**VTT Technical Research Centre of Finland**

# Securing Public Safety Communications on Commercial and Tactical 5G Networks

Suomalainen, Jani; Julku, Jukka; Vehkapera, Mikko; Posti, Harri

*Published in:*
IEEE Open Journal of the Communications Society

Published: 02/07/2021

*Document Version*
Publisher's final version

Received 30 May 2021; accepted 27 June 2021. Date of publication 2 July 2021; date of current version 15 July 2021.

*Digital Object Identifier 10.1109/OJCOMS.2021.3093529*

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

**JANI SUOMALAINEN [1], JUKKA JULKU [1], MIKKO VEHKAPERÄ [2], AND HARRI POSTI [3]**

[1] VTT Technical Research Centre of Finland, 02044 Espoo, Finland

[2] VTT Technical Research Centre of Finland, 90571 Oulu, Finland

[3] Centre for Wireless Communications, University of Oulu, 90570 Oulu, Finland

CORRESPONDING AUTHOR: J. SUOMALAINEN (e-mail: jani.suomalainen@vtt.fi)

This work was supported in part by the Business Finland and in part by the consortium partners of the PRIORITY Project.

**ABSTRACT** The forthcoming communication networks for public safety authorities rely on the fifth generation (5G) of mobile networking technologies. Police officers, paramedics, border guards, as well as fire and rescue personnel, will connect through commercial operator's access network and rapidly deployable tactical bubbles. This transition from closed and dedicated infrastructure to hybrid architecture will expand the threat surface and expose mission-critical applications and sensitive information to cyber and physical adversaries. We explore and survey security architecture and enablers for prioritized public safety communication in 5G networks. We identify security threat scenarios and analyze enabling vulnerabilities, threat actors, attacks vectors, as well as risk levels. Security enablers are surveyed for tactical access and core networks, commercial infrastructure, and mission-critical applications, starting from push-to-talk and group video communication and leading to situational-awareness and remote-controlled systems. Two solutions are trialed and described in more detail: remote attestation enhanced access control for constrained devices, and securing of satellite backhauls. We also discuss future research directions highlighting the need for enablers to automate security of rapid deployments, for military-grade cost-effective customizations of commercial network services to ensure robustness, and for hardening of various types of public safety equipment.

**INDEX TERMS** 5G, cybersecurity, hybrid architecture, mobile network, public safety, security, survey, tactical bubble, trials.

## I. INTRODUCTION

PUBLIC safety actors, including law enforcement, border control, as well as fire and rescue services, have traditionally used closed networks with high-security and narrow-bandwidth properties for voice and text-based communication. However, the high costs of maintaining a dedicated communication infrastructure as well as potential advantages from emerging applications—such as surveillance and situational-awareness based on unmanned aerial systems, wireless and wearable sensor networks, high-definition video, augmented reality, as well as autonomous vehicles and robots—necessitate an upgrading of the networking approach. The next generation of public safety networks are expected [1] to be based on 3GPP specified broadband mobile technologies and to follow hybrid architecture consisting of both commercial mobile operator network infrastructure as well as rapidly deployable tactical network bubbles. Tactical bubbles provide extra capacity and coverage for public safety users in remote rural locations and in cases where availability of commercial network is disrupted, e.g., due to congestion, failure, cyber-attack, or disaster. The hybrid network infrastructure promises cost-effective means to achieve communication in any location with good quality (broadband, low latency, low jitter, and scalability). However, sharing infrastructure between civilian and public safety users introduces new challenges for

**TABLE 1.** Surveys in the area of public safety communications (PSC), rapidly deployable network (RDN), and 5G and beyond network security. The main focus is marked with ● and shortly covered topics are marked with ○.

| *Author* | *Short description* | *Scope* | | | | | |
|---|---|---|---|---|---|---|---|
| | | *Pre 5G security* | *5G security* | *RDN security* | *RDN for PSC* | *PSC in pre 5G* | *PSC in 5G* |
| Ahmad et al. [12] | Security for 5G and beyond | ○ | ● | - | - | - | - |
| Arfaoui et al. [14] | Architectural security requirements for 5G | ○ | ● | - | - | - | - |
| Barca et al. [20] | Security in European TETRA networks | ● | - | - | - | ● | - |
| Burbank et al. [23] | Challenges in military tactical networks | - | - | ○ | ○ | ○ | - |
| Clark et al. [19] | Security challenges in American P25 network | ● | - | - | - | ● | - |
| Ghafghazi et al. [21] | Security and privacy in LTE based PSC | ● | - | - | - | ● | - |
| Hastings et al. [25] | LTE security for PSC | ● | - | - | - | ● | - |
| Höyhtyä et al. [1] | PCS in RDN and commercial 5G | ○ | ○ | - | ● | ○ | ● |
| Khan et al. [13] | 5G privacy and security | ○ | ● | - | - | - | - |
| Kumbhar et al. [15] | PSC in LTE and 5G | - | - | - | - | ● | ● |
| McGee et al. [18] | Security requirements for dedicated PSC | ● | - | - | - | ● | - |
| Miranda et al. [22] | Rapidly deployable solutions for PSC | - | - | - | ● | ● | - |
| Ponsam et al. [24] | Mobile ad-hoc network security | ○ | - | ● | - | - | - |
| Oueis et al. [5] | 3GPP's solutions for isolated operations | - | - | ○ | ● | ○ | - |
| Rao et al. [167] | Mobile network specific threat collection | ● | ● | - | - | - | - |
| Raza et al. [17] | Applications and standards for 5G PSC | - | - | - | - | ○ | ● |
| Yu et al. [16] | User and network side solutions for PSC | - | - | - | - | ○ | ● |
| Our contribution | Tactical and commercial 5G security for PSC | ○ | ● | ● | ○ | ○ | ● |

ensuring availability, trustworthiness, and security. The threat landscape in commercial and Internet-exposed networks is significantly larger when compared to dedicated and closed networks.

5G standardization, being carried out by the third generation partnership project (3GPP) and industry, is progressing to secure the access and core networks [2], [3] and to support public safety communications with isolated operational capabilities [4]–[6], with mission-critical voice [7], data [8], and video [9] applications, and with a security framework [10]. However, the standardization focuses on the network perspective and ignores many application, user equipment, life cycle, infrastructure, and use case specific issues needed for a holistic point of view. Recent surveys [11]–[14] on security of the 5G networks have identified and classified threats without focusing on public safety specific requirements. On the other hand, existing surveys [1], [15]–[17] on public safety communication have addressed mission-critical applications on commercial 5G mobile networks without a security focus. Surveys on security for public safety communication have focused on dedicated networks [18]–[20] or previous generations [5], [21] and have emphasized particular challenges like rapid deployment [22]–[24], privacy [21], or identification [25]. Table 1 highlights the existing surveying efforts and their relation to our contributions.

We complement the existing research efforts by providing an up-to-date comprehensive survey of security threats and solutions for public safety in the 5G era. We provide an analysis of public safety communication related security requirements and characteristics. Specifically we provide insights and observations on challenges arising from a) the utilization of the 5G communication standards and civilian infrastructure, b) the emergence of IoT equipment, c) tactical communications in remote locations with potentially limited or disconnected backhaul, and d) distributed mission-critical application architectures.

We point-out current challenges and highlight the needs for future research. We also contribute by demonstrating solutions to two pressing challenges.

1) We show a scalable and secure approach to attach IoT devices to tactical bubbles. Instead of just authenticating identities of devices, we recognize and verify the type and software of devices. By remotely attesting [26] the configuration and integrity of equipment software, we minimize the threat of malware compromising mission-critical operations.
2) We also experiment with and analyze secure satellite links for tactical backhauls. The development of non-terrestrial 5G is progressing [27]–[30] and can provide a viable alternative to increase resiliency and redundancy for mission-critical applications. We research and analyze what the limited backhaul connection means for the mission-critical applications. Do the security solutions prevent optimization of communications? Will the limited backhaul become the weakest link or lead to vulnerabilities that adversaries may exploit?

The remainder of the paper is organized as follows. In Section II, we provide an introduction to hybrid architecture and technologies that will support future public safety user cases. The section will also identify the assets that are at stake. Section III introduces a framework for analyzing security threats and use cases. The section categorizes adversaries, main vulnerabilities, attack vectors, and risk levels within the public safety scene. Section IV explores security—at the intersections of mobile communication networks and public safety use cases—by analyzing threatened assets against the threat analysis framework. The section presents a set of scenarios that characterize typical and unique threats in public safety communications. Section V identifies and classifies security requirements and solutions. Section VI describes our trials and two demonstrated security enablers in more detail. The enablers are analyzed against the framework

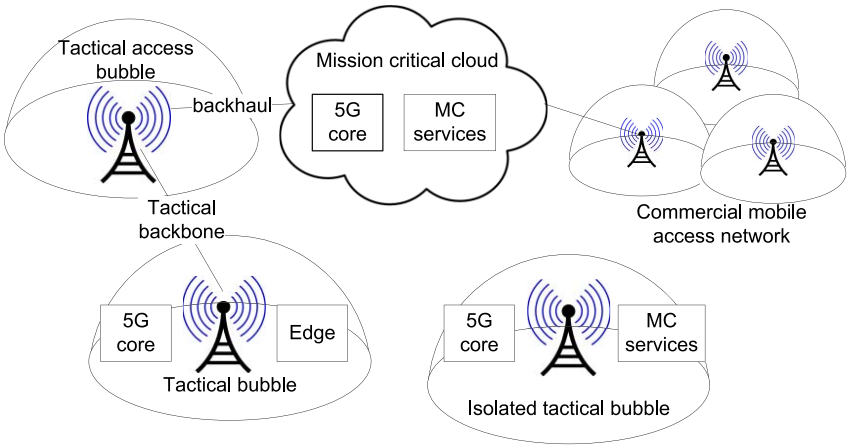


**FIGURE 1.** The next generation communication architecture for public safety utilizes both tactical bubbles and commercial operators' infrastructure.

and the threat scenarios. Section VII provides a discussion on future challenges and research directions. Section VIII presents our conclusions.

## II. PUBLIC SAFETY NETWORK EVOLUTION AND USE CASES

This section provides an overview of next generation public safety communication by describing the characteristics of technologies and highlighting typical use cases as well as their requirements and involved security critical assets. The central elements are illustrated in Fig. 1.

### A. EVOLUTION TOWARDS HYBRID 5G BASED ARCHITECTURE

New mission-critical applications services demand improved quality properties, higher bandwidth, and lower latency from the network. Latest releases of 3GPP specifications, long-term evolution (LTE) and 5G, provide the technology to fulfil these requirements. Commercial operators can support the public safety authorities by allowing them to share the network with civilian users. However, in many countries and cases, commercial networks cannot fulfil the requirements for the coverage and capacity alone.

The need for cost-efficient capacity with sufficient reliability and coverage can be achieved with hybrid approach. Commercial network infrastructure that is shared with civilians allocates capacity for public safety users. Tactical bubbles provide connectivity during emergency missions when the commercial network is not sufficient. This vision requires that both the commercial mobile networks and tactical bubbles security fulfil the security requirements of the public safety organizations.

Security in mobile networks has been an evolution. The first generation of 3GPP's specifications provided user identification for billing purposes. The second generation—including the adaptations developed for public safety communications such as European TETRA [20], [31]–[34] or North American Project 25 [19], [35]—provided cryptography for authentication and to prevent outsider eavesdropping. The third generation authenticated the network for users. The fourth generation extended security to support new services such as device-to-device communication, isolated operations, multicasting, and mission critical applications. These extensions included end-to-end confidentiality and authenticity in the application layer. The fifth generation increased robustness against internal threats, enhanced privacy, and eased customization of services and security for different types of users. All generations have also patched different vulnerabilities and trade-offs that were left over from the previous generations.

### B. AUTHORITIES IN COMMERCIAL OPERATORS' ACCESS NETWORKS

Commercial mobile operators have ready infrastructures that can provide both access and backhaul services, i.e., connect user equipment or tactical networks to centralized mission-critical services. Public safety operators act as mobile virtual network operators and manage the core network and application services in the cloud. Network products and services supporting mobile virtual network operator (MVNO) architecture have emerged from different manufacturers [36]–[39] and commercial networks are also taken into operational use by public safety authorities in different countries [40]–[42].

As radio access infrastructures are shared with civilian users and may occasionally be congested, the public safety users typically require a priority over other users. Operators may provide differentiated, application specific, service levels with diverse availability guarantees and QoS properties. Differentiated services are based on contractual agreements, service level agreements (SLA), between operators and public safety organizations. The policy control function (PCF) enable application provider to dynamically request availability guarantees for traffic flows. The technical alternatives and protocols for controlling the sharing of network resources and prioritizing users are described in Table 2.

Core network services, mission-critical services (MCX), and critical data services, including databases containing

**TABLE 2.** Traffic prioritization and infrastructure sharing mechanisms and their security assumptions.

| Priority mechanism | Summary |
|---|---|
| Access class barring (ACB) | Limiting communication with voluntary UE or with mandatory base-station enforced mechanism. Subscribers' coarse-granule access class data is stored in USIM. ACB assumes thus trustworthy and uncompromised UEs. |
| Guaranteed bit rate (GBR) | Reserving resources (bandwidth in RAN or core) for particular subscribers. In competition situation, trusted base stations and core components enforce that non-GBR users yield. |
| Allocation and retention priority (ARP) | Prioritizing subscribers who are allowed to get service. ARP priority is stored in subscriber profiles on user database. During operation priority is assigned to bearers, which is a higher abstraction concept for RAN or core connection specific QoS parameters. |
| Pre-emption | Determining order of subscribers to be disconnected in overload situations. Policies are stored in the user database on the core network. |
| Quality classes (QC) | Classifying subscribers according to service and priority levels (including ACB, GBR, ARP). QC identifiers (QCI) are subscriber specific and stored on the user database. |
| Differentiated services (DiffServ) | Limiting and prioritizing core and backhaul IP communication. DiffServ code point (DSCP) in IP packet's header maps to bearer's QCI. Routers drop packets during congestion. Relies on network or transport layer mechanisms to secure headers. |
| RAN sharing | Enabling multiple operators to utilize the same access network and base stations. |
| Network slicing | Differentiating end-to-end service for user or user groups with network softwarization, which decouples data and control layers. Switches enforce forwarding according to policy rules from software-defined networking (SDN) controller and isolate flows of different users from each other. |

public safety user information, health records or crime registers, are not necessary within a commercial network infrastructure. Authorities are likely to keep these critical services on their own private servers and only utilize connectivity provided by the commercial operator's access network.

### C. TACTICAL BUBBLES

Tactical bubbles are movable, stand-alone, and rapidly deployable networks that provide 3GPP specified 4G or 5G connectivity [1], [43]. Tactical bubbles contain access network, essentially a 4G or 5G base station, as well as core network functions and application services to enable their usage in isolated scenarios without backhaul connections to remote services. Several tactical bubbles can be connected with a tactical backbone to a tactical network. Tactical bubbles provide additional communication coverage and capacity when needed, e.g., in rural blind spots within a commercial network or in failure situations. They may also increase security by as when they are securely isolated from the commercial infrastructure. The bubbles can be utilized in three main alternative modes.

1) The tactical *access bubble* incorporates access network functions while core network and application services are external, received from functions in the cloud or in another bubble.
2) The *regular bubble* uses its own access and core functions but receives application services from the cloud or another bubble.
3) The *isolated bubble* does not have backhaul and serves its users independently with all the necessary access, core, and application functions.

Requirements for tactical bubbles include minimal configuration time and efforts. Automation and self-configuration capabilities are essential as public safety users are not assumed to be experts in network configuration. Public safety users typically have primary access to the licensed radio frequency band. Other users, such as commercial network operators and civilian traffic, are secondary users and are given access only when the primary user is not using the spectrum. The spectrum usage is managed using a centralized database or by sensing the usage of the spectrum.

### D. USE CASES AND ASSETS

The *mission critical push-to-talk (PTT) within tactical bubble* use case implements the most fundamental service — group communication (many-to-many audio) — within an isolated tactical bubble. The use case requires a local and independent core network and services for group communication application and security. Sensitive information include organizational user and group data, which must be available locally, as well as operational information on the location, role, and activity of particular users.

The *video surveillance within tactical bubble* use case illustrates the capability to transmit larger data streams within an isolated tactical network. Services needed to implement this use case include broadband access and core, video servers and, optionally, local edge acceleration. Broadcasting services may be utilized to optimize the use of bubble bandwidth and prioritization services to ensure service for the most critical users and applications, typically audio, in overload situations. Jeopardized information includes video stream as well as the location of cameras.

