Service-Level Threat Scenarios and Resilience Approaches in Private 5G Networks[*]

Seungjoon Na, Jinha Kim and Hwankuk Kim[†]

Kookmin University, Seoul, South Korea
{nsj43885, bradypus404, rinyfeel}@kookmin.ac.kr

Abstract

The 5G network, with ultra-high speed, low latency, and massive connectivity, supports diverse industrial services. Technologies such as network slicing and MEC-based IoT services have been introduced, but new threats have also emerged. Recent 5G security studies focus mainly on protocol-level analysis, with little attention to service-level attacks or resilience scenarios. This paper proposes attack and resilience scenarios for 5G-based services such as CCTV, video conferencing, and MEC-based IoT services. We analyze service-level threats and countermeasures, offering basic insights for 5G security research. The proposed scenarios and strategies can serve as a foundation for resilience-oriented security design.

Keywords: 5G Networks, Network Security, Resilience, Network Slicing

1 Introduction

The 5G network has evolved to provide ultra-high speed, low latency, and massive connectivity. To achieve this, technologies such as network slicing [1], large-scale IoT control, and Multi-access Edge Computing (MEC) [2] have been introduced. These technologies form the basis of various industrial services, including autonomous driving, smart factories, and healthcare. However, reports from ENISA [8] and NSA [9] indicate that these new technologies extend existing vulnerabilities in mobile networks and create new attack vectors. As the scope of 5G services expands, the potential impact of security incidents also increases, ranging from individual service disruption to wide-scale systemic risks. Despite this, recent 5G security research has mainly focused on threat analysis or protocol-level vulnerabilities, while studies on concrete service-level attack scenarios remain limited. Service-level attacks go beyond simple communication delays or data corruption [3]. In real-time industrial control systems or remote healthcare services, they can lead to safety incidents or threats to human life. Thus, attacks in the 5G environment have social and economic impacts beyond technical issues. To mitigate such risks, resilience measures are required [4]. Resilience refers to strategies that maintain service continuity and minimize impact even under attack. Therefore, this paper presents potential service-level attack scenarios and discusses resilience strategies to address them, complementing the limitations of prior research.

[*] Proceedings of the 9th International Conference on Mobile Internet Security (MobiSec'25), Article No. 43, December 16-18, 2025, Sapporo, Japan. © The copyright of this paper remains with the author(s).

[†] Corresponding author

2 Background and Related Works

2.1 5G Network Overview

The 5G network is an infrastructure that enables new service models across industries and society beyond simple speed improvements. Figure 1 shows how applications in factories, construction sites and airports achieve real-time data transmission and ultra-low latency communication through 5G. In each service domain many devices such as sensors, drones and robots connect to the network and generate large volumes of data. This data passes through the wireless segment to the core network. The 5G RAN supports three representative service models: eMBB (Enhanced Mobile Broadband), uRLLC (Ultra-Reliable Low-Latency Communication) and mMTC (massive Machine-Type Communication) [5]. These models meet the service requirements of different industries. The 5G core is designed on virtualization and cloud-native principles to deploy and scale network functions flexibly [5]. This architecture uses technologies such as network slicing to guarantee QoS required by industrial services [4].

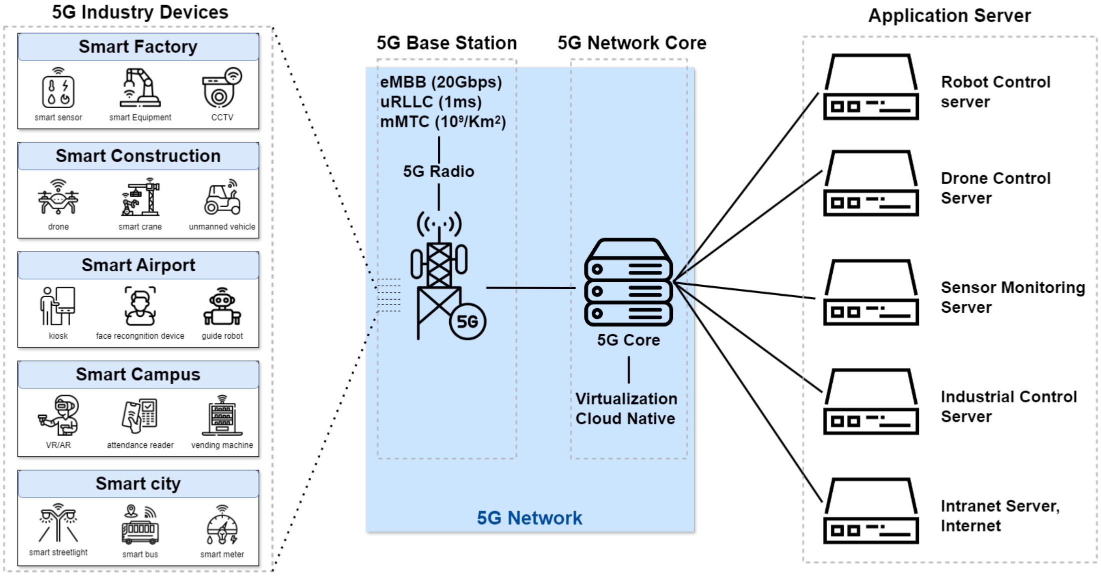

Figure 1: 5G Network Architecture and Industrial Use Cases

2.2 5G Network Architecture

The 5G network is built on a Service-Based Architecture (SBA). The core network consists of independent functions such as the Access and Mobility Management Function (AMF), Session Management Function (SMF), and User Plane Function (UPF) [5]. These functions interact through HTTP/2-based APIs [6]. The RAN, centered on the gNB, adopts a CU/DU split structure to meet high cell density and low latency requirements [7]. Interfaces N1, N2, and N3 are defined between the terminal and the core network, while the N6 interface connects the UPF to external data networks. Network slicing, based on the S-NSSAI parameter, provides virtual networks dedicated to specific terminals and services, ensuring QoS guarantees.

