Department of Computer Science

# Intelligent Security for 5G Networks and Beyond

## Enablers of Customized Active Defenses for Mobile Communication Applications

Jani Suomalainen

Aalto University

DOCTORAL THESES

Aalto University publication series
**DOCTORAL THESES** 35/2022

# Intelligent Security for 5G Networks and Beyond

## Enablers of Customized Active Defenses for Mobile Communication Applications

**Jani Suomalainen**

A doctoral dissertation completed for the degree of Doctor of Science (Technology) to be defended, with the permission of the Aalto University School of Science, at a public examination held at the lecture hall TU1 of the school on 28th March 2022 at 12 noon.

**Aalto University**
**School of Science**
**Department of Computer Science**

**Supervising professor**
Professor Tuomas Aura, Aalto University, Finland

**Thesis advisors**
Professor Tuomas Aura, Aalto University, Finland
Professor Aarne Mämmelä, VTT Technical Research Centre of Finland, Finland

**Preliminary examiners**
Professor Andrei Gurtov, Linköping University, Sweden
Professor Alf Zugenmaier, Munich University of Applied Sciences, Germany

**Opponent**
Professor Simone Fischer-Hübner, Karlstads University, Sweden

Aalto University publication series
**DOCTORAL THESES** 35/2022



ISBN 978-952-64-0722-7 (printed)
ISBN 978-952-64-0723-4 (pdf)
ISSN 1799-4934 (printed)
ISSN 1799-4942 (pdf)
http://urn.fi/URN:ISBN:978-952-64-0723-4

Unigrafia Oy
Helsinki 2022

Finland

NORDIC SWAN ECOLABEL
Printed matter
4041-0619

Aalto University

# Abstract

Aalto University, P.O. Box 11000, FI-00076 Aalto www.aalto.fi

**Author**
Jani Suomalainen

**Name of the doctoral thesis**
Intelligent Security for 5G Networks and Beyond - Enablers of Customized Active Defenses for Mobile Communication Applications

**Publisher** School of Science

**Unit** Department of Computer Science

**Series** Aalto University publication series DOCTORAL THESES 35/2022

**Field of research** Telecommunications software

**Manuscript submitted** 8 October 2021 **Date of the defence** 28 March 2022

**Permission for public defence granted (date)** 7 January 2022 **Language** English

☐ **Monograph** ☒ **Article thesis** ☐ **Essay thesis**

**Abstract**

The evolution of security in mobile communication networks is driven by vulnerabilities in previous generations, the need to address insider threats, diverse requirements from different user sectors, as well as opportunities and challenges arising from the emerging technologies. For new users, such as industry and public safety authorities, transitions from own dedicated network infrastructures to commercial networks and 3GPP-based technologies mean large changes also from the security perspective. The transition enables cost-efficiency and new user applications but changes the threat landscape and increases the risks of disturbances and information leaking due to adversaries who are sharing the infrastructure. To manage the growing complexity and threat landscape, intelligent and active defense solutions are needed. Intelligent security means the capability to achieve security goals in different situations with the optimal use of resources. Active defense means the capability to make attacks harder with dynamic network and security measures. Intelligent security requires solutions to collect and share information, analyze the security situation and react accordingly. The tools for intelligent security include artificial intelligence and machine learning, which provide rapid means to react against previously unseen threats but which may also open up new vulnerabilities.

This dissertation explores requirements and solutions for customizing network security for different applications and for enabling active defenses. The dissertation includes articles, which analyze selected concepts and enablers for intelligent security. Literature analyses focus on special challenges in communications for public safety authorities as well as new threats arising from the use of machine learning. The enablers include micro-segmentation, which is a method for creating fine-grained logical network slices on top of a shared infrastructure. A designed intelligent security approach for micro-segmentation is based on software networks and continuous learning. Adaptive pseudonymization is an example of the use of real-time threat analysis to adapt active security and privacy defenses. Tactical bubbles are rapidly deployable networks, which are targeted for public safety users and which can be isolated from the commercial infrastructure by logical and physical solutions. The explored use cases provide examples of how the security of mobile communication networks can be adapted to fulfill the needs of different applications and how security resources can be focused on security-critical communications.

**Keywords** mobile network, cybersecurity, customization, intelligence

**ISBN (printed)** 978-952-64-0722-7 **ISBN (pdf)** 978-952-64-0723-4

**ISSN (printed)** 1799-4934 **ISSN (pdf)** 1799-4942

**Location of publisher** Helsinki **Location of printing** Helsinki **Year** 2022

**Pages** 192 **urn** http://urn.fi/URN:ISBN:978-952-64-0723-4

Aalto-yliopisto

# Tiivistelmä

**Aalto-yliopisto, PL 11000, 00076 Aalto** www.aalto.fi

**Tekijä**
Jani Suomalainen

**Väitöskirjan nimi**
Älykäs tietoturva viidennen ja tulevien sukupolvien verkoissa - mahdollistajia mobiiliviestinnän sovelluskohtaiselle aktiiviselle puolustukselle

**Julkaisija** Perustieteiden korkeakoulu

**Yksikkö** Tietotekniikan laitos

**Sarja** Aalto University publication series DOCTORAL THESES 35/2022

**Tutkimusala** Tietoliikenneohjelmistot

**Käsikirjoituksen pvm** 08.10.2021 **Väitöspäivä** 28.03.2022

**Väittelyluvan myöntämispäivä** 07.01.2022 **Kieli** Englanti

☐ **Monografia** ☒ **Artikkeliväitöskirja** ☐ **Esseeväitöskirja**

**Tiivistelmä**

Matkapuhelinverkkojen tietoturvan evoluutiota ajavat aikaisemmissa sukupolvissa havaitut heikkoudet, tarve puolustaa verkkoja myös sisäisiä uhkia vastaan, eri käyttäjäryhmien hyvin erilaiset tietoturvatarpeet sekä uusien teknologioiden tuomat mahdollisuudet ja haasteet. Uusille käyttäjille, kuten omia verkkoinfrastruktuureitaan aiemmin ylläpitäneille teollisuudelle ja viranomaisille, siirtymä kaupallisiin verkkoihin ja 3GPP:n määrittelemiin matkapuhelinteknologioihin on suuri muutos tietoturvanäkökulmasta. Kustannushyötyjen ja uusien sovellusten vastapainoksi tulevat uhat häiriöistä ja tiedon vuotamisesta kaupallisen verkon kautta ilmaantuvien hyökkäyksien takia. Kasvaneiden kompleksisuuden ja uhkakentän hallintaan tarvitaan älykkäitä ja aktiivisia puolustuskeinoja. Älykäs tietoturva tarkoittaa kykyä saavuttaa tietoturvatavoitteita eri ympäristöissä ja optimaalisilla resursseilla. Aktiivinen puolustus tarkoittaa kykyä vaikeuttaa hyökkääjän toimintaa muuttuvilla verkko- ja tietoturvakeinoilla. Älykkyys ja aktiivisuus vaativat kykyä kerätä ja jakaa tietoa, analysoida tietoturvatilannetta sekä reagoida uhkiin sopivalla tavalla. Älykkään tietoturvan työkaluihin kuuluvat tekoäly ja koneoppiminen, jotka mahdollistavat nopean reagoimisen ennen näkemättömiin uhkiin mutta voivat myös aiheuttaa uusia heikkouksia.

Tässä väitöskirjassa tutkitaan vaatimuksia ja ratkaisuja verkkojen tietoturvan sovelluskohtaiseen sopeuttamiseen ja aktiiviseen puolustamiseen. Väitöskirja koostuu artikkeleissa, joissa analysoidaan valittuja käsitteitä ja mahdollistajia älykkääseen tietoturvaan. Kirjallisuusanalyyseissa paneudutaan erityisesti viranomaiskommunikaation erityishaasteisiin ja koneoppimisen luomiin uusiin uhkakuviin. Suunniteltuihin mahdollistajiin kuuluu mikro-segmentointi, joka on menetelmä luoda hienojakoisia samaa verkkoinfrastruktuuria hyödyntäviä loogisia verkkoviipaleita. Sen yhteyteen toteutettiin ohjelmistoverkkoihin ja jatkuvaan oppimiseen perustuva tietoturvaratkaisu. Adaptiivinen pseudonymisointi on esimerkki reaaliaikaisesta tietoturva-analyysiin perustuvasta aktiivisesta verkkopuolustuksesta, jossa arvioitu uhka käyttäjien identiteetin paljastumisesta säätelee suojausmekanismia. Taktinen kupla on viranomaiskäyttöön tarkoitettu nopeasti käyttöön otettava verkko, joka voidaan eristää kaupallisen verkon muusta liikenteestä fyysisin ja loogisin keinoin. Tutkitut tapaukset luovat esimerkkejä, kuinka matkapuhelinverkkojen tietoturvaa voidaan säätää sovelluksen tarpeiden mukaiseksi ja kuinka tietoturvaresursseja voidaan kohdistaa tietoturvakriittiseen kommunikaatioon.

**Avainsanat** matkaviestinverkko, kyberturva, sovelluskohtaisuus, älykkyys

**ISBN (painettu)** 978-952-64-0722-7 **ISBN (pdf)** 978-952-64-0723-4

**ISSN (painettu)** 1799-4934 **ISSN (pdf)** 1799-4942

**Julkaisupaikka** Helsinki **Painopaikka** Helsinki **Vuosi** 2022

**Sivumäärä** 192 **urn** http://urn.fi/URN:ISBN:978-952-64-0723-4

This dissertation is dedicated to Katriina, my radiant, and amazing daughter, who loves stories, bursts soap bubbles, and practices resilience with anything resembling a trampoline.

# Preface

"Gold flakes! He's on the trail of the philosopher's stone, too!"
—Scrooge McDuck [22]

Artificial intelligence and new generations of mobile networks have generated substantial research efforts. There are lots of hype and promise but also criticism and disbelief. It is the role of us researchers to explore the nature and significance of emerging technologies and explain whether we will be seeing an evolution with small improvements and optimizations or whether the concepts have the potential to revolutionize the world. As in the story—The Fabulous Philosopher's Stone [22]—we may be able to find our "philosopher's stones" and turn "metal into gold" but the things we discover may also be unexpected and dangerous. Hence, it is also the responsibility of us cybersecurity professionals to develop these concepts to be safe and secure.

When I started my post-graduate studies, I did not like the common view that the end-users must be responsible for their cybersecurity and that they must continuously learn new skills and increase their security awareness. Instead, I have always felt that technology should solve problems, not cause new ones. The security should be provided by systems transparently for the end-users. This has lead me sometimes to consider how products, services, and networks could be more security aware and smart, and take this responsibility away from the users. My trail towards the dissertation has been a long and winding but it also has been my own and personal. While carrying out customer and project work on various topics, finding a common theme for the dissertation was not an easy task. During, my career I have studied, for instance, platform and device security, software security, cryptography, and network security from physical to application layers. Eventually, the common thread to my dissertation emerged from projects focusing to the security of 5G networks. The results included in this dissertation are part of the work done at VTT Technical Research Centre of Finland in two EU-funded and in one Business Finland-funded joint research projects: District of Future, 5G-ENSURE, and PRIORITY.

VTT is a fine organization and provided me with the opportunity to finalize this dissertation.

I would like to thank the personnel at Aalto University and my colleagues at VTT. I am not going to list you all. Professor Tuomas Aura supervised my post-graduate studies and gave feedback that improved the quality of my dissertation greatly. Professor Aarne Mämmelä encouraged me to finally finish my studies and gave excellent feedback. Arto Juhola, Jukka Julku, Juha Koivisto, Markku Kylänpää, Juha Pärssinen, and Aarne Rantala have given me lots of inspiring ideas during our lunch breaks. Hanna Jokisalo gave peer support on my study path and commented the dissertation. Doctor Ijaz Ahmad demonstrated a catching enthusiasm for writing and publishing and also gave good feedback. Kimmo Ahola's wizardry with networks enabled building and testing of overlaying security features, which are described in the attached publications. Professor N. Asokan gave great lessons when writing my first journal article. Professor Kimmo Halunen once said that a dissertation is not a magical charm that gives its writer a supernatural capability for making science.

Finally, I would like to thank and mention some important members of my family—present and past—Lea, Seppo, Timo, Laura, Diana, Aini, Maire, Mailis, and Katriina.

Espoo, February 19, 2022,

Jani Suomalainen

# Contents

# List of Publications

This dissertation consists of an overview and of the following publications, which are referred to in the text by their Roman numerals.

**I** Ijaz Ahmad, Jani Suomalainen, Jyrki Huusko. 5G-Core Network Security. *Wiley 5G Ref: The Essential 5G Reference Online*, 2019.

**II** Jani Suomalainen, Jukka Julku, Mikko Vehkaperä, Harri Posti. Securing Public Safety Communications on Commercial and Tactical 5G Networks: A Survey and Future Research Directions. *IEEE Open Journal of the Communications Society*, vol. 2, pp. 1590-1615, 2021.

**III** Olli Mämmelä, Jani Suomalainen, Kimmo Ahola, Pekka Ruuska, Mikko Majanen, Mikko Uitto. Micro-Segmenting 5G. In *the 3rd International Conference on Internet of Things, Big Data and Security (IoTBDS 2018)*, Funchal, Madeira, Portugal, pp. 17-28, March 2018.

**IV** Jani Suomalainen, Kimmo Ahola, Mikko Majanen, Olli Mämmelä, Pekka Ruuska. Security Awareness in Software-Defined Multi-Domain 5G Networks. *Future Internet*, vol. 10, no. 27, pp. 914-927, MDPI, 2018.

**V** Jani Suomalainen, Jukka Julku. Enhancing Privacy of Information Brokering in Smart Districts by Adaptive Pseudonymization. *IEEE Access*, vol. 4, pp. 914-927, 2016.

**VI** Jani Suomalainen, Arto Juhola, Shahriar Shahabuddin, Aarne Mämmelä, Ijaz Ahmad. Machine Learning Threatens 5G Security. *IEEE Access*, vol. 8, pp. 190822-190842, 2020.

# Author's Contribution

### Publication I: "5G-Core Network Security"

The book chapter surveys central features and enabling technologies for security in 5G-core networks. The author was the main contributor of the parts which describe the security of essential 3GPP functions and interfaces as well as the security of network virtualization. The initiative for writing the survey came from Ijaz Ahmad.

### Publication II: "Securing Public Safety Communications on Commercial and Tactical 5G Networks: A Survey and Future Research Directions"

The journal article surveys security requirements, adaptation needs, and solutions for private and commercial mobile networks that are utilized by the public safety organizations. The author was the main contributor of the survey parts. He provided the analysis framework, threat scenarios, and solution survey and contributed to the future research direction part. He also supported in defining the trialed security solutions.

### Publication III: "Micro-Segmenting 5G"

The conference paper introduces a fine-grained network slicing approach, its enablers, and use cases. The author participated in the definition of the micro-segmentation concept and architecture. He implemented the security monitoring and trust metric enablers as well as participated in the use case definition and analysis. Olli Mämmelä explored the concept of micro-segmentation, and Kimmo Ahola implemented the SDN enabler and the alternative authentication use case.