In the *UAV control within tactical bubble* use case public safety users within an isolated tactical network acquire aerial situational data from the local mission site. Essential elements needed to realize the use case include local connectivity and remote control applications. Jeopardized information includes navigation and control data flows toward UAV, situational data toward public safety personnel, as well as operational data, such location and type of UAVs.

In the *mission-critical services (MCX) in the cloud* use case application servers and the database are operated in a remote location. Cloud services and the tactical bubble are connected with a backhaul, e.g., a commercial mobile network or satellite. The scale of centralized information is more massive, as it can contain national databases, and thus more information is in jeopardy. The central service is also

more critical as geographically distributed users rely on its availability.

The *access through a civilian private network* use case provides public safety users an alternative access network, which can be utilized when dedicated or commercial networks is unavailable. For instance, a mining company's 5G private network or a smart city could support rescue operations by providing connectivity. Optionally, access could also be provided to services in private networks, such as databases containing information on buildings and infrastructures. The use case requires federation and cooperation between private network operators and public safety organizations to enable users to acquire the credentials and authorization required for network and service access.

In the *access through commercial operator's network* use case, safety users connect to the civilian infrastructure to gain access to services in a public safety organization's or partner's private cloud. Communication resources are now shared with civilians and thus exposed to interferences. A commercial network may also simultaneously support different public safety organizations, who should be allowed to cooperate but not to disrupt each other.

## III. THREAT LANDSCAPE: AN ANALYSIS FRAMEWORK

This section describes the main factors affecting to the security of public safety communication. It provides a framework that enables the analysis of security in different use cases and particular threat scenarios.

### A. THREAT ACTORS

Threat actors can be classified into six main categories which are characterized by attackers' motivations and capabilities. The first category are actors who do not intentionally target public safety operations but cause unintentional or collateral damage or interference. The second class is random hackers, trying to show their skills or get some benefits, but not focusing particularly on public safety networks. The third class are insiders, personnel or cooperating companies, causing security harm intentionally. The fourth class is the criminals and terrorists trying to prevent particular operation, e.g., to evade detection or prevent rescue, or for financial gains (e.g., blackmail ransoms). The fifth class comprises advanced persistent threat (APT) groups, i.e., adversarial groups with significant resources, who target public safety agencies or operators in particular. The sixth class is the foreign agencies attacking or intruding into a communication network as part of hybrid warfare.

### B. ROOT VULNERABILITIES

Vulnerabilities enabling security breaches can be caused by failures, errors, or compromises that are made during a different stage of the technology or product life-cycle. The first vulnerabilities are introduced during *standardization*. 3GPP's security specification has been an evolution where previous compromises and failures have been corrected. The trend may also continue in the future.

*Implementation failures* can be minimized with verification, testing, and certification but they cannot be completely removed. For instance, TLS, which is a central security protocol for mission-critical applications and management interfaces of 5G core, is mature but has seen some relatively recent vulnerabilities [44]–[46]. Also, implementation failures may be intentional and products contain backdoors [47].

*Architectural failures* relate to the design and planning of public safety communication and security architecture as well as its deployment. For instance, architectures with interfaces to less trustworthy systems, such as the Internet, expose communication to threats originating from these systems. Distributing security functions and data geographically increases points for adversaries to attack, though distribution makes architecture stronger by removing the single point of failure. *Process vulnerabilities* are incidents that occur in non-operational phases of the products and services lifecycle. For instance, devices may be lost or physically tampered with during development, supply, storage or maintenance phases and credentials may become compromised during deployment.

Configuration and operational failures are typically the most common types of root vulnerabilities. *Operational failures* are caused by normal end-users. For instance, project 25 had usability issues and non-mandatory end-to-end security, which led to the network being used in an unsecure manner [19]. The number of such failures can be minimized with standards and implementations where security is not an optional feature. *Configuration failures* are intentional or non-intentional mistakes made by administrators. Differences in security cultures [48] may be one exposing factor in this transition in public safety communication, which involves cooperation between authorities and civilians. Public safety actors and solution providers are accustomed to strict security policies and practices, while actors coming from the civilian side may have more relaxed security attitudes and know-how. These are situations where authorities' and civilians' assumptions and capabilities may lead to unanticipated conflicts and exposures.

### C. ATTACK VECTORS AND TYPES

Attacks on public safety communication networks can emerge from five main directions. Open air interface or *local radio* attacks can be made by an adversary within the coverage of a radio access network. Such adversaries may be visible and, while actively transmitting, their presence can be sensed. *Physical* adversaries can intrude on user equipment or devices in a tactical bubble. The tactical bubble cannot be guarded in every mission. *Remote cyber-adversaries* may advance through different interfaces or with the help of malware. Insiders are malicious or non-malicious adversary that have a bridgehead to the operators' infrastructure. In general, in the IT world 34% of security incidents involve internal actors [49]. *Non-operational* attacks can happen in the different phases of the assets lifecycle. For instance, products

may be planted backdoors or compromised during storage or maintenance.

The attack type can then be classified according to the adversarial goal. Our threat classification follows STRIDE methodology [50], which classifies threats to seven main categories: spoofing, tampering, repudiation, information disclosure, denial-of-service (DoS), and elevation of privileges.

### D. RISK LEVELS

Risk is a function of the likelihood of a security incident as well as the scale and duration of the impact. Risk depends on the use case and the assets that the use case exposes. The impact depends on the scale of the affected parties and assets:

1) Large scale—society's public safety operations are prevented. This may lead to life threatening situations.
2) Medium scale—impact against assets or information belonging to network or network segment operator or public safety service operator; limited impact does not prevent society's operational capabilities completely.
3) Small scale—impact is limited to an individual user or device, or causes only QoS degradation without limiting service access completely.

The impact depends on the life-time of the impacted information or the duration of the asset's unavailability. Long-term threats typically include organizational information, destructed devices, as well as privacy critical databases on civilians. Temporary threats include attacks against operational assets, such as leakage of information that is valid only during the operation or temporarily failure within a device.

## IV. PUBLIC SAFETY SCENARIO ANALYSIS

This section analyses security in the intersection of public safety use cases and 5G.. The analysis starts from the public safety assets that are threatened. The assets include users (subscribers and operators); devices (hardened, commercial-of-the-self, and IoT); resources (e.g., spectrum, signaling, RAN and backhaul capacity, traffic priorization, computing resources, energy, and infrastructure in general); application services (remote control, positioning, and end-to-end communication); and system services (e.g., security functions); as well as information (e.g., user and organizational information, identifiers and credentials, and communication metadata). From the assets, we have defined threat scenarios. The goal has not been to define every potential scenario but the most characterizing ones that contain typical or unique security challenges of public safety communications. The scenarios are analyzed against the framework proposed in the previous section and categorized according to their typical location within the communication architecture domains. The results are summarized in Table 3.

### A. THREAT SCENARIOS IN THE ACCESS NETWORK DOMAIN

Access networks—both commercial 4G/5G base stations as well as tactical bubbles—face various threats from local actors. These threats may occur through the open-air (radio) or physical interfaces. Adversaries in the radio interface include nearby UEs and devices that may be outsiders, civilian devices, or misbehaving insiders, certified or uncertified devices belonging to public safety organizations.

Several weaknesses exists in 4G and 5G protocols [51]–[54]. A central challenge is that part of the control plane communication is unprotected, which exposes communication for passive eavesdropping, tracking of user equipment, - or for active tampering (DoS) or man-in-the-middle attacks. Also, integrity protection for user plane communication, which was lacking in LTE, is still optional in 5G. 5G provides additional security features and some patches to LTE vulnerabilities but downgrading attacks are still possible. 5G is also vulnerable to jamming attacks [55] and spoofed positioning [56] by malicious nodes; interferences; and attacks against databases, when positioning is based on training databases

Operational information of public safety actors' capabilities can be leaked to eavesdroppers. For instance, adversary may learn how many operatives or drones are in the field, what type of devices are used (application, manufacturer etc.), and where the devices are located. Attacks are possible since, even though 5G protects user identifiers with asymmetric cryptography, device capability information [57] and temporary identifiers are still transmitted in clear text both in 4G and 5G [58]. Further, traffic analysis based on traffic timing, amounts, and frequencies or physical layer fingerprints of the radio transmitter may be utilized to (encrypted) traffic flows but also on some meta-data to identify UEs. Device type or in some cases the users' roles can also be identified through fingerprinting. In the network layer (see, e.g., [59], [60]), different applications have different transmission profiles. In the physical layer (e.g., [61]), signals can be fingerprinted due to different radio transmitters that have unique properties because of imperfections in manufacturing processes. In loaded prioritized communication situation, latencies and traffic amounts reveal which UEs have priority over others and which QoS is provided for which user. The significance of the threat depends on adversarial capabilities. Detailed physical layer analysis may require specialized hardware not available to every adversary. The active transmissions needed to identify the target [58] may reveal adversary and require that an adversary has gained privileges to reach users in the public safety network.

The failure of cryptographic protection leaves application layer communication, containing long-term organizational secrets, vulnerable to eavesdroppers and man-in-the-middle attackers. Currently, there are no known cryptographic weaknesses in 4G or 5G algorithms that would enable practical attacks. However, in the future, vulnerabilities may emerge. Disruptive adversarial capabilities, such as quantum computing, may enable future attacks on cryptography [62], [63]. Implementation failures such as poor random number generators, the use of null encryption algorithm EEA-0, accepting older protocols and thus enabling downgrading attacks, or

**TABLE 3.** **Threat scenario analysis.**

| *Threat scenarios against public safety assets* | *Risk[1] / use case* | | | | | | *Threat attributes* | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | *PTT @ bubble* | *Video @ bubble* | *UAV @ bubble* | *MCX @ cloud* | *Priv.net access* | *Commerc. access* | *Attack type[2]* | *Root vulner.[3]* | *Threat actors[4]* | *Attack vector[5]* | *Domain* |
| Compromise of hardened UE | ● | ● | ● | ● | ● | ● | STRIDE | IPCO | AF | PCN | UE and devices |
| Compromise of unhardened IoT devices or civilian UEs | - | ● | ● | ● | ● | ● | STRIDE | IPCO | * | PCN | |
| Loss of devices | ● | ● | ● | ● | ● | ● | SDE | CPO | * | P | |
| Leaking of credentials, device cloning | ● | ● | ● | ● | ● | ● | SIE | IPO | CAF | PCN | |
| Denied remote control | - | ● | ● | - | - | - | D | SIAC | * | R | |
| Leaking situational data | ● | ● | ● | ● | ● | ● | I | SIAC | CAF | R | |
| Traffic and metadata observation | ● | ● | ● | ● | ● | ● | I | S | CAF | R | Access |
| Unprotected communication (failing of crypto) | ● | ● | ● | ● | ● | ● | STRIDE | SIPA | CAF | RC | |
| Jamming | ● | ● | ● | ● | ● | ● | D | A | * | R | |
| Denial of priority | ● | ● | ● | ● | ● | ● | D | C | IAF | RC | |
| Prevented sharing of spectrum allocation data | ● | ● | ● | ● | - | - | D | A | RICAF | RC | |
| Orphan/disconnected bubbles | ● | ● | ● | ● | ● | - | D | C | IAF | RP | |
| Spoofing positioning | ● | ● | ● | ● | ● | ● | TD | IAC | IAF | RPN | |
| Signalling storms leading to resource exhaustion | ● | ● | ● | ● | ● | ● | D | IA | UCAF | RC | Core |
| Subscriber identity and profile data leakage | ● | ● | ● | ● | ● | ● | SI | IAC | IAF | CN | |
| Attacks through third-party APIs | ● | ● | ● | ● | ● | ● | STRIDE | IAC | IAF | CN | |
| Misconfigured priority and quality policies | ● | ● | ● | ● | ● | ● | SIDE | C | IAF | CN | |
| Insider threats by operator personnel | ● | ● | ● | ● | ● | ● | STRIDE | AC | I | PCN | Infrastructure |
| Advanced persistent threats in infrastructure | ● | ● | ● | ● | ● | ● | STRIDE | IAC | IAF | CN | |
| Information leaking in virtual infrastructure | ● | ● | ● | ● | ● | ● | I | IA | AF | RPCN | |
| Interferences in virtual infrastructure (intra-slice) | ● | ● | ● | ● | ● | ● | D | IA | AF | RPCN | |
| Lightweight security detection and response | ● | ● | ● | ● | ● | ● | IDE | A | * | RCN | |
| Security breach in cloud | - | - | - | ● | ● | ● | STRIDE | IAC | CIAF | C | |
| Indirect attacks against support systems | ● | ● | ● | ● | ● | ● | D | CIAF | IAF | RPC | |
| Network attacks against backhaul traffic | - | - | - | ● | ● | ● | STRID | IAC | CAF | RC | Transit |
| Unavailable cloud or limited backhaul | - | - | - | ● | ● | ● | D | IA | AF | C | |
| DoS attack against transit perimeter | - | - | - | ● | ● | ● | D | A | CAF | C | |
| Adversary gains access through bubble perimeters | ● | ● | ● | - | - | - | STRIDE | IAC | CAF | C | |
| Security breach causing leakage of transit keys | ● | ● | ● | ● | ● | ● | STID | IC | CAF | PC | |
| Spoofed situational awareness | ● | ● | ● | ● | ● | ● | STR | SIAC | URAF | RC | Application |
| End-to-end (E2E) security breakout at the edge | ● | ● | ● | ● | ● | ● | STRIDE | IAC | IAF | PC | |
| E2E security failing | ● | ● | ● | ● | ● | ● | STRIDE | SIACO | CIAF | PC | |
| Performance degradation due to E2E security | ● | ● | ● | ● | ● | ● | D | SIAC | - | - | |
| Masquerading | ● | ● | ● | ● | ● | ● | S | ICO | CIAF | RC | |
| Federation degrades performance | ● | ● | ● | - | ● | ● | D | A | CAF | C | |
| Federation opens side-channels | ● | ● | ● | - | ● | ● | STRIDE | A | IAF | C | |
| Misconfigured group memberships | ● | ● | ● | ● | ● | ● | STIDE | C | IAF | CN | |

[1] Subjective risk classification: high impact, low likelihood: ●; high impact, medium likelihood: ●; high impact, high likelihood: ●; medium impact, low likelihood: ●; medium impact, medium likelihood: ● ; medium impact, high likelihood: ●; small impact, low likelihood: ●; small impact, medium likelihood: ●; small impact, low likelihood: ●.
[2] Attack types (STRIDE): Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, and Elevation of privileges.
[3] Root vulnerabilities: Standardization, Implementation, Architecture, Process, Configuration, Operational, *=all
[4] Threat actors: Unintentional, Random hackers, Insiders, Criminals, Advanced persistent threat, Foreign agencies, *=all
[5] Attack vector: local Radio, Physical, remote Cyber, Non-operational, *=all

optional end-to-end security [19] may lead to failure of protection.

Denial-of-service adversaries may exploit the few public safety specific mechanisms in their attack. Firstly, in public safety scenarios where total bandwidth is limited, some UEs have higher priority. Malicious UEs that have gained priority have the potential to cause more harm. For instance, a priority user without bit rate limitations can more easily deny service from lower-priority users. Secondly, the public safety users should have primary access to the licensed band. Other users, i.e., commercial network operators and civilian traffic, are secondary users and are given access only when the public safety user is not using the spectrum. The spectrum usage is managed through a brokering service with a centralized database [64] or by sensing the usage of spectrum locally. Information on the available spectrum may not be available from the centralized database, e.g., due to network attack [65]. Consequently, a commercial mobile network will continue using the same frequencies needed by the tactical bubble and cause interferences making the communication less efficient. Thirdly, the distributed hybrid architecture may make some tactical bubbles 'orphans',

**TABLE 4.** Assets of tactical bubble in jeopardy.

| Asset / data | Description |
|---|---|
| User/UE identifiers and profiles (role or classifications) | Enable field commander or bubble administrator to assign user and devices dynamically to communication groups. This information cannot be anonymized. It may be stored permanently to bubble or provided from UE. |
| Authentication information (keys, certificates) | Must be distributed i.e. copied to every isolated bubble to enable authentication. As bubbles have less resources for security and typically less physical protection, this information may leak to adversaries who may then a) learn operational information, b) masquerade as a legitimate user |
| Fleet map (access control matrix) | Defines which user is allowed to access which service or communication group. Matrix is delivered to a bubble from a central service or created in the bubble in ad-hoc manner. May utilize abstractions or user attributes/roles to ease the configuration. |
| Backhaul and backbone shared secrets | IPsec credentials and keys for backhaul and inter-bubble communication security need to be available in isolated, access, and regular bubbles. When leaked, adversaries may deploy own rogue tactical bubbles until authentication information in UEs is revoked. |
| Application services, network functions and edge infrastructure | May provide adversary the means to intercept signaling and access application layer user data. Cyber and physical attacks may compromise availability. |

if an adversary manages to disconnect them from the mission-critical services. A UE that has connected to an orphan bubble may not be able to set-up an alternative access route to the services.

