Navigating Privacy Challenges in Mission Critical Communication: Insights for 6G Networks

Prajnamaya Dass
Barkhausen Institut
Dresden, Germany
prajnamaya.dass@bb-dd.de

Marcel D.S.K. Gräfenstein
Technische Universität Dresden
Dresden, Germany
marcel_daniel_sven_kevin.graefenstein
@mailbox.tu-dresden.de

Stefan Köpsell
Barkhausen Institut
Dresden, Germany
stefan.koepsell@bb-dd.de

***Abstract*—This paper explores privacy issues in mission critical communication (MCC), a vital yet under-explored area of research for mission critical services over cellular networks. MCC facilitates emergency services like police and fire brigade during critical incidents. Due to the limited data capacity and coverage of TETRA-based services, MCC over 4G and 5G cellular networks has emerged as an alternative. However, network operator involvement in MCC raises significant privacy concerns, for instance, disclosing a policeman's location. To our knowledge, no existing work considers privacy issues in MCC over cellular networks. Therefore, we analyze privacy challenges in 3GPP-standardized MCC architecture within the context of 5G core network concepts and emerging technologies to be introduced in 6G. Our goal is to guide future actions in developing a privacy-preserving MCC architecture for 6G. We assess privacy implications for MC users, network entities, and MC servers, adhering to MCC deployment strategies. Finally, we suggest privacy controls to establish a next-generation privacy-preserving MCC architecture.**

***Index Terms*—Mission critical communication, MCC, privacy, trust domain, threats, 5G, 6G, 3GPP**

I. Introduction

Mission critical services are the backbone of essential operations across various sectors, ensuring safety, security, and functionality in society. From police and fire brigade responses to healthcare delivery, transportation management, and industrial automation, these services play a pivotal role in safeguarding public welfare [1]. Mission critical communication (MCC) refers to the communication systems and technologies used to support and facilitate these functions and operations [2]. The evolution of MCC began with land mobile radio (LMR) systems, following standards like P25 in the US and TETRA in Europe, to ensure interoperability among different equipment and agencies [3].

The architecture of LMR system was initially adopted for voice functionality due to its limited spectrum, coverage, and data capabilities [1], [2]. However, with the increasing demand for data-intensive applications, LTE gained traction in MCC domain. 3GPP (3rd Generation Partnership Project) defined standards and services for mission Critical Push-to-Talk (MCPTT) and in next release (Rel-14), added two additional services – mission Critical Video (MCVideo) and mission Critical Data (MCData).

A. Motivation

The 3GPP technical specification for MCC architecture [4] primarily addresses security but overlooks privacy issues, especially with 5G and 6G technologies that introduce new privacy concerns for MC users [5]. Although the existing security methods are necessary, they are not sufficient to address privacy issues. Additionally, the security and privacy solutions developed for 5G networks are not directly applicable to MCC due to its distinct deployment scenarios and functional architecture [4].

Introducing 5G into mission critical architecture discloses sensitive MC user details, such as a policeman's location, communication partners, and movement patterns, to the network operator, posing privacy risks. Moreover, the 6G technology like joint communication and sensing (JCAS) can reveal the precise location, human gestures, and other personal attributes of the MC users [6]. Application service providers within the MCC framework can control user equipment and the MC client application, potentially extracting details like a policeman's identity and communication keys. Conversely, they may deduce sensitive network information, such as ingress points and resource identifiers, posing privacy threats to the network.

B. Contributions

This paper focuses on privacy challenges and suggests measures to guide future developments in privacy-preserving 6G-based mission critical communications. The specific contributions are:

- Considering various deployment scenarios in the standard 3GPP-MCC functional architecture, we analyze the privacy issues – how entities (network operators, application service providers, or MC service providers) can extract or learn personally identifiable information within the MC system.
- We also explore privacy issues related to emerging topics (not yet applied in practice for MCC), such as off-network communication and non-3GPP access, as well as some upcoming 6G technologies like joint communication and sensing (JCAS).
- To address these privacy risks, we recommend different privacy controls as suggestive measures for the 6G-based MCC architecture.

