using wi-fi», *Journal of Computer Virology and Hacking Techniques*, no. 4, pp. 219–227, Nov. 2014. [Online]. Available: https://doi.org/10.1007/s11416-013-0196-1.

[DPČ19] A. Dagelić, T. Perković, and M. Čagalj, «Location privacy and changes in wifi probe request based connection protocols usage through years», *2019 4th International Conference on Smart and Sustainable Technologies (SpliTech)*, pp. 1–5, 2019.

[DSBa] DSB, *Hva er nødnett?* [Online]. Available: https://www.nodnett.no/om-nodnett/hva-er-nodnett/ (last visited: Feb. 4, 2022).

[DSBb] DSB, *Nødnettdekning*. [Online]. Available: https://www.nodnett.no/om-nodnett/nodnettdekning/ (last visited: Jun. 12, 2022).

[DSBc] DSB, *Startside | nødnett*. [Online]. Available: https://www.nodnett.no/ (last visited: Jun. 2, 2022).

[DSB17] DSB, *Neste generasjon nødnett i kommersielle nett*, Oct. 2017. [Online]. Available: https://www.dsb.no/globalassets/dokumenter/nyheter/neste-generasjon-nodnett-i-kommersielle-nett---fremgangsmate-for-videre-arbeid.pdf (last visited: Jun. 2, 2022).

[DSB18] DSB, *Alternatives for mission-critical services in public mobile networks in norway*, May 2018. [Online]. Available: https://www.nodnett.no/siteassets/bibliotek/rapporter/20180503-conceptual-models-for-ngn-v1.0.pdf (last visited: May 12, 2022).

[DSB20] DSB, *Nødnett i bruk*, Jun. 2020. [Online]. Available: https://www.nodnett.no/siteassets/bibliotek/brukerveiledninger/nodnett-i-bruk-2020.pdf (last visited: Jun. 12, 2022).

[Dua13] S. Duan, «Security analysis of tetra», Jun. 2013. [Online]. Available: https://ntnuopen.ntnu.no/ntnu-xmlui/bitstream/handle/11250/262890/656471_FULLTEXT01.pdf.

[Ele] Electronic-Notes, *Ieee 802.11a wi-fi standard*. [Online]. Available: https://www.electronics-notes.com/articles/connectivity/wifi-ieee-802-11/802-11a.php (last visited: Jun. 5, 2022).

[ETS] ETSI, *Tetra*. [Online]. Available: https://www.etsi.org/technologies/tetra.

[Fira] First Responder Network Authority, *Firstnet authority*. [Online]. Available: https://www.firstnet.gov/ (last visited: Mar. 14, 2022).

[Firb] FirstNet, «Phones & devices», [Online]. Available: https://www.firstnet.com/devices/phones.html (last visited: Jun. 1, 2022).

[Fon20] S. Fonyi, «Overview of 5g security and vulnerabilities», *The Cyber Defense Review*, vol. 5, no. 1, pp. 117–134, 2020. [Online]. Available: https://www.jstor.org/stable/26902666.

[Fre15] J. Freudiger, «How talkative is your mobile device? an experimental study of wi-fi probe requests», *Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks*, 2015. [Online]. Available: https://doi.org/10.1145/2766498.2766517.

[GP09] P. Golle and K. Partridge, «On the anonymity of home/work location pairs», *Pervasive Computing*, H. Tokuda, M. Beigl, *et al.*, Eds., pp. 390–397, 2009.

[GSCC20] S. Gerke, C. Shachar, *et al.*, «Regulatory, safety, and privacy concerns of home monitoring technologies during covid-19», 2020. [Online]. Available: https://www.nature.com/articles/s41591-020-0994-1.

[GSM] GSMA, *Representing the worldwide mobile communications industry*. [Online]. Available: https://www.gsma.com/.

[HBH22] A. Heinrich, N. Bittner, and M. Hollick, «Airguard - protecting android users from stalking attacks by apple find my devices», *WiSec '22: Proceedings of the 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, Mar. 2022. [Online]. Available: https://dl.acm.org/doi/abs/10.1145/3507657.3528546.