### Publication IV: "Security Awareness in Software-Defined Multi-Domain 5G Networks"

The journal article describes a security monitoring and security information sharing approach for software-defined networks. The author designed and implemented the enablers for security monitoring, for security event correlation and analysis, as well as for anomaly detection. He specified the use cases and performed the data analysis. He was also the main contributor for the introduction, related work, discussion and conclusions sections. Kimmo Ahola developed the SDN enabler, and Mikko Majanen collected data from the test network.

### Publication V: "Enhancing Privacy of Information Brokering in Smart Districts by Adaptive Pseudonymization"

The journal article explores the security of information sharing within smart cities using a brokering approach. The author proposed the concept of adaptive pseudonymization for enhancing privacy and enforcing access control. He implemented the adversarial algorithm for analyzing the need to trigger re-pseudonymization. He also described the smart city use case, platform, and security architecture. Jukka Julku provided and processed smart city data.

### Publication VI: "Machine Learning Threatens 5G Security"

The journal article surveys and analyzes the security threats and solutions that will emerge for 5G networks and beyond alongside machine learning. The idea for the paper came from Ijaz Ahmad. The author was the main contributor for the sections analyzing threats in ML use cases, describing attacks, as well as surveying security solutions. He also contributed to the description of future research directions.

### Language check

The language of the dissertation has been checked by Lingsoft. The author has personally examined and accepted/rejected the results of the language check one by one. This has not affected the scientific content of the dissertation.

# Abbreviations

**3GPP** Third Generation Partnership Project

**5G** The Fifth Generation Technology Standard for Mobile Networks

**5G-PPP** The 5G Infrastructure Public Private Partnership

**AAA** Authentication, Authorization, and Accounting

**AI** Artificial Intelligence

**API** Application Programming Interface

**CSOC** Cybersecurity Operations Center

**CTI** Cyber Threat Intelligence

**DTLS** Datagram TLS

**E2E** End-to-End

**EAP-TLS** Extensible Authentication Protocol - Transport Layer Security

**ENI** Experiential Networked Intelligence

**eSIM** Embedded Subscriber Identity Module

**ETSI** European Telecommunications Standardization Institute

**GSMA** The GSM (Global System for Mobile Communications) Association

**HTTPS** Hypertext Transfer Protocol Secure

**IDS** Intrusion Detection System

**IoT** Internet of Things

**IPS** Intrusion Prevention System

**ITU-T** International Telecommunications Union – Telecommunications

**LTE** Long-Term Evolution - Fourth Generation Mobile Networks Standard

**NF** Network Function

**NGSI** Next Generation Service Interface

**MEC** Multi-Access Edge Computing

**MISP** Open Source Threat Intelligence and Sharing Platform

**ML** Machine Learning

**MC** Mission-Critical

**NFV** Network Function Virtualization

**O-RAN** Open RAN Initiative

**OpenID** Open Standard and Decentralized Authentication Protocol

**OpenIoC** Open Indicators of Compromise

**OMA** Open Mobile Alliance

**QoS** Quality of Service

**RAN** Radio Access Network

**RMON** Remote Network Monitoring

**RTSPS** Real Time Streaming Protocol over TLS

**SBA** Service Based Architecture

**SDN** Software-Defined Network

**SIEM** Security Information and Event Management

**SLA** Service Level Agreement

**SNMP** Simple Network Management Protocol

**SOAR** Security Orchestration, Automation and Response

**SRTP** Secure Real Time Protocol

**STIX** Structured Threat Information Expression

**TAXII** Trusted Automated Exchange of Indicator Information

**TCCA** The Critical Communications Association

**TLS** Transport Layer Security

**UE** User Equipment

**VNF** Virtual Network Function

# 1. Introduction

Mobile communication networks evolve with gradual upgrades. Currently we are on the verge of one major transition from the fourth generation to the fifth generation of mobile networking technologies, and the following evolution and subsequent generations are already being studied by the industry and scientific community. At the same time, the evolution of mobile technologies is revolutionizing communication solutions for various mission and business critical applications. Public safety, smart city, and industrial users, who have previously operated dedicated communication infrastructures with limited service and quality capabilities, will benefit from the improved quality and cost-efficiency of the 5G networks and beyond.

One major objective in technology development has been the need for increased automation and customization of the operators' service provisioning. At the same time, security solutions need to evolve to keep up with the development of network technologies, on one hand, and to keep up with the capabilities of attackers in the cyber and physical worlds, on the other hand. This dissertation explores the intersection between security, autonomy, and customization within 5G networks. The dissertation explores enablers—architectural concepts and software functions for network security, which make it possible—to evolve the intelligence of mobile network security.

## 1.1 Security Drivers in 5G and Beyond

The development of security for the fifth and for the consecutive generations of mobile networks is motivated by several drivers. The first major driver is the ***hardening evolution***. Security in 5G networks and beyond means patching of vulnerabilities [124, 96, 79, 78, 77] from the previous generations. Past mistakes and compromises are corrected and the new challenges from the emerging technologies are addressed. Security of the system components, protocols, and interfaces are hardened to increase the

trustworthiness of the devices and systems.

The second driver is the ***focus on insiders***. The previous generations of standards focused on external threats against the operator or the end-user and, hence, secured the interactions between the network and the user equipment. In 5G systems, more parties are cooperating to provide end-to-end service and, because of that, the trust models are changing [27]. Additionally, the adversaries and attacks have evolved, and strong fortifications at the network boundaries are no longer sufficient. Defenders must assume that advanced adversaries will compromise the system and will likely have insiders' positions, i.e., bridge-heads for attacks. Solutions are, hence, needed for controlling and isolating insiders and for enabling cooperation between parties that do not fully trust each other.

The third driver is the ***customization*** of security, which is needed as the users from industry and society are integrating their networks and new applications more closely with a shared commercial infrastructure. The security that the applications demand is more than just protecting end-to-end voice and data connections with an overlay of cryptography. The domain-specific security requirements are diverse and often contradictory. Typically, applications require confidentiality, authenticity and replay-protection for user-plane communication but also dependability, which is a factor involving several attributes [19], including reliability, availability, integrity, and maintainability. Solutions are needed, e.g., to support alternative radio access technologies, devices with restricted computing capabilities and energy resources, as well as applications with high security requirements. Security solutions need to support, or not disturb, services with different quality of service requirements, which are related, e.g., to latency, jitter, and throughput.

The fourth driver is the ***emergence of new technologies*** and the complexity and opportunities they bring. Network softwarization and virtualization [10, 14] provide flexibility to infrastructure deployment by enabling the use of a standard routing infrastructure instead of manufacturer-specific network equipment and by decoupling functionality from the hardware. Cloudification and multi-access edge computing (MEC) [150, 117] optimize the management of computing resources by allowing utilization of centralized, i.e., highly-scalable, as well as local, i.e., latency-minimizing, computational capacities. Artificial intelligence (AI) and machine learning (ML) [114, 66, 167] bring further advances to network management and, e.g., enable learning from the past experiences and adapting the use of resources (materials, energy, information, time, frequency, and space) [107] accordingly. From the security perspective, these emerging technologies will facilitate customization and differentiation of security services. They also increase the complexity, which is a major challenge for security in mobile networks. On the other hand, new technologies can also provide means to manage the complexity and to minimize security interference and infor-

mation leaking. For instance, with softwarization, we can achieve logical means to separate—to slice or micro-segment—different applications horizontally even though they share the same common infrastructure. With clouds and MECs, we get more opportunities to isolate different geographical network domains from each other into physically or logically separated application security realms, e.g., privacy-protecting edge, "tactical bubbles", or hardened cloud environments.

5G network security consists of several subareas. User equipment (UE) protects credentials, subscriber's data, and software integrity. Radio access network (RAN, between the UE and base station) and backhaul (between base stations and remote services) security provides confidentiality and authenticity of communication. Core network security provides of enabling functionality including authentication, authorization and accounting (AAA). Infrastructure, e.g., MEC and cloud, security protects the integrity and trustworthiness of the hardware hosting virtual and physical mobile network functions. Application and end-to-end security, provided by application providers or operators, ensure the protection of user data and user applications.

## 1.2 Intelligent Security and Active Defenses

Intelligence, in general, can be defined in many ways [100] including "*the capacity to acquire and apply knowledge*" [1], "*the ability to learn, understand and make judgments or have opinions that are based on reason*" [2], "*the capability of a system to adapt its behavior to meet its goals in a range of environments*" [55], "*achieving complex goals in complex environments*" [60], or a measurement of "*an agent's ability to achieve goals in a wide range of environments*" [100]. Recent definitions also include the use of resources as a part of the definition, e.g., "*behaving in the world so that you get exactly what you want, given the resources (physical and mental) available*" [138]. We define **intelligent security** as an agent's ***ability to achieve security goals in a wide range of environments with optimal use of resources***.

Intelligent security systems can be autonomous or directed by humans. Autonomous systems [21] use their capabilities to pursue goals without intervention, oversight, or control by any other agent. Autonomous [89] or self-adaptive network security [53, 154] systems sense and collect information from the network, analyze the data for security knowledge, and respond by changing the behavior of network. Figure 1.1 illustrates the central enablers of intelligent security as well as the central elements in the security of mobile networks. Information sensing and sharing, analytics, and response—the enablers in the management layer (also called the intelligent agent)—are connected to the security systems in the 5G

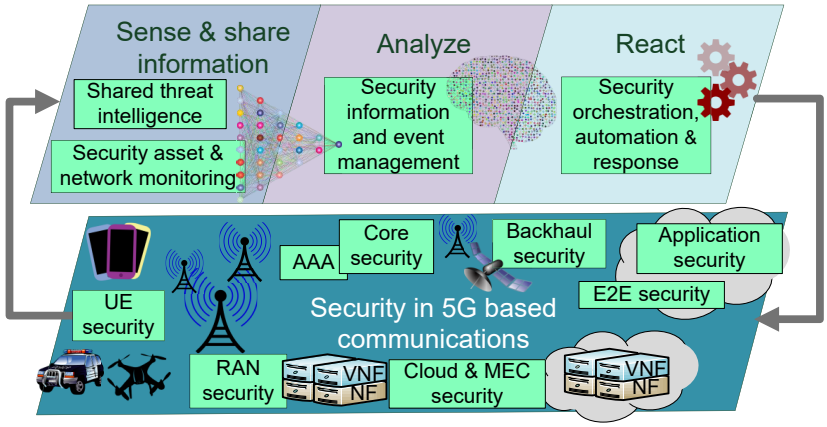


**Figure 1.1.** Elements of mobile network security with enablers for security adaptation in a separate layer.

network with a feedback loop.

Intelligent security can be distributed to different locations in 5G systems or centralized in cybersecurity operations centers (CSOC). CSOCs [169] are centralized units that monitor system behavior, traffic flows, and security posture in order to adapt the network behavior and to respond to attacks. CSOCs incorporate people, technologies, and processes to improve security and manage risks of the monitored systems. CSOCs collect information widely from different domains and strata of networks and also utilize shared security information and threat databases. They apply monitoring, analytics, visualizations and other tools to provide knowledge on the system security status and to enable decision making by human administrators.

Active defense [44], or **active cyber defense**, is a ***mechanism to destroy, nullify, or reduce the effectiveness of cyber-threats***. Active defense strategies are typically asymmetric, i.e., the adversarial action is different to the defense. Actions reducing effectiveness of threats include moving target defenses [133] and throttling potentially adversarial or low-priority traffic, which increase the costs of attacks. Actions to nullify threats include blocking or filtering adversarial data flows or removing devices from the network. Actions to destroy threats include preemptive [155] or reactive attacks against hostile persons or computers, for instance, to physically damage devices or corrupt software. Typical actions include the active collection of sharable information, e.g., by probing status information or deploying honeypots [121].

Particular security goals where intelligence is important are intrusion detection and intrusion prevention. Intrusion detection systems (IDS) [87, 102] monitor the network for malicious activity and policy violations. IDS systems with reactive preventive capabilities are often called as intrusion prevention systems (IPS). IDS and IPS systems can be seen as subsets of

two more recent concepts: security information and event management (SIEM) [29], as well as security orchestration, automation and response (SOAR) [81]. SIEM and SOAR systems provide a more holistic perspective of security awareness and responsiveness by combining intrusion alarms with other security information and controls, including security posture and security performance indicators.

Machine learning (ML) is a central enabler of autonomy and intelligence. ML comprises data analysis methods and is a branch of artificial intelligence (AI). An ML system learns from data, identifies patterns, and makes decisions with minimal human intervention after a possible training period. For network security applications [9, 20, 56], ML is beneficial for detecting known attacks as well as anomalies indicating threats such as previously unseen, so called zero-day, attacks. ML can analyze network equipment for malware, and traffic patterns and the transmitted data for network attacks. ML can also be utilized in solutions trying to test and find weaknesses in network interfaces and equipment.

## 1.3 About the Dissertation

This dissertation explores security monitoring and ML-based security algorithms as well as segregating architectural enablers as a mean to make mobile network security more intelligent and active. This dissertation consists of articles which contribute to scientific and technical knowledge via literature surveys, architectural analysis, as well as practical prototypes and experiments.

### 1.3.1 Objectives, Questions, and Methodology

The main objective of the dissertation is to explore a) security of emerging mobile networking technologies as well as b) emerging security technologies for mobile networks. In particular, the focus is on the needs of application domains and the trend of increasing automation and autonomy. We will cover selected concepts related to network softwarization and machine learning as well as address the need to customize the network to support the use cases of public safety communication. Table 1.1 lists the enablers and technologies as well as the central research questions that have been explored in the dissertation. Later, in Table 4.1, we summarize the contributions to these questions.

The research methodology in this work is based on a) literature surveys and systematization of existing knowledge; b) security, threat, and architecture analysis; as well as c) trials and experiments. We survey security solutions for 5G network as well as for next-generation public safety communications. We survey and analyze security vulnerabilities

**Table 1.1.** Enablers in the foci and the main research questions of the dissertation.

| Enabler | Research questions |
|---|---|
| Customized 5G security architectures | What architectural elements are needed to enable security in 5G networks and beyond to be customizable and self-adaptive? What are the unique security needs that public safety users have for 5G networks? |
| Micro-segmentation | What is the impact of fine-grained network slicing for security? |
| Intelligent threat mitigation in software networks | How can real-time SDN monitoring and threat detection with ML-based security analytics be realized? What is the best way to respond to attacks in different 5G use cases? |
| Adaptive pseudonymization | How can adversarial algorithms be utilized to make defenses, for instance, for privacy and access control, more self-adaptive? |
| Tactical bubble | What are the security requirements and characteristics in geographically isolated rapidly deployable networks for public safety? What is the impact of the tactical bubble on security? |

and mitigation possibilities related to machine learning in mobile network use cases. We analyze architectural concepts—micro-segmentation and tactical bubbles—to understand their relation with security. We prototype solutions for security monitoring and ML-based threat detection analysis in software-defined networks as well as for enhancing security of information brokering for security intelligence. We use a 5G test network [122, 69] to gain practical experiences as well as to acquire realistic data so that we can analyze the enablers.

### 1.3.2 Organization of the Dissertation

The overview part of the dissertation describes a high-level vision for increasing automation, autonomy, active defenses, and, customizability for security in mobile networks. It serves as a common thread that links together the studied enablers. The overview provides a high-level umbrella under which the included articles provide more focused viewpoints and results.