### B. THREAT SCENARIOS IN THE NETWORK DOMAIN

Threats in the network domain can be looked at from the perspective of the 5G core network services (software and data), infrastructure (hardware), as well as transit (internetwork) communication. Assets that the hybrid architecture exposes with geographic distribution are listed in Table 4.

*Core Network Services*

The 5G core network provides routing and security services for access networks. Perhaps the most critical service is the authentication server function (AUSF), which manages subscriber information and controls, which users are allowed to access the network and get the connectivity service. Authentication server function has access to authentication information and profiles of public safety users and hence it requires extensive protection. When isolated scenarios are supported [5], an authentication database must be distributed to the tactical bubble and the database must contain information for at least those public safety personnel that are expected to participate in the mission and hence must be allowed access to the network. Leakage of this information may have serious consequences. As 3GPP authentication relies on symmetric cryptography, leakage in one tactical bubble could enable an adversary to masquerade as a public safety user in every bubble.

Availability focused threats are emphasized when the number of devices used in public safety operations increases. A high number of simultaneously authenticating IoT devices may cause a signaling spike that exhausts the resources of authentication functions in a core or home network [66]. For instance, civilian devices from a tourist bus going past a mission site may initiate a large amount of new signaling. The availability of prioritized applications in high-traffic loaded situations depends on the configuration of user and application priorities and QoS rules. These policies are stored in core functions and enforced in core and access domain functions. The potential vulnerabilities lie in the implementation and operation. Unauthorized parties may be given access to policy control functions. Also, misconfiguration in a multi-organization setting may lead to loss of availability. In dynamic scenarios where priorities are set-up automatically or by application request, false situational information may lead to misconfiguration. As 5G is increasingly utilizing machine learning to automate configuration, the threat of bogus situational data is gaining importance [67].

5G has introduced new opportunities enabling easier customization of network to support application or customer organization services. The opening of the mobile network's service API's [68], [69] to customer organizations enables, e.g., public safety actors to customize network configurations and QoS. However, opened interfaces, such as policy control functions (PCF) must be secured and access to them authorized. The opening of the networks make services more vulnerable to insider attacks.

*Infrastructure*

Network slicing and virtualization, which are characterizing features of 5G, provide flexibility for the resourcing of public safety applications [70]–[72]. Network function virtualization means that shared hardware can host network and mission-critical software from different sources. In the hybrid architecture, core network functions can be located, hosted, and operated in the tactical bubble, commercial network providers' servers or in a public safety dedicated virtual operator's cloud. In a typical configuration, access functions are located in civilian network or in a tactical bubble, which are connected to the public safety operator's core services through the 3GPP S1 interface. Hence, critical functions are typically not hosted on infrastructure that is shared with civilian users. However, in isolated backhaul-less situations this is not possible and core services must be brought to tactical bubbles. If shared hardware hosts critical assets belonging to different civilian or governmental organizations, there is a risk that the other misbehaves and gains access to them. The potential attack may utilize weaknesses in the virtualization layer enabling misbehaving tenant to circumvent defenses protecting the other assets [73]. Such an attack can have a big impact, as the adversary gets access to all information, stored or flowing through the assets. Furthermore, interferences [74] and information leaking [75] are possible in SDN based network slicing. An adversary may gain information from users in other slices, e.g., by monitoring the response times

of shared hardware. Misbehaving software that consumes all the resources may also cause a denial-of-service situation. Network slicing minimizes these threats by dedicating own functions and resources for each slice. However, some of the functions are shared, typically, e.g., part of the control plane, hardware infrastructure, external services, and authentication services (user registers). A higher number of shared functions also means a higher number of potential attack vectors between the slices sharing the functions.

Communication infrastructure may also be vulnerable through indirect attacks that target systems that the communication infrastructure is reliant on. For instance, power supply, heating and cooling, and navigation of cars or aerial vehicles hosting base stations provide alternative attack paths. Cyber and physical attacks against, e.g., a power grid or a car supplying power, which are increasing dependent on ICT, may cause denial-of-service situations. A simple attack is where the driver, who is driving infrastructure to an operation site, gets spoofed instructions. More advanced threats include adversaries that have gained inside access to the support system.

*Transit*

Connections between tactical networks and remote mission-critical services as well as between tactical bubbles are typically secured with virtual private network (VPN) tunnels and application layer security. Further, the perimeters are secured with firewalls that accept only authorized tunneled traffic. Due to the complexity of situations an adversary may find exploitable weaknesses in the backhaul security. A central challenge for transit and backhaul networks is how to assure availability.

### C. THREAT SCENARIOS IN THE APPLICATION DOMAIN

Mission-critical application related assets include connectivity services (capability to voice and video based group communication and information sharing), application servers in the cloud and tactical bubble, client software in devices, organizational information (e.g., long-term information on operatives and their identification data, command hierarchies and communication practices), as well as operational data (e.g., situational information from the mission site). Further, application specific information may be highly privacy critical information. For instance, health care records should be available only for first aid personnel (with the potential exception of contagious situations that may also threaten other personnel) and crime registers should be available only for relevant law enforcement officers. Information leaking through compromised databases in tactical networks or by eavesdropped communication as well as external adversaries trying to prevent communication are hence the main security worries.

End-to-end application layer communication is typically protected but this security may be broken due to practical or efficiency reasons. Application layer security functions cause overhead to communication and often prevent performance optimizations. Applications that require low latency benefit from 5G's edge computation capabilities to process information quickly and close users. For instance, it is often beneficial to do video processing and transcoding at the edge for performance or interoperability reasons. However, edge processing means a security breakout. This leads to a more complicated situation, where an additional middle point (at the edge) must be verified and trusted. When the threat surface expands, it is more difficult to determine how secure the application is.

Public safety users communicate within push-to-talk groups where one user transmits at a time while others receive. A central issue for security and efficiency of group-based communication is who has the authority to join a group and send or receive. Typically, groups are formed using predefined hierarchies and rules or using ad-hoc mission specific requirements. Misconfiguration of authorization policies may lead to:

1) inefficient communication (data is delivered for people not needing information and thus bandwidth or human time is wasted),
2) denial-of-service or denial-of-information for some parties, or
3) leaking of classified information to a device without proper certification or for a user without proper clearances.

Misconfigurations may be due to human error. The probability of mistakes increase in isolated or multi-organizational settings without assigned and educated administrators, or where responsibilities are unclear and may change during the mission. In dynamic scenarios where group memberships are defined automatically during the operation, false situational awareness may lead to misconfiguration.

Cooperation between public safety actors and civilian network operators as well between the public safety core network and tactical bubbles requires federation in both the network and application layers. Common practices and mechanisms for information and policy exchange increase complexity. Liabilities and responses between cooperating actors may be unclear [76]. These factors may lead to information leakage or open up side-channels to systems of federating party.

### D. THREAT SCENARIOS IN THE USER DEVICE DOMAIN

Devices have different security levels depending on the control features in the hardware and operating system, enforced policies, as well as maturity and trustworthiness of software. Security controls include access control, firewalls, data encryption, as well as software configuration and integrity management. In terms of security, the main types of user devices include a) security hardened cellphones that are certified for public safety operations, b) unhardened civilian or bring-your-own (BYOD) phones, and c) other unhardened systems such as unmanned aerial devices [77] or autonomous robots [78]. Cellphones can be compromised by different

**TABLE 5.** Security enablers.

| Enabler class | Access and network realms | Mission-critical application realm | Device realm |
|---|---|---|---|
| Identity, access management | 3GPP authentication functions (AUSF) [3]<br>3GPP IOPS [5]<br>3GPP QPP based prioritization policies<br>Firewalls | 3GPP MC security [10]<br>Hierarchical group management - fleet mapping<br>Authentication federation | Network credentials (USIM, IOPS SIM apps [11], eSIM [114])<br>MC service credentials |
| Authentication | 3GPP authentication and key agreement (5G-AKA, EAP-AKA'[3], IOPS [4]) | 3GPP MC security [10]<br>3GPP secondary authentication[3],<br>Application specific credentials (e.g. multi-factor authentication) | Security bootstrapping: out-of-band delivery of network and application credentials, OAuth2 authentication and authorization delegation [117], [118], [168] |
| Confidentiality & Integrity | 3GPP access stratum security algorithms (SNOW, AES-CTR, or ZUC) [3]<br>Prose security [83]–[85]<br>eMBMS security [86]<br>Backhaul / inter-bubble security (IPsec) | Protocol security (TLS, SRTP, RTSPS)<br>Centralized architecture | Device and operating system level controls<br>Hardened and disabled interfaces<br>Physical guarding |
| Availability | Redundancy/capacity: e.g. mesh architectures [87], spectrum sharing<br>Responsiveness: function migration, dynamic routing [88], [89], resourcing[90]<br>Interference tolerance: slice isolation, softwarization, cloudification, channel robustness, | Distributed architecture | |
| Privacy | Location confidentiality (SUPI encryption & GUTI (re)pseudonymization [58]) | Sensor type confidentiality / anti-application fingerprinting | |
| Audit | Network specific threat monitoring and response (SIEM, SOAR).<br>International [98] and national e.g. [99]–[101] requirement and auditing criteria. | Application specific threat monitoring, security situational awareness, and response. | Audit trail for remote SIM provisioning [116] |
| Trust, assurance | Trust anchors (trusted computing, remote attestation)<br>Threat intelligence sharing<br>Physical guarding | Trusted application infrastructure<br>Physical guarding | Device platform security and remote attestation<br>Security testing |
| Compliance | GSMA certification [96], [97],<br>Security metrics in service level agreements | | Certification, device policies |

cyber-attacks [79], [80]. For hardened devices with stricter security polices and white listed software, attacks are more difficult in general but they also remain susceptible to physical or over-the-air cloning of USIM [81], [82], for leaking of application layer credentials enabling masquerading attacks, for physical hacking, as well as for thefts or losses of devices. Public safety devices may also rely on centralized security management (for delivery of patches, enforcement of software configuration, updating of security policies, as well as access to revoked certificate information and virus databases) and thus prolonged isolation may damage devices' security levels.

The consequences of compromise include unavailability or tampered situational awareness, unauthorized access to critical services, unavailability of networks services (e.g., when unhardened devices are attached to a botnet performing a DoS attack), and a device becoming unusable, which may lead to safety threats, e.g., crashing towards public or a failed rescue operation. Uncertified devices should be given fewer privileges, making the impact of compromise will be lower.

## V. SECURITY ENABLERS

This section surveys the security requirements and solutions proposed and researched for 5G networks and public safety communications. The solutions for the network, application, and user equipment realms are identified and then classified according to the taxonomy proposed in the 5G-ENSURE security architecture [14]. The results are summarized in Table 5.

### A. ARCHITECTURE AND SOLUTIONS FOR NETWORK SECURITY

The baseline network security relies on the 3GPP specified mechanisms for authentication and communication confidentiality and integrity. Additionally, we survey transit network, network infrastructure, and network management related domains and their security solutions.

*Access and Core Network Domains:* 3GPP and industry have specified security architecture — mechanisms and protocols — for the 5G network [3]. The architecture provides confidentiality, integrity, and mutual authenticity as well as some availability protection for wireless connectivity. Access management is based on 3GPP specified Authentication and Key Management (AKA) protocol variations (EAP-AKA, EAP-AKA', or 5G-AKA). User credentials are stored in a USIM application, which carries symmetric keys that match the user register in home networks. 3GPP has also introduced [3] new authentication approaches including certificate-based authentication EAP-TLS, and secondary authentication, where the core network forwards

the authentication result to the application server, which provides alternatives for IoT and private types of networks. Subsequent communication, which follows the authentication, is protected with 3GPP access stratum confidentiality and integrity algorithms EEA1-3, EIA1-3, which are based on: SNOW, AES-CTR, or ZUC.

For tactical bubbles without backhaul, 3GPPP has specified [4], [5] isolated operation for public safety (IOPS) mode of operation. Essentially, devices are expected to hold two USIM applications, one for normal operations and one for operations within an isolated network. The core network in an isolated network holds a local user register, the authentication function (AUSF), for authenticating the UEs using IOPS USIM.

Two specific communication modes are important in public safety scenarios and have their own security solutions: device-to-device communication and broadcasting. Proximity communication service (ProSe) enables direct connectivity between nearby mobile devices. Confidentiality and authenticity of proximity communication as well as authentic and authorized discovery of proximity services (and nearby devices) is based on ProSe-specific security protocols and network-assisted key management mechanisms [83], [84]. There are also research proposals to enhance the standards, such as cryptographic pairing solutions for disaster scenarios [85]. The multimedia broadcast and multicast service (eMBMS) security [86] defines functions for authenticating and authorizing the user, for group and key management, as well as for MIKEY-based key distribution. The standard uses SRTP and HTTPS to protect streaming and downloads.

Defenses against the UE tracking threat (and leaking of operational information) include the concealing of UE identifiers that are transmitted in the open air when reaching the UE. Firstly, subscription permanent identifiers (SUPI), which are globally unique IDs and are used when device registers to the network, are protected in 5G with a mechanisms based on asymmetric cryptography. The solution is effective as long as older 4G solutions are not accepted and thus the downgrading attack to previous generations is mitigated. Secondly, after registration UEs are identified with temporary pseudonyms (GUTI). These temporary identifiers should be frequently changed to prevent de-pseudonymization [58].

*Transit Domain:* Backhaul and inter-bubble security is required when connecting tactical bubbles to each other or base stations to distant cores. In mobile networks, backhaul communication is typically encapsulated using GPRS Tunneling Protocol (GTP) and secured with Internet Protocol Security (IPsec). Secured tunneling causes some challenges as a tunnel hides higher layer headers and thus prevents application specific optimizations and as IPsec configuration is typically quite heavy process. Transit communication makes tactical bubbles reachable for remote attacks through open interfaces and ports and, consequently, firewalls are mandatory in communication perimeters. The key strategies to ensure availability include redundancy as well as protocols and architectures that are designed to be tolerant against different denial-of-service attacks. For instance, mesh architectures [87], software defined dynamic routing [88], dynamic backhaul selection [89], and AI based backhaul resourcing schemes [90] have been proposed.

*Infrastructure Domain:* Infrastructure security relates to the control enablers in the hardware hosting access and core network functions, including base stations and security services. Protection is required at different layers: physical guarding and hardware controls, operating system-level access controls, as well as controls for the virtualization layer. ETSI has specified [91], [92] security solutions and requirements for network function virtualization. The approaches include monitoring [93] and trusted computing [94] to verify and enforce that devices are running in the expected software configuration and are providing desired security level. The Cloud Security Alliance has also proposed guidance for security management approaches [95] within cloud-edge environments.

Network device vendors utilize their own and third-party test laboratories, which are accredited by GSMA [96], for assuring the trustworthiness of products. 3GPP has developed generic and product specific security assurance specifications as well as a generic process [97] for creating test specifications and for evaluating security compliance for product development and product lifecycle management.

Generic requirements for information security management systems, such as ISO 27000 standards [98], provide guidelines for defining and measuring security of infrastructure and systems – both in the network and application domain – from a holistic perspective. Different nations also have their own adaptations for such security requirement and audit criteria, e.g., the American NIST 800-53 [99], German BSI protection catalogues [100], and the Finnish KATAKRI [101], which identify and specify technical and procedural solutions for information security of critical assets.