II. Related Work

There are very few works focused on the security and privacy aspects of the MCC architecture, which is the reason for discussing fewer papers in this section. In the literature, some works focused on the architectural concepts of MCC. The common functional architecture, procedures, and information flows to support mission critical services over cellular networks are proposed by 3GPP [4]. The technical specification also specifies different possible deployment scenarios in which the functional MCC model can be applied. In [1], the challenges of using the 5G new radio interface for public safety MCC have been discussed. In [3], feasibility issues of mission critical push-to-talk (MCPTT) in 3GPP are discussed. In a similar work [7], the feasibility of MCPTT communications over 4G has been analyzed. The work in [8] analyzes the impact of the evolution from 4G architectures toward 5G on MCPTT key performance indicators. Different transition possibilities of migration of mission critical services from the land mobile radio-based systems discussed in [2]. The support of network slicing for MCC in 5G has been studied in [9].

The security architecture and procedures to safeguard mission critical services have been specified by 3GPP in [4]. This specification outlines security mechanisms pertaining to on-network use, off-network use, roaming, and migration. Security threats to 5G interfaces have been analyzed in [10], where standard security measures for these interfaces are discussed alongside categorized threats in their absence. The work in [11] discusses privacy threats in 5G stemming from newly introduced technologies like software-defined networking (SDN) and network function virtualization (NFV). In [12], a privacy-preserving architecture has been proposed to protect user identity and location details without changing the physical infrastructure. The proposed solutions in the architecture also consider network latency and claim to have no added latency and no need for direct cooperation from the network operator. A location-privacy solution has been proposed in [13]. The authors analyze the identifiability of users from the cell tower traces probabilistically and conclude that by renewing the identifiers and remaining offline for a certain time, the identifiability of users can be significantly reduced. These privacy-preserving approaches are suitable for 5G subscriber privacy protection in cellular networks; however, they are not applicable to MCC due to the existence of different protocols and architectural interfaces, where the privacy risks are different as well.

III. Mission Critical Communication Architecture

The architecture for mission critical communication, shown in Fig. 1, provides a framework where mission critical (MC) users, as existing subscribers of the home network, use its infrastructure to communicate with MC servers [4]. Similar to cellular users, the home network (HN) and serving network (SN) with the radio access network (RAN) facilitate the initial connection for MC users.

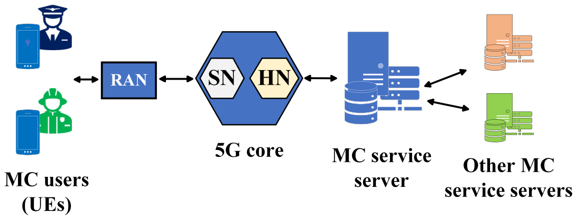

Fig. 1. Existing 5G-based mission critical communication architecture

Each MC user establishes a secure channel with the MC server, ensuring communication integrity and confidentiality. The MC service server can also connect MC users with other MC service servers, enabling seamless communication and collaboration. In the core network, each function is designed for specific tasks to efficiently manage and process communication traffic and data. For example, the authentication server function (AUSF) in 5G networks authenticates and authorizes user equipment (UE) attempting to access the network [14].

IV. Privacy Threats

This section explores threats in the MCC architecture that risk MC users, network components, the MC server, and their communications. We analyze how personally identifiable information (PII) can be exposed or acquired by other entities.