The included articles—describing the explored enablers in more detail and providing more complete literature surveys—are organized as follows. The first two articles [I, II] provide an overview and relevant background of 5G security particularly from the perspectives of the core network and one particular user group: public safety communications. The second two [III, IV] explore the security of network slicing and SDN, which are central new technologies of 5G. We explore a particular SDN-based concept,

namely micro-segmentation, and describe SDN-based security applications for security situation awareness and resilience. Publications [IV, V] also explore information brokering to collect and correlate security-relevant information and to share security intelligence data. The last publication [VI] explores ML, which is a central enabler in security intelligence and analytic, and surveys ML-related use cases, threats, and hardening solutions in the context of 5G networks. The article illustrates that there are still large areas of future research ahead before the visions become full reality. The mapping of articles to the feedback loop of intelligent security is illustrated in Figure 1.2.

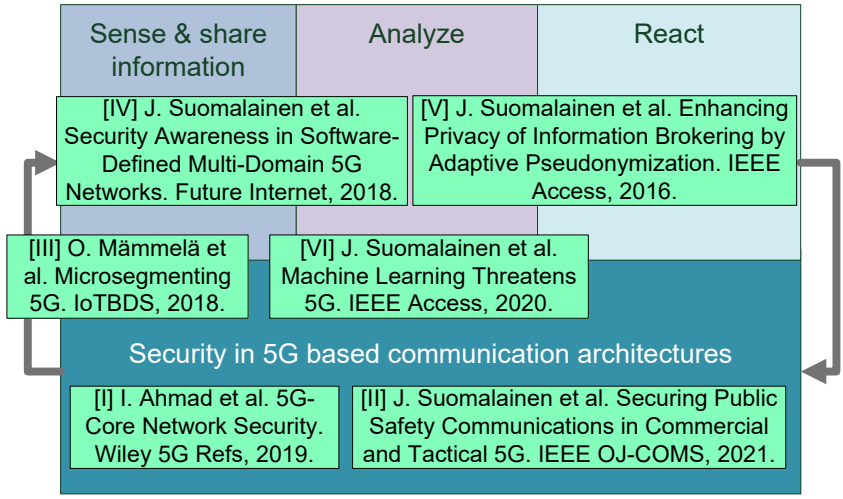


**Figure 1.2.** Mapping the publications to the technology scope of the dissertation

The rest of this overview is organized as follows. Section 2 presents generic technology enablers for customizing and increasing the intelligence of security. Section 3 presents use cases and applications needing custom and intelligent security and also some approaches to achieving these goals. Sections 2 and 3 show the main ideas and context for the studied enablers. They also discuss the novelty and impact of the results, as well as highlight some recent developments since the publication of the included articles. Section 4 summarizes the main contributions and results and suggests paths for future research.

# 2. Enablers of Intelligent Security

The central recipe for intelligent security is the feedback loop, which we divided into four main ingredients in the previous section (Figures 1.1 and 1.2). In this section, we will look at each of these building blocks more closely starting from the system (security architecture in Section 2.1), continuing to information sensing and sharing (security data in Section 2.2) and security analytics (in Section 2.3) and ending with security actions (in Section 2.4). Each part provides an overview of the topic and highlights the related research contributions from the articles included in the dissertation.

## 2.1 Security Architecture

According to the definition of ITU-T X.805 [82] security architecture logically divides a complex set of end-to-end network security-related features into separate components. The security architecture provides a systematic approach to end-to-end security that facilitates planning and design of new security solutions and enables assessments of the security of existing networks.

### 2.1.1 Security Architecture for 5G

3GPP introduced the security architecture for 5G networks in Release 15 [4] of the standards. The 3GPP security architecture consists of the six security domains. Network access domain security provides features for user devices to authenticate and securely access network services. Network access security includes the security of 3GPP and non-3GPP access technologies, and the delivery of the security context from the serving network to the UE. Network domain security protects signaling and exchange of user plane data. User domain security protects the end-user's access to UE. Application domain security enables secure application communication between the end-user and application provider domains.

The visibility and configurability of security includes features that inform users whether security features are in operation or not. Service-based architecture (SBA) domain security provides security features for network element registration, discovery, and authorization, as well as security for service-based interfaces. The last domain is new for 5G while the others have seen evolution.

In [I], we surveyed the requirements, architecture, and functions for security in the 5G core network. In addition to addressing the specification efforts of 3GPP, we covered security and standardization within the central enablers of 5G: cloud platforms, software networks, and network virtualization.

### 2.1.2 Architecture Analysis

Analyses of security requirements utilize taxonomies to identify and capture relevant characteristics and features that affect to the security landscape. Figure 2.1 illustrates the different dimensions that were included in the frameworks that we have proposed for analyzing the security of mobile networks. A generic architecture framework for representing and analyzing 5G security was described by us in [17]. The architecture was defined as a part of the European 5G-ENSURE project. In [II], we utilized, adapted, and extended the framework to analyze security requirements of applications, particularly emerging public safety communication networks. In [VI], we analyzed the security of ML solutions.

The 5G-ENSURE security architecture [17] consist of four dimensions. *Domains* group network elements according to their physical and logical location and functionality. The 5G aspects are emphasized with domains related to management and network virtualization (decoupling of physical and logical infrastructure). A *stratum* groups protocols, data and functions that are provided by one or several domains. *Security realms* capture the security needs of one or more strata or domains. *Security control classes* are collections of security functions or mechanism that address specific security objectives.

The security analysis framework for application domains, which was presented in [II], focuses on security vulnerabilities, threats, and risks from the perspective of network user. The framework captures threat actors, attack types, attack vectors, root vulnerabilities, as well as risk levels. The framework also adopted domain and security control class definitions from the 5G-ENSURE architecture. Security challenges were captured by defining threat scenarios, which were identified from the use cases and assets, and which aim to characterize unique security characteristics of the network application area.

The security threats and solutions of ML solutions were explored using another framework [VI] that derived its dimensions from the 3GPP security

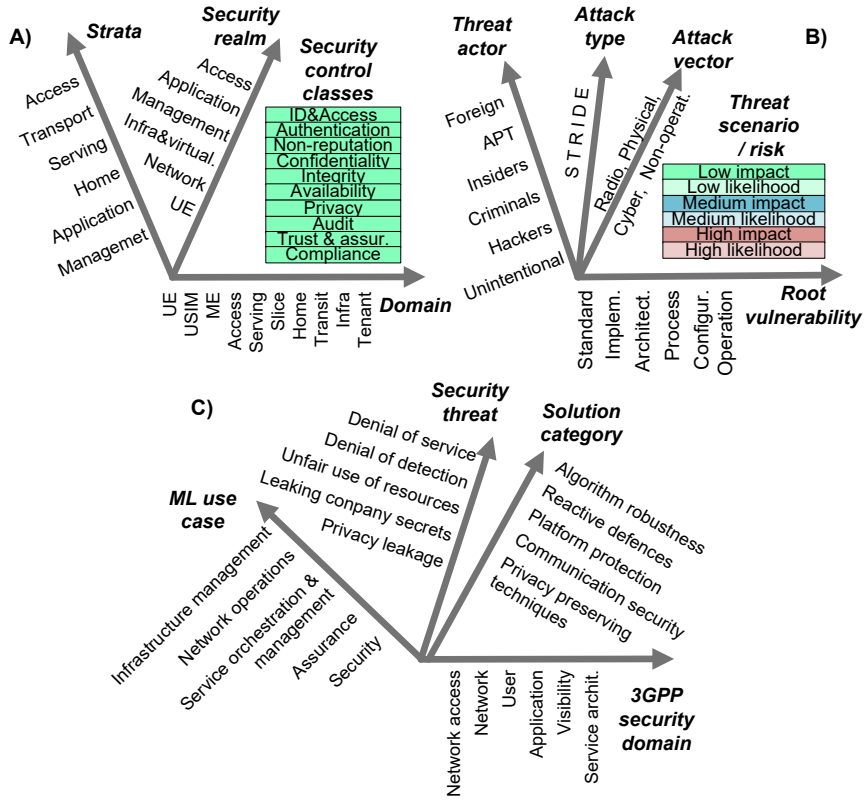


**Figure 2.1.** Dimensions for the security analysis of 5G systems and applications : A) dimensions in the 5G-ENSURE architecture [17], B) threat analysis framework for public safety [II], and C) analysis framework for ML security [VI]

architecture and ETSI specifications [48] (see Subsection 2.4) and proposed our own dimensions for the security threat and solution categories.

*Significance of the Contributions and Current Outlook*

The applied taxonomies for security analysis are based on established classifications, including [136, 4, 17]. By combining several classification we gathered a wide and comprehensive perspective on the security landscape and, hence, enabled a holistic analysis of security requirements for 5G application domains. Some recent threat modeling taxonomies have addressed the mobile network perspective, e.g. [152, 128, 50], but as far as the author is aware, the survey [II] combining the perspective of 5G as well as public safety use cases was the first one.

### 2.1.3 Security in Micro-Segmented Networks

Security management in mobile networks is a complex challenge, which is further complicated by the need for additional customization. An obvious approach to manage the complexity is to divide the problem into smaller

pieces. Network slicing [115, 57] is a concept emerging with 5G. Slices are independent, logical, and virtualized [40, 92, 13] networks, which share the same physical network infrastructure and, typically, rely on SDN technologies [111, 99, 54, 12]. They are end-to-end networks customized to fulfill the requirements of particular applications. The 3GPP efforts [7] often highlight three main application categories: enhanced mobile broadband, massive machine type communications, and ultra-reliable and low-latency communications.

In [108] and [III, IV], we explored the security of network slicing and the concept of micro-segmentation. Micro-segmentation, which was originally proposed for datacenters [158] is the process of creating and managing isolated and fine-grained network slices, which are dedicated to a particular end-user or application. While network slices are typically considered more coarse-grained and dedicated to particular application categories as well as end-to-end concepts, the focus of our research was on more fine-grained and potentially domain-restricted logical isolation of applications.

For security, network slicing provides the following main benefits:

- Security or quality policies can be customized for each application-specific slice. The policies may be more or less strict when compared to generic policies, which involve every application.

- The applications, protocols, connections, services, and users can be whitelisted for each slice. Often the allowed and expected users for a network slice, which is created for particular application or use case, are known in advance, and only those traffic flows, which are related to authorized users, can be allowed. Non-whitelisted connections can be prevented or treated as indications of potential threats.

- A single network slice must support fewer data flows and there is less noise, when compared to the overall capacity of operator' network. Analyzing the traffic flows of a slice requires less computing resources, than analyzing traffic flows of the whole network. As the traffic flows are more homogeneous, anomalies are easier to detect.

- Monitoring resources, within a network slice, can focus on the most critical parts of communication and according to the preferences of the application. For example, some slices can be scrutinized with deep-packet inspection while other slices can be set under focused surveillance only after the detection of suspicious activities.

Challenges to the fine-grained approach include that dedicating own resources and network functions to each slices may cause some overhead. Also, orchestrating resources to support slicing requires new software

solutions and will introduce additional complexity and costs for network management. Further, if operators share the same virtual network function instances between several slices, the security benefits of isolation are partly lost.

Micro-segmentation is an enabler of intelligent security. Even though, it does not enable a system to achieve security goals in wider range of environments, it limits the amount of environments where security goals must be achieved. Consequently, it in practice enables deployment of intelligent systems that are able to operate with limited set of environments. Further, the concept enables operators to deploy systems that are optimized to achieve security goals in particular environments.

*Significance of the Contributions and Current Outlook*
We disseminated the micro-segmentation concept through 5G public-private partnership cooperation, a white-paper [63], and several publications ([108] and [III, IV]). The work was part of our architecture definition [17] in the 5G-ENSURE project, which supported pre-standardization efforts for 5G. Our architecture was presented to the 3GPP technical specification group that is responsible for services and systems aspects related to security and privacy (SA3).

The need for customization remains an important research challenge when approaching 6G networks [43, 94]. Relevant trends affecting to the 6G security architecture includes also the trend towards open interfaces. For instance, the open RAN (O-RAN) initiative [37] aims to facilitate the cross-layer cooperation and manage complexity by utilizing software-defined radio and an open cross-industry agreed specification. The openness will introduce new means for network security customization but may also introduce new challenges.

## 2.2 Security Data

Mobile networks produce large amounts of data that can be used to determine the state of the network, its components and users. Security-relevant information can be related to security systems or to resources or systems that the adversary may target.

*Security Monitoring*
Typically, network statistics, system logs, packet headers, and payloads provide indicators to detect networks attacks, while security function-specific performance indicators, like the throughput of deep packet analysis or identifiers of security algorithms in use, provide information on the state of the protection. Existing network monitoring techniques include, e.g., the simple network management protocol (SNMP) for resource usage

data from network equipment, remote network monitoring (RMON) for traffic flows on Ethernet segments, NetFlow and sFlow for IP statistics, active probing for analyzing network properties, deep packet inspection for analyzing transmitted headers and payloads, as well as firewall and server logs for user accesses. [103] Network equipment manufacturers and service providers have their interfaces for collecting large amount of performance indicators from the access and core networks. SDN, which has been adopted to 5G, provides its interfaces for collecting information. In particular, OpenFlow [99] is a protocol between switches and SDN controllers and that gives access to meta-information related to data flows. SDN controllers provide north-bound interfaces for SDN applications. One monitoring approach for SDN is presented in [IV]. The requirements, architecture, and potential interfaces for network monitoring within the context of virtualized network functions (NFV) have been defined, e.g., by ETSI [49].

The volume of data traffic in mobile networks is increasing rapidly; the total monthly volume is expected [47] to increase from 51 exabytes in the year 2020 to 226 exabytes in 2026. At the same time, advances in AI are demanding [153] more computing resources, and this development rate is expected to decelerate in the era of post Moore's law [46]. Consequently, more algorithmic and architectural solutions, such as micro-segmentation in [III, IV], are needed to enable network defenders to target the available computing resources cost-effectively.

*Distributed Security Intelligence*

Security intelligence is the practice of collecting and analyzing security information to achieve security situational awareness. Cyber threat intelligence (CTI) [159, 109] data is information describing threat actors in the cyber world. CTI can be acquired from the mobile network or from other other stakeholders and sources. CTI sources include, e.g., open source intelligence, social media intelligence, human intelligence, as well as signaling intelligence, which consist of electronic intelligence (referring to non-communication based surveillance of target capabilities such as location), and communication intelligence.

Architectures and protocols exists for CTI sharing [159]. A typical architecture is based on a centralized repository or broker, which stores and distributes threat and vulnerability information. Solutions for sharing security information include domain-specific security standards as well as semantic security ontologies and mechanisms [53, 145, 144]. The standards and common tools for CTI include, e.g., the open indicators of compromise (OpenIoC) framework, structured threat information expression and trusted automated exchange of indicator information (STIX-TAXII), and the open source threat intelligence and sharing platform (MISP).