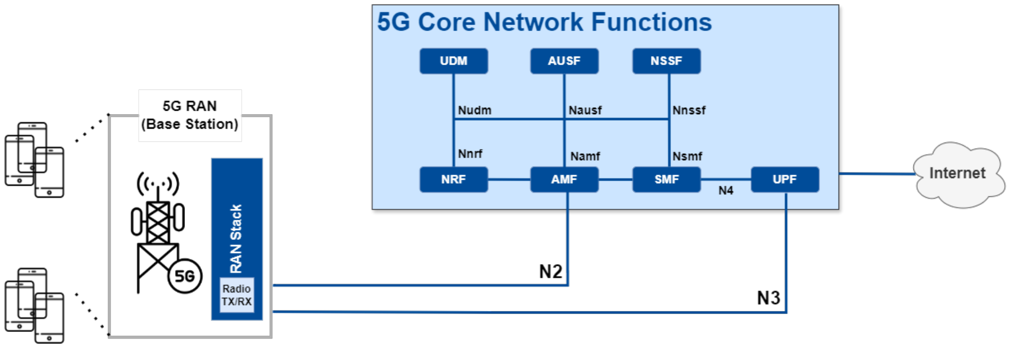

Figure 2: 5G Network Architecture

2.3 5G Security Challenges

The service-based architecture of 5G uses APIs for NF-to-NF communication, which increases application-layer threats such as authentication bypass and API abuse [8]. Distributed structures like MEC expand potential attack surfaces compared to centralized networks, raising the risk of edge-level intrusions [2]. Network slicing ensures QoS for each service, but isolation failures may lead to cross-slice attacks or unauthorized slice access. The rapid growth of IoT devices also drives large-scale DDoS and botnet traffic, causing network congestion and service disruption [10]. Public cloud adoption offers cost and scalability benefits, yet misconfigurations or account compromise can expose critical functions. These threats go beyond performance degradation and undermine both service stability and social trust.

2.4 Resilience in 5G Networks

The 5G network creates new opportunities through advanced architectures and service models, but it also introduces security threats that cannot be completely eliminated [8][9]. Due to diverse attack surfaces and unpredictable vulnerabilities, prevention-based security alone is insufficient to ensure service stability [10]. To address this limitation, the concept of resilience has emerged [11]. Resilience means maintaining service continuity and minimizing damage even under attack or failure. This involves strengthening slice-level isolation to prevent attack propagation, reallocating resources in real time to mitigate overload, and automatically adjusting security policies to adapt to evolving threats. In critical sectors such as remote healthcare and industrial control, where service disruption is fatal, resilience technologies serve as essential mechanisms to reduce social and economic damage.

2.5 Related works

Research on 5G network security has been conducted from multiple perspectives, including network architecture, protocol analysis, and AI-based threat detection. Foukas et al. [1] provided a comprehensive survey on network slicing, highlighting challenges in isolation, management, and orchestration that directly affect service reliability. Building on this, Khan et al. [10] and L. U. Khan et al. [11] discussed privacy and security issues in slicing and virtualization, emphasizing the risks of misconfiguration and inter-slice interference. In parallel, Ranaweera et al. [2][3] analyzed security vulnerabilities in MEC environments, identifying edge-level threats such as resource hijacking, unauthorized access, and VM compromise. Dutta and Hammad [4] proposed a system-level approach to 5G security, arguing that the complexity of 5G requires holistic strategies combining prevention, detection, and resilience. Machine learning techniques have also been explored to strengthen anomaly detection. Kaur et al. [12] reviewed AI-based traffic analysis methods such as CNNs, LSTMs, and Autoencoders, which can identify network anomalies in real time. Kukliński et al. [13] demonstrated the potential of NWDAF (Network Data Analytics Function) for intelligent monitoring of traffic and QoS metrics, suggesting a path toward autonomous network resilience. Service-specific studies have addressed vulnerabilities in real-world systems. Kalbo et al. [14] and Stabili et al. [15] revealed critical flaws in IP-based CCTV systems, including default credentials and weak input validation. Blancaflor et al. [18] examined RTSP streaming attacks on IP cameras, detailing their impact on service integrity. Similarly, Hasan and Hasan [19] analyzed weaknesses in WebRTC-based video conferencing systems, proposing threat models for DTLS and ICE mechanisms. For IoT environments, Andy et al. [20] identified authentication and authorization flaws in MQTT, while Ekoramaradhya and Thorpe [21] introduced a DevSecOps model to enhance MQTT-based security. These works show that many IoT services still rely on insecure defaults or inadequate policy enforcement, posing threats to service-level stability. Recent efforts have begun to address resilience as a complement to traditional security. Hakiri et al. [22] discussed mechanisms for secure and differentiated 5G operations, including redundancy, automated recovery, and slice-level isolation. Nevertheless, few studies provide integrated resilience procedures that connect detection with real-time mitigation at the service layer. Therefore, while prior research has addressed individual components—network slicing, MEC, or AI-driven detection—there remains a gap in service-level resilience modeling that connects these layers. The present work aims to bridge this gap by proposing explicit attack and resilience scenarios for real 5G-based services such as CCTV, video conferencing, and MEC IoT systems.