[HBK18] B. Hong, S. Bae, and Y. Kim, «Guti reallocation demystified: Cellular location tracking with changing temporary identifier», *Network and Distributed Systems Security*, 2018. [Online]. Available: http://dx.doi.org/10.14722/ndss.2018.23349.

[HCMB18] S. R. Hussain, O. Chowdhury, *et al.*, «Lteinspector: A systematic approach for adversarial testing of 4g lte», *Network and Distributed Systems Security*, Feb. 2018. [Online]. Available: http://dx.doi.org/10.14722/ndss.2018.23313.

[HEC+] S. R. Hussain, M. Echeverria, *et al.*, «Privacy attacks to the 4g and 5g cellular paging protocols using side channel information», *Network and Distributed Systems Security (NDSS) Symposium 2019*,

[HEK+19] S. R. Hussain, M. Echeverria, *et al.*, «5greasoner: A property-directed security and privacy analysis framework for 5g cellular network protocol», *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, pp. 669–684, 2019. [Online]. Available: https://doi.org/10.1145/3319535.3354263.

[IEE] IEEE, *Standard group mac addresses: A tutorial guide*. [Online]. Available: https://standards.ieee.org/wp-content/uploads/import/documents/tutorials/macgrp.pdf (last visited: Jun. 2, 2022).

[IEE21] IEEE, *802.11-2020 - ieee standard for information technology–telecommunications and information exchange between systems - local and metropolitan area networks–specific requirements - part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications*, 2021. [Online]. Available: https://ieeexplore.ieee.org/document/9363693.

[IET] IETF, *The network access identifier*. [Online]. Available: https://www.rfc-editor.org/rfc/rfc7542.

[IET22] IETF, *Mac address randomization*, Mar. 2022. [Online]. Available: https://www.ietf.org/id/draft-ietf-madinas-mac-address-randomization-01.html.

[ISO91] ISO, «Information technology — open systems interconnection — local area networks — medium access control (mac) service definition», May 1991.

[ITU] ITU, «The international public telecommunication numbering plan», *SERIES E: OVERALL NETWORK OPERATION, TELEPHONE SERVICE, SERVICE OPERATION AND HUMAN FACTORS*, vol. E.164, [Online]. Available: https://www.itu.int/rec/T-REC-E.164-201011-I/en.

[KM20] H. Khan and K. M. Martin, «A survey of subscription privacy on the 5g radio interface - the past, present and future», *Journal of Information Security and Applications*, vol. 53, p. 102 537, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2214212620300235.

[KS19] U. N. Kar and D. K. Sanyal, «A critical review of 3gpp standardization of device-to-device communication in cellular networks», *SN Computer Science*, vol. 1, 2019.

[LHC+20] G. Liu, Y. Huang, *et al.*, «5g deployment: Standalone vs. non-standalone from the operator perspective», *IEEE Communications Magazine*, vol. 58, no. 11, pp. 83–89, 2020.

[Mat17] C. Matte, «Wi-fi tracking : Fingerprinting attacks and counter-measures», 2017. [Online]. Available: https://tel.archives-ouvertes.fr/tel-01921596.

[MCRV16] C. Matte, M. Cunche, *et al.*, «Defeating mac address randomization through timing attacks», *Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks*, pp. 15–20, 2016. [Online]. Available: https://doi.org/10.1145/2939918.2939930.

[MH21] R. Mac and K. Hill, *Are apple airtags being used to track people and steal cars?*, 2021. [Online]. Available: https://www.nytimes.com/2021/12/30/technology/apple-airtags-tracking-stalking.html.

[Mil] J. Miller, *City of london calls halt to smartphone tracking bins.* [Online]. Available: https://www.bbc.com/news/technology-23665490.

[MMD+17] J. Martin, T. Mayberry, *et al.*, «A study of mac address randomization in mobile devices and when it fails», 2017. [Online]. Available: https://arxiv.org/abs/1703.02874.

[MN21] J. P. Mattsson and P. K. Nakarmi, «Nori: Concealing the concealed identifier in 5g», *CoRR*, vol. abs/2105.10440, 2021. [Online]. Available: https://arxiv.org/abs/2105.10440.