Cooperation between different operators and between operators and ap-

plication providers is based on contractual agreements and trust. The required QoS characteristics and performance indicators, which the network should provide, are defined using service level agreements (SLA) [88, 160, 125]. The contracting parties may also agree on security practices through security level agreements [71]. If they do not completely trust each other, additional assurance of SLA protection and trustworthiness, e.g., technical [163] or reputation-based assurance [127], is needed. Privacy and scalability are also challenges. Operators could in theory exchange all the data collected from the network, but the exchange of massive amounts of data would not be practical and might disclose privacy or company-critical secrets.

In [V], we explored access controls for an information brokering approach that was based on the Next Generation Service Interface (NGSI) architecture from the Open Mobile Alliance (OMA, see also Section 3.3.2). In [IV], we presented an Apache Kafka-based publish-and-subscribe information brokering approach for sharing security data from our SDN/5G testbed as well as security and trustworthiness-related knowledge derived with our security analytics tools (see also Subsection 3.3.1).

## 2.3 Security Analytics

The analysis of security situational information leads to security situational awareness. Combining or correlating information that is collected from different sources is a process called security information and event management (SIEM) [29]. Security analytics can be used, e.g., to detect various threats such as zero-day exploits, advanced malware, traffic to adversarial command servers, evasive activities, advanced persistent threats, as well as device and service misconfiguration. The challenges in security analytics include scalability and performance, the amount of noise and false alarms, difficulty in detecting previously unseen attacks without known signatures, heterogeneity of information, and dynamicity of events. Security analysis is based on the availability of large amounts of data. Consequently, various solutions to automate the analysis and to help in the decision-making process have been introduced.

*Potential and Challenges of Machine Learning*

ML has been seen as a central enabler for reducing the manual human efforts required and for increasing the effectiveness of security analysis and threat detection. ML has many applications in the network context [9, 20, 56]. ML algorithms can analyze and classify streaming information to detect patterns of known threats. A major potential of ML is the ability to detect previously unseen attacks and threats by detecting anomalies. However, ML is not likely to be a magical solution that will

address all security issues. It also introduces new vulnerabilities. There are various attacks against ML [24, 23, 119, 165, 112] including poisoning (manipulating models), interference (influencing training data), extraction (model stealing), and evasion (confusing a classier with noise). Security for ML solutions is required both by their adopters as well as regulators [51].

In [IV], we utilized an ML-based algorithm to detect anomalies in traffic flows within SDN-based network slices (see Subsection 3.3.1). In [VI], we surveyed vulnerabilities and potential attack vectors against ML in 5G as well as solutions that can be utilized to mitigate the threats.

*Significance of the Contributions and Current Outlook*
The security threat survey of ML in 5G networks that was presented in [VI] was among the first published surveys combining the dimensions of ML in 5G, vulnerability analysis, and security mitigation. At the same time, [26] addressed the same topic and surveyed AI as a defense and offense enabler for beyond 5G networks. Security and privacy of AI are expected [43, 123] to remain an important research question for the development of 6G technologies.

## 2.4 Security Actions

Security-related actions that are performed based on the security situational awareness can be various. Security actions can be preemptive responses, reactions, to identified security threats or corrective measures to ongoing security attacks. Sometimes actions can also be randomized, proactive measures that mitigate the capabilities of the adversaries. The actions depend on the security goal. Security resilience [139, 30, 18] is an example of a security goal which requires active responses and is vital for mobile networks. Security resilience means the ability of networks to dynamically adapt to security threats by preparing for, responding to, and recovering from cyber and physical attacks. Compared to robustness, which aims to prevent or withstand security incidents due to invalid external inputs, or to tolerance, which aims for continued operations despite the incident or its detection, security resilience aims to recover from threats that are detected and incidents that have penetrated the defenses.

Optimal and possible response strategies depend, in addition to security goal, on the application, and use case. ETSI has defined use cases in four main categories in its experiential networked intelligence (ENI) specifications [48]. In [VI], we studied these use cases and explored potential vulnerabilities. In the following list, we identify examples of autonomous security actions that fit to the ETSI use case categories for networked intelligence.

1. Infrastructure management—These use cases include intelligent load balancing and managing of peak traffic, which are essential for assuring availability. Optimized energy consumption supports the sustainability of security, which is essential when ensuring the economic viability of security solutions. Infrastructure specific security responses include actions towards cooperative parties, other operators, infrastructure providers, or subscribers. For instance, sending notifications on detected malware on their systems or eventually initiating legal actions.

2. Network operations—Management, deployment, and migration of security functions and network services can be optimized based on estimates of load and security situations. The deployment of security updates can be prioritized based on their security importance. Network operations can be adapted based on applications security characteristics. Network-specific security responses include, e.g., blocking, quarantining, prioritizing, and rate-limiting, i.e., throttling, traffic flows as well as moving target defenses [133], e.g., reorganizing typologies and addresses to make network aiming harder [105, 168] or pseudonymizing network or application-specific data [IV,V].

3. Service orchestration and management use cases customize end-to-end network services to ensure availability. Security scenarios include optimizing network defenses, access controls [166], and content caching based on security, trustworthiness, and availability attributes. Honeypots [121] and other deception techniques may make attacks harder and provide information on the attacks.

4. Assurance and security related reactions include launch of advanced security monitoring, like initiate anti-virus scanning or deep-packet inspection activities, which increase the costs of attack as adversaries must spent more resources to remain undetected. Results of security monitoring can be linked to network, infrastructure, or service specific actions. For instance, network slices may be dedicated for user that are less trusted and user with high-security requirements or replace compromised resources with trusted. Misbehaving users, functions and services can be quarantined. Resource allocation, which is guided by failure identification and root-cause analysis, can support recovery. Decision trees for root-cause analysis can guide recovery and security response. Counterattacks targeting software or hardware of adversary are restricted by legislation to specific scenarios, such as confiscation of jamming devices.

Table 2.1 summarizes the findings by categorizing the potential defenses according to the use case and the defense strategy: mitigate (i.e. increase cost of attack), nullify (i.e. prevent consequences of attack by stopping it

**Table 2.1.** Examples of strategies for defense actions in the 5G networks and beyond.

| Use cases | Mitigate | Nullify | Destroy |
|---|---|---|---|
| Infrastructure | Increased capacity and load balancing. | Alternative isolated capacity, e.g., tactical bubbles [II]. | Legal actions against untrustworthy providers. |
| Network | Prioritized and throttled traffic flows [II]. Moving target defense. | Blocked traffic flows. Resource isolation, slicing [III]. Reallocation of resources. | Notifying users with misbehaving UE, e.g., detected malware. |
| Services | Distributed content and controls. Pseudonyms [V]. | Honeypots and other deceptions. Service-specific access management. | Prevent distribution of malware from the application stores. |
| Assurance and security | Anti-virus scanning and deep-packet inspection. | Quarantines of services, NFs, or UE [IV]. Root-cause guided resource allocation. | Direct counter-attacks with physical or cyber means. |

within the network), and destroy (i.e., stop the attack within its source). The table also gives examples of defensive actions. Some of the examples may be relevant for several categories and use cases but are mapped to the most fitting class in the table.

Often, the security architecture and security functions available in the network enable alternative actions. Finding the best response may not always be easy and compromises are needed. For instance, in public safety scenarios [II] with high security requirements, rapid reactions are necessary, but as availability is also vital, blocking users on a suspicion of misuse may not be a viable option. In these cases, solutions which prioritize critical applications and users and adjust their quality-of-service levels to ensure the availability of the network may be more appropriate [146]. In many cases, there are trade-offs between the interests of different stakeholders. For instance, the automated allocation of additional resources for security functions or initiating an update of temporary identifiers, as in [V], are transparent and, thus, viable responses for the end-users but demand software or infrastructure investments from the network operator. Tactical bubbles [II] provide an example of responses where a completely independent network is deployed, e.g., as a reaction to a cyber-attack that has disabled a commercial mobile infrastructure.

Determining the optimal defensive actions depends, typically, on the analysis producing a correct situational awareness which in turn depends on the security data. To support decision making and selection of defensive strategy, different recommender systems [31] have been proposed, including knowledge-based systems, decision trees, and dimensionality-reduction.

We utilized a dimensionality-reduction approach, multidimensional scaling [73], in [IV] to visualize and analyze traffic heterogeneity in network slices.

# 3. Customized and Active Defenses for Network Applications

5G networks and beyond can be used to implement communication solutions for specific industries and application domains, so called verticals, which previously had their own dedicated networks and technologies. Table 3.1 lists examples of such verticals. The table also gives references to survey and research articles that have explored their security requirements. Compared to domain-specific or proprietary networks, 3GPP-based technologies are cost effective and often provide better guarantees of service quality and availability. However, the application domains have their own requirements for security and quality-of-service, and different processes for adopting new technologies. In order to replace the domain-specific networks, 5G network operators need to adapt their service to match these expectations.

Section 3 presents use cases for customized security needs as well as active defenses of network applications. In Section 3.2, we first look at the requirements. We focus on needs in public safety communications [II]. In Section 3.3, we take the technology perspective and look at two active defense solutions: threat detection in software-defined networks [III, IV] and adaptive pseudonymization [V] to secure user identifiers.

## 3.1 Application-Layer Security

The central enablers for the application-layer security are the end-to-end cryptographic protocols, which provide confidentiality, integrity, and authenticity. Different applications have their own security protocols and services for achieving their specific security goals. For instance, application domains have their own practices for the selection of cryptographic algorithms, key management and authentication protocols, and authorization. Many deployed solutions are based on Transport Layer Security (TLS). For example, datagram TLS (DTLS) is used for IoT, secure real-time streaming protocols (SRTP, RTSPS) are used for audio and video, and the secure hypertext transfer protocol (HTTPS) is used for the web. These protocols

**Table 3.1.** Examples of 5G verticals, their security requirements and existing security surveys.

| Vertical | Short description of security requirements | Ref. |
|---|---|---|
| Industry | Isolated business-critical networks with immaterial properties, organizational and customer-specific secrets and assets. Business continuity and safety-critical applications require availability assurance. | [129, 156] |
| Transport | Logistics and vehicular networks for ships, trains, and cars with high numbers of sensors and actuators. Safety critical systems require integrity protection and non-autonomous systems continuous assured availability. | [76, 104, 98, 135, 70] |
| Healthcare | Remote medicare and hospital networks with privacy as an overarching requirement. Some applications require high-availability guarantees. | [36, 11] |
| Utilities | Civil infrastructure, e.g., electricity grids or gas, oil, and water distribution, requires scalable and reliable control and monitoring infrastructure, as well as privacy for monitored consumers. | [35, 16], [V] |
| Military | 5G may support some operational use cases, which demand high-secure application layer, availability, and minimal leakage of operational or organizational information. | [141, 62] |
| Public safety | Mission-critical services requiring high-availability, prioritization, hardened applications and certified UEs for classified communication. | [II] |

protect the application payload but do not ensure quality or service or optimal performance, and they leak some communication metadata. To control who can access which resources, applications can utilize various identity and access management approaches [80, 45, 147, 142, 143, 85]. Applications may also have their own requirements for communication availability and privacy. These requirements, in addition to the performance requirements, limit the choice of security solutions. For example, applications may benefit from edge computing to reduce latency, but edge computing requires that the users trust the local network provider to process their data.

Mobile network operators can support application-specific security objectives in different ways. To support availability, 3GPP has introduced [8, 61] policy functions, enabling customers to request prioritized and controlled QoS levels for particular UEs. To simplify application-layer identity and subscriber management, the 5G specifications introduced [4] secondary authentication. With secondary authentication, application providers can use and rely on the authentication and key management provided by network

operators. 3GPP also adopted a certificate and private key-based authentication alternative, EAP-TLS [4], to support private networks and IoT scenarios. To support more flexible and remote management of subscribers and enable users to more easily change operator, GSMA introduced [65] architecture and protocols for the remote provisioning of credentials, i.e., eSIMs. Emerging technologies enable operators to deploy and orchestrate customized security functions as virtual functions for application domain specific network slices and scale their computing resources for security functions [95].

## 3.2 Securing Next-Generation of Public Safety Communications

Public safety authorities (police, firefighters, emergency response) have previously used dedicated technologies, including TETRA in Europe and Project 25 in the US, and infrastructure for communication. To enable cost-savings and new broadband applications, these dedicated approaches are being replaced with a hybrid approach where the authorities use commercial 5G infrastructure and, when coverage or capacity from civilian networks is not enough, rapidly deployable networks or tactical bubbles. Figure 3.1 illustrates the hybrid architecture with mission critical services are accessible either through commercial operators' infrastructure or through tactical bubbles. The figure also shows the deployment alternatives for enablers of security intelligence. We explored the security requirements stemming from the transition of the public safety sector from dedicated technologies to 3GPP-based technologies in [II].

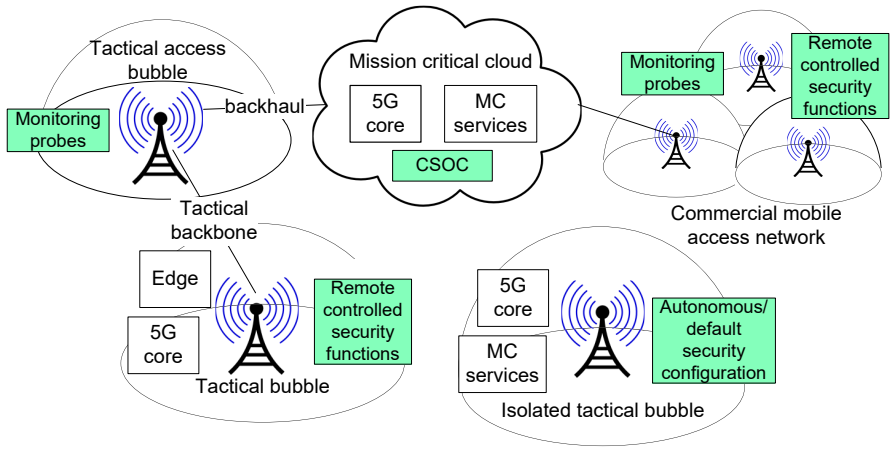


**Figure 3.1.** A hybrid architecture for public safety communications is based on commercial infrastructure and tactical bubbles [II]. Central elements of intelligent security are illustrated with with green.

### 3.2.1 Security for Mission-Critical Communications

The main security objective for the public safety vertical is to assure society's rescue, law enforcement, safety and security related operations. Consequently, availability can be considered the highest priority. In addition, the authorities need information security to protect long-term organizational secrets as well as short-term operational data and the integrity of situational awareness information. The big challenge in the ongoing transition towards 5G is that public safety assets will be exposed to attacks from the civilian infrastructure, including remote attacks coming from the Internet. Additionally, public safety communication is a strategic target for advanced and foreign adversaries. When public safety users share the commercial infrastructure with civilian applications, the following questions must be addressed in a secure manner:

- It is essential to isolate public safety communication from civilian traffic to prevent information leaks and denial-of-service attacks. There is a need for end-to-end security in the application layer as well as for secure slicing in the network layer. 3GPP technologies provide multiple means to differentiate the QoS levels of different applications. The mechanisms have different security assumptions; e.g., some rely on information stored on UEs, some are voluntary, and some are enforced by the network but assume that the network operators have not made configuration mistakes. New technologies, like SDN-based slicing, may leak operational information to the users in the other slices [42].