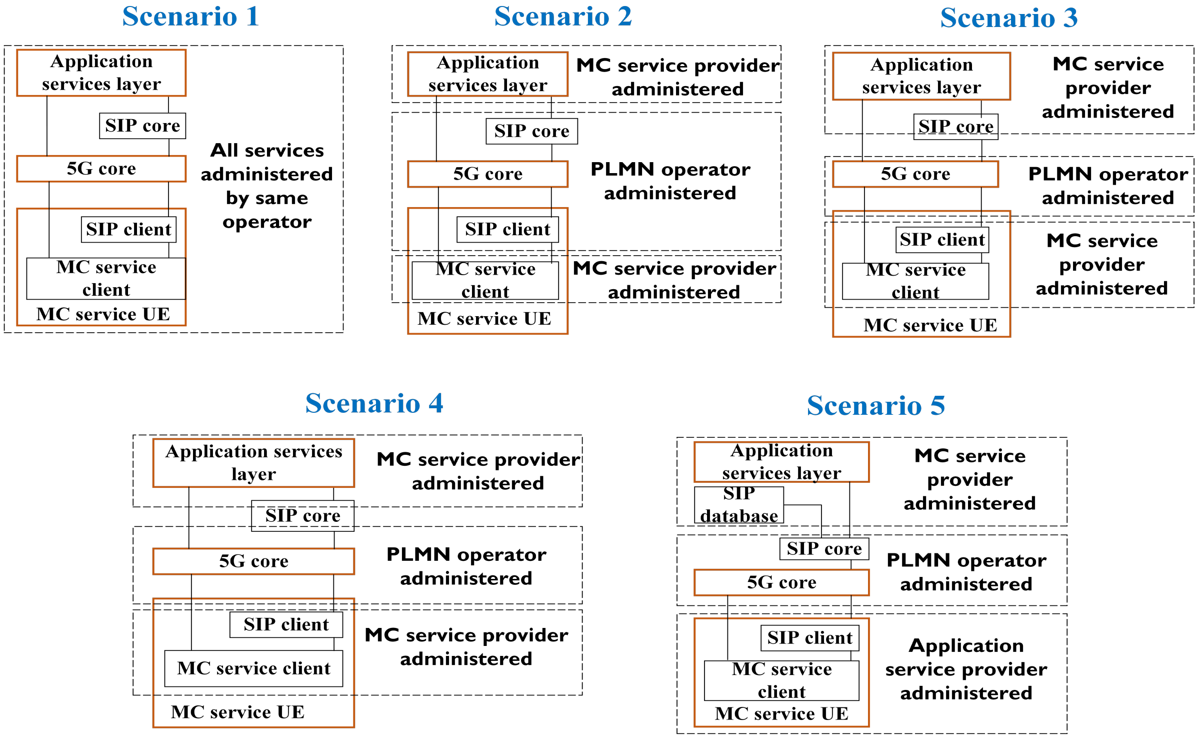
Scenario 1
Application services layer
SIP core
5G core
SIP client
MC service client
MC service UE
All services administered by same operator
Scenario 2
Application services layer
MC service provider administered
SIP core
5G core
PLMN operator administered
SIP client
MC service client
MC service provider administered
MC service UE
Scenario 3
Application services layer
MC service provider administered
SIP core
5G core
PLMN operator administered
SIP client
MC service client
MC service provider administered
MC service UE
Scenario 4
Application services layer
MC service provider administered
SIP core
5G core
PLMN operator administered
SIP client
MC service client
MC service provider administered
MC service UE
Scenario 5
Application services layer
SIP database
MC service provider administered
SIP core
5G core
PLMN operator administered
SIP client
MC service client
MC service UE
Application service provider administered

Fig. 2. Different deployment scenarios for mission critical communication over 5G

A. *Privacy threats from the administering entities*

Fig. 2 illustrates five deployment scenarios described in [4]. In scenario 1, regardless of ownership, each resource is managed by the same operator. This scenario can be described as: i) the PLMN operator administers network services, application services, and the MC service client, ii) the MC service server manages its own services and the underlying core network, iii) a third party, distinct from both the PLMN operator and the MC service server, manages all resources. However, in deployment scenarios 2, 3, and 4, some resources are managed by the MC service server while the remainder are overseen by the PLMN operator. In this paper, the terms ‘PLMN operator’ and ‘network operator’ refer to the same entity. In deployment scenario 5, the MC service user equipment is administered by the application service provider. It is important to note that a component may be owned by an entity different from the one administering it.

In MCC, most privacy threats arise from the administering entities. When an entity controls a resource or protocol, it often gains access to sensitive information. For instance, in deployment scenario 5 (refer to Fig. 2), if an MC service client is managed by an application service provider, encryption keys and identities may be disclosed. This can lead to spoofing and non-repudiation attacks. Similarly, in scenarios 2 and 5, if the session initiation protocol (SIP) is managed by the network operator, identifiable information, such as the MC user’s registered ID, may be exposed.