3 Derivation and Analysis of Attack Scenarios

3.1 Attack Scenario on CCTV Service

Scenario Preconditions

Three conditions must be met for an attacker to target a CCTV service. First, the attacker must obtain the IP address and port information of the CCTV server. Although such information is typically not exposed, it can be identified using network scanning tools such as Nmap. If a management portal or API endpoint is misconfigured and exposed to the internet, it may also allow access to internal resources [14]. Second, the attacker must have access rights to the eMBB slice. While unauthorized devices are unlikely to connect to slices in commercial networks, open-source tools such as Open5GS [16] and UERANSIM [17] enable connection in research environments. Thus, this scenario assumes that the attacker has already secured terminal access to the eMBB slice. Finally, the CCTV server must be using default accounts and passwords or lack proper input validation. Such vulnerabilities create realistic threats that allow attackers to bypass authentication [15].

Attack Procedure

The attack procedure against the CCTV service is divided into three phases: information gathering, access attempts, and attack execution. In the information gathering phase, the attacker performs port scanning within the slice to identify the IP address and ports of the CCTV server. This may reveal RTSP port 554 or web management ports 80 and 443. In the access attempt phase, if the CCTV management portal is exposed, the attacker may exploit default credentials or use SQL injection techniques to gain administrator privileges or bypass authentication [18]. In the attack execution phase, the attacker uses the obtained privileges to manipulate the system, such as deleting stored videos or uploading falsified footage. Since CCTV systems often retain default accounts or weak authentication mechanisms, such attacks are highly feasible in real-world environments. Figure 3 illustrates the step-by-step procedure of the attack.

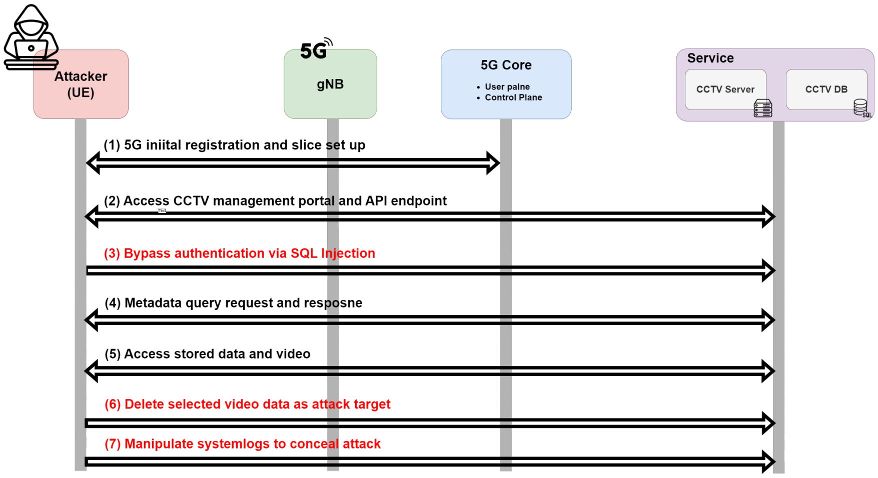
Attacker (UE)
5G
gNB
5G Core
User palne
Control Plane
Service
CCTV Server
CCTV DB
SQL
(1) 5G iniital registration and slice set up
(2) Access CCTV management portal and API endpoint
(3) Bypass authentication via SQL Injection
(4) Metadata query request and resposne
(5) Access stored data and video
(6) Delete selected video data as attack target
(7) Manipulate systemlogs to conceal attack

Figure 3: Attack Scenario on CCTV Service

The attacker first (1) registers a device in the 5G network and connects to the eMBB slice. Through this process, the attacker enters the network segment where the CCTV service operates and secures a position from which the portal and database can be accessed. Next, the attacker (2) accesses the CCTV management portal or API endpoint. If the management portal is exposed externally or within the slice, the attacker can view the login page like a normal user and secure an entry point to service management functions. The attacker then (3) bypasses authentication. The simplest method is to try default accounts and passwords. Furthermore, the attacker may exploit input validation vulnerabilities such as SQL injection to bypass authentication, thereby gaining access to CCTV video management privileges. After obtaining such privileges, the attacker (4) controls the management portal and database. At this stage, the attacker can access video metadata and execute system commands while imitating legitimate administrator actions. The attacker then (5) reviews stored data and videos, examining video files and metadata kept on the CCTV server to identify targets for deletion or manipulation. In the next step, the attacker (6) deletes video files, removing important footage using the acquired administrative rights. Finally, the attacker (7) deletes log records to conceal traces of the attack. Account takeover and manipulation attacks directly compromise the integrity and trustworthiness of CCTV services, unlike simple service delays or temporary failures. Considering that CCTV plays a role in public safety and criminal investigation, defense and response against such attacks are essential for stable service operation.

3.2 Attack Scenario on Video Conferencing Service

Scenario Preconditions

Three conditions must be met for an attacker to target a video conferencing service. First, the attacker must identify the server's IP address and port information. Ports commonly used for WebRTC signaling (443) and RTP/SRTP (UDP 10000–20000) may be exposed and can be discovered through network scanning tools [19]. Second, the attacker must obtain access rights to the eMBB slice. While unauthorized devices are restricted in commercial networks, open-source tools such as Open5GS and UERANSIM allow device connection in research environments. Thus, this scenario assumes the attacker has terminal access to the eMBB slice. Finally, the WebRTC stack or DTLS implementation on the video conferencing server must lack the latest security patches or have insufficient input validation, making it possible to process tampered handshake messages [19].