- An important architectural development challenge is how end-to-end applications can benefit from the performance accelerations at the MEC without compromising security. In architectures where exceptions to UE-to-cloud security are necessary, there is a need for additional security protection and verification of the services and infrastructure that get to inspect the traffic.

- Diverse applications and devices are emerging for public safety operations. IoT gadgets, augmented and virtual reality interfaces, autonomous vehicles, robots, as well as commercial-of-the-shelf phones, for instance, will be connected through the network. Often there is a need to apply devices which have not been security tested and certified for classified use by the authorities. Untrustworthy devices which are accepted by the network could disrupt mission-critical services.

In [II] and [85], we proposed and trialed a device attestation approach for tactical bubbles. The device attestation [64], or remote attestation of devices, is a process of measuring software configuration of a device

and proving its integrity for a remote party. The attestation was integrated with the identity and access management service. The OpenID Connect [131] based identity and delegated access management follows the 3GPP mission-critical security framework [6], which provides end-to-end security for the application-layer. The attestation solution enabled us to verify the hardware type, software configuration, and software integrity of IoT devices requesting access to services within tactical bubbles. Consequently, the solution provided additional assurance of the trustworthiness of devices and collected data.

### 3.2.2 Security for Tactical 5G Bubbles

Public safety users require connectivity also in remote locations and in failure, disaster and cyber-attack situations where commercial networks are unavailable. A tactical bubble is an ad-hoc communication concept incorporating both communication solutions and the processes and practices of the authorities in field operations. The authority-extended tactical bubble concept is a rapidly deployable network [52, 113] that is built with standard 3GPP technologies [3, 5, 118]. It incorporates lightweight access and possibly core network functions and mission-critical services, enabling it to operate in an isolated mode without connection to the operator's datacenter or to cloud application providers.

We have explored and trialed tactical bubbles in [74, 69]. The security requirements and challenges for tactical bubbles were explored in [II]. The central security challenges include:

- The backhaul connection—between the bubble and mission-critical services in the cloud—may become a bottleneck. Security applications must hence tolerate backhaul limitations. For instance, the security applications should not assume that access control information or cyber-threat intelligence is always available without delays.

- To enable isolated operation, tactical bubbles must host large amounts of security information and assets. These local assets are vulnerable to physical and cyber-attacks due to potentially weaker physical protection and lack of security controls and CSOC that require connected administrators. For instance, secret keys, security and access control information, profile data on end-users, and organizational information on group assignments, as well as operational information on capabilities such as the type, location, and number of devices, may leak to outsiders. Isolated operations means, hence, compromises between the risk of leaking information, the costs of additional security controls, as well as mission-critical functionality, such as the capability to create fine-grained communication groups.

- Security functions based on ML can support dynamic configuration in new situations of ongoing missions. One challenges is the limited availability of operation-specific data for learning. Each operation and deployment of a tactical bubble instance is different, as the applications, users, adversaries, as well as the physical radio environment are different. Hence, data points can be used for learning as operations are often unique and generic models may not be applicable. The detection of anomalies is difficult if there are no models of normal or typical behavior at the start of the short-term operation. Furthermore, the use of security models that are generated in a centralized cloud and then distributed to a bubble is a security risk as the models may reveal organizational or operational information.

- Applications and traffic flows in tactical bubbles can be white-listed and controlled. Consequently, data flows are more homogeneous and have less noise, which may ease the deployment of security monitoring and enables faster security response. However, in isolated scenarios the users on the operation site cannot be assumed to have the time or skills for configuring complex SIEM and SOAR solutions. Hence, tactical bubbles must rely on remote CSOCs and host only security functions which require minimal local configuration or no configuration at all.

In [II] and [157], we explored a satellite-based backhaul solution to provide additional resilience for the cases where a terrestrial link is unavailable. The development of non-terrestrial 5G is progressing and provides a viable alternative or backup of the backhaul to reach mission-critical applications. We studied the implications of the limited backhaul connection for mission-critical applications as well as the limitations that IPsec-based secure tunnels sets for the optimization of communications.

*Significance of the Contributions and Current Outlook*

The security survey presented in [II] was the first survey in the scope of 5G and the public safety communications, as far as the author is aware. Previous surveys [41, 110, 68, 59] have focused on previous technology generations. The security of the tactical bubble, or 3GPP networks in isolated mode, have been addressed by standardization. We contributed by combining several viewpoints—end-users', user agencies', operators', virtual (authority) operators', and manufacturers'— to provide a holistic security analysis. We combined the network perspective with the security requirements stemming from the processes of public safety users and surveyed the research efforts and solutions from the involved stakeholders.

Our results related to the public safety communications and tactical bubbles are parts of the on-going research effort within the PRIORITY project. The results are disseminated through the project for the Finnish

ecosystem of public safety communication. Further, we have disseminated generic security results related to public safety adaptations of 5G and tactical bubbles through publications [74, 116, 157, 69], [II] and The Critical Communications Association (TCCA) events.

## 3.3 Self-Adaptive Active Defenses

This section focuses on two specific technology scenarios for adaptive active defenses. The technologies give examples of how the enablers presented in Section 2 are linked together.

### 3.3.1 Threat Detection and Prevention in Software Networks

SDN provides a framework that can support deployment and operation of intelligent security applications [130, 34, 86]. Switches in the infrastructure layer of SDN enforce routing policies and can also provide information on the traffic flows. SDN controllers in the control layer connect the infrastructure and applications. Security applications that have been proposed for the application layer, include, e.g., firewalls [140, 120, 132, 83] as well as detection and mitigation of network intrusion [67, 151], distributed denial of service [38, 32, 75, 15, 91, 148, 126] and other attacks [90, 39, 33].

In [IV] and [72], we described our design and implementation of a monitoring and security analysis framework for network slices, or micro-segments. The monitoring part of the framework utilized scalable open-source components, particularly SDN Ryu, Apache Kafka, and Apache Spark, to realize a data pipeline to collect and process real-time streams of network metadata, i.e., network flow statistics and events. We utilized an ML algorithm to detect anomalies in traffic flows within the SDN slices. We explored the streaming-k-means algorithm [106, 58], which is an unsuper-

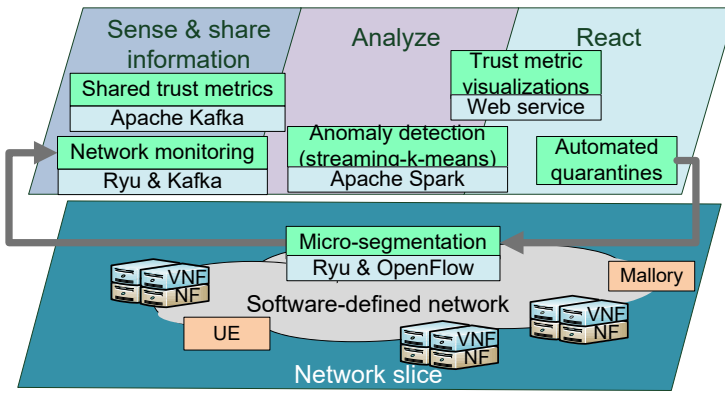


**Figure 3.2.** An approach for active defense of software networks.

vised continuously learning clustering algorithm for detecting anomalies. The analysis solution was implemented as an Apache Spark application that can be distributed to a computing cluster. Detected anomalies were reported to our trust-metric enabler, which is a tool to correlate security events and visualize the security state of the network slices. The trust-metric enabler [72] uses customized policy rules to determine the security posture of monitored systems and illustrates the results with a web-based "traffic-light" interface. Clearly anomalous devices were also quarantined from the SDN to prevent them causing interference and denial-of-service situations. Figure 3.2 illustrates the main elements and technologies of our approach.

Our monitoring approach [IV] was targeted towards micro-segmented software-defined network slices, which were dedicated to particular users or applications. Hence, the data flows are homogeneous and the amount of data and noise can be minimized. This increases the effectiveness as the monitoring resources can be flexibly targeted to the slices that are the most interesting from the security perspective. However, focusing the monitoring on a particular application is a risk if adversaries have access to multiple slices. By splitting activities and transmitting, e.g., the control and attack payloads in different slices, an adversary may be able to circumvent the detection. Consequently, inter-slice cooperation and information sharing—as enabled the trust metric enabler—is needed to detect advanced threats. Another challenge in network slicing is that the different slices typically share resources and functions. The more fine-grained the slices are, the more economic pressure there is to share resources, which then become bottleneck resources for an adversary to impact applications also in other slices. Our monitoring approach that can be customized and distributed to slice-specific resources is one answer to this challenge.

*Significance of the Contributions and Current Outlook*

The monitoring approach developed in [IV] utilized existing interfaces for SDN networks and, hence, validated many existing efforts and ideas for security monitoring. The novel contribution was the unique combination of open source tools in the data pipeline. We selected tools which were designed and tested to enable scalable analysis and information sharing. As far as the author is aware, these tools have not previously been used for monitoring in a similar context.

AI-defined security remains a major security challenge for 6G networks [164]. Cloud, edge, and fog technologies and movable virtualized security functions provide further opportunities to optimize security monitoring and to enable proactive security decision making. The concepts of SDN, programmable APIs, and security information sharing for global security visibility and awareness are expected to be key building blocks for making

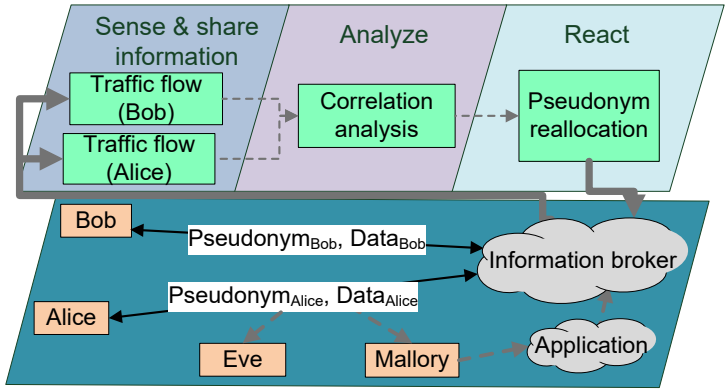


**Figure 3.3.** Adaptive pseudonymization.

mobile networks more resilient against attacks also in the future.

### 3.3.2 Adaptive Pseudonymization

Pseudonymization is a process where identifiable information is removed from data and replaced with random identifiers, or pseudonyms. De-pseudonymization is an adversarial process [84] where the pseudonymized data is linked to original identifiers using external indicator information. Existing research [149, 137, 161, 101, 28] has developed several metrics for analyzing the risk of de-pseudonymization.

In [V], we proposed the concept of adaptive pseudonymization. The main idea is based on an observation that an adversary who is following and analyzing two correlated pseudonymized data streams or time series can compromise both if the adversary can a) de-pseudonymize one and b) determine a correlation between the two. The longer the same pseudonym—or temporary identifier—is used, the higher the success probability of the attack is. The attack is more difficult if the pseudonyms are changed frequently. However, the change causes an overhead, and there is a need to find an optimal time to make the change. The proposal triggers re-pseudonymizations, i.e., adds discontinuation points, so that an adversary who succeeded in de-pseudonymization cannot know which consecutive data entries belong to the revealed stream. To make the proposal adaptive, we proposed an algorithm to analyze when an adversary may have been able to correlate the data streams. Our proposal has an analysis part for executing the adversarial algorithm and a response part for initiating the reallocation of pseudonyms. Figure 3.3 illustrates the main elements of the solution as well as the threat with Eve as passive observer and Mallory as the adversary that is able to influence another time stream. The goal is to find out whether Bob and Alice are in the same location.

Adaptive pseudonymization was applied to the access control of an

application-layer information broker in [V]. We presented an adversarial algorithm for the adaptation and studied the adaptive pseudonymization scheme in the smart city context. The adversarial problem was to find a correlation between two time series, which contained energy consumption measurements from smart homes. A security architecture supporting the idea was proposed for an OMA/NGSI [25] based information broker.

The application of the adaptive pseudonymization in the context of mobile RAN—to prevent UE location tracking—was discussed in [IV]. Location tracking of the UEs is possible [97, 93] by eavesdropping global unique temporary identifiers (GUTI), which are pseudonyms that are transmitted in clear text to reach idle devices, e.g., to initiate a call or message. Frequent changing of the temporary identifiers has been proposed as a solution against UE tracking. However, in 4G, operators have been known [134] to reuse the same identifiers for long periods of time. The approach we proposed was to analyze the correlation between application-layer messaging, which may be adversary initiated, and RAN signaling to detect potential threats and to trigger a refresh of the temporary identifiers. The revealing correlated pattern in the time series can be caused by the adversary or it may be caused by the network. An example of the first is adversary-initiated messaging whose size and timing the adversary can control. An example of the latter is the handshake in specific protocols. For instance, remote attestation enhanced identity management, which was proposed in [II], will always initiate a similar message exchange with the identity server. An adversary who is able to follow the messaging, even when encrypted, may determine the UE's capability for device attestation which may also reveal the UE's other capabilities.

*Significance of the Contributions and Current Outlook*

The adaptive pseudonymization concept is an unorthodox approach for securing brokered communication. It defends against a correlation-based privacy attack [97, 149], which is a good example of how an attacker might use AI or data analytics. The use of the same correlation techniques for adaptive defense was an experimental and resource consuming idea, and the author is unaware of any similar proposals or practical implementations so far.

To address the tracking of UEs via a persistent GUTI threat, the 3GPP 5G specifications (in Release 15 of the security architecture [4]) have mandated the refresh of GUTI in four network initiated events: initial registration, mobility and periodic registration updates, and service request, e.g., due to paging. These changes are believed [93] to prevent attacks related to the GUTI persistence. Compared to our adaptive proposal [IV], they may create a greater signaling overhead but, as the identifier change is more frequent, they also imply less processing overhead.

For the smart city use case, access control and privacy objectives can be

achieved with more traditional cryptographic protection and authorization solutions. Such solutions are likely to be more feasible and effective from the security perspective. However, the adaptive approach may be suitable for resource restricted devices—IoT devices, sensors—without capabilities for application-layer cryptographic authentication and encryption. Currently, low-cost encryption methods for 5G and beyond are being researched [162]. 5G has introduced secondary authentication enabling application-layer servers to rely on the UE identification and authorization that is done in the network-layer by the operator. The secondary authentication, thus, removes the need for resource restricted UEs to implement additional application-layer mechanisms in those cases where the network-layer authentication functions are sufficient and trusted.

# 4. Conclusions

This section summarizes the main findings of the research articles. In Table 4.1, we give compact answers to the research questions which were asked in Table 1.1, and, in Table 4.2, we make some additional observations and initiate discussion of topics to address in future research.

## 4.1 Summary of the Main Results

Customization of mobile network security for different applications requires solutions that are able to facilitate the cooperation between the operator and the application domains. Open interfaces, services, and technical solutions have a central role in customization, but understanding of the security requirements is also needed. Network slicing and software-networks with programmable APIs provide one approach towards customization. [III, IV] Opening of the interfaces of core network functions for the application domains, e.g., allowing use of policy functions to prioritize traffic flows [II] or sharing security-relevant information [IV], is another enabling step. 3GPP has recognized the need to support different application domains, and this development is visible in the 5G specification [I] through the service-based architecture, through the deployment of security as virtual functions, and through specific security solutions such as secondary authentication, certificate-based authentication, and mission-critical security framework [II]. We applied [II, VI] security analysis methods to understand the security threats, vulnerabilities, risks, and requirements of several application domains and use cases.