B. *Privacy threats during identity mapping and information sharing*

The PLMN operator, tasked with managing sensitive data such as the location details of cellular subscribers, maintains a centralized repository known as the unified data repository (UDR) [15]. In instances, where access to this data is necessary for mission critical (MC) services, such as during emergencies or urgent communications, the UDR plays a pivotal role. Upon request, the PLMN operator facilitates the sharing of location information with the MC service server [4], enabling swift and effective communication between MC users.

The process of facilitating this information exchange involves a critical step known as identity mapping, depicted in Fig. 3. During this process, the PLMN operator or the MC server undertakes the conversion of the MC user’s identity (MC ID) into the subscription permanent identifier (SUPI), a unique identifier associated with the subscriber’s network subscription. While this conversion is essential for establishing the necessary communication channels, it inadvertently exposes the

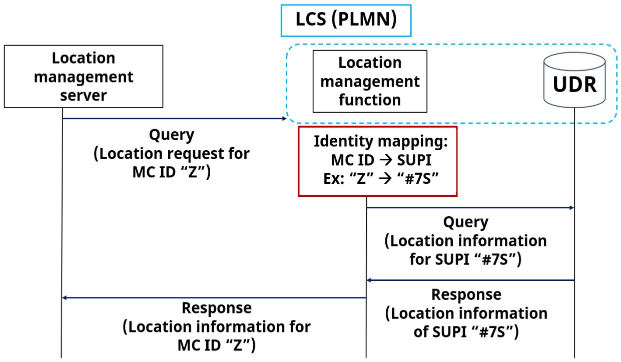
LCS (PLMN)
Location management server
Location management function
UDR
Query (Location request for MC ID "Z")
Identity mapping: MC ID → SUPI Ex: "Z" → "#7S"
Query (Location information for SUPI "#7S")
Response (Location information of SUPI "#7S")
Response (Location information for MC ID "Z")

Fig. 3. Privacy issues during information sharing between MC server and the PLMN operator

MC ID to the PLMN operator, which raises significant privacy concerns of identifiability and linkability. By associating the MC ID with the SUPI, the operator can link communications to individual users, compromising their anonymity and allowing for potential unauthorized surveillance. Even if mapping occurs on the MC server side, the operator may not access the MC ID but can still identify the server and the user's SUPI.

C. Privacy risks due to prioritization

5G networks allow for prioritization at different stages of the communication establishment. It allows MC users and the related services have higher priority than "normal" users to guarantee availability of the network, which can be used to identify MC users, posing privacy risks.

At the user plane, i.e., related to the data transport, a quality of service flow ID (QFI) is assigned to every data session. The QFI value, known to entities, such as the RAN and SN, can be used to identify mission critical communication. For instance, QFI value 65, which is assigned to "Mission Critical user plane Push-To-Talk voice" (please refer to Table 5.7.4.1-1 in [16]), gives identifiable information of an MC user. The concept of unified access control deals with an overloading situation at the RAN. Therefore, every establishment of a radio session between an UE and the RAN contains an Access Category and one or more Access Identities (AI). The AI value for mission critical services is 2. It allows MC users to get access to the RAN even if the RAN is currently overloaded. Therefore, "normal" users will be disconnected to allow service to MC users. Finally, during the connection establishment, a value referring to the cause of the establishment (EstablishmentCause in RRCSetupRequest) is specified in the request [17]. By analyzing these values (QFI, AI, and EstablishmentCause), the network operators can get rich contextual information about MCC, which can lead to linkability and identifiability threats.

D. Threats from the MC-SIP core and clients

Privacy threats can arise from SIP clients that reside in the MC service UE and SIP core infrastructure in the MCC systems. SIP clients, responsible for initiating and managing MC sessions, may inadvertently disclose sensitive user information, including identity details and communication patterns of the MC user. Such leaks could be exploited by adversaries for profiling or targeted attacks, compromising user privacy. Within the literature, various solutions have been proposed to anonymize header information in SIP [18]. Nonetheless, identifiable details regarding the MC user are still revealed in instances, where the SIP client is managed either by the PLMN operator (deployment scenarios 1 and 2 in Fig. 2) or by another service provider (deployment scenario 5 in Fig. 2).