Attack Procedure

The attack procedure against the video conferencing service consists of three phases: information gathering, access attempt, and attack execution. In the information gathering phase, the attacker performs port scanning to identify the server's IP address and ports. During this process, DTLS port 443 and RTP/SRTP ports may be revealed, allowing the attacker to select targets for the attack. In the access attempt phase, the attacker initiates a WebRTC session request as if it were a legitimate device and secures a communication path with the server through ICE candidate exchange. In the execution phase, the attacker tampers with the Client_Hello message during the DTLS handshake and repeatedly transmits it, disrupting the server's session management logic [19]. This attack threatens both the integrity and availability of the video conferencing service and, under certain conditions (outdated DTLS libraries or weak security settings), may result in actual service disruption. Figure 4 illustrates the step-by-step process of the Client_Hello modification attack. The attacker first (1) registers a device in the 5G network and connects to the eMBB slice, thereby securing a network environment with access to the video conferencing server. Next, the attacker (2) requests WebRTC session creation and (3) establishes a connection path with the server through ICE candidate exchange. The attacker then (4) tampers with the Client_Hello message during the DTLS handshake.

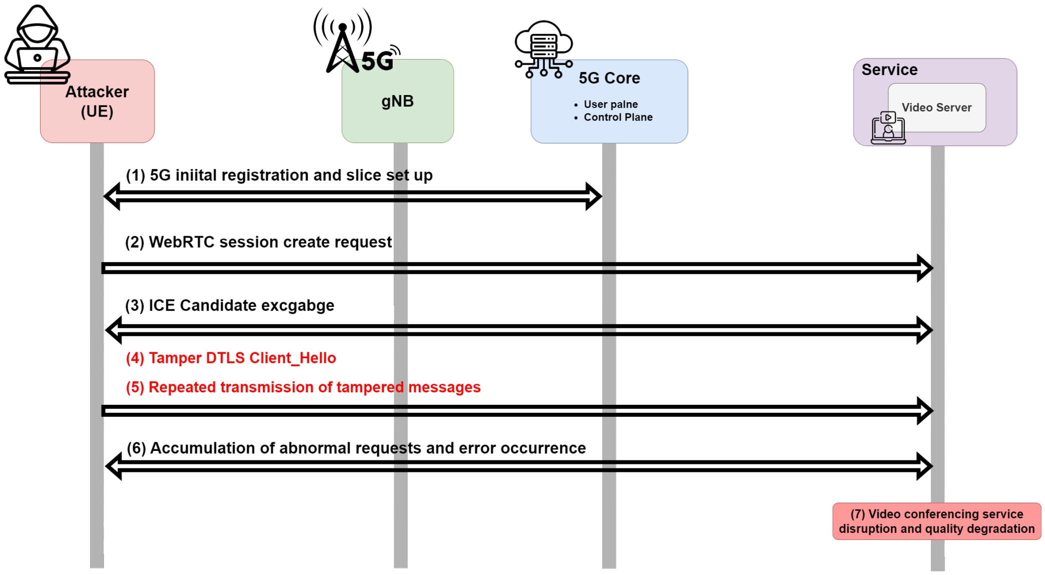
Attacker (UE)
5G
gNB
5G Core
• User palne
• Control Plane
Service
Video Server
(1) 5G iniital registration and slice set up
(2) WebRTC session create request
(3) ICE Candidate excgabge
(4) Tamper DTLS Client_Hello
(5) Repeated transmission of tampered messages
(6) Accumulation of abnormal requests and error occurrence
(7) Video conferencing service disruption and quality degradation

Figure 4: Attack Scenario on Video Conferencing Service

Message manipulation includes specifying unsupported algorithms in the cipher_suites field or abnormally altering the record_length value. The attacker (5) repeats this process to launch a DoS attack on the server. As a result, the application server (6) continuously processes abnormal requests, consuming resources until errors such as session conflicts or thread hangs occur, and (7) the video conferencing service suffers degraded quality or temporary disruption. Such data-tampering DoS attacks compromise the availability and stability of video conferencing services. In environments where real-time interaction is critical, such as remote collaboration or telemedicine, defense and response against these attacks are essential to ensure reliable service operation.

3.3 Attack Scenario on MEC-based IoT Service

Scenario Preconditions

Three conditions must be met for an attacker to target an MQTT broker. First, the attacker must identify the IP address and ports (1883, 8883) of the MQTT broker deployed in the MEC environment [20]. This can be achieved through port scanning or by probing misconfigured endpoints. Second, the attacker must obtain access rights to the mMTC slice. While unauthorized devices are restricted in commercial networks, open-source tools such as Open5GS and UERANSIM allow device connections in research environments. Thus, this scenario assumes the attacker has terminal access to the mMTC slice. Finally, the MQTT broker must have weak access control policies. In fact, many commercial services using MQTT have been compromised due to insufficient access control [21].

Attack Procedure

The attack against the MQTT broker consists of three phases: information gathering, access attempt, and attack execution. In the information gathering phase, the attacker conducts port scanning to detect the active ports of the MQTT broker. Ports 1883 or 8883 are identified, after which the attacker can attempt direct access. In the access attempt phase, the attacker exploits weaknesses in the broker's authentication. If default credentials are used or ACL (Access Control List) policies are poorly enforced, the attacker can obtain publisher or subscriber privileges without authorization [20][21]. In the execution phase, the attacker bypasses access control to subscribe to sensitive topics or publish malicious data, resulting in unauthorized subscription/publishing attacks. Such attacks are highly feasible in environments with weak access control. Figure 5 illustrates the step-by-step process of the unauthorized subscription/publishing attack.