*Management Domain:* For public safety users, a major requirement is authorization of access priority over available bandwidth and resources in congested networks. Control over QoS services as well as access permissions to network slices, which are dedicated to public safety users, are is based on the 3GPP's security architecture and 3GPP's prioritization and QoS management approaches. QoS, priority, and pre-emption (QPP) policies are either static (stored in user registers) or dynamically requested. QPP policies are enforced by the network components (access or core function). Policies are managed through policy control function and exposure API [102], which enable third parties, such as public safety actors, to access and customize 5G services. The interfaces are HTTP/2-based and secured with HTTPS, as well as with authorization and identity management solutions. Tactical bubbles are likely to have some default policies that are in place when the network is started. If policies are derived dynamically, security must also cover

**TABLE 6.** Security mechanisms for MC applications.

| Security requirement | Security mechanism | Advantages | Challenges |
|---|---|---|---|
| Identity management and authorization delegation | 3GPP MC security [10] and OpenID Connect [169] | The standard is based on mature, widely-used and trusted security protocols: OAuth2 [168] and TLS | OpenID has some known [170] security issues. Asymmetric protocols may not be suitable for restricted devices or restricted channels. |
| Security bootstrapping / credential delivery | MCX provider-specific; e.g., OAuth2 device authorization grant [118] | Providers can support flexible solutions, e.g. remote over-the-air credential provisioning. | Provider specific solutions may also imply interoperability challenges. Proprietary means also that solutions are not as widely tested. Authorization grant is immature. |
| Group key management | Multimedia internet keying (MIKEY) [103] | Standard and mature approach. | Key management discontinuation when tactical bubble changes from isolated mode to access (cloud based MCX) mode. |
| Signaling (HTTP and SIP) security | HTTPS and IPsec respectively | Standard and mature approach. | Suitability of security solutions for restricted channels (e.g. satellite backhaul) and devices (IoT) is unclear. |
| Communication security (generic) | Transmission layer security (TLS) protocol | Standard and mature approach. | End-to-end security breakouts due to MEC acceleration. |
| Securing MCPTT, which is based on real time protocol (RTP) | Secure RTP (SRTP) | Standard and mature approach. | |
| Securing MC video, which is based on real time streaming protocol (RTSP) | RTSP secure (RTSPS) | Standard and mature approach. | Capacity of tactical bubble is limited and security adds overhead. Optimizations based on broadcasting means e2e-security breakout. |
| IoT control or data security | 3GPP MC security, non-3GPP standard, or proprietary | Alternatives enable that different IoT devices can be supported. | Multiple security alternatives imply vulnarabilities due to complexity. E2E MC security may not be suitable for resource restricted devices. No standard solution to verify security posture and integrity of devices? Provider specific solutions may also imply interoperability challenges and vulnerabilities. |
| Authorization policies | MCX provider-specific | Provider may achieve innovative concepts for authorization | |

the policy creation processes (e.g., collection of data, which is used for decision making).

Security information and event management (SIEM) and secure orchestration automation response (SOAR) solutions are used to automate security management and to respond dynamically to detected threats. Security situation awareness is achieved by monitoring infrastructure, network, and services — to collect statistics and event information — and is needed when trying to detect on-going threats, including attacks and situations where security controls are not in place or are not working properly. Security monitoring approaches include both the detection of known attack patterns as well as the detection of anomalies. In typical civilian mobile networks, the possibilities of monitoring end-users is limited due to privacy regulation [104], however, in bubbles or slices dedicated for public safety users' opportunities to analyze end-user traffic to detect threats may be greater.

### B. SECURITY FOR MISSION-CRITICAL APPLICATIONS

Communication between public safety users should always be secured end-to-end. Application layer security is needed for critical applications with highly sensitive information or valuable assets or for situations where network layer mechanisms are not trusted to provide sufficient security level. End-to-end security services include: identity and access management as well as confidentiality and integrity – essentially key management and cryptographic protocols – for unicast and group communication.

3GPP has a specified mission-critical security framework [10] for application layer defenses. The framework provides

1) authentication and authorization between MC servers and clients,
2) signaling security, and
3) end-to-end security of media transmission between clients and between client and server.

The framework is distributed and service-based: an identity management service enables federated authentication, a key management server provides cryptographic keys, and a group management server controls group communication. These security functions may be implemented within MCX servers or deployed to separate signaling proxy, which relays between servers and clients or other services in other domains. The security framework is built on top of existing and mature security protocols, which are listed in Table 6.

In addition to the 3GPP framework, non-3GPP mechanisms can be used for some applications, e.g., due to performance, legacy, or interoperability reasons, and connected to 5G via gateways. In particular, different IoT devices may have their own solutions for securing both control and data flows. For instance, a common UAV connectivity solution, MAVlink, is secured though proprietary algorithms [105], [106] and a common sensor and actuator protocol, the constrained application protocol (CoAP), is secured with Datagram TLS, while LoRaWAN [107]

provides its own security services and AES based communication security [108].

Mission-critical group communication applications ensure that only legitimate users have access to communication groups. In 3GPP's MC security framework, the access control enforcement functions are decoupled from identification and authentication functions and authorization policies; the user authenticates to a separate identity management (IdM) function and MC services only check that the user has been authenticated properly. Authorization policies are managed by public safety organizations using MC service vendor specific solutions, e.g., [109].

Identity and access management services can in principle be centralized and locate in the cloud or distributed to the tactical bubble. In distributed scenarios, the authentication and authorization information is synchronized between the tactical bubble and remote services. Synchronization requires federation – common policies and mechanisms. To enable isolated operations, user information needs to be copied to distributed locations and is thus more exposed to data breaches by cyber or local adversaries. Federation may also be needed between public safety organizations, as missions often involve users and services from different agencies. Policies and practices are needed to agree on how authorization policies are created, by which organization and whom, and how changing situations are handled.

The authorization policies—so-called 'fleet mapping' specifying users' group assignments – are specified to protect confidentiality and integrity but also for efficiency and availability of communication. Primarily, users are assigned to groups to enable efficient cooperation and mission fulfilment. Typically, group communication is hierarchical. For instance, a group of rescue personnel may communicate within a group and one person in that group may then communicate with the field commander, remote mission center, or other groups of police officers and fire fighters. Secondarily, other attributes, user and device clearances as well as context-specific information, may be considered in authorization. For instance, while the basic security classification for mission-critical communication is restricted it is possible to implement communication groups that authorize only UEs with proper certification.

The threat of data breach and leaking of authentication and authorization information can be lowered by minimizing data that is stored within databases in tactical bubbles. This may affect the feasibility and usability of applications within the bubble. Table 7 illustrates potential mitigation alternatives. Nevertheless, bubbles must contain some information. Authentication information, e.g., private keys, used for authenticating bubble services for UEs must be present. Such critical information should be safeguarded adequately, e.g., using operating system and device trusted hardware specific access controls. Another alternative for minimizing the threat of data breach is to increase the amount of security controls within the tactical bubble.

### C. HARDENED DEVICES

UEs used by authorities are typically cellphones with a contemporary operating system, such as Android. Additionally, more and more IoT devices – sensors, cameras, vehicles– are utilized in public safety missions. The cellphones are hardened and certified for the public safety use cases, i.e., for handling classified information. Essentially, the goal of hardening is to minimize the risk of security breaches and threats towards the network by preventing untrusted features and configurations. The hardening features include, e.g.,

1) whitelisting of applications, services, and system software versions,
2) protecting physical interfaces (e.g., USB) by whitelisting devices and accessories that can be connected,
3) protecting network interfaces, e.g., with firewalls, and
4) securing critical information, software, and credentials with secure hardware solutions (so-called root-of-trusts).

Additional means to harden devices include: protection and verification of software integrity, e.g., assuring particular software configuration with secure boot during startup. Trusted platform technologies can be used to protect, detect, and recover from attacks on integrity of UEs and to provide security services, such as secure storage or domain isolation.

Hardware root-of-trust provides strong identity to act as a trust anchor for identification and authentication in the form of a secret key bound to the hardware. In a secure or trusted boot, each layer of the system measures and verifies the integrity of the next layer before execution to detect tampering of software images, establishing a chain of trust starting from a small trusted computing base, and reaching the OS and application software.

Typically, mobile devices protect the most sensitive data and execution using hardware-backed trusted execution environments, TEEs, that isolate execution and data to different trust domains. TEEs provide code and data integrity and confidentiality for sensitive data, e.g., they can implement secure storage for credentials. Similar security features are increasingly available in the hardware for constrained IoT devices, e.g., in the form of ARM TrustZone [110] or RISC-V [111] security extensions.

Device integrity measurements can function as evidence of the trustworthiness of a UE, e.g., toward a network or a public safety service provider. Remote attestation [112] allows a remote agent, called a verifier, to challenge a device, called a prover, to report its identity and software configuration over a secure channel to the agent, which then verifies the integrity state of the device by comparing the measurements against a known good state. In addition to single prover/single verifier challenge-response protocols, collective remote attestation protocols have been proposed for the scalable remote attestation of networks of devices [113].

The detection of integrity violations enables the recovery of a compromised UE to a known good state, e.g., using secure software over-the-air update mechanisms. Device

**TABLE 7.** Strategies to minimize the threat of information leakage from isolated tactical bubbles.

| Approach | Description | Advantages | Challenges |
|---|---|---|---|
| Asymmetric authentication | Use of certificates (asymmetric cryptography and public key infrastructure), instead of shared secrets, minimizes exposed authentication data and thus identity thefts. Potential solutions include 3GPP's EAP-TLS for network layer and different application layer approaches for OpenID Connect. | Addresses the threat that leaking authentication data from local databases in a mission-site. | Does not address threat of leaking authorization information. e.g., group assignments. |
| Authorization certificates | Authorization or attribute certificates minimize exposed organizational information by storing users role, credentials, or group hierarchy information on UEs and enable device-to-device authorizations. | Addresses threat that authorization information due to security breach in local databases. | Requires solutions for management, provisioning and revocation of certificates. |
| Minimized user and fleet map database | Maintaining and deploying user databases that contain only those users that are expected for mission sites. User database may contains some information from national databases or it may be created solely for the isolated operations purposes. | Minimizes threat of leaking organization information and user-specific secrets. Impact of leaking IOPS credentials, do not compromise regular credentials. | Minimized database may limit features (e.g., prevent isolated mode) or cause feasibility challenges in complex and dynamic operations, when, e.g., group information is unavailable. Requires additional operations from end-user to switch local credentials. |
| Additional physical and cyber-security controls | Physical guarding and different information security functions deployed with tactical bubbles. | Approach reduces the probability of data breach. Interoperable and easily deployable approach. | Costs due to additional personnel at the mission site, investments, and maintenance. May not still provide required security level. |

updates should be protected using encryption and digital signing of software images.

Security bootstrapping—the delivery of credentials providing UEs an access to network or application services—can be based on different alternatives. In a mobile network, the security is typically based on hardware tokens (USIM). To support IOPS operations [4], public safety UEs may be provisioned with IOPS USIM applications providing access to tactical bubbles. A new alternative is the virtualized credential platform eSIM, which provides more flexibility for public safety users. Common-off-the-self phones and devices with eSIM capability can be easily deployed to the public safety network. Similarly, public safety UEs with eSIM may be provided with credentials to access civilians' private networks. With remote SIM provisioning (RTP) architecture [114] end-users connect to the network, for instance, by scanning an operator-generated QR code, by manually entering, or by using some other out-of-band mechanisms to deliver server addresses and activation codes. Alternatively, M2M model of the eSIM architecture enables network to push eSIM profiles automatically to compatible devices with bootstrap profiles that are pre-registered to the network. Automated push could be triggered, e.g., when the devices are moving outside of the public safety network coverage but are still reachable from a private network. The subscription manager server generates subscriber profiles, which are loaded to an embedded universal integrated circuit card (eUICC) in the device. The server must be GSMA certified [115] and authenticated with TLS. To address the threat of compromised servers cloning eSIMs, additional mechanism for leaving audit trails for provisioning actions have been proposed in [116].

Current MC security specifications [10] do not define how new devices are registered and authorized to network services. Different out-of-band mechanisms (USB, memory card etc.) can support credential provisioning. For instance, certificates for authentication can be delivered to devices using a USB or memory card and after this the device can perform mutual TLS authentication [117] with the OAuth2-based authorization server. Alternatively, OAuth2 supports the delegation of credentials. For instance, the device authorization grant [118] enables input constrained equipment to be authorized, e.g., with the help of a cellphone and QR codes.

## VI. SECURITY SOLUTIONS IN PUBLIC SAFETY TRIALS

We have implemented and trialed different public safety communications related use cases in the PRIORITY project [119]. In this section, we analyze and describe two specific security solutions. An overview of the security architecture is illustrated in Fig. 2. The solutions have been analyzed against the use cases described in Section II-D, the threat framework from Section III, and the identified threat scenarios from Section III. Table 8 highlights the main findings.

### A. REMOTE ATTESTATION ENHANCED ACCESS MANAGEMENT WITHIN TACTICAL BUBBLES

IoT devices, e.g., surveillance cameras or UAVs are increasingly utilized in public safety missions. These devices are susceptible to remote cyber-adversaries trying to install malware and taking control of the device as discussed in Section III-C. To mitigate this threat, remote attestation [112] can be used to verify the integrity of the device and to detect unauthorized changes in the device firmware. Such additional evidence of device's trustworthiness could also be used, e.g., as one attribute in prioritization of users or the device could even be required to prove the absence of malware by remote attestation before it is allowed to join the network.

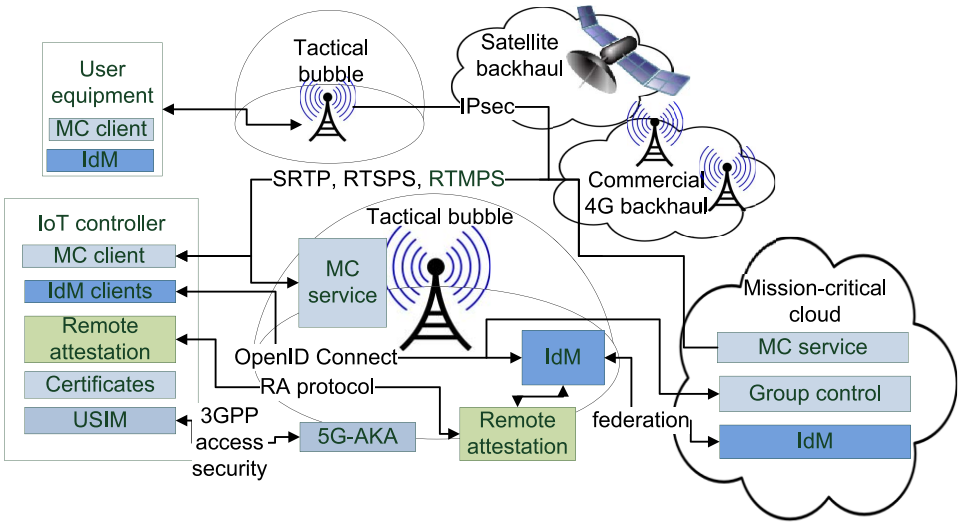


**FIGURE 2.** Security enablers explored in the trials include satellite backhaul securing with IPsec, identity management (IdM) for mission-critical (MC) services in tactical bubble, and remote attestation of IoT devices.

**TABLE 8.** Threat mitigations* by trialed solutions.

| *Mitigated threat scenario* | *IdM with remote attestation* | | *Secure satellite backhaul* | | *Description* |
|---|---|---|---|---|---|
| | *Video @ bubble* | *UAV @ bubble* | *MCX @ cloud* | *Priv.net access* | |
| Compromise of unhardened IoT devices | ▼ | ▼ | | | Remote attestation for Nuvoton NuMicro M2351 based IoT sensor |
| Leaking of credentials, device cloning | ▼ | ▼ | | | ARM TrustZone based secure storage for credentials and identifiers |
| Traffic and metadata observation | | | ▼ | ▼ | IPsec hides headers and addresses; though satellite DL is widely visible |
| Jamming | | | ▼ | ▼ | Redundant satellite backhaul ensures availability |
| Denial of priority | | | ▲ | ▲ | Limited satellite channel stresses prioritization |
| Signalling storms | | | ▲ | ▲ | Limited satellite channel more vulnerable to be a bottleneck |
| Subscriber identity and profile data leakage | ▼ | ▼ | | | Symmetric secrets not used |
| Indirect attacks against support systems | | | ▲ | ▲ | Attacks against satellite network |
| Network attacks against backhaul traffic | | | ▲ | ▲ | Attacks against satellite communications network |
| Unavailable cloud | | | ▼ | ▼ | Redundant cloud connection ensures availability |
| Security breach, leakage of transit keys | | | ▲ | ▲ | Leaking IPsec keys within tactical bubble |
| Spoofed situational awareness | ▼ | ▼ | | | Remote attesting trustworthiness of data sources |
| End-to-end (E2E) security breakout at the edge | | | ▲ | ▲ | Breakouts due to performance acceleration |
| Performance degradation due to E2E security | ▲ | ▲ | ▲ | ▲ | Overhead due to asymmetric crypto / IPsec |
| Masquerading | ▼ | ▼ | | | Strong, mature certificate authentication; no exposed authentication database |
| Federation degrades performance | ▲ | ▲ | | ▲ | Decoupled IdM causes overhead |
| Federation opens side-channels | ▲ | ▲ | | ▲ | Local identity server may become compromised |

*Arrow down (▼) - risk is mitigated; Arrow up (▲) - risk is emphasized. Colour coding and arrow sizes illustrate risk levels as in Table II.