Similarly, adversaries could exploit these weaknesses to compromise user privacy, conduct traffic analysis attacks, or disrupt services through denial-of-service (DoS) attacks. When the SIP core is administered by entities other than the MC service server (deployment scenarios 2, 4, and 5 in Fig. 2), identifiable information of the MC server and the MC users are revealed to the administering entity.

E. Privacy issues during connection with MC server

Before establishing a secure channel with TLS 1.3, the DNS mapping process, which is managed by recursive solvers and name servers, occurs. When a subscriber initiates a connection, the recursive solver (managed by the PLMN operator) translates the destination address into an IP address for routing. This process can reveal that the subscriber is likely using an MC service if the destination is an MC server. Even without DNS hostname resolution, the destination IP address can expose the nature of the communication, posing risks to user linkability and identifiability by revealing sensitive information about the MC user's activities and affiliations.

If the PLMN operator controls the name servers in the DNS mapping process, it heightens privacy risks by revealing subscriber communication patterns and preferences. While TLS encrypts content, it doesn't protect metadata. Proxy servers can anonymize the source address, but the destination address remains visible, challenging user anonymity. Despite TLS encryption, the PLMN operator can still identify requests to MC servers, distinguish MC users from standard 5G users via identifiers like subscription permanent identifier (SUPI), and monitor the distribution of MC users geographically.

F. Threats from the authentication protocol

The 5G authentication protocol, known as 5G AKA (authentication and key agreement) [14], faces privacy threats like linkability and traceability [5], [19]. The use of subscription concealed identifier (SUCI) does not completely eliminate privacy threats; instead, it introduces its own challenges. Moreover, given the involvement of sensitive services from the MC server, the 5G AKA protocol introduces additional threats.

After successful authentication in 5G AKA, the SUPI is exchanged with the serving network [19]. This exchange is a critical step in legally establishing the user's network connection and enabling access to services. However, sharing the SUPI raises privacy considerations. The transfer of SUPI between the MC user and the serving network (SN) exposes the user's permanent identifier to SN entities. While essential for network operations, this exposure could potentially be exploited by the SN and malicious actors to monitor the activities of MC users. The SUPI, as a permanent identifier linked to the user's subscription, uniquely identifies and tracks users across various communication sessions or contexts, raising concerns about user privacy and anonymity.

G. Privacy risks from inter-trust domain interactions

In an MC system, the trust domain encompasses one or more MC service functions managed by either the same or distinct service providers (such as the MC service provider or PLMN operator), who have agreed to exchange sensitive information. A PLMN operator is restricted to sharing sensitive information exclusively with entities of that same trust domain. However, given the limited number of PLMN operators in the market, establishing trust domains for information sharing presents a challenge. Additionally, if a single PLMN operator serves multiple MC service servers, defining trust boundaries for the exchange of sensitive information becomes impractical. In such a scenario, an ill-intent PLMN operator common to two different trust domains can pose threats to linkability, identifiability, and non-repudiation.

H. Threats due to MCC network slice

A mission critical user, subscribed to a dedicated network slice for critical services, communicates sensitive information like location data and MC organization details. Data intended for the MCC slice may unintentionally leak into other slices, exposing PII of MC users, identities of network entities or MC servers to unauthorized parties. Network operators or malicious actors might perform traffic analysis across slices to identify patterns or behaviors associated with MC users. By analyzing traffic patterns or metadata, adversaries could gain insights into the activities of MC users across different slices, compromising their privacy and security. The user's identity is tied to a SUPI, which is shared across slices. The network operators could exploit SUPIs or other identifiers to correlate the identities of users across different slices. This linking of identities could lead to privacy violations, as it enables adversaries to aggregate and analyze PII from multiple sources, potentially revealing sensitive information.

I. Privacy Issues in emerging and upcoming 6G technologies

Although off-network communication (using proximity-based services or ProSe) [4] and non-3GPP access are specified in the 3GPP standards for 5G, these aspects are still in a very preliminary stage for MCC. Additionally, emerging 6G technologies such as JCAS [20] introduce further privacy concerns due to the incorporation of personally identifiable information in sensing data.