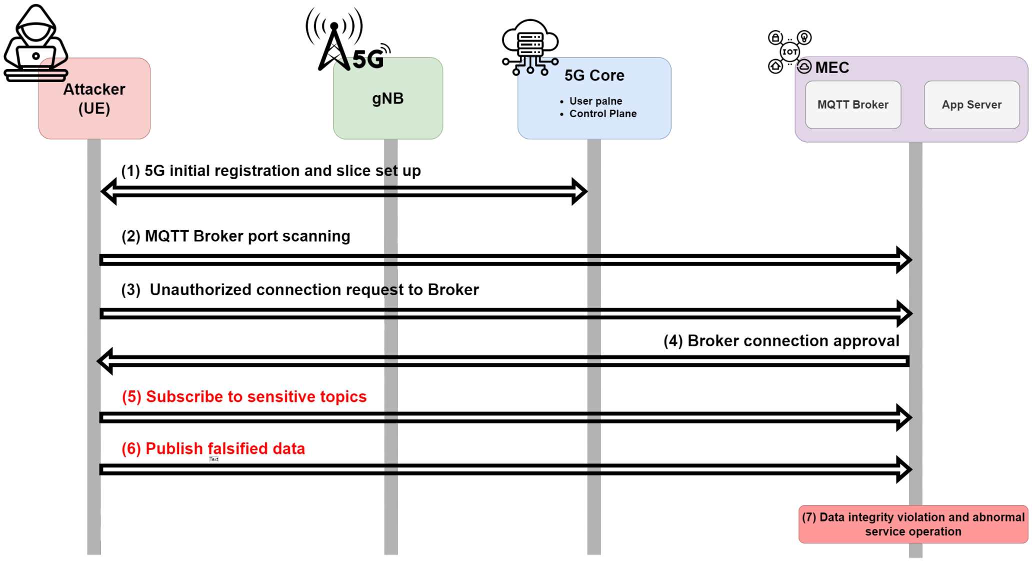
Attacker
(UE)
5G
gNB
5G Core
User palne
Control Plane
IOT
MEC
MQTT Broker
App Server
(1) 5G initial registration and slice set up
(2) MQTT Broker port scanning
(3) Unauthorized connection request to Broker
(4) Broker connection approval
(5) Subscribe to sensitive topics
(6) Publish falsified data
(7) Data integrity violation and abnormal service operation

Figure 5: Attack Scenario on MEC-based IoT Service

The attacker (1) registers a device in the 5G network and connects to the slice. Next, the attacker (2) sends a connection request to the MQTT broker and, if authentication is insufficient, (3) unlawfully acquires publisher or subscriber privileges. The attacker then (4) subscribes to sensitive topics (e.g., smart meter usage, sensor data) to steal information, and (5) publishes falsified data to deliver incorrect information to applications. Finally, (6) the falsified data directly impacts service operation, leading to abnormal behavior in industrial control systems or false positives/negatives in monitoring devices. Unauthorized subscription/publishing attacks undermine not only service continuity but also the fundamental data integrity of the entire MEC environment. If an attacker manipulates critical IoT service data, the consequences may include incorrect billing in smart meters, malfunctions in industrial control systems, and improper operation of medical devices. Therefore, this paper selects unauthorized subscription/publishing attacks on the MQTT broker as a representative scenario and, in Section 4, discusses resilience-based countermeasures against such threats.

4 Resilience Approaches in 5G Environments

4.1 Resilience Strategies

In 5G networks, security threats cannot be completely prevented. Thus, resilience is required to maintain service continuity even after an attack is detected [22]. While traditional security focuses on prevention, resilience emphasizes ensuring normal service operation despite ongoing attacks. This section explains three core mechanisms. First, session release terminates malicious sessions immediately to protect resources. Detection is carried out by the IDS in the UPF or by application security modules. When a detection event is reported, the AMF sends a PDU Session Release Command to the device, and the SMF instructs the UPF to release the N4 session [23]. This quickly blocks the attack session. Second, slice isolation prevents the attack from spreading to other slices. The UPF monitors traffic volume and resource usage per session, and if anomalies are detected, events are reported to the AMF and NSSF. The NSSF then places the affected device into the Rejected NSSAI list, and the AMF notifies the device. As a result, the device is denied reconnection to the slice [5]. Third, bandwidth and priority control resets QoS to guarantee stable resources for legitimate users. If a device consumes abnormal bandwidth, an event is reported, and the AMF and SMF perform the UE Context Modification procedure. Consequently, the gNB and UPF apply new QoS rules, limiting the malicious device to minimal bandwidth and low priority [5][23]. These three mechanisms can be applied to maintain service continuity even after an attack.