*Approach:* In the trial, the devices within a tactical bubble communicate with backend services that verify the devices' identity using the OpenID Connect and OAuth 2.0-based authentication and authorization framework. Thus, the services act as OAuth 2.0 resource servers. The authorization server authenticates devices using OAuth 2.0 mutual-TLS client authentication (RFC-8705) [117] and X.509 certificates. We extend this framework to perform integrity verification of device firmware as part of authentication and to convey attestation status of the device to resource servers within the OAuth 2.0 access token. Our prototype implementation is based on IdentityServer4 [120].

In the solution we describe, remote attestation is based on Trusted Computing Group's (TCG) implicit identity-based device attestation specification [121], which uses a device identifier composition engine (DICE) as the root-of-trust for the integrity measurement. Following the specification, device's secure bootloader generates a device ID key pair that is used as device's identity. Furthermore, it derives another key pair, called alias key pair, and certifies it using the device ID credentials. The integrity of the device firmware

is measured before the firmware is executed and the measurements embedded into the alias key certificate to form a basis for remote attestation.

The IoT device is represented by a NuMicro M2351 [122] microcontroller. Device boot, key derivation, and integrity measurements are isolated from the device firmware using ARM TrustZone for ArmV8-M [110] technology. The device ID private key never leaves the device's trusted environment and cannot be accessed by the device firmware. The alias key pair's private key and certificate are exposed to the device firmware to be used as TLS credentials.

When new devices are introduced into a tactical bubble, they are not assumed to have pre-established trust relations or authentication credentials. As the result mutual-TLS based authentication cannot be used to authenticate the device at this point. In the trial we implement end-user assisted security bootstrapping of devices. This method is based on OAuth 2.0 Device Authorization Grant (RFC-8628) [118]. In this method, a device requests for end-user authorization to register itself with the authorization server. It does so by first requesting a device authorization code from the authorization server, which it then delivers to an end-user, who is deploying the device, via out-of-band channel, e.g., device's display or near field communication with another UE. The end-user then authenticates herself with the authorization server, e.g., using a mobile phone, and provides the code to the authorization server which grants an OAuth 2.0 access token to the device on behalf of the end-user. The device uses the access token to register its device ID certificate with the authorization server.

After registration, the device can authenticate itself directly with the authorization server and request for OAuth 2.0 access tokens without end-user involvement. We extend device authentication by remote attestation so that the device provides evidence of its integrity to the authorization server as follows:

1) The device requests an access token from the authorization server. It authenticates to the server using X.509 based mutual-TLS authentication and the alias key certificate as its TLS client certificate.
2) The authorization server authenticates the device during the TLS handshake against a database of registered device ID certificates. If authentication is successful and DICE certificate extensions are present, it forwards the certificate to an attestation service for integrity verification.
3) The attestation service verifies the integrity of the device by validating the alias key certificate and comparing embedded integrity measurements against a reference integrity metric database. The service issues an attestation token describing the result of the integrity verification procedure and returns the token to the authorization server.
4) The authorization server issues an access token and embeds the attestation token into the access token as an additional claim. Following RFC-8705 [117] the access token is bound to the client's TLS certificate. The access token is passed to the device.
5) The device receives the access token and passes it to the resource server with the request it intends to perform.
6) The resource server verifies that the client's TLS-certificate matches the certificate fingerprint bound to the access token, establishing proof-of-possession. Furthermore, it contacts the authorization server to validate the access token.
7) The resource server extracts the attestation token from the access token and uses its information to make decisions about the trustworthiness of the device and the data it provides.

The device registration phase can be enhanced with remote attestation in the same way. However, since security bootstrapping is not yet completed, the trust to the attestation report must be established by other means.

The authorization policies can be created when new devices are introduced to network by the users within tactical bubbles or by a remote control service. Default policy templates for particular device types or user roles can be created during non-operational time. Policies should be stored in a secure database that is attached to the authorization server. The server and database can be kept either in the tactical bubble or in the mission-critical cloud. The user experience of fine-grained authorization can be simplified with the solution. As the attestation provides verified information on the type of device, access permissions can be granted implicitly. Access control objects and predicates, i.e., services and actions, that should be available for devices with particular type or role are typically known in advance. Hence, the end-user making ad-hoc decisions in the mission-site is not required to be queried on each authorization separately. Similarly, it is possible to make security policies that limit particular services accessible only for devices that are attested to be trustworthy.

The reference integrity metric database that the attestation server needs to verify UEs' integrity is delivered to tactical bubble in similar fashion, e.g., from public safety operator's centralized service, which collects the information on acceptable devices from the manufacturers.

*Discussion:* Remote attestation of constrained IoT devices is still an emerging topic and far from a standard practice. However, several initiatives [121], [123], [124] are enabling gradual shift towards more trustworthy devices. The approach discussed in this section has various advantages.

The solution delegates the verification of device integrity to the attestation service and thus provides similar benefits by separation of concerns for remote attestation as OpenID Connect and OAuth 2.0 frameworks provide for authentication and authorization: simplicity of implementation and configuration management, as well as, scalability

as the mechanisms can be distributed. Moreover, the solution re-uses a mature framework already used in many cloud environments and supported by 3GPP for identity management [10].

The solution requires no modifications to the authentication and authorization flow from the client's or the resource server's perspective. On the contrary, both the integrity measurements and the attestation token are embedded in the existing protocol messages, allowing the same mechanism to be used with devices, authorization servers, or resource servers that do not support our remote attestation solution. Rather, the solution allows remote attestation capable devices to provide additional evidence of their trustworthiness. In fact, due to the heterogeneity of IoT devices and lack of remote attestation support in the existing products, this kind of mixed mode operations is likely.

The solution is based on TLS and uses X.509 certificates and asymmetric key cryptography, which could cause too much overhead for the most constrained devices. A more recent TCG DICE specification [125] discusses symmetric key cryptography for TLS-PSK based authentication and provides a remote attestation mechanism that could be more suitable for such devices.

The solution is targeted at constrained devices, where all the software is typically installed and run as a single application firmware image provided by one source, e.g., the device manufacturer. Richer UEs, e.g., mobile devices, typically run various applications from many sources, each updated separately, complicating integrity measurement and reference integrity metrics management. Hence, these systems also require more complex integrity verification and remote attestation solutions. Nevertheless, public safety authorities' typically have strict security policies in place that limit the number of acceptable devices, whitelist permitted software configurations, and strictly control software installation. Consequently, due to well-known device configurations compared to, e.g., civilian operators, remote attestation could also be a viable option for richer UEs in the public safety domain.

### B. SECURING SATELLITE BACKHAUL FOR TACTICAL BUBBLES

Since tactical networks must be rapidly deployable in remote and rural locations, wireless backhaul is sometimes the only solution for connecting the tactical bubble to the core network or application server. Dedicated point-to-point microwave links (7–40 GHz) are often used in commercial cellular networks for wireless backhauling, but they have limited range and require expertise, time, and licenses to deploy [126]. Commercial satellite services, on the other hand, provide near ubiquitous connectivity across the globe, can be at best deployed in a matter of minutes without expertise and do not require spectrum licensing. Satellite backhauls are therefore attractive candidates for providing the required connectivity to the core network and application services for access and regular bubbles [127]–[130]. Satellite networks can also be deployed as redundancy to improve availability, for example, in situations where the terrestrial network or other backhaul options are congested, unavailable or compromised due to an attack.

**TABLE 9.** GEO satellite network features.

| Feature | Description |
|---|---|
| Coverage | The transmissions from the satellite towards a user inside a spot beam are received by everyone within the range of the beam, which is in the order of hundreds or thousands of kilometers across. |
| Latency | Minimum one-way delay of a GEO satellite link is around 240 ms. |
| Capacity | Unlike microwave links that can have several Gbps two-way data rates, the maximum uplink / downlink bit rates of portable GEO satellite terminals are typically less than 10 / 100 Mbps, respectively. |
| Protocols | Instead of 3GPP based waveforms and protocols, GEO satellite links often rely on DVB-S2/RCS and/or proprietary solutions. |
| Architecture | GEO satellites are in a fixed position 35,786 km above the earth's equator and commonly have a bent pipe architecture. The ground stations that connect the satellites to the backbone network may reside in a different country than the tactical bubble. |

In the trial, a geosynchronous equatorial orbit (GEO) satellite link was selected as a backhaul solution due to the maturity of the technology, availability of commercial portable devices, and the capability for sufficient data rates in the selected use cases. Some of the main threats arising from the use of GEO satellite link for connections between the access network and remote core or MCX servers are listed in Table 8. Many of the threats are due to the unique features of the GEO satellite networks that are summarized in Table 9.

#### 1) SECURITY REQUIREMENTS

Since the backhaul may contain both the user plane data as well as the control plane signaling, the confidentiality and integrity of the satellite link traffic are of paramount importance. The features listed in Table 8 may, however, compromise the backhaul security and availability, unless appropriate measures are taken to protect it, as discussed in detail below.

The coverage of a high throughput GEO satellites is typically divided into several spot beams (like cells in terrestrial networks) that each span a geographic area several hundreds of kilometers across [131]. Due to the high altitude of the GEO satellites and broadcast nature of the transmissions, the downlink (satellite-to-ground) traffic can be intercepted and signal tampered at any location within the spot beam with roughly equal signal quality using low-cost commercial equipment [132], [133]. This is in stark contrast to microwave links that are extremely directional, require specialized equipment, and are difficult to intercept without detection. Furthermore, unlike terrestrial 5G that has confidentiality and integrity protected air interface, many satellite operators use either simple scrambling or do not protect their

over-the-air traffic at all [134], [135], exposing the downlink data to passive eavesdropping within a large geographic area. Adversaries might, for example, intercept all transmissions towards the tactical bubbles in the capital region from a fixed location that is hundreds of kilometers away from it. Intercepting the uplink (ground-to-satellite) transmission, on the other hand, is more challenging due to the highly directional antenna of the very-small-aperture terminal (VSAT) user equipment. In practice, the adversary would need to be very close to the VSAT on the ground or a UAV or a crane car would be needed to lift the intercept receiver near the main lobe of the transmit signal [136]. While this is significantly more challenging than eavesdropping of the downlink transmission, intercepting the uplink signal is still feasible, at least at higher latitudes, where the elevation angle of the GEO satellite is low.

To combat the long latency of the GEO satellite link, the extensive use of edge processing and local storage (caching) may be needed to guarantee desired QoS for the users in the tactical bubble [128]–[130]. For the same reason, commercial satellite networks use performance enhancing proxies (PEPs) and acceleration techniques, such as TCP spoofing, to improve the performance of the satellite link. Some satellite operators also offer proprietary solutions for GTP-U acceleration of the LTE backhaul traffic [137]. However, the use of edge processing and different acceleration techniques expand the threat surface by creating security breakouts, as discussed earlier. Typical PEP implementations also break the end-to-end semantics of IP connections and prohibit the use of IPsec. But failing to protect the transport layer data opens up the possibility for TCP session hijacking due to the long latency of the satellite link [135]. The delay and jitter of the satellite link also prevent the synchronization of the access network from the master clock using precision time protocol (PTP) messages, as specified in the IEEE 1588-2008/2019 standards [138]. The tactical bubble therefore needs to use global navigation satellite system (GNSS) based synchronization, which is prone to jamming and DoS attacks [133], or to rely on the accuracy of local oscillators. Both approaches can have an impact on the performance and security of the system if not properly addressed.

The limited uplink capacity has a direct impact especially on the operation and security of the access bubbles that rely on external core network functions. A great number of simultaneously authenticating devices, whether civilian devices or critical users, may overload the satellite uplink and temporarily block the registration of legitimate users to the bubble. A similar issue may arise unintentionally if, e.g., many legitimate IoT devices inside the bubble activate simultaneously, causing a signaling storm between the tactical bubble and the core network due to the control signaling overhead arising from the creation of a large number of GTP-tunnels. Furthermore, the limited capacity of the satellite connection may lead to an extensive use of edge processing and acceleration techniques in access and regular bubbles. Traffic prioritizing and selection for the backhaul may also be necessary to avoid exhausting the limited resources of the satellite link. While such techniques improve the user experience, they also complicate the architecture and expand the threat surface.

Although standardization activities aiming at harmonizing the terrestrial and non-terrestrial networks in 5G are progressing with the initial target for 3GPP Release 17 [139], [140], current GEO satellite systems are mostly based on DVB-S2/RCS and/or proprietary solutions. Since many of the security and control mechanisms listed, e.g., in Table 1 and Table 4 require support from the system, they cannot be enforced on the satellite link that relies on different standards and security mechanisms [141] than the 5G based access and core networks. For example, access control, user prioritizing, reservation of resources and security measures may not be in the control of the tactical network operator, implying that the satellite backhaul of the critical user is treated the same as any other link in the satellite network. This may lead, e.g., to insufficient security measures and service disruption if the spot beam is heavily congested. For the same reason, priorities of the traffic flows may not be inherited by the streams in the satellite link, so that traffic prioritizing and selection needs to be carried out in the tactical bubble before the backhaul, creating a potential security threat, as discussed earlier.

The last features of the GEO satellite networks discussed in this section stem from the architecture and geography of the system. The simplest GEO satellites operate as radio frequency (RF) repeaters (so-called bent pipe architecture) that translate and amplify the RF signal from the uplink frequency to the downlink frequency, and vice versa. At worst, all uplink RF signals at correct carrier frequency, malicious or legitimate, are mixed and re-transmitted in the downlink. If the malicious signal is strong and of the same form as the legitimate signal, it may block the transmissions of the legitimate users. Since commercial systems may not be protected against malicious interference, a denial-of-service attack via hostile electromagnetic interference is possible [133], [136], [142]. The downlink signal to the tactical bubble can also be jammed directly, but due to the highly directional antenna of the user equipment, the malicious transmitter would need to be very close to the VSAT, or elevated near the main lobe of the receiving antenna, as in the case of uplink eavesdropping discussed earlier. A geographic feature that has a direct impact on the security is that the ground station that connects the GEO satellite to the operator's backbone network may reside in a different country than the tactical bubble, potentially exposing the internal network traffic to insiders of foreign nations. The connection between, e.g., the access bubble and the core network may also cross several borders over a public IP network, expanding the threat surface significantly.

### 2) APPROACH

Satellite backhaul has some obvious security implications on the operation of the tactical network, as can be observed

from Table 7 and the above discussion. It should be clear that a commercial GEO satellite link must be treated as an inherently unsecure transmission medium, requiring at the very minimum a strong end-to-end security solution to satisfy the requirements of MC operations.

In the trial, Dawson Ka-Sat SC-Zero 70K nomadic terminal from Viasat was used as a connectivity option for a Goodmill multichannel router. In addition to selected application-layer security features listed in Table 5, IPsec encapsulating security payload (ESP) tunnels were chosen to provide confidentiality, integrity, and replay protection for the satellite backhaul. Security gateways that guarantee hiding of the IP addresses and fully encrypted communication between the tactical bubble and core network or MCX server were installed. While the use of IPsec implies overhead and degraded performance of TCP traffic, the protection of MC data, servers and operation was deemed to be of higher priority than the diminished user experience. It should be noted, however, that IPsec tunneling does not solve all issues raised in this section. For example, the threats due to jamming, signaling storms, congestion of the satellite network, or architectural enhancements, like edge processing, traffic prioritizing and traffic selection, cannot be mitigated simply by using IPsec tunneling.

Instead of accepting the performance degradation due to end-to-end IPsec ESP tunnel, the use of trusted PEP in the satellite operator premises could be considered. Either the entire stream could be decrypted, or just the headers that are needed to enable the acceleration [131], [143]–[145]. This creates a security breakout at the operator premises, potentially located abroad and subject to local rules and regulation, paving the way for several infrastructure and transit threats as described in Table 2. For the regular bubble, it would be possible to rely on transport/application layer security measures listed in Table 5, but this still leaves open security threats that may be unacceptable to MC users. An alternative approach based on the QUIC protocol and specifically designed for the GEO satellite links, QPEP, has been proposed recently [146]. However, more work is needed, to verify its compatibility with the MC services and requirements. It should also be noted that the higher layer security mechanisms are not an option for the access bubble since the protocol stack for the communication between the access network and the core network is inherently unsecure [147].