Off-network mission critical communication: Proximity-based services enable devices to communicate directly with each other when they do not have connectivity with the network infrastructure. Off-network communication is a part of the future MC services [4], [21]. However, without active support from MC server, off-network communication is more prone to security and privacy threats. As devices exchange information directly, their proximity to each other can be inferred, potentially revealing sensitive information about MC users' locations and movements. ProSe communications may expose device identifiers or MC identities, compromising user anonymity and privacy. Adversaries may exploit this information to track users' activities or identify individuals participating in ProSe interactions. Due to the absence of connection with MC server, the direct communication between the MC users may bypass traditional security measures implemented by network operators, increasing the risk of data leakage. In addition to network operators, other MC users serving as relays or being available to nearby communicating MC users may also have the ability to infer sensitive information.

Joint communication and sensing (JCAS): This technology refers to using the same radio signal for both communication and sensing functions [6]. JCAS applications, due to the nature of sensing data involved, which often includes PII of individuals, are vulnerable to privacy attacks such as location tracking, identity disclosure, profiling, and misuse of sensed data. With sensing capabilities, PLMN operators can accurately pinpoint the location of MC users if distinguished from other users. Moreover, aggregating sensing data from multiple MC users may create detailed profiles of individuals' behaviors, preferences, and activities, raising concerns about MC user profiling, algorithmic discrimination of MC services, and potential misuse of personal information by third parties.

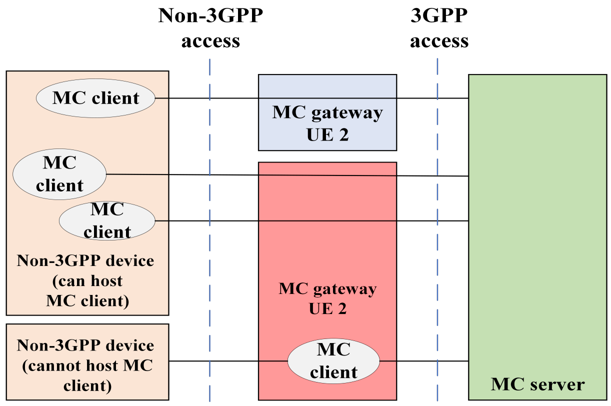

Fig. 4. Communication between non-3GPP MCC devices and the MC server

Non-3GPP access for MC users: In mission critical services, non-3GPP devices can connect to the MC server through non-3GPP and 3GPP access [4]. As shown in Fig. 4, the non-3GPP devices, which cannot host MC clients, use the MC gateway (MC UE) to connect with the MC server. The connection of non-3GPP devices to the MC UEs through non-3GPP access, presents a range of privacy threats stemming from various factors. These devices often collect and transmit sensitive mission critical data over unsecured channels, making them susceptible to interception or unauthorized access. In addition, they may rely on communication protocols lacking robust security mechanisms, leaving the MC user communications vulnerable to eavesdropping or man-in-the-middle attacks. Non-3GPP devices often rely on third-party services or cloud platforms for data storage, processing, and analysis. In scenarios, where the PLMN operator manages certain components of the MC server (deployment scenario 5 in Fig. 2), information about the non-3GPP devices could be revealed to the PLMN.

V. Suggestive Privacy Controls for 6G-Based MCC Systems

The proposed security aspects specified in 3GPP-MCC architecture [21] primarily align with the 4G network architecture and may not fully incorporate the advancements and innovations introduced in the 5G and B5G landscape. Although many privacy issues are challenging to solve, in this section, we discuss possible solutions to counter some of the privacy issues in 6G-based MCC.

Privacy-preserving information retrieval: Several methods can be employed to retrieve information, such as the location history of MC user from the core network, without revealing the real identity designated to the user by the MC server. It should be noted that the privacy-preserving information retrieval must ensure authentication and authorization checks. Private information retrieval (PIR) schemes [22] ensure confidentiality and privacy during information retrieval by concealing the user's query from the database server. Therefore, PIR protocols could be used to retrieve information from the UDR in the core network without revealing which MC user information records are being accessed. Authentication methods, such as blind signatures, anonymous authentication, and zero-knowledge proofs, could be used to verify the authenticity [23] of the MC server requesting information from the UDR. Furthermore, the use of anonymous communication networks that route user traffic through a series of encrypted relays, such as Tor (The onion router) [24], can help preserve the anonymity of the origin of the location information request (MC server).