4.2 Resilience Scenario for CCTV Service

CCTV services, as noted in Section 3.1, face major threats from account takeover and database manipulation. When abnormal behavior is detected during the stage in which an attacker acquires administrator credentials or performs SQL injection, the response procedure begins with session release. (4) The detection system in front of the CCTV server identifies SQL injection patterns. (5) The detected event is transmitted through the security management system to the AMF. (6) Upon receiving the detection event, the AMF instructs the SMF to release the session using the PDUSession_ReleaseSMContext message [6][23]. (7) The SMF then sends an N4 Session Release Request to the UPF, deleting the user plane path, and (8) the device is forced to terminate the session through the PDU Session Release Command, a NAS message generated by the SMF and delivered by the AMF. (9) The AMF subsequently cooperates with the UDM to perform Nudm_UECM_Deregistration [24]. This invalidates the authentication information of the compromised account, and any NAS Registration Request using the same credentials is automatically rejected. This process not only blocks the device but also prevents the reuse of stolen credentials. As a result, the resilience scenario for CCTV services is designed to focus on account and privilege protection, ensuring that the same access path cannot be exploited repeatedly.

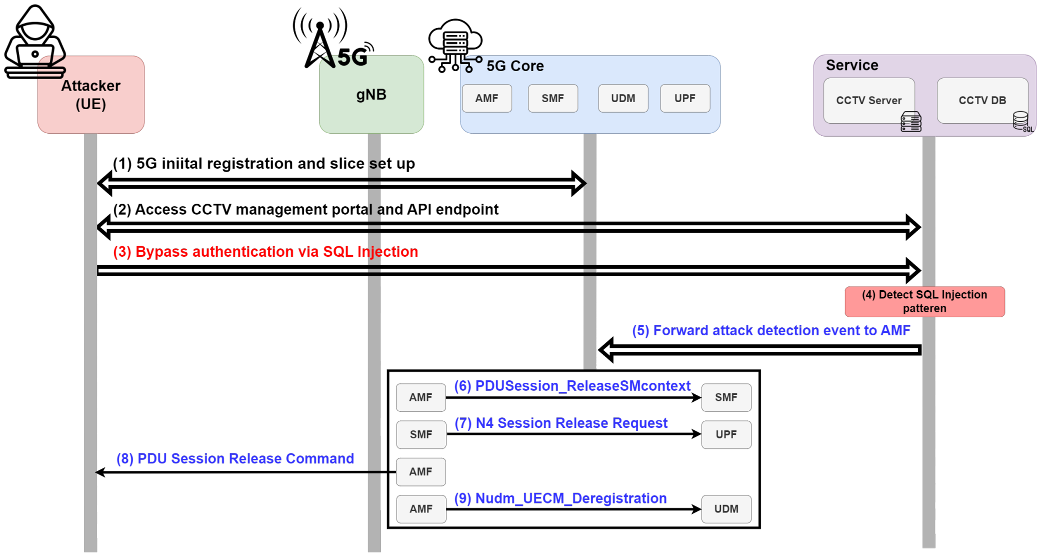
Attacker
(UE)
5G
gNB
5G Core
AMF
SMF
UDM
UPF
Service
CCTV Server
CCTV DB
SQL
(1) 5G iniital registration and slice set up
(2) Access CCTV management portal and API endpoint
(3) Bypass authentication via SQL Injection
(4) Detect SQL Injection patteren
(5) Forward attack detection event to AMF
AMF
(6) PDUSession_ReleaseSMcontext
SMF
SMF
(7) N4 Session Release Request
UPF
(8) PDU Session Release Command
AMF
AMF
(9) Nudm_UECM_Deregistration
UDM

Figure 6: Resilience Scenario for CCTV Service

4.3 Resilience Scenario for Video Conferencing Service

As discussed in Section 3.2, video conferencing services require real-time performance, making DoS-style session disruption attacks such as DTLS Client_Hello manipulation a major threat. When an attacker repeatedly sends tampered messages, the server consumes unnecessary session resources, leading to service delays and quality degradation. The response procedure to mitigate this threat begins with QoS control. (6) The detection system in front of the video server identifies DoS attack patterns. (7) The detected event is reported through the security management system to the AMF. (8) Upon receiving the detection event, the AMF initiates the UE Context Modification procedure and cooperates with the SMF to reconfigure QoS policies. During this process, new QoS flow rules are applied. (9) The UPF then enforces the updated QoS rules through N4 Session Modification [25]. (10) The AMF notifies the gNB of the revised QoS rules [5][23]. As a result, the attacking device is downgraded to minimal bandwidth and low priority, while legitimate devices retain their guaranteed QoS. This procedure maintains service continuity through QoS-based isolation rather than direct session termination. Consequently, video conferencing services can continue to support real-time applications such as emergency meetings, remote education, and telemedicine even during an attack.