[MO17] S. F. Mjølsnes and R. F. Olimid, «Easy 4g/lte imsi catchers for non-programmers», pp. 235–246, 2017.

[Mot] Motorola, *Motorola - home.* [Online]. Available: https://www.motorola.com/us/ (last visited: Jun. 2, 2022).

[MOT20] MOTOROLA SOLUTIONS, «Mtp3000 series tetra radios», May 2020. [Online]. Available: https://www.radiocoms.co.uk/wp-content/uploads/2020/05/motorola-mtp3000-data-sheet.pdf.

[MP18] E. Markakis and I. Politis, «5g emergency communications», 2018. [Online]. Available: https://futurenetworks.ieee.org/images/files/pdf/applications/Emergency-Communications030518.pdf.

[NKO21] NKOM, *Mens vi venter på 5g-utbyggingen – norge på femteplass i europa*, Nov. 2021. [Online]. Available: https://www.nkom.no/aktuelt/mens-vi-venter-pa-5g-utbyggingen--norge-pa-femteplass-i-europa (last visited: May 29, 2022).

[NND16] K. Norrman, M. Näslund, and E. Dubrova, «Protecting imsi and user privacy in 5g networks», MobiMedia '16, pp. 159–166, 2016.

[Nom] K. Nomeland, *Sikker mobilkommunikasjon i forsvaret.* [Online]. Available: http://www.mobilagenda.no/wp-content/uploads/04_FMA_Mobil_Agenda_Nomeland.pdf (last visited: May 29, 2022).

[OCL+17] J. Oueis, V. Conan, *et al.*, «Overview of lte isolated e-utran operation for public safety», *IEEE Communications Standards Magazine*, vol. 1, no. 2, pp. 98–105, 2017.

[PCB+17] A.-C. Petre, C. Chilipirea, *et al.*, «Chapter 14 - wifi tracking of pedestrian behavior», *Smart Sensors Networks*, pp. 309–337, 2017. [Online]. Available: https://www.sciencedirect.com/science/article/pii/B9780128098592000188.

[PGBB21] I. Palamà, F. Gringoli, *et al.*, «Imsi catchers in the wild: A real world 4g/5g assessment», *Computer Networks*, vol. 194, p. 108 137, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1389128621002061.

[PHT11] A. Pfitzmann, M. Hansen, and H. Tschofenig, «Terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management», Feb. 2011. [Online]. Available: https://datatracker.ietf.org/doc/html/draft-hansen-privacy-terminology-01.

[PKR10] Y.-S. Park, C.-S. Kim, and J.-C. Ryou, «The vulnerability analysis and improvement of the tetra authentication protocol», vol. 2, pp. 1469–1473, 2010. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/5440307.

[Qua] Qualcomm, *5g mmwave helps realize significant return on investment.* [Online]. Available: https://www.qualcomm.com/research/5g/5g-nr/mmwave (last visited: Jun. 2, 2022).

[RKHP19] D. Rupprecht, K. Kohls, *et al.*, «Breaking lte on layer two», pp. 1121–1136, 2019.

[RM16] C. Robson and K. McCartan, *Real World Research*, ser. 4. Edition. Wiley, United Kingdom, 2016.

[Sam20] Samsung, «What is the "turn on wi-fi automatically" feature?», Oct. 2020. [Online]. Available: https://www.samsung.com/my/support/mobile-devices/what-is-the-turn-on-wi-fi-automatically-feature/ (last visited: Jun. 1, 2022).

[SBA+15] A. Shaik, R. Borgaonkar, *et al.*, «Practical attacks against privacy and availability in 4g/lte mobile communication systems», *CoRR*, 2015. [Online]. Available: http://arxiv.org/abs/1510.07563.

[SBPS19] A. Shaik, R. Borgaonkar, *et al.*, «New vulnerabilities in 4g and 5g cellular access network protocols: Exposing device capabilities», WiSec '19, pp. 221–231, 2019. [Online]. Available: https://doi.org/10.1145/3317549.3319728.