Intelligence of security depends on several factors. AI and ML algorithms may play a major role in the detection of new threats and in finding optimal reaction strategies, but changes to the security architecture are also needed. Concepts for isolation—such as micro-segmentation [III, IV] and tactical bubbles [II]—provide security architects options to organize application-specific security solutions in the most meaningful manner. The isolation enables the mitigation of threats effectively with reasonable resources.

**Table 4.1.** Enablers in the foci and the main research results related to them.

| Enabler | Results |
|---|---|
| Customized 5G security architectures | Explored micro-segmentation [III] and tactical bubbles [II] as concepts to manage complexity and to isolate applications. Proposed and applied taxonomies for security analysis both for public safety [II] and ML [VI] use cases. |
| Micro-segmentation | Explored the creation of fine-grained network slices to enable monitoring resources to be focused and application specific reactions to be planned. Data flows in the slices can be whitelisted and are typically homogeneous, which may reduce noise and increase efficiency of threat detection [III, IV]. |
| Intelligent threat mitigation in software networks | A data security pipeline based on scalable open-source components was implemented in [IV]. Continuously learning anomaly detection, the analysis of a network slice's trustworthiness, and autonomous quarantining were prototyped in [III, IV]. |
| Adaptive pseudonymization | Explored a data analysis as the basis for attacks against privacy and a self-adaptive defensive strategy. [V] Increased understanding of the needs and trade-offs of dynamic identifier allocation. |
| Tactical bubble | Identified and analyzed security requirements [II] for public safety applications of mobile networks, which require strong segregation—logical security isolation—between the public safety and civil domains. Explored the impact of a restricted or missing backhaul, which may require security compromises, expose critical assets and data, or limit the availability of MC services. |

## 4.2 Future Research Directions

Our research—with micro-segmentation and security monitoring of network slices—aimed at increasing the efficiency, flexibility, and scalability of security. These objectives will remain open research topics within the security field for several years to come. One phenomenon that forces us to strive for continuous improvement is the arms race between the adversaries and defenders. The adversaries will react to active defenses and develop more sophisticated attacks. Hence, here is a need for solutions and algorithms that detect advanced, slowly progressing, stealth, and previously unseen threats in mobile networks. This is challenging as the mobile networks are complex, dynamic, and constantly changing. The requirement to catch advanced persistent threats is not a new one, but it is a moving target and hence difficult to fulfill.

The vision of intelligent security is far from being reality despite the large amount of research on many enablers. In Table 4.2, we highlight some promising directions for future research and give references to articles where the topics are discussed in more detail. There is a need to develop technologies for automated and autonomous security and there is a need to tailor these enablers—systems, functions, protocols, and algorithms—for mobile networks and for specific applications of mobile networks. At the same time, when developing solutions for commercial use, there is a need for compromises; the goal is not perfect security but to achieve good-enough, cost-effective, and practical solutions. Solutions based on AI and ML may reduce the human workload but may incur high processing costs, and sometimes the same security objectives can be achieved with more straightforward security controls.

There is still a lot of of work to be done on understanding the security requirements of different application domains. In addition to public safety communications, there are other application domains with unique characteristics and needs including transport and logistics, healthcare, military, and various industrial scenarios. Future research and new solutions are needed to support these use cases of mobile networks.

In this dissertation, we looked at selected enablers and applications. However, more research and experimentation is needed to go deeper into the limits of the technologies and to better understand the possibilities and challenges. Continuous development is required to address problems that arise from emergence of new technologies for 5G, 6G, 7G, or any future generations as well as from advances of adversarial capabilities.

**Table 4.2.** Directions for future research.

| Theme | Short description of research topics | Ref |
|---|---|---|
| Tactical SIEM & SOAR | Enabling the creation of tailored, tactical bubble-specific threat detection models, which address specific requirements in each public safety operation. Supporting isolated operations by automated threat detection and response with minimal use of computing and human resources. Minimizing data leaks when federating shared knowledge and threat detection models between cloud and tactical bubbles. | [II] |
| Satcom support in security | If the backhaul for 5G networks and beyond is through a satellite, we enter new territory. How is the security of the satellite backhaul ensured? How can distributed the security architecture and CTI sharing be optimized to tolerate backhaul limitations? | [II] |
| Resilience-optimized responses | Exploring requirements and alternatives to find optimal strategies for security response in different applications. Understanding trade offs in reactions, end-user needs, and legislative limitations. | [II, IV, VI] |
| Inter-slice security | There are still different research areas to be explored in network virtualization. Threats involving multiple slices provide new attack paths and require inter-slice CTI sharing and advanced analytics. Functions which are shared between several slices leak information but practical mitigation is still lacking. Further, threat and anomaly detection solutions are needed to address challenges from dynamic ad-hoc creation of slices. | [I, IV] |
| AI-driven security | A little work is still done within the scope of mobile networks to apply or harden ML-based security. There is a need to tailor existing ML-based security algorithms for mobile networks and for different verticals. | [II, VI] |
| Measured security intelligence and robustness of AI | AI-based systems introduce new challenges and complexity. Strategies based on a single algorithm or defense are not likely to be enough. Instead, we need to understand dependencies between different factors, solutions, and systems. There is a need for methodologies to measure the strength of AI systems, e.g., by studying how the level of trustworthiness of situational information impacts to situational awareness and by developing "security intelligence quotient (IQ)" and AI robustness metrics. | [II, VI] |

# References


[1] *The American Heritage Dictionary of the English Language*. The American Heritage Dictionary of the English Language. Houghton Mifflin, 2000.

[2] *Cambridge advanced learner's dictionary*. Cambridge University Press, 2008.

[3] 3GPP. Isolated Evolved Universal Terrestrial Radio Access Network (E-UTRAN) operation for public safety. TS 22.346. Release 13, 2014.

[4] 3GPP. Security architecture and procedures for 5G system. TS 33.501. Release 15, 2018.

[5] 3GPP. Mission critical services support in the Isolated Operation for Public Safety (IOPS) mode of operation. TS 23.180. Release 17, 2019.

[6] 3GPP. Security of the mission critical service. TS 33.180. Release 16, 2019.

[7] 3GPP. Evolution across three major releases. Poster at Mobile World Conference. 2020. Available online: `https://www.3gpp.org/ftp/Information/presentations/presentations_2020/Poster_2020_MWC_v6_OPTIMIZED.pdf`).

[8] 3GPP. Policy and charging control framework for the 5G System (5GS). TS 23.503. Release 17, 2021.

[9] Naveed Naeem Abbas, Tanveer Ahmed, Syed Habib Ullah Shah, Muhammad Omar, and Han Woo Park. Investigating the applications of artificial intelligence in cyber security. *Scientometrics*, 121(2):1189–1211, 2019.

[10] Sherif Abdelwahab, Bechir Hamdaoui, Mohsen Guizani, and Taieb Znati. Network function virtualization in 5G. *IEEE Communications Magazine*, 54(4):84–91, 2016.

[11] Abdul Ahad, Mohammad Tahir, and Kok-Lim Alvin Yau. 5G-based smart healthcare network: architecture, taxonomy, challenges and future research directions. *IEEE Access*, 7:100747–100762, 2019.

[12] Ijaz Ahmad, Suneth Namal, Mika Ylianttila, and Andrei Gurtov. Security in software defined networks: A survey. *IEEE Communications Surveys & Tutorials*, 17(4):2317–2346, 2015.

[13] Ijaz Ahmad, Jarno Pinola, Ilkka Harjula, Jani Suomalainen, Erkki Harjula, Jyrki Huusko, and Tanesh Kumar. An overview of the security landscape of virtual mobile networks. *IEEE Access*, 2021.

[14] Ijaz Ahmad, Shahriar Shahabuddin, Tanesh Kumar, Jude Okwuibe, Andrei Gurtov, and Mika Ylianttila. Security for 5G and beyond. *IEEE Communications Surveys & Tutorials*, 21(4):3682–3722, 2019.

[15] M. Ejaz Ahmed and Hyoungshick Kim. DDoS attack mitigation in Internet of Things using software defined networking. In *2017 IEEE third international conference on big data computing service and applications (BigDataService)*, pages 271–276. IEEE, 2017.

[16] Adnan Akhunzada, Saif ul Islam, and Sherali Zeadally. Securing cyberspace of future smart cities with 5G technologies. *IEEE Network*, 34(4):336–342, 2020.

[17] Ghada Arfaoui, Pascal Bisson, Rolf Blom, Ravishankar Borgaonkar, Håkan Englund, Edith Félix, Felix Klaedtke, Prajwol Kumar Nakarmi, Mats Näslund, Piers O'Hanlon, Juri Papay, Jani Suomalainen, Mike Surridge, Jean-philippe Wary, and Zahariev Alexander. A security architecture for 5G networks. *IEEE Access*, 6:22466–22479, 2018.

[18] Ghada Arfaoui, José Manuel Sanchez Vilchez, and Jean-Philippe Wary. Security and resilience in 5G: Current challenges and future directions. In *2017 IEEE Trustcom/BigDataSE/ICESS*, pages 1010–1015. IEEE, 2017.

[19] Algirdas Avizienis, J.-C. Laprie, Brian Randell, and Carl Landwehr. Basic concepts and taxonomy of dependable and secure computing. *IEEE transactions on dependable and secure computing*, 1(1):11–33, 2004.

[20] Jayashree Banerjee, Sumana Maiti, Sumalya Chakraborty, Surajit Dutta, Arpita Chakraborty, and Jyoti Sekhar Banerjee. Impact of machine learning in various network security applications. In *2019 3rd International Conference on Computing Methodologies and Communication (ICCMC)*, pages 276–281. IEEE, 2019.

[21] K. Suzanne Barber and Cheryl E. Martin. Agent autonomy: Specification, measurement, and dynamic adjustment. In *Proceedings of the autonomy control software workshop at autonomous agents*, volume 1999, pages 8–15, 1999.

[22] Carl Barks. The Fabulous Philosopher's Stone. *Uncle Scrooge*, (10), 1954.

[23] Marco Barreno, Blaine Nelson, Anthony D Joseph, and J Doug Tygar. The security of machine learning. *Machine Learning*, 81(2):121–148. Springer, 2010.

[24] Marco Barreno, Blaine Nelson, Russell Sears, Anthony D. Joseph, and J. D. Tygar. Can machine learning be secure? In *Proc. 2006 ACM Symposium on Information, Computer and Communications Security (ASIACS'06)*, pages 16–25, New York, NY, USA, 2006. ACM.

[25] Martin Bauer, Ernö Kovacs, Anett Schülke, Naoko Ito, Carmen Criminisi, Laurent-Walter Goix, and Massimo Valla. The context API in the OMA next generation service interface. In *2010 14th International Conference on Intelligence in Next Generation Networks*, pages 1–5. IEEE, 2010.

[26] Chafika Benzaid and Tarik Taleb. AI for Beyond 5G Networks: A Cyber-Security Defense or Offense Enabler? *IEEE Network*, 34(6):140–147, 2020.

[27] Chafika Benzaid, Tarik Taleb, and Muhammad Zubair Farooqi. Trust in 5G and beyond networks. *IEEE Network*, 2021.

[28] Michele Bezzi. An entropy based method for measuring anonymity. In *2007 Third International Conference on Security and Privacy in Communications Networks and the Workshops-SecureComm 2007*, pages 28–32. IEEE, 2007.

[29] Sandeep Bhatt, Pratyusa K. Manadhata, and Loai Zomlot. The operational role of security information and event management systems. *IEEE security & Privacy*, 12(5):35–41, 2014.

[30] Fredrik Björck, Martin Henkel, Janis Stirna, and Jelena Zdravkovic. Cyber resilience–fundamentals for a definition. In *New contributions in information systems and technologies*, pages 311–316. Springer, 2015.

[31] Jesús Bobadilla, Fernando Ortega, Antonio Hernando, and Abraham Gutiérrez. Recommender systems survey. *Knowledge-based systems*, 46:109–132. Elsevier, 2013.

[32] Julien Boite, Pierre-Alexis Nardin, Filippo Rebecchi, Mathieu Bouet, and Vania Conan. Statesec: Stateful monitoring for DDoS protection in software defined networks. In *2017 IEEE Conference on Network Softwarization (NetSoft)*, pages 1–9. IEEE, 2017.

[33] Krzysztof Cabaj, Marcin Gregorczyk, Wojciech Mazurczyk, Piotr Nowakowski, and Piotr Żórawski. Network threats mitigation using software-defined networking for the 5G internet of radio light system. *Security and Communication Networks*, 2019.

[34] Luiz Fernando Carvalho, Taufik Abrão, Leonardo de Souza Mendes, and Mario Lemes Proença Jr. An ecosystem for anomaly detection and mitigation in software-defined networking. *Expert Systems with Applications*, 104:121–133. Elsevier, 2018.

[35] Sheshadri Chatterjee, Arpan Kumar Kar, and M.P. Gupta. Critical success factors to establish 5G network in smart cities: Inputs for security and privacy. *Journal of Global Information Management (JGIM)*, 25(2):15–37. IGI Global, 2017.

[36] Baozhan Chen, Siyuan Qiao, Jie Zhao, Dongqing Liu, Xiaobing Shi, Minzhao Lyu, Haotian Chen, Huimin Lu, and Yunkai Zhai. A security awareness and protection system for 5G smart healthcare based on zero-trust architecture. *IEEE Internet of Things Journal*, 2020.

[37] I. Chih-Lin, Slawomir Kuklinski, Tao Chen, and Latif Ladid. A perspective of O-RAN integration with MEC, SON, and network slicing in the 5G era. *IEEE Network*, 34(6):3–4, 2020.

[38] Tommy Chin, Xenia Mountrouidou, Xiangyang Li, and Kaiqi Xiong. Selective packet inspection to detect DoS flooding using software defined networking (SDN). In *2015 IEEE 35th international conference on distributed computing systems workshops*, pages 95–99. IEEE, 2015.

[39] Tommy Chin, Kaiqi Xiong, and Chengbin Hu. Phishlimiter: A phishing detection and mitigation approach using software-defined networking. *IEEE Access*, 6:42516–42531, 2018.

[40] Mosharaf Chowdhury and Raouf Boutaba. A survey of network virtualization. *Computer Networks*, 54(5):862–876. Elsevier, 2010.

[41] Sandy Clark, Travis Goodspeed, Perry Metzger, Zachary Wasserman, Kevin Xu, and Matt Blaze. Why (special agent) Johnny (still) can't encrypt: A security analysis of the APCO project 25 two-way radio system. In *USENIX Security Symposium*, volume 2011, pages 8–12, 2011.

[42] Heng Cui, Ghassan O. Karame, Felix Klaedtke, and Roberto Bifulco. On the fingerprinting of software-defined networks. *IEEE Transactions on Information Forensics and Security*, 11(10):2160–2173, 2016.