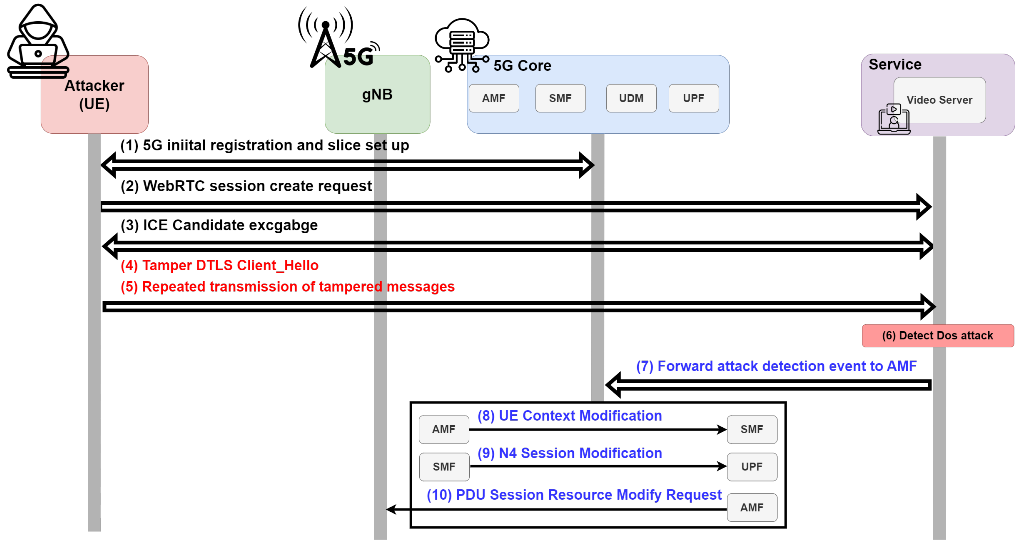
Attacker
(UE)
5G
gNB
5G Core
AMF
SMF
UDM
UPF
Service
Video Server
(1) 5G iniital registration and slice set up
(2) WebRTC session create request
(3) ICE Candidate excgabge
(4) Tamper DTLS Client_Hello
(5) Repeated transmission of tampered messages
(6) Detect Dos attack
(7) Forward attack detection event to AMF
AMF
(8) UE Context Modification
SMF
SMF
(9) N4 Session Modification
UPF
(10) PDU Session Resource Modify Request
AMF

Figure 7: Resilience for Video Conferencing Service

4.4 Resilience Scenario for MEC-based IoT Service

MEC-based IoT services, such as smart meters, rely on MQTT brokers that are vulnerable to unauthorized publishing attacks, as noted in Section 3.3. When abnormal patterns are detected at the stage where the attacker (5) subscribes to sensitive topics or (6) publishes falsified data, the response procedure begins with session release. (7) The detection system in front of the broker identifies the malicious activity. (8) The detected event is reported through the security management system to the AMF. (9) The AMF sends an Nsmf_PDUSession_ReleaseSMContext message to the SMF, instructing it to release the session [23]. (10) The SMF forwards an N4 Session Release Request to the UPF to release the user plane path [25]. (11) The SMF generates a PDU Session Release Command NAS message, which the AMF delivers to the device, forcing session termination. However, simple session release alone cannot prevent recurrence if the same device attempts to reconnect. In MQTT-based IoT environments, where the number of devices is massive, repeated access attempts from problematic devices pose a threat to stability. Therefore, recurrence prevention procedures are required after session release. (12) The UDM updates the device's slice subscription information based on operator policies, ensuring that the problematic device can no longer access the specified slice. (13) The AMF collaborates with the NSSF to perform slice re-evaluation, including the device in the Rejected NSSAI list [5]. This procedure blocks unauthorized publishing attempts by individual devices while allowing normal data transmission from other IoT devices to remain unaffected.

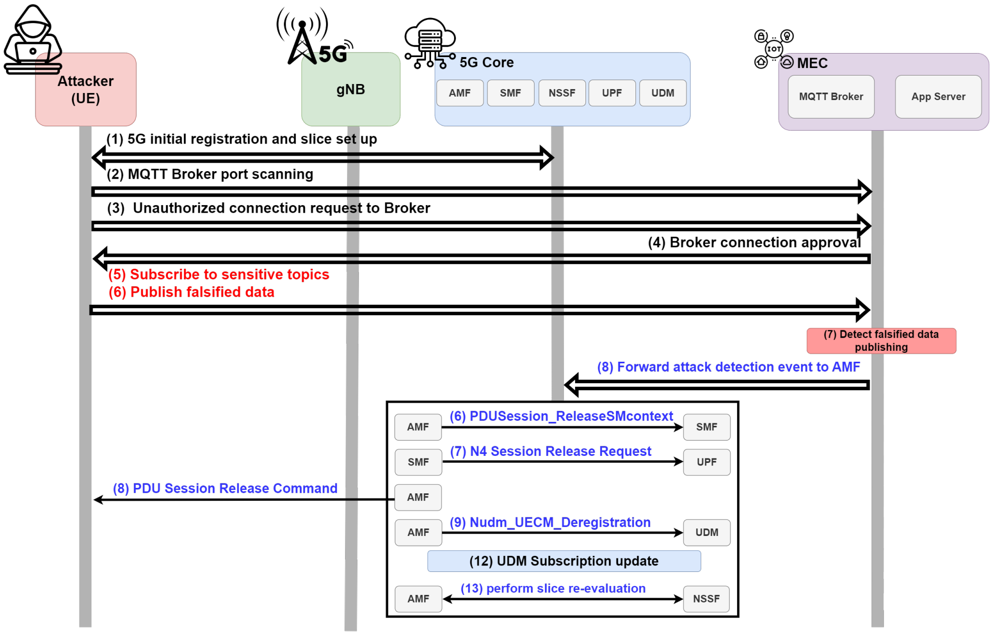
Attacker (UE)
5G
gNB
5G Core
AMF
SMF
NSSF
UPF
UDM
IOT
MEC
MQTT Broker
App Server
(1) 5G initial registration and slice set up
(2) MQTT Broker port scanning
(3) Unauthorized connection request to Broker
(4) Broker connection approval
(5) Subscribe to sensitive topics
(6) Publish falsified data
(7) Detect falsified data publishing
(8) Forward attack detection event to AMF
AMF
(6) PDUSession_ReleaseSMcontext
SMF
SMF
(7) N4 Session Release Request
UPF
(8) PDU Session Release Command
AMF
AMF
(9) Nudm_UECM_Deregistration
UDM
(12) UDM Subscription update
AMF
(13) perform slice re-evaluation
NSSF