To avoid blocking due to signaling storms arising from simultaneous device registrations, the user register and authentication function could be located inside the access bubble, but additional security measures are then needed to protect them from adversaries. The signaling storms due to GTP-tunnel creation could be mitigated by prioritizing the devices and allowing only a limited number of data sessions to be opened within a given period. With extra cost, priority in the satellite network might also be available from the satellite network operator and, for example, VPN tunnels could be established between the satellite operator's backbone and core network to avoid unsecure delivery over a public IP network.

## VII. FUTURE RESEARCH DIRECTIONS

This section introduces potential paths for future research to harden public safety communicatons.

### A. TACTICAL SECURITY SITUATIONAL AWARENESS AND ORCHESTRATION

The security posture of tactical bubbles depends on environmental parameters, which are different and variable in every mission – different users, different communications, different adversaries, different threats, and different security resources. Security requires configuration, monitoring, and adaptation to changing situations and security events. Dynamic configurations can be partly based to remote configurations by centralized security operations centers (SOC). However, in isolated scenarios, the possibilities of doing on-site configuration is virtually non-existent due to other operational hurries. Consequently, there is a need to research security automation solutions for tactical bubbles, i.e., to develop tactical SOC capabilities.

Tactical networks must be rapidly deployed to remote locations and must be operational as soon as they arrive or within a few minutes. Security configuration tasks of the deployment time include: setting up security associations between network components, allocating resources for security services, launching or deploying (e.g., migrating virtualized) security functions to support operations and to monitor and respond to emerging threats, as well as enabling isolated scenarios by choosing and deploying user and authorization policies (e.g., a complete national database of every public safety organization or some subset). Risk-driven security analysis tools could be beneficial when automating deployment of security control and assets. For instance, the risks within tactical bubbles depend on the assets and criticality of information stored in them as well as security controls that are available. Analysis tools could determine, e.g., whether a particular bubble is secure and guarded enough to be deployed with user databases.

Machine learning solutions may be beneficial in facilitating automation and increasing security situational awareness [148]–[150]. They can support security monitoring, collecting and analyzing security KPIs, verifying run-time situation against (complex) security policies, as well as intrusion, malware, and anomaly detection. They can also support security event management and orchestration of security responses.

Security automation and applications of ML can leverage the unique characteristics of public safety scenarios. First, the security awareness and skills of public safety users can be assumed to be above average when compared to other users of mobile networks. Consequently, automated security responses can be more aggressive and rapid. For instance, a detected anomaly may initiate quicker user notification and UE quarantine, than would be possible in civilian use

cases. Second, privacy is not a similar issue, as private applications and personal communications are typically limited. Consequently, privacy regulations [104] that may limit monitoring in civilian networks may not be a problem in public safety communications. Third, the threat detection may in some cases be more accurate in homogeneous public safety networks as the used applications and protocols are known in advance and produce traffic patterns that repeat in every mission. Hence, there is less unanticipated traffic and noise that could cause false alarms. The accuracy of these assumptions and speculations need verification through future research.

However, there are also challenges in automated configuration:

1) The strong requirement for availability in public safety scenarios may limit some reactions, as service disruptions are not tolerated.
2) Automation and ML may open up new kinds of vulnerabilities [67], [151] to the 5G systems.
3) The mission environment is different in almost every mission, so it is difficult to learn what is normal and thus detect anomalies. Tactical networks are rapidly deployed to locations and environments with operational parameters—channel characteristics, sources of interference, amount and type of users, number of groups and their members, used application, number and type of local and cyber adversaries—that are often unpredictable and unknown in advance.
4) Data that is available locally in tactical bubbles is limited. Centralized cloud services have, hence, superior learning abilities. Solutions are needed to enable federation between tactical and centralized SOC functions. Solutions should enable isolated security operability without compromising sensitive centralized information.

Further research is needed to understand what operational parameters remain the same and can be utilized to learn models, which are describing normal behavior. Research is also needed to increase trustworthiness and protection of inferred security awareness and data, which is collected from civilian devices [152] or a heterogeneous sensor device landscape, or which shared between different federative actors.

### B. CUSTOMIZING COMMERCIAL NETWORK SERVICES TO ENSURE AVAILABILITY

Commercial operators can customize their networks for particular users. The policy control function and 5G's exposure APIs provide the means to customize allocated resources and QoS. Network slicing provides more means to allocate virtualized resources for different applications. The customization could also include different kinds of security services. Future research is needed to reveal the full potential of security customizations and to identify security applications that can provide added-value to customers. Some potential means to customize network include

1) guaranteed availability via additional capacity, redundancy, and optionally reserving alternative backhauls such as satellite links [129] for just-in-case situations,
2) assured trustworthiness, e.g., by utilizing only customer approved hardware and software components and attesting the integrity of the network configuration at run time,
3) new routing architectures, such as Secure Internet Architecture (SCION) [153], [154] promise additional availability guarantees and end-to-end security awareness for 5G backbone networks, as well as
4) extensive security monitoring and customized security policies and controls.

### C. MILITARY-GRADE CUSTOMIZATIONS

While 3GPP technologies have been developed from commercial and cost-effectiveness perspectives, military grade technology research for secure communications, e.g., [155], [156], could provide new perspectives to enhance (and customize) the security of public safety communications. Military-grade solutions can mitigate risks of growing importance or which play a more vital role in public safety and disaster recovery operations.

For instance, physical-layer security solutions [157], [158] provide one perspective for providing additional defense against adversaries in the radio channel. Secrecy coding provides confidentiality against eavesdroppers and has been simulated [159], e.g., in the LTE context. Physical layer fingerprints have also been proposed as an identification approach in 5G [160].

Current 5G security algorithms are not fully resistant against quantum computer based cryptanalysis. Quantum resistance is currently being standardized [161] and also planned for mobile networks [62] Consequently, new development, i.e., algorithms and protocols that can support additional overhead, are needed both in the network layer but also for application and backhaul communications. However, many applications of public safety communications are by nature operational and tactical and there are not many long-term secrets that the future emergence of quantum computers would threaten.

Effective cooperation between various parties, such as allied armies or different public safety organizations, requires federation and interoperability both in the practices and technologies. Federated approaches where different but, not necessarily fully trusting, actors cooperate emphasize, e.g., layered cryptographic protection [162]. Such mechanisms utilized in the military domain may also be utilized in public safety communications to support cooperation between different public safety agencies or between public safety and civilian organizations.

### D. CERTIFICATION OF VARIOUS TYPES OF PUBLIC SAFETY EQUIPMENT

UEs targeted at public safety missions are typically certified by nationally accredited laboratories. They are assured

to provide a security level that enables them to handle information classified, e.g., as restricted or confidential.

However, existing certification approaches [96], [97] have been dedicated for cellphones or network equipment. As the device landscape for public safety operations is rapidly expanding, new solutions and schemes for testing and certifying [163] UAVs, sensors, cyber-physical systems, rescue robots, and other equipment used by authorities are needed. Similarly, these new devices also require platform security solution, which increase their robustness against different attacks but are also usable and easily deployable for public safety missions.

On the other hand, as unhardened devices will be used in public safety operations, access control solutions both in the network and application layer must be made more tolerant against threats caused by compromised and misbehaving devices.

### E. INTEGRATED SATELLITE-TERRESTRIAL ACCESS

A promising future solution for mission-critical communications would be a 5G network with an integrated 3GPP compliant satellite access based on a LEO megaconstellation. Many of the protocol and signaling weaknesses of the satellite link would be mitigated by conforming to the terrestrial 3GPP requirements and security mechanisms. Integration of the networks would also allow, e.g., user and traffic prioritizing, QoS control, traffic selection, and network management to be orchestrated jointly, improving the overall security of the system [164]. In addition, the short delay and high throughput of a LEO megaconstellation would eradicate many of the threats present in the GEO satellite links and multiple satellites offer redundancy.

While the impact of LEO satellite links on the 5G air interface are well studied, research on the security aspects of direct 5G LEO satellite access for mission-critical users is lacking. For example, the transmissions from the LEO satellites are prone to eavesdropping both from the ground and space, frequent inter-beam and inter-satellite handovers as well as inter-satellite routing complicate the system architecture, and requirement for low manufacturing costs open possibilities for satellite device based threats. Some potential research topics could include

1) secure and dynamic three-dimensional routing and handover procedures,
2) confidentiality and integrity protected inter-satellite communication, including use of free space optical communications, physical layer security and quantum communications,
3) use of on-board processing, e.g., to enable novel cross-layer approaches to detect and reject malicious signals at the satellite,
4) remote attestation of the satellites and network configuration,
5) securing of core network functions and MEC functionality in the non-terrestrial segment.

### F. COST-EFFECTIVENESS OF COMMERCIAL AND TACTICAL CONTROLS

Customized security services in the operator's network or physical or cyber controls in tactical bubbles require additional human resources for management and operations as well as software and computing investments and maintenance. Consequently, they will incur additional costs. Decisions to invest in new security solutions require balanced security trade-off analysis between quantified risks, costs of attacks, and costs of defenses. The goal of the analysis is to minimize the costs of security (additional physical and cybersecurity controls), to minimize risk (which is a function dependent on exposed assets, cost of impact, and probability of impact), as well as to maximize feasibility. Further research is needed to understand how existing risk-driven cost-benefit analysis frameworks for cybersecurity, e.g., [165], [166], can be utilized in a mobile network and public safety context.

## VIII. CONCLUSION

This article explored the security characteristics of public safety communications using 5G technologies. The transition from dedicated infrastructure to hybrid architecture is expanding the threat landscape mainly due to:

1) sharing of globally-connected civilian-operated infrastructure (that is more open for remote cyber-adversaries and for attacks from the Internet),
2) vulnerabilities inherited from 5G technologies (which are complex and inherit many compromises and vulnerabilities from the previous generations),
3) distributed architecture (increasing physical and geographical exposure, introducing breakouts to end-to-end security), as well as
4) heterogeneous devices and applications (bringing added complexity and vulnerabilities).

The essential challenge of public safety communications is the need for assured availability, which can be achieved by a combination of various device, network, and application layer approaches. Central issues include how to guarantee the capabilities of the commercial operators' networks to ensure quality and to support prioritization mechanisms in dynamic and complex scenarios. Commercial and virtual public safety network operators must protect against interferences from civilians and information leaking towards advanced adversaries. The need to support isolated operations also requires special arrangements and increases the risk of leaking critical user identification and organizational data.

Different risks can be minimized with additional technical and physical security controls or by limiting applications, features, and information that are deployed to tactical bubbles. Additional layers of protection can be added on top or under the standard 5G security: a) the network operator can customize the security services it provides for public safety users and b) the public safety users can deploy own application layer and device-specific security solutions. The trialed satellite-backhaul was an example of network-layer

means to assure availability while remote attestation provide an example of additional means to assure trustworthiness of the device layer. However, additional layers and controls come with costs and the cost benefits of using commercial communications networks are partly lost. Hence, the security investment decisions should be preceded by thorough risk and cost-benefit analyses.

Future technological development is needed in the area of automated security configurations and improved security reactiveness of networks and tactical bubbles. As network scenarios are becoming more complex and isolated operations are performed under an assumption of zero-configuration, adaptive and learning-based security applications could help to maximize the security performance with minimal efforts. The 5G architecture provides many promises for improved performance and latency but also new security risks by distributing processing to edges, to private networks, or to tactical bubbles. More development and research, e.g., in the area of federation, is needed before mission-critical applications can fully benefit from these opportunities. Further, security of new types of public safety devices from augmented reality and aerial surveillance to rescue robots and autonomous systems require new methodologies for cost-efficient security hardening, testing, and certification for public safety missions.

## ACKNOWLEDGMENT

The authors would like to thank the members of the cybersecurity working group of the PRIORITY project. The authors thank also Kalle Lähetkangas and Topias Uotila for helpful comments.

## REFERENCES

[1] M. Höyhtyä *et al.*, "Critical communications over mobile operators' networks: 5G use cases enabled by licensed spectrum sharing, network slicing and QoS control," *IEEE Access*, vol. 6, pp. 73572–73582, 2018.

[2] "Study on the security aspects of the next generation system," 3GPP, Sophia Antipolis, France, 3GPP Rep. TR 33.899 v.1.1.0, 2017.

[3] *5G; Security Architecture and Procedures for 5G System (Release 15)*, 3GPP Standard TS 33.501, 2018.

[4] *Isolated Evolved Universal Terrestrial Radio Access Network (E-UTRAN) Operation for Public Safety; Stage 1*, 3GPP Standard TS 22.346, 2014.

[5] J. Oueis, V. Conan, D. Lavaux, R. Stanica, and F. VAlois, "Overview of LTE isolated E-UTRAN operation for public safety," *IEEE Commun. Stand. Mag.*, vol. 1, no. 2, pp. 98–105, 2017.

[6] *Mission Critical (MC) Services Support in the Isolated Operation for Public Safety (IOPS) Mode of Operation*, 3GPP Standard TS 23.180, 2020.

[7] *Mission Critical Push to Talk (MCPTT); Stage 1, Release 13*, 3GPP Standard TS 22.179, 2015.

[8] *Mission Critical Data, Release 14*, 3GPP Standard TS 22.282, 2017.

[9] *Mission Critical Video, Release 14*, 3GPP Standard TS 22.281, 2018.

[10] *Security of the Mission Critical (MC) Service (Release 17)*, 3GPP Standard TS 33.180 V17.0.0, 2020.

[11] *Threat Landscape for 5G Networks*, ENISA, Attiki, Greece, 2019.

[12] I. Ahmad, S. Shahabuddin, T. Kumar, J. Okwuibe, A. Gurtov, and M. Ylianttila, "Security for 5G and beyond," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 4, pp. 3682–3722, 4th Quart., 2019.

[13] R. Khan, P. Kumar, D. N. K. Jayakody, and M. Liyanage, "A survey on security and privacy of 5G technologies: Potential solutions, recent advancements, and future directions," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 1, pp. 196–248, 1st Quart., 2020.

[14] G. Arfaoui *et al.*, "A security architecture for 5G networks," *IEEE Access*, vol. 6, pp. 22466–22479, 2018.

[15] A. Kumbhar, F. Koohifar, I. Güvenç, and B. Mueller, "A survey on legacy and emerging technologies for public safety communications," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 1, pp. 97–124, 1st Quart., 2017.

[16] W. Yu, H. Xu, J. Nguyen, E. Blasch, A. Hematian, and W. Gao, "Survey of public safety communications: User-side and network-side solutions and future directions," *IEEE Access*, vol. 6, pp. 70397–70425, 2018.

[17] U. Raza, M. Usman, M. R. Asghar, I. S. Ansari, and F. Granelli, "Integrating public safety networks to 5G: Applications and standards," in *Enabling 5G Communication Systems to Support Vertical Industries*. Hoboken, NJ, USA: Wiley, 2019, pp. 233–251.

[18] A. R. McGee, M. Coutière, and M. E. Palamara, "Public safety network security considerations," *Bell Labs Techn. J.*, vol. 17, no. 3, pp. 79–86, Dec. 2012.

[19] S. Clark, T. Goodspeed, P. Metzger, Z. Wasserman, K. Xu, and M. Blaze, "Why (special agent) Johnny (still) can't encrypt: A security analysis of the APCO project 25 two-way radio system," in *Proc. 20th USENIX Security Symp.*, 2011, p. 4.

[20] C. D. Barca, "Information security in digital trunking systems," *Database Syst. J.*, vol. 8, no. 1, pp. 40–48, 2017.

[21] H. Ghafghazi, A. El Mougy, H. T. Mouftah, and C. Adams, "Security and privacy in LTE-based public safety network," in *Wireless Public Safety Networks 2*, Oxford, U.K.: Elsevier, 2016, pp. 317–364.

[22] K. Miranda, A. Molinaro, and T. Razafindralambo, "A survey on rapidly deployable solutions for post-disaster networks," *IEEE Commun. Mag.*, vol. 54, no. 4, pp. 117–123, Apr. 2016.

[23] J. L. Burbank, P. F. Chimento, B. K. Haberman, and W. T. Kasch, "Key challenges of military tactical networking and the elusive promise of MANET technology," *IEEE Commun. Mag.*, vol. 44, no. 11, pp. 39–45, Nov. 2006.

[24] J. G. Ponsam and R. Srinivasan, "A survey on MANET security challenges, attacks and its countermeasures," *Int. J. Emerg. Trends Technol. Comput. Sci.*, vol. 3, no. 1, pp. 274–279, 2014.