[43] Chamitha De Alwis, Anshuman Kalla, Quoc-Viet Pham, Pardeep Kumar, Kapal Dev, Won-Joo Hwang, and Madhusanka Liyanage. Survey on 6G frontiers: Trends, applications, requirements, technologies and future research. *IEEE Open Journal of the Communications Society*, 2021.

[44] Dorothy E. Denning. Framework and principles for active cyber defense. *Computers & Security*, 40:108–113.

[45] Ed Kamya Kiyemba Edris, Mahdi Aiash, and Jonathan Kok-Keng Loo. The case for federated identity management in 5G communications. In *2020 Fifth International Conference on Fog and Mobile Edge Computing (FMEC)*, pages 120–127. IEEE, 2020.

[46] Chris Edwards. Moore's law: what comes next? *Communications of the ACM*, 64(2):12–14, 2021.

[47] Ericsson. Ericsson mobility report, 2020. Available online at www.ericsson.com/4adc87/assets/local/mobility-report/documents/2020/november-2020-ericsson-mobility-report.pdf.

[48] ETSI. Experiential Networked Intelligence (ENI); ENI Use Cases; Standard ETSI GR ENI 001, 2011.

[49] ETSI. Network Functions Virtualisation (NFV) Release 3; Security; Security Management and Monitoring specification, Standard ETSI NFV-SEC 013, 2017.

[50] European Commission. Cybersecurity of 5G networks - EU toolbox of risk mitigating measures, 2020. Available online: https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures.

[51] European Commission. Proposal for a regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), 2021. Available online: ec.europa.eu/newsroom/dae/document.cfm?doc_id=75788. Accessed on 21 April 2021).

[52] J.B. Evans, G.J. Minden, K.S. Shanmugan, G. Prescott, V.S. Frost, B. Ewy, R. Sanchez, C. Sparks, K. Malinimohan, J. Roberts, R. Plumb, and D. Petr. The rapidly deployable radio network. *IEEE Journal on Selected Areas in Communications*, 17(4):689–703, 1999.

[53] Antti Evesti, Jani Suomalainen, and Eila Ovaska. Architecture and knowledge-driven self-adaptive security in smart space. *Computers*, 2(1):34–66. MDPI, 2013.

[54] Hamid Farhady, HyunYong Lee, and Akihiro Nakao. Software-defined networking: A survey. *Computer Networks*, 81:79–95. Elsevier, 2015.

[55] David B. Fogel and Lawrence J. Fogel. Evolution and computational intelligence. In *International Conference on Neural Networks (ICNN'95)*, volume 4, pages 1938–1941. IEEE, 1995.

[56] Vitaly Ford and Ambareen Siraj. Applications of machine learning in cyber security. In *27th International Conference on Computer Applications in Industry and Engineering*, volume 118. IEEE, 2014.

[57] Xenofon Foukas, Georgios Patounas, Ahmed Elmokashfi, and Mahesh K. Marina. Network slicing in 5G: Survey and challenges. *IEEE Communications Magazine*, 55(5):94–100, 2017.

[58] Jeremy Freeman. Introducing Streaming k-Means in Apache Spark 1.2. Databrics, Engineering Blog., 2015. Available online at databricks.com/blog/2015/01/28/introducing-streaming-k-means-inspark-1-2.html. Accessed 17 May 2021.

[59] Hamidreza Ghafghazi, Amr El Mougy, Hussein T. Mouftah, and Carlisle Adams. Security and Privacy in LTE-based Public Safety Network. In *Wireless Public Safety Networks 2*, pages 317–364. Elsevier, 2016.

[60] Ben Goertzel. *The hidden pattern: A patternist philosophy of mind*. Universal-Publishers, 2006.

[61] German Peinado Gomez, Jordi Mongay Batalla, Yoan Miche, Silke Holtmanns, Constandinos X. Mavromoustakis, George Mastorakis, and Noman Haider. Security policies definition and enforcement utilizing policy control function framework in 5G. *Computer Communications*, 172:226–237, 2021.

[62] Pål Grønsund, Andres Gonzalez, Kashif Mahmood, Kennet Nomeland, Jan Pitter, Antonios Dimitriadis, Tom-Kristian Berg, and Stephen Gelardi. 5G service and slice implementation for a military use case. In *2020 IEEE International Conference on Communications Workshops (ICC Workshops)*, pages 1–6. IEEE, 2020.

[63] 5G PPP Security Group. 5G PPP phase1 security landscape - white paper, 2017. Available online at 5g-ppp.eu/new-security-group-5g-ppp-white-paper-phase-1-security-landscape/.

[64] Trusted Computing Group. Implicit identity based device attestation, version 1.0, revision 0.93, standard, 2018.

[65] GSMA. RSP Architecture, version 2.2. SGP.21, standard, 2017. Available online at www.gsma.com/newsroom/wp-content/uploads/SGP.21_v2.2.pdf.

[66] Noman Haider, Muhammad Zeeshan Baig, and Muhammad Imran. Artificial intelligence and machine learning in 5G network security: Opportunities, advantages, and future research trends. *arXiv preprint arXiv:2007.04490*, 2020.

[67] Yogita Hande and Akkalashmi Muddana. A survey on intrusion detection system for software defined networks (SDN). In *Research Anthology on Artificial Intelligence Applications in Security*, pages 467–489. IGI Global, 2021.

[68] Nelson Hastings and Joshua M. Franklin. *Considerations for identity management in public safety mobile networks*. US Department of Commerce, National Institute of Standards and Technology, 2015.

[69] Marjo Heikkilä, Pekka Koskela, Jani Suomalainen, Kalle Lähetkangas, Tero Kippola, Pentti Eteläaho, Juha Erkkilä, and Ari Pouttu. Field trial with tactical bubbles for mission critical communications. *Transactions on Emerging Telecommunications Technologies*, 32. Wiley, 2021.

[70] Marjo Heikkilä, Jani Suomalainen, Ossi Saukko, Tero Kippola, Kalle Lähetkangas, Pekka Koskela, Juha Kalliovaara, Hannu Haapala, Juho Pirttiniemi, Anastasia Yastrebova, et al. Unmanned agricultural tractors in private mobile networks. *Network*, 2(1):1–20. MDPI, 2022.

[71] Ronda R. Henning. Security service level agreements: quantifiable security for the enterprise? In *1999 Workshop on New Security Paradigms*, pages 54–60. ACM, 1999.

[72] Jouni Hiltunen, Pekka Ruuska, and Jani Suomalainen. Trust metric enabler open specifications. 5G-ENSURE project. deliverable D3.6. 5G-PPP security enablers open specifications (v2.0), 2017.

[73] Michael C. Hout, Megan H. Papesh, and Stephen D. Goldinger. Multidimensional scaling. *Wiley Interdisciplinary Reviews: Cognitive Science*, 4(1):93–103, 2013.

[74] Marko Höyhtyä, Kalle Lähetkangas, Jani Suomalainen, Mika Hoppari, Kaisa Kujanpää, Kien Trung Ngo, Tero Kippola, Marjo Heikkilä, Harri Posti, Jari Mäki, et al. Critical communications over mobile operators' networks: 5G use cases enabled by licensed spectrum sharing, network slicing and QoS control. *IEEE Access*, 6:73572–73582, 2018.

[75] Dingwen Hu, Peilin Hong, and Yixin Chen. FADM: DDoS flooding attack detection and mitigation system in software-defined networking. In *2017 IEEE Global Communications Conference (GLOBECOM 2017)*, pages 1–7. IEEE, 2017.

[76] Rasheed Hussain, Fatima Hussain, and Sherali Zeadally. Integration of VANET and 5G Security: A review of design and implementation issues. *Future Generation Computer Systems*, 101:843–864.

[77] Syed Hussain, Omar Chowdhury, Shagufta Mehnaz, and Elisa Bertino. LTEInspector: A systematic approach for adversarial testing of 4G LTE. In *Network and Distributed Systems Security (NDSS) Symposium*, 2018.

[78] Syed Rafiul Hussain, Mitziu Echeverria, Imtiaz Karim, Omar Chowdhury, and Elisa Bertino. 5GReasoner: A property-directed security and privacy analysis framework for 5G cellular network protocol. In *2019 ACM SIGSAC Conference on Computer and Communications Security*, pages 669–684, 2019.

[79] Syed Rafiul Hussain, Mitziu Echeverria, Ankush Singla, Omar Chowdhury, and Elisa Bertino. Insecure connection bootstrapping in cellular networks: the root of all evil. In *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*, pages 1–11. ACM, 2019.

[80] I. Indu, P. M. Rubesh Anand, and Vidhyacharan Bhaskar. Identity and access management in cloud environment: Mechanisms and challenges. *Engineering science and technology, an international journal*, 21(4):574–588. Elsevier, 2018.

[81] Chadni Islam, Muhammad Ali Babar, and Surya Nepal. A multi-vocal review of security orchestration. *ACM Computing Surveys (CSUR)*, 52(2):1–45, 2019.

[82] ITU-T. X.805: Security architecture for systems providing end-to-end communications, 2003. Available online at `www.itu.int/rec/T-REC-X.805-200310-I/en`.

[83] Tariq Javid, Tehseen Riaz, and Asad Rasheed. A layer2 firewall for software defined network. In *2014 Conference on Information Assurance and Cyber Security (CIACS)*, pages 39–42. IEEE, 2014.

[84] Marek Jawurek, Martin Johns, and Konrad Rieck. Smart metering de-pseudonymization. In *Proceedings of the 27th annual computer security applications conference*, pages 227–236. ACM, 2011.

[85] Jukka Julku, Jani Suomalainen, and Kylänpää Markku. Delegated device attestation for IoT. In *8th International Conference on Internet of Things: Systems, Management and Security (IoTSMS)*. IEEE, 2021.

[86] Hammad Kabir, Raimo Kantola, and Jesus Llorente Santos. Customer edge switching: A security framework for 5G. pages 195–230, 2018.

[87] Peyman Kabiri and Ali A. Ghorbani. Research on intrusion detection and response: A survey. *International Journal of Network Security*, 1(2):84–102. National Chung Hsing University, 2005.

[88] Evgenia Kapassa, Marios Touloupou, Argyro Mavrogiorgou, and Dimosthenis Kyriazis. 5G & SLAs: Automated proposition and management of agreements towards QoS enforcement. In *2018 21st Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN)*, pages 1–5. IEEE, 2018.

[89] Josh Karlin, Stephanie Forrest, and Jennifer Rexford. Autonomous security for autonomous systems. *Computer Networks*, 52(15):2908–2923. Elsevier, 2008.

[90] Kallol Krishna Karmakar, Vijay Varadharajan, and Uday Tupakula. Mitigating attacks in software defined networks. *Cluster Computing*, 22(4):1143–1157, 2019.

[91] Gaganjot Kaur and Prinima Gupta. Hybrid approach for detecting ddos attacks in software defined networks. In *2019 Twelfth International Conference on Contemporary Computing (IC3)*, pages 1–6. IEEE, 2019.

[92] Ashiq Khan, Alf Zugenmaier, Dan Jurca, and Wolfgang Kellerer. Network virtualization: a hypervisor for the internet? *IEEE Communications Magazine*, 50(1):136–143, 2012.

[93] Haibat Khan and Keith M. Martin. A survey of subscription privacy on the 5G radio interface-the past, present and future. *Journal of Information Security and Applications*, 53:102537.

[94] Latif U. Khan, Ibrar Yaqoob, Nguyen H. Tran, Zhu Han, and Choong Seon Hong. Network slicing: Recent advances, taxonomy, requirements, and open research challenges. *IEEE Access*, 8:36009–36028, 2020.

[95] Yacine Khettab, Miloud Bagaa, Diego Leonel Cadette Dutra, Tarik Taleb, and Nassima Toumi. Virtual security as a service for 5G verticals. In *2018 IEEE Wireless Communications and Networking Conference (WCNC)*, pages 1–6. IEEE, 2018.

[96] Hongil Kim, Jiho Lee, Eunkyu Lee, and Yongdae Kim. Touching the untouchables: Dynamic security analysis of the LTE control plane. In *2019 IEEE Symposium on Security and Privacy (SP)*, pages 1153–1168. IEEE, 2019.

[97] Denis Foo Kune, John Koelndorfer, Nicholas Hopper, and Yongdae Kim. Location leaks on the GSM air interface. In *Annual Network & Distributed System Security (NDSS) Symposium*. Internet Society, 2012.

[98] Chengzhe Lai, Rongxing Lu, Dong Zheng, and Xuemin Sherman Shen. Security and privacy challenges in 5G-enabled vehicular networks. *IEEE Network*, 34(2):37–45, 2020.

[99] Adrian Lara, Anisha Kolasani, and Byrav Ramamurthy. Network innovation using OpenFlow: A survey. *IEEE communications surveys & tutorials*, 16(1):493–512, 2013.

[100] Shane Legg and Marcus Hutter. A collection of definitions of intelligence. *Frontiers in Artificial Intelligence and applications*, 157:17. IOS press, 2007.

[101] Ninghui Li, Tiancheng Li, and Suresh Venkatasubramanian. t-closeness: Privacy beyond k-anonymity and l-diversity. In *2007 IEEE 23rd International Conference on Data Engineering*, pages 106–115. IEEE, 2007.

[102] Hung-Jen Liao, Chun-Hung Richard Lin, Ying-Chih Lin, and Kuang-Yuan Tung. Intrusion detection system: A comprehensive review. *Journal of Network and Computer Applications*, 36(1):16–24. Elsevier, 2013.

[103] Madhusanka Liyanage, Ijaz Ahmad, Jude Okwuibe, E. Montes de Oca, Hoang Long Mai, O. López, and M. Uriarte. Software defined security monitoring in 5G networks. In *A comprehensive guide to 5G security*, pages 231–243. Wiley Hoboken, NJ, USA, 2018.

[104] Rongxing Lu, Lan Zhang, Jianbing Ni, and Yuguang Fang. 5G vehicle-to-everything services: Gearing up for security and privacy. *Proceedings of the IEEE*, 108(2):373–389, 2019.

[105] Duohe Ma, Zhen Xu, and Dongdai Lin. Defending blind DDoS attack on SDN based on moving target defense. In *International Conference on Security and Privacy in Communication Networks*, pages 463–480. Springer, 2014.

[106] James MacQueen. Some methods for classification and analysis of multivariate observations. In *Proceedings of the fifth Berkeley symposium on mathematical statistics and probability*, volume 1, pages 281–297. Oakland, CA, USA, 1967.

[107] Aarne Mämmelä, Jukka Riekki, Adrian Kotelba, and Antti Anttonen. Multidisciplinary and historical perspectives for developing intelligent and resource-efficient systems. *IEEE Access*, 6:17464–17499, 2018.

[108] Olli Mämmelä, Jouni Hiltunen, Jani Suomalainen, Kimmo Ahola, Petteri Mannersalo, and Janne Vehkaperä. Towards micro-segmentation in 5G network security. In *European Conference on Networks and Communications (EuCNC 2016) Workshop on Network Management, Quality of Service and Security for 5G Networks*, 2016.

[109] Vasileios Mavroeidis and Siri Bromander. Cyber threat intelligence model: an evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence. In *2017 European Intelligence and Security Informatics Conference (EISIC)*, pages 91–98. IEEE, 2017.