Privacy in inter-trust domain communications: Ensuring privacy within trust domains, especially when a single PLMN operator spans multiple domains, requires a multifaceted approach. First, strict compliance with privacy regulations and standards, such as the general data protection regulation (GDPR), is essential for legal data sharing, processing, and protection across domains. Transparency with data subjects about mission critical data usage is crucial. Limiting shared PII to what is necessary is a best practice. Anonymizing or pseudonymizing PII can help obfuscate identifiers of users. Using one-time tokens with a short lifespan reduces the risk of unauthorized access across trust domains, thereby enhancing privacy against third-party service providers [25].

Privacy controls for MCC network slice: Ensuring privacy of MCC in network slices, especially when the core network functions are shared among multiple slices, requires a comprehensive approach that combines technical measures and governance policies. Strict data segregation mechanisms prevent cross-contamination between slices, if the MCC network slice has its own dedicated data storage and processing resources. Implementing granular access controls can help to regulate access to data and resources within the MCC network slice. Use of role-based access control (RBAC) or attribute-based access control (ABAC) will help to enforce least privilege principles and restrict access to authorized users only [26].

Privacy controls for emerging MCC technologies: During off-network communication and sensing activities in JCAS, techniques such as masking and randomization can obscure PII of the MC users participating in MCC. Achieving unlinkability and unobservability for ProSe-based MCC can be attained through covert operations, noise injection, anonymization, data fragmentation, decoy traffic, and differential privacy techniques. Employed individually or in combination, these methods aim to obscure and obfuscate intra and inter-service group communications.

VI. Conclusions and Future Work

Privacy in mission critical communication is crucial due to the involvement of sensitive information related to public safety, national security, and critical infrastructure. The significant role of network operators and application service providers necessitates rigorous privacy safeguards. This paper examines the privacy aspects of current MCC standards, analyzing architectural weaknesses that pose privacy threats to MC users, network entities, and MC servers. Additionally, we also anticipate potential privacy threats from emerging 6G technologies. Then, we suggest a suite of privacy controls to mitigate current and future threats, aiming to address next-generation privacy concerns in MCC. Looking ahead, we plan to delve deeper into protocol and interface-level threat analysis in the MCC architecture, with an aim for identifying and offering highly specific and detailed privacy-preserving solutions to safeguard this critical domain in 6G.

Acknowledgement

This work has been partly funded by the German Federal Office for Information Security (BSI) project 6G-ReS (grant no. 01MO23013D). The authors from Barkhausen Institut are also financed based on the budget passed by the Saxonian State Parliament in Germany.

References

[1] J. Li, K. K. Nagalapur, E. Stare, S. Dwivedi, S. A. Ashraf, P.-E. Eriksson, U. Engström, W.-H. Lee, and T. Lohmar, "5G new radio for public safety mission critical communications," *IEEE Communications Standards Magazine*, vol. 6, no. 4, pp. 48–55, 2022.

[2] A. U. Chaudhry and R. H. Hafez, "LMR and LTE for public safety in 700 mhz spectrum," *Wireless communications and mobile computing*, vol. 2019, pp. 1–17, 2019.

[3] S. W. Choi, Y.-S. Song, W.-Y. Shin, and J. Kim, "A feasibility study on mission-critical push-to-talk: Standards and implementation perspectives," *IEEE Communications Magazine*, vol. 57, no. 2, pp. 81–87, 2019.

[4] 3GPP, "Technical Specification Group Services and System Aspects; Common functional architecture to support mission critical services; Stage 2 (Release 19)," Tech. Rep. TS 23.280 V19.0.1 (2023-09), 2023.

[5] A. Koutsos, "The 5G-AKA authentication protocol privacy," in *Proc. of European symposium on security and privacy (EuroS&P)*. IEEE, 2019, pp. 464–479.

[6] P. Dass, S. Ujjwal, J. Novotny, Y. Zolotavkin, Z. Laaroussi, and S. Köpsell, "Addressing privacy concerns in joint communication and sensing for 6G networks: challenges and prospects," in *Proc. of 12th Annual Privacy Forum (APF), 2024, Karlstad, Sweden*. Springer Nature Switzerland, 2024, pp. 87–111.