[25] N. Hastings, K. Dempsey, and C. Paulsen, "Considerations for identity management in public safety mobile networks," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Interagency Rep. 8014, 2015.

[26] G. Coker *et al.*, "Principles of remote attestation," *Int. J. Inf. Security*, vol. 10, no. 2, pp. 63–81, Jun. 2011.

[27] *Study on New Radio (NR) to Support Non-Terrestrial Networks*, 3GPP Standard TS 38.811 V15.4.0, 2020.

[28] "Study on using satellite access in 5G; stage 1," 3GPP, Sophia Antipolis, France, 3GPP Rep. TR 22.822 V16.0.0, 2018.

[29] "Solutions for NR to support non-terrestrial networks (NTN)," 3GPP, Sophia Antipolis, France, 3GPP Rep. TR 38.821 V16.0.0, 2019.

[30] "Study on architecture aspects for using satellite access in 5G," 3GPP, Sophia Antipolis, France, 3GPP Rep. TR 23.737 V17.1.0, 2020.

[31] D. W. Parkinson, "TETRA security," *BT Technol. J.*, vol. 19, no. 3, pp. 81–88, 2001.

[32] S. M. Lee, S. Y. Lee, and D. H. Lee, *Efficient Group Key Agreement for Dynamic TETRA Networks* (Lecture Notes in Computer Science (Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics, 4362)). Heidelberg, Germany: Springer, 2007.

[33] G. Velianitis, K. Adel, S. Kotrba, and B. P. Manavalan, "Comparison of VoIP and TETRA regarding security in a safety critical environment," *J. Comput.*, vol. 13, no. 3, pp. 279–286, 2018.

[34] *Terrestrial Trunked Radio (TETRA); Voice Plus Data (V+D); Part 7: Security*, ETSI Standard EN 300 392-7 V3.2.0, 2010.

[35] S. Glass, V. Muthukkumarasamy, M. Portmann, and M. Robert, *Insecurity in Public-Safety Communications: APCO Project 25* (Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), vol. 96. Heidelberg, Germany: Springer, 2012.

[36] "Secure MVNO—Building a network fit for heroes," Nokia, Espoo, Finland, White Paper, 2019.

[37] "Ensuring critical communication with a secure national symbiotic network," Ericsson, Kista, Sweden, White Paper, 2018.

[38] "Why secure MVNO is your next smart move," Airbus, Leiden, The Netherlands, White Paper, 2017.

[39] "The case for dedicated public safety networks. Why commercial networks are not an option for PS-LTE," NEC, Minato City, Japan, White Paper, 2018.

[40] FirtsNet. (2021). *First Responder Network Authority, The Network*. Accessed: Mar. 11, 2021. [Online]. Available: https://firstnet.gov/network

[41] U.K. Home Office. (2021). *Emergency Services Network: Overview*. Accessed: Mar. 11, 2021. [Online]. Available: https://www.gov.uk/government/publications/the-emergency-services-mobile-communications-programme/emergency-services-network

[42] Erillisverkot. (2021). *Virve 2.0*. Accessed: Mar. 11, 2021. [Online]. Available: https://www.erillisverkot.fi/virve2-0/

[43] X. Chen and D. Guo, "Public safety broadband network with rapid-deployment base stations," in *Wireless Public Safety Networks 2: A Systematic Approach*. Oxford, U.K.: Elsevier, 2016, pp. 173–198.

[44] Z. Durumeric *et al.*, "The matter of heartbleed," in *Proc. Conf. Internet Meas. Conf.*, Nov. 2014, pp. 475–488.

[45] M. Bland, "Finding more than one worm in the APPLE," *Commun. ACM*, vol. 57, no. 7, pp. 58–64, 2014.

[46] A. Mettler, Y. Zhang, and V. Raman, *SSL Vulnerabilities: Who Listens When Android Applications Talk?*, FireEye Inc, Milpitas, CA, USA, 2014. Accessed: Oct. 29, 2020. [Online]. Available: https://www.fireeye.com/blog/threat-research/2014/08/ssl-vulnerabilities-who-listens-when-android-applications-talk.html

[47] K. Kaska, H. Beckvard, and T. Minárik, *Huawei, 5G, and China as a Security Threat*, NATO Cooperat. Cyber Defence Centre Excellence, Tallinn, Estonia, 2019, pp. 159–184.

[48] W. Karwowski and H. W. Glaspie, "Human factors in information security culture: A literature review," in *Proc. Int. Conf. Appl. Hum. Factors Ergon.*, vol. 593, 2018, pp. 267–280.

[49] *2019 Data Breach Investigations*, Verizon, New York, NY, USA, 2019, pp. 1–78.

[50] A. Shostack, "Experiences threat modeling at microsoft," in *Proc. Workshop Model Security (MODSEC) Int. Conf. Model Driven Eng. Lang. Syst. (MODELS)*, 2008.

[51] S. R. Hussain, O. Chowdhury, S. Mehnaz, and E. Bertino, "LTEInspector: A systematic approach for adversarial testing of 4G LTE," in *Proc. Netw. Distrib. Syst. Security Symp.*, 2018.

[52] S. R. Hussain, M. Echeverria, I. Karim, O. Chowdhury, and E. Bertino, "5GReasoner: A property-directed security and privacy analysis framework for 5G cellular network protocol," in *Proc. ACM SIGSAC Conf. Comput. Commun. Security*, 2019, pp. 669–684.

[53] S. R. Hussain, M. Echeverria, A. Singla, O. Chowdhury, and E. Bertino, "Insecure connection bootstrapping in cellular networks," in *Proc. 12th Conf. Security Privacy Wireless Mobile Netw. (WiSec)*, 2019, pp. 1–11.

[54] H. Kim, J. Lee, E. Lee, and Y. Kim, "Touching the untouchables: Dynamic security analysis of the LTE control plane," in *Proc. IEEE Symp. Security Privacy (SP)*, San Francisco, CA, USA, 2019, pp. 1153–1168.

[55] M. Lichtman, R. Rao, V. Marojevic, J. Reed, and R. P. Jover, "5G NR jamming, spoofing, and sniffing: Threat assessment and mitigation," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, Kansas City, MO, USA, 2018, pp. 1–6.

[56] E. S. Lohan *et al.*, "5G positioning: Security and privacy aspects," in *A Comprehensive Guide to 5G Security*. Hoboken, NJ, USA: Wiley, 2018, pp. 281–320.

[57] A. Shaik, R. Borgaonkar, S. Park, and J.-P. Seifert, "New vulnerabilities in 4G and 5G cellular access network protocols: Exposing device capabilities," in *Proc. 12th Conf. Security Privacy Wireless Mobile Netw. (WiSec)*, 2019, pp. 221–231.

[58] A. Shaik, J.-P. Seifert, R. Borgaonkar, N. Asokan, and V. Niemi, "Practical attacks against privacy and availability in 4G/LTE mobile communication systems," in *Proc. 23rd Annu. Netw. Distrib. Syst. Security Symp. (NDSS)*, 2016.

[59] K. Kohls, D. Rupprecht, T. Holz, and C. Pöpper, "Lost traffic encryption: Fingerprinting LTE/4G traffic on layer two," in *Proc. 12th Conf. Security Privacy Wireless Mobile Netw.*, 2019, pp. 249–260.

[60] F. Meneghello, M. Rossi, and N. Bui, "Smartphone identification via passive traffic fingerprinting: A sequence-to-sequence learning approach," *IEEE Netw.*, vol. 34, no. 2, pp. 112–120, Mar./Apr. 2020.

[61] O. Ureten and N. Serinken, "Wireless security through RF fingerprinting," *Can. J. Elect. Comput. Eng.*, vol. 32, no. 1, pp. 27–33, May 2007.

[62] T. C. Clancy, R. W. Mcgwier, and L. Chen, "Post-quantum cryptography and 5G security: Tutorial," in *Proc. ACM 12th Conf. Security Privacy Wireless Mobile Netw. (WiSec)*, 2019, p. 285.

[63] C. J. Mitchell, "The impact of quantum computing on real-world security: A 5G case study," *Comput. Security*, vol. 93, Jun. 2020, Art no. 101825.

[64] X. Chen and J. Huang, "Database-assisted distributed spectrum sharing," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 11, pp. 2349–2361, Nov. 2013.

[65] J.-M. Park, J. H. Reed, A. A. Beex, T. C. Clancy, V. Kumar, and B. Bahrak, "Security and enforcement in spectrum sharing," *Proc. IEEE*, vol. 102, no. 3, pp. 270–281, Mar. 2014.

[66] R. P. Jover, "Security and impact of the Internet of Things (IoT) on mobile networks," in *Security and Privacy in Internet of Things (IoTs): Models, Algorithms, and Implementations*. Boca Raton, FL, USA: CRC Press, 2016, pp. 545–564.

[67] J. Suomalainen, A. Juhola, S. Shahabuddin, A. Mämmelä, and I. Ahmad, "Machine learning threatens 5G security," *IEEE Access*, vol. 8, pp. 190822–190842, 2020.

[68] *Common API Framework for 3GPP Northbound APIs*, 3GPP Standard TS 23.222, 2018.

[69] N. D. Tangudu, N. Gupta, S. P. Shah, B. J. Pattan, and S. Chitturi, "Common framework for 5G northbound APIs," in *Proc. IEEE 3rd 5G World Forum 5GWF Conf.*, Bangalore, India, 2020, pp. 275–280.

[70] M. R. Spada, J. Perez-Romero, A. Sanchoyerto, R. Solozabal, M. A. Kourtis, and V. Riccobene, "Management of mission critical public safety applications: The 5G ESSENCE project," in *Proc. Eur. Conf. Netw. Commun. (EuCNC)*, Valencia, Spain, 2019, pp. 155–160.

[71] M. Casoni, C. A. Grazia, and M. Klapez, "A software-defined 5G cellular network with links virtually pooled for public safety operators," *Trans. Emerg. Telecommun. Technol.*, vol. 28, no. 3, p. e3092, Mar. 2017.

[72] A. Othman and N. A. Nayan, "Public safety mobile broadband system: From shared network to logically dedicated approach leveraging 5G network slicing," *IEEE Syst. J.*, vol. 15, no. 2, pp. 2109–2120, Jun. 2021.

[73] M. Pattaranantakul, R. He, Q. Song, Z. Zhang, and A. Meddahi, "NFV security survey: From use case driven threat analysis to state-of-the-art countermeasures," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 3330–3368, 4th Quart., 2018.

[74] I. Afolabi, T. Taleb, K. Samdanis, A. Ksentini, and H. Flinck, "Network slicing and softwarization: A survey on principles, enabling technologies, and solutions," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 3, pp. 2429–2453, 2018.

[75] H. Cui, G. O. Karame, F. Klaedtke, and R. Bifulco, "On the fingerprinting of software-defined networks," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 10, pp. 2160–2173, Oct. 2016.

[76] C. Gaber *et al.*, "Liability-aware security management for 5G," in *Proc. IEEE 3rd 5G World Forum 5GWF Conf.*, Bangalore, India, 2020, pp. 133–138.

[77] R. Altawy and A. M. Youssef, "Security, privacy, and safety aspects of civilian drones: A survey," *ACM Trans. Cyber Phys. Syst.*, vol. 1, no. 2, pp. 1–25, Feb. 2017.

[78] D. V. Solé and A. C. Augé, "A distributed man-machine dispatching architecture for emergency operations based on 3GPP mission critical services," *IEEE Access*, vol. 6, pp. 11614–11623, 2018.

[79] B. E. Strom, A. Applebaum, D. P. Miller, K. C. Nickels, A. G. Pennington, and C. B. Thomas, "MITRE ATT&CK™: Design and philosophy," MITRE, McLean, VA, USA, Technical Paper, 2018.

[80] MITRE. (2020). *MITRE ATT&CK® Mobile Matrices*. Accessed: Oct. 29, 2020. [Online]. Available: https://attack.mitre.org/matrices/mobile/

[81] J. Singh, R. Ruhl, and D. Lindskog, "GSM OTA SIM cloning attack and cloning resistance in EAP-SIM and USIM," in *Proc. Int. Conf. Soc. Comput. SocialCom/PASSAT/BigData/EconCom/BioMedCom*, Alexandria, VA, USA, 2013, pp. 1005–1010.

[82] M. Meyer, E. A. Quaglia, and B. Smyth, "Attacks against GSMA's M2M remote provisioning (Short Paper)," in *Proc. Int. Conf. Finan. Cryptogr. Data Security*, vol. 10957, 2018, pp. 243–252.

[83] *Proximity-Based Services (ProSe); Security Aspects (Release 12)*, 3GPP Standard TS 33.303, 2018.

[84] M. Haus, M. Waqas, A. Y. Ding, Y. Li, S. Tarkoma, and J. Ott, "Security and privacy in device-to-device (D2D) communication: A review," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 2, pp. 1054–1079, 2nd Quart., 2017.

[85] J. Zhang, X. Huang, W. Wang, and Y. Yue, "Unbalancing pairing-free identity-based authenticated key exchange protocols for disaster scenarios," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 878–890, Feb. 2019.

[86] *3G Security; Security of Multimedia Broadcast/Multicast Service (MBMS)*, 3GPP Standard TS 33.246, 2020.

[87] G. Egeland and P. E. Engelstad, "The reliability and availability of wireless backhaul mesh networks," in *Proc. IEEE Int. Symp. Wireless Commun. Syst.*, Reykjavik, Iceland, 2008, pp. 178–183.

[88] M. Dräxler and H. Karl, "Dynamic backhaul network configuration in SDN-based cloud RANs," 2015. [Online]. Available: https://arxiv.org/abs/1503.03309.

[89] A. Ting, D. Chieng, K. H. Kwong, I. Andonovic, and K. D. Wong, "Dynamic backhaul sensitive network selection scheme in LTE-WiFi wireless HetNet," in *Proc. IEEE Int. Symp. Pers. Indoor Mobile Radio Commun. (PIMRC)*, London, U.K., 2013, pp. 3061–3065.

[90] I. Loumiotis, T. Stamatiadi, E. Adamopoulou, K. Demestichas, and E. Sykas, "Dynamic backhaul resource allocation in wireless networks using artificial neural networks," *Electron. Lett.*, vol. 49, no. 8, pp. 539–541, Apr. 2013.

[91] *Network Functions Virtualisation (NFV); NFV Security; Problem Statement*, ETSI Standard GS NFV-SEC 001, 2014.

[92] *Network Functions Virtualisation (NFV); NFV Security; Cataloguing Security Features in Management Software*, ETSI Standard GS NFV-SEC 002, 2014.

[93] *Network Functions Virtualisation (NFV) Release 3; Security; Security Management and Monitoring Specification*, ETSI NFV-SEC 013 V0.0.9, 2017.

[94] *NFV Security; Security and Trust Guidance, V1.1.1*, ETSI Standard GS NFV-SEC 003, 2014.

[95] A. Celesti, M. Fazio, A. Galletta, L. Carnevale, J. Wan, and M. Villari, "An approach for the secure management of hybrid cloud–edge environments," *Future Gener. Comput. Syst.*, vol. 90, pp. 1–19, Jan. 2019.

[96] *Network Equipment Security Assurance Scheme—Overview. FS.13*, GSM Assoc., London, U.K., 2019.

[97] "Security assurance methodology (SCAS) for 3GPP network products," 3GPP, Sophia Antipolis, France, 3GPP Rep. TR 33.916, 2019.

[98] *Information Technology—Security Techniques—Information Security Management Systems—Overview and Vocabulary*, Standard ISO/IEC 27000:2009, 2018.

[99] National Institute of Standards and Technology. *National Vulnerability Database. NIST Special Publication 800-53*. Accessed: Feb. 15, 2021. [Online]. Available: https://nvd.nist.gov/800-53

[100] *IT-Grundschutz Catalogues—13th Version*, BSI, Germany, 2013.

[101] *Katakri 2020—Information Security Audit Tool for Authorities /Tietoturvallisuuden Auditointityökalu Viranomaisille*, Ministry Foreign Affairs Finland, Helsinki, Finland, 2020.

[102] G. Mayer, "RESTful APIs for the 5G service based architecture," *J. ICT Stand.*, vol. 6, no. 1, pp. 101–116, 2018.

[103] J. Arkko, E. Carrara, F. Lindholm, K. Norrman, and M. Naslund, "MIKEY: Multimedia Internet keying," IETF, RFC 3830, 2004.

[104] S. Rizou, E. Alexandropoulou-Egyptiadou, and K. E. Psannis, "GDPR interference with next generation 5G and IoT networks," *IEEE Access*, vol. 8, pp. 108052–108061, 2020.