[Sca] Scapy, *Scapy: Interactive packet manipulation tool.* [Online]. Available: https://pypi.org/project/scapy/ (last visited: Jun. 9, 2022).

[SMS+16] J. Scheuner, G. Mazlami, *et al.*, «Probr - a generic and passive wifi tracking system», *2016 IEEE 41st Conference on Local Computer Networks (LCN)*, pp. 495–502, 2016.

[SNMB10] N. Seddigh, B. Nandy, *et al.*, «Security advances and challenges in 4g wireless networks», pp. 62–71, 2010.

[Sou] South Korea government, *Disaster and safety communications network (korea safe-net)*. [Online]. Available: https://mois.go.kr/eng/sub/a03/bestPractices7/screen.do (last visited: May 29, 2022).

[Syv20] S. A. Syverud, «Security of next generation emergency communication in norway», Jun. 2020.

[Sør17] C. Sørseth, «Location disclosure in lte networks by using imsi catcher», Jun. 2017. [Online]. Available: https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/2462189.

[Tel] Telenor, *Utbygging 2020*. [Online]. Available: https://www.telenor.no/privat/artikler/dekning/utbygging-2020/ (last visited: Jun. 2, 2022).

[The] The Tcpdump Group, *Home | tcpdump*. [Online]. Available: https://www.tcpdump.org/ (last visited: Jun. 9, 2022).

[UCF+20] M. Uras, R. Cossu, *et al.*, «Wifi probes sniffing: An artificial intelligence based approach for mac addresses de-randomization», *2020 IEEE 25th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*, pp. 1–6, 2020.

[UK 22] UK government, *About the emergency services network*, Apr. 2022. [Online]. Available: https://www.gov.uk/government/publications/the-emergency-services-mobile-communications-programme/emergency-services-network (last visited: May 29, 2022).

[Val] M. Valle, *Netcom lanserte 4g*. [Online]. Available: https://www.tu.no/artikler/netcom-lanserte-4g/229959 (last visited: Mar. 21, 2022).

[Var21] S. Varhaugvik, «Privacy analysis of next generation emergency communication network devices in norway», *Project Topic Paper*, Nov. 2021.

[VMC+16] M. Vanhoef, C. Matte, *et al.*, «Why mac address randomization is not enough: An analysis of wi-fi network discovery mechanisms», *Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security*, ASIA CCS '16, pp. 413–424, 2016. [Online]. Available: https://doi.org/10.1145/2897845.2897883.

[Wi-a] Wi-Fi Alliance, *Discover wi-fi enterprise*. [Online]. Available: https://www.wi-fi.org/discover-wi-fi/enterprise (last visited: May 21, 2022).

[Wi-b] Wi-Fi Alliance, *Wi-fi alliance*. [Online]. Available: https://www.wi-fi.org/ (last visited: Jun. 9, 2022).

[Wi-c] Wi-Fi Alliance, *Wi-fi easymesh*. [Online]. Available: https://www.wi-fi.org/discover-wi-fi/wi-fi-easymesh (last visited: Jun. 5, 2022).

[Wi-20] Wi-Fi Alliance, *Wi-fi protected setup protocol and usability best practices, 2.0.2*, Nov. 2020. [Online]. Available: https://www.wi-fi.org/download.php?file=/sites/default/files/private/Wi-Fi_Protected_Setup_Best_Practices_v2.0.2.pdf (last visited: Jun. 2, 2022).

[Wig] Wigle, *All the networks. found by everyone*. [Online]. Available: https://wigle.net/ (last visited: Jun. 2, 2022).

[Wir] Wireshark, *Wireshark · go deep.* [Online]. Available: https://www.wireshark.org/ (last visited: Jun. 9, 2022).

[WK16] O. Waltari and J. Kangasharju, «The wireless shark: Identifying wifi devices based on probe fingerprints», *MobiData '16: Proceedings of the First Workshop on Mobile Data*, pp. 1–6, Jun. 2016.

Sigurd Varhaugvik

Privacy Analysis of Next Generation Emergency Communication Network Devices in Norway

NTNU
Norwegian University of
Science and Technology