[110] Andrew R. McGee, Matthieu Coutière, and Maria E. Palamara. Public safety network security considerations. *Bell Labs Technical Journal*, 17(3):79–86, 2012.

[111] Nick McKeown, Tom Anderson, Hari Balakrishnan, Guru Parulkar, Larry Peterson, Jennifer Rexford, Scott Shenker, and Jonathan Turner. Openflow: enabling innovation in campus networks. *ACM SIGCOMM computer communication review*, 38(2):69–74, 2008.

[112] David J. Miller, Zhen Xiang, and George Kesidis. Adversarial learning targeting deep neural network classification: A comprehensive review of defenses against attacks. *Proceedings of the IEEE*, 108(3):402–433, 2020.

[113] Karen Miranda, Antonella Molinaro, and Tahiry Razafindralambo. A survey on rapidly deployable solutions for post-disaster networks. *IEEE Communications Magazine*, 54(4):117–123, 2016.

[114] Manuel Eugenio Morocho-Cayamcela, Haeyoung Lee, and Wansu Lim. Machine learning for 5G/B5G mobile and wireless communications: Potential, limitations, and future directions. *IEEE Access*, 7:137184–137206, 2019.

[115] Next Generation Mobile Network Alliance. Description of network slicing concept, technical report. 2016. Available online: `www.ngmn.org/wp-content/uploads/Publications/2016/161010_NGMN_Network_Slicing_framework_v1.0.8.pdf`. Accessed on 21 April 2021.

[116] Kien Trung Ngo, Mika Hoppari, Jani Suomalainen, and Marko Höyhtyä. Distributed LSA controller for public safety communications. In *2018 IEEE 4th International Conference on Computer and Communications (ICCC)*, pages 1134–1138. IEEE, 2018.

[117] Jude Okwuibe, Madhusanka Liyanage, Ijaz Ahmad, and Mika Ylianttila. Cloud and MEC security. In *A Comprehensive Guide to 5G Security*, pages 373–397. Wiley Hoboken, NJ, USA, 2018.

[118] Jad Oueis, Vania Conan, Damien Lavaux, Razvan Stanica, and Fabrice Valois. Overview of LTE isolated E-UTRAN operation for public safety. *IEEE Communications Standards Magazine*, 1(2):98–105, 2017.

[119] Nicolas Papernot, Patrick McDaniel, Arunesh Sinha, and Michael P. Wellman. SoK: Security and privacy in machine learning. In *Proc. 2018 IEEE European Symposium on Security and Privacy (EuroS&P)*, pages 399–414. IEEE, 2018.

[120] Justin Gregory V Pena and William Emmanuel Yu. Development of a distributed firewall using software defined networking technology. In *2014 4th IEEE International Conference on Information Science and Technology*, pages 449–452. IEEE, 2014.

[121] Richard Piggin and Ian Buffey. Active defence using an operational technology honeypot. In *11th International Conference on System Safety and Cyber-Security (SSCS 2016)*. IET, 2016.

[122] Esa Piri, Pekka Ruuska, Teemu Kanstrén, Jukka Mäkelä, Jari Korva, Atso Hekkala, Ari Pouttu, Olli Liinamaa, Matti Latva-Aho, Kari Vierimaa, et al. 5GTN: A test network for 5G application development and testing. In *2016 European Conference on Networks and Communications (EuCNC)*, pages 313–318. IEEE, 2016.

[123] Pawani Porambage, Gürkan Gür, Diana Pamela Moya Osorio, Madhusanka Liyanage, Andrei Gurtov, and Mika Ylianttila. The roadmap to 6G security and privacy. *IEEE Open Journal of the Communications Society*, 2:1094–1122, 2021.

[124] Anand R. Prasad, Sivabalan Arumugam, B. Sheeba, and Alf Zugenmaier. 3GPP 5G security. *Journal of ICT Standardization*, 6(1):137–158. River Publishers, 2018.

[125] Haneya Naeem Qureshi, Marvin Manalastas, Syed Muhammad Asad Zaidi, Ali Imran, and Mohamad Omar Al Kalaa. Service level agreements for 5G and beyond: Overview, challenges and enablers of 5G-healthcare systems. *IEEE Access*, 2020.

[126] Jayaprakash Ramprasath and V. Seethalakshmi. Improved network monitoring using software-defined networking for DDoS detection and mitigation evaluation. *Wireless Personal Communications*, 116(3):2743–2757. Springer, 2021.

[127] Omer Rana, Martijn Warnier, Thomas B. Quillinan, and Frances Brazier. Monitoring and reputation mechanisms for service level agreements. In *International Workshop on Grid Economics and Business Models*, pages 125–139. Springer, 2008.

[128] Siddharth Prakash Rao, Silke Holtmanns, and Tuomas Aura. Threat modeling framework for mobile communication systems. *arXiv preprint arXiv:2005.05110*, 2020.

[129] Sriganesh K. Rao and Ramjee Prasad. Impact of 5G technologies on industry 4.0. *Wireless Personal Communications*, 100(1):145–159. Springer, 2018.

[130] Rishikesh Sahay, Weizhi Meng, and Christian D. Jensen. The application of software defined networking on securing computer networks: A survey. *Journal of Network and Computer Applications*, 131:89–108. Elsevier, 2019.

[131] Natsuhiko Sakimura, John Bradley, Mike Jones, Breno De Medeiros, and Chuck Mortimore. OpenID connect core 1.0. *The OpenID Foundation*, 2014.

[132] Dhaval Satasiya et al. Analysis of software defined network firewall (sdf). In *2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, pages 228–231. IEEE, 2016.

[133] Sailik Sengupta, Ankur Chowdhary, Abdulhakim Sabur, Adel Alshamrani, Dijiang Huang, and Subbarao Kambhampati. A survey of moving target defenses for network security. *IEEE Communications Surveys & Tutorials*, 22(3):1909–1941, 2020.

[134] Altaf Shaik, Ravishankar Borgaonkar, N. Asokan, Valtteri Niemi, and Jean-Pierre Seifert. Practical attacks against privacy and availability in 4G/LTE mobile communication systems. In *Annual Network & Distributed System Security (NDSS) Symposium*. Internet Society, 2016.

[135] Vishal Sharma, Ilsun You, and Nadra Guizani. Security of 5G-V2X: Technologies, standardization, and research directions. *IEEE Network*, 34(5):306–314, 2020.

[136] Adam Shostack. Experiences Threat Modeling at Microsoft. In *Proceedings of the Workshop on Modeling Security (MODSEC08) held as part of the 2008 International Conference on Model Driven Engineering Languages and Systems (MODELS)*, CEUR Workshop Proceedings. CEUR-WS.org, 2008.

[137] Chris J. Skinner and M.J. Elliot. A measure of disclosure risk for microdata. *Journal of the Royal Statistical Society: series B (statistical methodology)*, 64(4):855–867. Wiley Online Library, 2002.

[138] Keith E. Stanovich, Richard F. West, and Maggie E. Toplak. *The rationality quotient: Toward a test of rational thinking*. MIT press, 2016.

[139] James Sterbenz, David Hutchison, Egemen Çetinkaya, Abdul Jabbar, Justin Rohrer, Marcus Schöller, and Paul Smith. Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines. *Computer Networks*, 54(8):1245–1265. Elsevier, 2010.

[140] Michelle Suh, Sae Hyong Park, Byungjoon Lee, and Sunhee Yang. Building firewall over the software-defined network controller. In *16th International Conference on Advanced Communication Technology*, pages 744–748. IEEE, 2014.

[141] Jing Sun, Qing Yu, Muheyat Niyazbek, and Fayuan Chu. 5G network information technology and military information communication data services. *Microprocessors and Microsystems*, page 103459. Elsevier, 2020.

[142] Jani Suomalainen. Flexible security deployment in smart spaces. In *International Conference on Grid and Pervasive Computing*, pages 34–43. Springer, 2011.

[143] Jani Suomalainen. Smartphone assisted security pairings for the Internet of Things. In *2014 4th International Conference on Wireless Communications, Vehicular Technology, Information Theory and Aerospace & Electronic Systems (VITAE)*, pages 1–5. IEEE, 2014.

[144] Jani Suomalainen and Pasi Hyttinen. Security solutions for smart spaces. In *2011 IEEE/IPSJ International Symposium on Applications and the Internet*, pages 297–302. IEEE, 2011.

[145] Jani Suomalainen, Pasi Hyttinen, and Pentti Tarvainen. Secure information sharing between heterogeneous embedded devices. In *Proceedings of the Fourth European Conference on Software Architecture: Companion Volume*, pages 205–212. ACM, 2010.

[146] Jani Suomalainen, Jukka Julku, Antti Heikkinen, Seppo J. Rantala, and Anastasia Yastrebova. Security-driven prioritization for tactical mobile networks. A manuscript submitted for publication, 2022.

[147] Jani Suomalainen, Jukka Valkonen, and N. Asokan. Standards for security associations in personal networks: a comparative analysis. *International Journal of Security and Networks*, 4(1-2):87–100, Inderscience Publishers, 2009.

[148] Rochak Swami, Mayank Dave, and Virender Ranga. Software-defined networking-based DDoS defense mechanisms. *ACM Computing Surveys (CSUR)*, 52(2):1–36, 2019.

[149] Latanya Sweeney. k-anonymity: A model for protecting privacy. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, 10(05):557–570. World Scientific, 2002.

[150] Tarik Taleb, Konstantinos Samdanis, Badr Mada, Hannu Flinck, Sunny Dutta, and Dario Sabella. On multi-access edge computing: A survey of the emerging 5G network edge cloud architecture and orchestration. *IEEE Communications Surveys & Tutorials*, 19(3):1657–1681, 2017.

[151] Tuan A. Tang, Lotfi Mhamdi, Des McLernon, Syed Ali Raza Zaidi, and Mounir Ghogho. Deep learning approach for network intrusion detection in software defined networking. In *2016 International Conference on Wireless Networks and Mobile Communications (WINCOM)*, pages 258–263. IEEE, 2016.

[152] The Mitre Corporation. MITRE ATT&CK® Matrices for Mobile, 2021. Available online: `attack.mitre.org/matrices/mobile/`. Accessed on 7 June 2021.

[153] Neil C. Thompson, Kristjan Greenewald, Keeheon Lee, and Gabriel F Manso. The computational limits of deep learning. *arXiv preprint arXiv:2007.05558*, 2020.

[154] Giannis Tziakouris, Rami Bahsoon, and Muhammad Ali Babar. A survey on self-adaptive security for large-scale open environments. *ACM Computing Surveys (CSUR)*, 51(5):1–42, 2018.

[155] Sun Tzu. *The art of war*. Delacorte Press, 1983.

[156] Pal Varga, Jozsef Peto, Attila Franko, David Balla, David Haja, Ferenc Janky, Gabor Soos, Daniel Ficzere, Markosz Maliosz, and Laszlo Toka. 5G support for industrial IoT applications–challenges, solutions, and research gaps. *Sensors*, 20(3):828. MDPI, 2020.

[157] Mikko Vehkaperä, Mika Hoppari, Jani Suomalainen, Jussi Roivainen, and Seppo J. Rantala. Testbed for Local-Area Private Network with Satellite-Terrestrial Backhauling. In *Third International Conference on Electrical, Communication and Computer Engineering (ICECCE)*. IEEE, 2021.

[158] VMware. Data Center Micro-Segmentation: A Software Defined Data Center Approach for a "Zero Trust" Security Strategy. Technical report, 2014.

[159] Thomas D. Wagner, Khaled Mahbub, Esther Palomar, and Ali E. Abdallah. Cyber threat intelligence sharing: Survey and research directions. *Computers & Security*, 87:101589. Elsevier, 2019.

[160] Min Xie, Qiong Zhang, Andres J Gonzalez, Pål Grønsund, Paparao Palacharla, and Tadashi Ikeuchi. Service assurance in 5G networks: A study of joint monitoring and analytics. In *2019 IEEE 30th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, pages 1–7. IEEE, 2019.

[161] William E. Yancey, William E. Winkler, and Robert H. Creecy. Disclosure risk assessment in perturbative microdata protection. In *Inference control in statistical databases*, pages 135–152. Springer, 2002.

[162] Jing Yang and Thomas Johansson. An overview of cryptographic primitives for possible use in 5G and beyond. *Science China Information Sciences*, 63(12):1–22. Springer, 2020.

[163] Lin Ye, Hongli Zhang, Jiantao Shi, and Xiaojiang Du. Verifying cloud service level agreement. In *2012 IEEE Global Communications Conference (GLOBECOM)*, pages 777–782. IEEE, 2012.

[164] Mika Ylianttila, Raimo Kantola, Andrei Gurtov, Lozenzo Mucchi, Ian Oppermann, Zheng Yan, Tri Hong Nguyen, Fei Liu, Tharaka Hewa, Madhusanka Liyanage, et al. 6G white paper: Research challenges for trust, security and privacy. *arXiv preprint arXiv:2004.11665*, 2020.

[165] Xiaoyong Yuan, Pan He, Qile Zhu, and Xiaolin Li. Adversarial examples: Attacks and defenses for deep learning. *IEEE Transactions on Neural Networks and Learning Systems*, 30(9):2805–2824, Sep. 2019.

[166] Salaheddine Zerkane, David Espes, Philippe Le Parc, and Frederic Cuppens. Software defined networking reactive stateful firewall. In *IFIP International Conference on ICT Systems Security and Privacy Protection*, pages 119–132. Springer, 2016.

[167] C. Zhang, P. Patras, and H. Haddadi. Deep learning in mobile and wireless networking: A survey. *IEEE Communications Surveys & Tutorials*, 21(3):2224–2287, 2019.

[168] Hong-qi Zhang, Cheng Lei, De-xian Chang, and Ying-jie Yang. Network moving target defense technique based on collaborative mutation. *Computers & security*, 70:51–71. Elsevier, 2017.

[169] Carson Zimmerman. Cybersecurity operations center. *The MITRE Corporation*, 2014.

The evolution of 5G networks and beyond is a path toward new applications and increased quality and cost-efficiency of communications and services. But how is the security of mobile networks evolving? Will the 5G and 6G networks revolutionize the security of communications for public safety, smart city, and industrial users? What customization do different end-users need to secure their applications? How do network operators, standardization parties, and application providers solve the requirements for differentiated security? What does active and intelligent defense mean in the context of mobile networks? How can we use edge and cloud technologies, network slicing, and micro-segmentation to keep different applications in isolated bubbles and to evolve intelligence of security solutions in mobile networks? What is the role of artificial intelligence and machine learning in the threat detection and trustworthiness of 5G networks and beyond?

Aalto-DT 35/2022

ISBN 978-952-64-0722-7 (printed)
ISBN 978-952-64-0723-4 (pdf)
ISSN 1799-4934 (printed)
ISSN 1799-4942 (pdf)

**Aalto University**
**School of Science**
**Department of Computer Science**
**www.aalto.fi**

**BUSINESS + ECONOMY**

**ART + DESIGN + ARCHITECTURE**

**SCIENCE + TECHNOLOGY**

**CROSSOVER**

**DOCTORAL THESES**