[105] A. Koubaa, A. Allouch, M. Alajlan, Y. Javed, A. Belghith, and M. Khalgui, "Micro air vehicle link (MAVlink) in a nutshell: A survey," *IEEE Access*, vol. 7, pp. 87658–87680, 2019.

[106] N. Prapulla, S. Veena, and G. Srinivasalu, "Development of algorithms for MAV security," in *Proc. IEEE Int. Conf. Recent Trends Electron. Inf. Commun. Technol. (RTEICT)*, 2017, pp. 799–802.

[107] R. Yasmin, J. Petäjäjärvi, K. Mikhaylov, and A. Pouttu, "On the integration of LoRaWAN with the 5G test network," in *Proc. IEEE 28th Int. Conf. Symp. Pers. Indoor Mobile Radio Commun. (PIMRC)*, Montreal, QC, Canada, 2018, pp. 1–6.

[108] H. Noura, T. Hatoum, O. Salman, J.-P. Yaacoub, and A. Chehab, "LoRaWAN security survey: Issues, threats and possible mitigation techniques," *Internet Things*, vol. 12, Dec. 2020, Art. no. 100303.

[109] *Tactilon Agnet 500—Agnet Organization Administrator User Manual*, AirBus, Leiden, The Netherlands, 2020.

[110] *Arm TrustZone Technology for the Armv8-M Architecture*, Arm Ltd., Cambridge, U.K., 2016.

[111] A. Waterman and K. Asanovic, *The RISC-V Instruction Set Manual, Volume II: Privileged Architecture*, document Version 20190608-Priv-MSU-Ratified," RISC-V, Zürich, Switzerland, Jun. 2019.

[112] G. Coker *et al.*, "Principles of remote attestation," *Int. J. Inf. Security*, vol. 10, no. 2, pp. 63–81, Jun. 2011.

[113] M. Ambrosin, M. Conti, R. Lazzeretti, M. M. Rabbani, and S. Ranise, "Collective remote attestation at the Internet of Things scale: State-of-the-art and future challenges," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 4, pp. 2447–2461, 4th Quart., 2020.

[114] *RSP Architecture, Version 2.2, SGP.21*, document SGP.21, GSMA, London, U.K., 2017.

[115] *RSP Technical Specification, Version 2.2.2, SGP.22*, GSMA, London, U.K., 2020.

[116] A. S. Ahmed, M. Thakur, S. Paavolainen, and T. Aura, "Transparency of SIM profiles for the consumer remote SIM provisioning protocol," *Ann. Telecommun.*, vol. 76, pp. 187–202, Aug. 2020.

[117] B. Campbell, J. Bradley, N. Sakimura, and T. Lodderstedt, "OAuth 2.0 mutual-TLS client authentication and certificate-bound access tokens," IETF, RFC 8705, 2020.

[118] W. Denniss, J. Bradley, M. Jones, and H. Tschofenig, "OAuth 2.0 device authorization grant," IETF, RFC 8628, 2019.

[119] M. Heikkila *et al.*, "Rapidly deployable LTE and 5G based tactical bubbles for authorities' mission critical communications," unpublished.

[120] IdentityServer. *IdentityServer · GitHub*. Accessed: Feb. 19, 2021. [Online]. Available: https://github.com/IdentityServer

[121] *Implicit Identity Based Device Attestation, Version 1.0, Revision 0.93*, Trusted Comput. Group, Beaverton, OR, USA, Mar. 2018.

[122] *NuMicro. ®. Family M2351 Series Technical Reference Manual*, Nuvoton Technol. Corp., Taipei, Taiwan, Aug. 2018.

[123] *Platform Security Model 1.0, DEN 0079, Release 0, Beta*, Arm Ltd., Cambridge, U.K., Sep. 2020.

[124] Linaro Limited. *Trusted Firmware—Open Source Secure World Software*. Accessed: Mar. 19, 2021. [Online]. Available: https://www.trustedfirmware.org/

[125] *Symmetric Identity Based Device Attestation, Version 1.0, Revision 0.95*, Trust. Comput. Group, Beaverton, OR, USA, Jan. 2020.

[126] J. Saunders and N. Marshall, *Mobile Backhaul Options: Spectrum Analysis and Recommendations*, GSMA, London, U.K., 2018.

[127] A. Kapovits *et al.*, "Satellite communications integration with terrestrial networks," *China Commun.*, vol. 15, no. 8, pp. 22–38, Aug. 2018.

[128] C. Politis, K. Liolis, M. Corici, E. Troudt, Z. Szabo, and J. Cahill, "Design of moving experimentation facility to showcase satellite integration into 5G," in *Proc. Eur. Conf. Netw. Commun. (EuCNC)*, Valencia, Spain, 2019, pp. 177–181.

[129] F. Völk, R. T. Schwarz, M. Lorenz, and A. Knopp, "Emergency 5G communication on-the-move: concept and field trial of a mobile satellite backhaul for public protection and disaster relief," *Int. J. Satellite Commun. Netw.*, vol. 39, no. 4, pp. 417–430, Sep. 2020.

[130] C. Politis, K. Liolis, P. Grønsund, and S. Heck, "Use cases and testbed solutions for 5G cellular backhauling via satellite," *Int. J. Satellite Commun. Netw.*, vol. 39, no. 4, pp. 400–416, Jul./Aug. 2021.

[131] A. Roy-Chowdhury, J. S. Baras, M. Hadjitheodosiou, and S. Papademetriou, "Security issues in hybrid networks with a satellite component," *IEEE Wireless Commun.*, vol. 12, no. 6, pp. 50–61, Dec. 2005.

[132] A. J. H. Fidler, G. Hernandez, M. Lalovic, T. Pell, and I. G. Rose, "Satellite—A new opportunity for broadband applications," *BT Technol. J.*, vol. 20, no. 1, pp. 29–37, 2002.

[133] *Security Threats Against Space Missions*, Standard CCSDS 350.1-G-2, 2015.

[134] J. Pavur, D. Moser, V. Lenders, and I. Martinovic, "Secrets in the sky," in *Proc. 12th Conf. Security Privacy Wireless Mobile Netw.*, 2019, pp. 277–284.

[135] J. Pavur, D. Moser, M. Strohmeier, V. Lenders, and I. Martinovic, "A tale of sea and sky on the security of maritime VSAT communications," in *Proc. IEEE Symp. Security Privacy (SP)*, San Francisco, CA, USA, 2020, pp. 1384–1400.

[136] M. Lichtman and J. H. Reed, "Analysis of reactive jamming against satellite communications," *Int. J. Satellite Commun. Netw.*, vol. 34, no. 2, pp. 195–210, Mar./Apr. 2016.
[137] D. Oren, *Satellite-Based Cellular Backhaul: Myths & Facts*, Gilat Satellite Netw., Petah Tikva, Israel, 2018.
[138] S. Ruffini, M. Johansson, B. Pohlman, and M. Sandgren, "5G synchronization requirements and solutions," Ericsson Technol. Rev., Kista, Sweden, White Paper, 2021.
[139] A. Anttonen, P. Ruuska, and M. Kiviranta, "3GPP nonterrestrial networks: A concise review and look ahead," VTT Techn. Res. Centre Finland, Espoo, Finland, VTT Research Rep. VTT-R-00079-19, 2019.
[140] F. Rinaldi *et al.*, "Non-terrestrial networks in 5G & beyond: A survey," *IEEE Access*, vol. 8, pp. 165178–165200, 2020.
[141] S. Iyengar, H. Cruickshank, P. Pillai, G. Fairhurst, and L. Duquerroy, "Security requirements for IP over satellite DVB networks," in *Proc. 16th IST Mobile Wireless Commun. Summit*, Budapest, Hungary, 2007, pp. 1–6.
[142] H. Rausch, "Jamming commercial satellite communications during wartime an empirical study," in *Proc. 4th IEEE Int. Workshop Inf. Assurance (IWIA)*, London, U.K., 2006, pp. 109–118.
[143] Y. Zhang, "A multilayer IP security protocol for TCP performance enhancement in wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 22, no. 4, pp. 767–776, May 2004.
[144] J. Puttonen *et al.*, "Multicast security framework for multi-spot beam satellite network," in *Proc. 21st Ka Broadband Commun. Conf.*, 2015.
[145] Y. Turk and E. Zeydan, "Satellite backhauling for next generation cellular networks: Challenges and opportunities," *IEEE Commun. Mag.*, vol. 57, no. 12, pp. 52–57, Dec. 2019.
[146] J. Pavur, M. Strohmeier, V. Lenders, and I. Martinovic, "QPEP: An actionable approach to secure and performant broadband from geostationary orbit," in *Proc. Netw. Distrib. Syst. Security Symp.*, 2021.
[147] C. Hu, L. Han, and S. M. Yiu, "Efficient and secure multi-functional searchable symmetric encryption schemes," *Security Commun. Netw.*, vol. 9, no. 1, pp. 34–42, Jan. 2016.
[148] A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 2, pp. 1153–1176, 2nd Quart., 2016.
[149] N. Haider, M. Z. Baig, and M. Imran, "Artificial intelligence and machine learning in 5G network security: Opportunities, advantages, and future research trends," Jul. 2020. [Online]. Available: https://arxiv.org/abs/2007.04490.
[150] Y. Sun, Z. Tian, M. Li, C. Zhu, and N. Guizani, "Automated attack and defense framework toward 5G security," *IEEE Netw.*, vol. 34, no. 5, pp. 247–253, Sep./Oct. 2020.
[151] M. Barreno, B. Nelson, A. D. Joseph, and J. D. Tygar, "The security of machine learning," *Mach. Learn.*, vol. 81, no. 2, pp. 121–148, Nov. 2010.
[152] B. Kantarci and H. T. Mouftah, "Trustworthy sensing for public safety in cloud-centric Internet of Things," *IEEE Internet Things J.*, vol. 1, no. 4, pp. 360–368, Aug. 2014.
[153] X. Zhang, H.-C. Hsiao, G. Hasker, H. Chan, A. Perrig, and D. G. Andersen, "SCION: Scalability, control, and isolation on next-generation networks," in *Proc. IEEE Symp. Security Privacy*, Oakland, CA, USA, 2011, pp. 212–227.
[154] S. C. Gupta, G. Gupta, and H. Saran, "New vision for 5G backbone network architecture," in *Proc. IEEE 3rd 5G World Forum 5GWF Conf.*, Bangalore, India, 2020, pp. 330–336.
[155] R. Matyszkiel, P. Kaniewski, M. Kustra, and J. Jach, "The evolution of transmission security functions in modern military wideband radios," in *Proc. XI Conf. Reconnaissance Electron. Warfare Syst.*, vol. 10418, 2017, Art. no. 104180E.
[156] F. Slimeni, B. Scheers, and Z. Chtourou, "Security threats in military cognitive radio networks," in *Proc. Int. Conf. Mil. Commun. Inf. Syst. (ICMCIS)*, Cracow, Poland, 2015, pp. 1–10.
[157] Y. Wu, A. Khisti, C. Xiao, G. Caire, K.-K. Wong, and X. Gao, "A survey of physical layer security techniques for 5G wireless networks and challenges ahead," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 679–695, Apr. 2018.
[158] L. Sun and Q. Du, "Physical layer security with its applications in 5G networks: A review," *China Commun.*, vol. 14, no. 12, pp. 1–14, Dec. 2017.
[159] C. K. Ngassa *et al.*, "Application cases of secrecy coding in communication nodes and terminals," in *Trusted Communications With Physical Layer Security for 5G and Beyond*. London, U.K.: Inst. Eng. Technol., 2017, pp. 501–531.
[160] H. Fang, X. Wang, and S. Tomasin, "Machine learning for intelligent authentication in 5G and beyond wireless networks," *IEEE Wireless Commun.*, vol. 26, no. 5, pp. 55–61, Oct. 2019.
[161] G. Alagic *et al.*, "Status report on the second round of the NIST post-quantum cryptography standardization process," NIST, Gaithersburg, MD, USA, NIST Internal Rep. 8309, 2017.
[162] A. M. Hegland, M. Hauge, and A. Holtzer, "Federating tactical edge networks: Ways to improve connectivity, security, and network efficiency in tactical heterogeneous networks," *IEEE Commun. Mag.*, vol. 58, no. 2, pp. 72–78, Feb. 2020.
[163] S. N. Matheu, J. L. Hernández-Ramos, A. F. Skarmeta, and G. Baldini, "A survey of cybersecurity certification for the Internet of Things," *ACM Comput. Surveys*, vol. 53, no. 6, pp. 1–36, Feb. 2021.
[164] P. Wang, J. Zhang, X. Zhang, Z. Yan, B. G. Evans, and W. Wang, "Convergence of satellite and terrestrial networks: A comprehensive survey," *IEEE Access*, vol. 8, pp. 5550–5588, 2020.
[165] B. R. Rowe and M. P. Gallaher, "Private sector cyber security investment strategies: An empirical analysis," in *Proc. 5th Workshop Econ. Inf. Security*, 2006, pp. 1–23.
[166] L. A. Gordon, M. P. Loeb, and L. Zhou, "Integrating cost-benefit analysis into the NIST cybersecurity framework via the Gordon-Loeb model," *J. Cybersecurity*, vol. 6, no. 1, 2020, Art. no. tyaa005.
[167] S. P. Rao, S. Holtmanns, and T. Aura, "Threat modeling framework for mobile communication systems," 2020. [Online]. Available: https://arxiv.org/abs/2005.05110.
[168] D. Hardt, "The OAuth 2.0 authorization framework," IETF, RFC 6749, 2012.
[169] N. Sakimura, J. Bradley, M. Jones, B. de Medeiros, and C. Mortimore, *OpenID Connect Core 1.0*, OpenID Found., San Ramon, CA, USA, 2014, p. S3.
[170] J. Navas and M. Beltrán, "Understanding and mitigating OpenID connect threats," *Comput. Security*, vol. 84, pp. 1–16, Jul. 2019.

**JANI SUOMALAINEN** received the M.Sc. (Tech.) degree in information technology from the Lappeenranta University of Technology, Finland in 2001, and the Lic.Sc. (Tech.) degree in telecommunications software from Aalto University, Finland, in 2013. Since 2000, he has been working with the VTT Technical Research Centre of Finland, Espoo, where he is a Senior Scientist. He is specialized on cybersecurity. Recently, he has been involved in both European and Finnish cooperation initiatives, including PHYLAWS, 5G-ENSURE, and CORNET, to develop and research secure next-generation technologies for mobile networks. He is currently working in researcher and VTT project manager roles with the Finnish Cooperation Project PRIORITY, which trials 5G technologies for public safety users. He has coauthored more than 30 scientific articles on network security. His research interests include threat modeling, security architectures, and adaptive security solutions for dynamic and heterogeneous network environments.

**JUKKA JULKU** received the M.Sc. (Tech.) degree in computer science and engineering from the Helsinki University of Technology, Finland, in 2009. He is currently pursuing the Doctor of Science (Tech.) degree in software systems with the Aalto University School of Science, Finland. He has been working with the VTT Technical Research Centre of Finland since 2007, and he is currently a Research Scientist in the cyber security research area. His research interests include trusted platforms for embedded devices, software security, and security testing and analysis.

**MIKKO VEHKAPERÄ** received the Ph.D. degree from the Norwegian University of Science and Technology, Trondheim, Norway, in 2010. He was a Postdoctoral Researcher with the KTH Royal Institute of Technology, Sweden, an Academy of Finland Postdoctoral Researcher with Aalto University, Finland, an Assistant Professor, Lecturer, with The University of Sheffield, U.K., and a Research Fellow with Aalto University. He is currently a Senior Scientist with the VTT Technical Research Centre of Finland. He is also an Adjunct Professor with the Aalto University. He held visiting appointments with the Massachusetts Institute of Technology, USA, Kyoto University, Japan, the Tokyo Institute of Technology, Japan, and Friedrich-Alexander University Erlangen–Nuremberg, Germany. His research interests span various aspects of communication networks and systems. He was the co-recipient of the Best Student Paper Award at the IEEE International Conference on Networks in 2011, and the IEEE Sweden Joint VT-COM-IT Chapter Best Student Conference Paper Award in 2015.

**HARRI POSTI** received the M.Sc. and D.Sc. (Tech.) degrees in electrical engineering from the University of Oulu, Finland, in 1991 and 2000, respectively. He has been working with the University of Oulu since 2012, and he is currently a Research Manager with the critical communication research area. His research interests include critical wireless communication as well as wireless network architecture and performance.