[7] C. Brady and S. Roy, "Analysis of mission critical push-to-talk (mcptt) services over public safety networks," *IEEE Wireless Communications Letters*, vol. 9, no. 9, pp. 1462–1466, 2020.

[8] A. Sanchoyerto, R. Solozabal, B. Blanco, and F. Liberal, "Analysis of the impact of the evolution toward 5G architectures on mission critical push-to-talk services," *IEEE Access*, vol. 7, pp. 115 052–115 061, 2019.

[9] D. Borsatti, C. Grasselli, L. Spinacci, M. Sellembre, W. Cerroni, and F. Callegati, "Network slicing for mission critical communications," in *Proc. of 16th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*. IEEE, 2020, pp. 1–6.

[10] M. Mahyoub, A. AbdulGhaffar, E. Alalade, E. Ndubisi, and A. Matrawy, "Security analysis of critical 5G interfaces," *IEEE Communications Surveys & Tutorials*, 2024.

[11] M. Liyanage, J. Salo, A. Braeken, T. Kumar, S. Seneviratne, and M. Ylianttila, "5G privacy: Scenarios and solutions," in *Proc. of 5G World Forum (5GWF)*. IEEE, 2018, pp. 197–203.

[12] P. Schmitt and B. Raghavan, "Pretty good phone privacy," in *Proc. of 30th USENIX Security Symposium*, 2021, pp. 1737–1754.

[13] K. Sung, B. Levine, and M. Zheleva, "Zipphone: Protecting user location privacy from cellular service providers. arxiv 2020," *arXiv preprint arXiv:2002.04731*.

[14] 3GPP, "Technical Specification Group Services and System Aspects; Security architecture and procedures for 5G System; (Release 16)," Tech. Rep. TS 133 501 V16.7.1 (2021-08), 2021.

[15] 3GPP, "5G System (5GS) Location Services (LCS); Stage 2," Tech. Rep. TS 123 273 V16.4.0 (2020-07), 2020.

[16] 3GPP, "Technical Specification Group Services and System Aspects; System architecture for the 5G System (5GS); (Release 18)," Tech. Rep. TS 23.501 V18.4.0 (2023-12), 2023.

[17] 3GPP, "5G; NR; Radio Resource Control (RRC); Protocol specification; (Release 15)," Tech. Rep. TS 38.331 v15.4.0 (2019-04), 2023.

[18] M. Munakata, S. Schubert, and T. Ohba, "Guidelines for using the privacy mechanism for sip," Tech. Rep., 2010.

[19] R. Borgaonkar, L. Hirschi, S. Park, and A. Shaik, "New privacy threat on 3G, 4G, and upcoming 5G AKA protocols," *Cryptology ePrint Archive*, 2018.

[20] 3GPP, "Feasibility Study on Integrated Sensing and Communication (Release 19)," 3GPP, Tech. Rep. TR 22.837 V19.2.1, 2024.

[21] 3GPP, "Technical Specification Group Services and System Aspects; Security of the Mission Critical (MC) service; (Release 17)," Tech. Rep. TS 33.180 V17.9.0 (2023-03), 2023.

[22] R. Ostrovsky and W. E. Skeith III, "A survey of single-database private information retrieval: Techniques and applications," in *Proc. of International Workshop on Public Key Cryptography*. Springer, 2007, pp. 393–411.

[23] S. Pape, *Authentication in insecure environments: using visual cryptography and non-transferable credentials in practise*. Springer, 2014.

[24] R. Dingledine, N. Mathewson, P. F. Syverson *et al.*, "Tor: The second-generation onion router." in *Proc. of USENIX security symposium*, vol. 4, 2004, pp. 303–320.

[25] S. Goldwasser, Y. T. Kalai, and G. N. Rothblum, "One-time programs," in *Proc. of 28th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2008.*, 2008, pp. 39–56.

[26] J. A. Khan, "Role-based access control (RBAC) and attribute-based access control (ABAC)," in *Improving Security, Privacy, and Trust in Cloud Computing*. IGI Global, 2024, pp. 113–126.