Figure 8: Resilience Scenario for MEC-based IoT Service

5 Conclusion and Future Work

This paper modeled security threats that may arise in 5G-based service environments and proposed resilience procedures to counter them. CCTV, video conferencing, and MEC-based IoT services were selected as representative cases, and their attack procedures were described step by step. Response measures were then discussed using 3GPP-standard message flows. Three directions remain for future research. First, the proposed scenarios should be applied to a real testbed environment to verify their validity and effectiveness. This will confirm whether the results of this study can operate not only as theoretical models but also in actual network environments. Second, further work is needed to leverage 5G network data analytics functions such as NWDAF to implement automated detection and response systems. This would enable real-time analysis of traffic patterns and resource usage and trigger automated responses based on detection results. Third, quantitative evaluation of the proposed resilience procedures is required using metrics such as latency, service availability, and resource consumption. Such evaluation will contribute to numerically comparing and validating the impact of the proposed mechanisms on actual service quality (QoS).

Acknowledgement

This work was supported by an Institute of Information & Communications Technology Planning & Evaluation (IITP) grant funded by the Korean government (MSIT) (RS-2024-00438156, Development of security resilience technology based on network slicing services in a 5G specialized network).

References

[1] Foukas, X., Patounas, G., Elmokashfi, A., & Marina, M. K. (2017). *Network Slicing in 5G: Survey and Challenges*. *IEEE Communications Magazine*, 55(5), 94-100

[2] Ranaweera, P., Jurcut, A. D., & Liyanage, M. (2021). Survey on Multi-Access Edge Computing Security and Privacy. *IEEE Communications Surveys & Tutorials*, 23(2), 1078-1124

[3] Ranaweera, P., Jurcut, A., & Liyanage, M. (2021, October). MEC-enabled 5G Use Cases: A Survey on Security Vulnerabilities and Countermeasures. *ACM Computing Surveys (CSUR)*, 54(9), Article 186, 1-37

[4] Dutta, A., & Hammad, E. (2020, September). 5G Security Challenges and Opportunities: A System Approach. *2020 IEEE 3rd 5G World Forum (5GWF)*, Bangalore, India, 109–114. IEEE.

[5] 3GPP TS 23.501, *System Architecture for the 5G System (5GS)*.

[6] 3GPP TS 29.510, *5G System; Session Management Services.*

[7] 3GPP TS 38.401, *NG-RAN; Architecture description*.

[8] ENISA, *Threat Landscape for 5G Networks*, 2020.

[9] National Security Agency (NSA). (2022, December). *ESF: Potential Threats to 5G Network Slicing*. Enduring Security Framework (ESF) Report.

[10] R. Khan, P. Kumar, D. N. K. Jayakody, & M. Liyanage, *A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements, and Future Directions*, IEEE Communications Surveys & Tutorials

[11] L. U. Khan, I. Yaqoob, N. H. Tran, S. Pandey, M. A. Khan, and C. S. Hong, *Network Slicing: Recent Advances, Taxonomy, Requirements, and Open Research Challenges*, *IEEE Access*

[12] Kaur, J., Khan, M. A., Iftikhar, M., Imran, M., & Ul Haq, Q. E. (2021). *Machine Learning Techniques for 5G and Beyond.* IEEE Access.

[13] S. Kukliński et al., "Data Collection Using NWDAF Network Function in a 5G Core Network with Real Traffic," *ISNCC*, 2023.

[14] Kalbo, N., et al. (2020). *The Security of IP-Based Video Surveillance Systems.*

[15] Stabili, D., Bocchi, T., Valgimigli, F., & Marchetti, M. (2024). *Finding (and Exploiting) Vulnerabilities on IP Cameras: The Tenda CP3 Case Study.* In K. Minematsu & M. Mimura (Eds.), *Advances in Information and Computer Security. IWSEC 2024*

[16] Park, S. J. (2019). *Open5GS: Open Source Implementation of 5G Core Network.* Retrieved from https://github.com/open5gs/open5gs

[17] Ueransim Project. (2020). *UERANSIM: Open Source Implementation of 5G UE and RAN.* Retrieved from https://github.com/aligungr/UERANSIM

[18] Blancaflor, E., Ong, A. P., Navarro, A. L. E., Sudo, K. F., & Villaso, D. A. (2023). *Exploring the Attacks, Impacts, and Mitigations in a Real-Time Streaming Protocol Service of IP Cameras.* In *ICCTA '23: Proceedings of the 2023 9th International Conference on Computer Technology Applications* (pp. 201–205).

[19] Hasan, R., & Hasan, R. (2021). *Towards a Threat Model and Security Analysis of Video Conferencing Systems.* In *Proceedings of the 2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC)*

[20] Andy, S., Rahardjo, B., & Hanindhito, B. (2017). Attack scenarios and security analysis of MQTT communication protocol in IoT system. In 2017 4th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI), Yogyakarta, Indonesia, pp. 1–6

[21] Ekoramaradhya, M., & Thorpe, C. (2022). *Novel DevSecOps model for robust security in an MQTT internet of things.* In International Conference on Cyber Warfare and Security (ICCWS), Vol. 17, No. 1, pp. 63–71.

[22] Hakiri, A., et al. (2022). *Techniques for realizing secure, resilient and differentiated 5G operations.* In 2022 14th IFIP Wireless and Mobile Networking Conference (WMNC)

[23] 3GPP TS 23.502, Procedures for the 5G System (5GS).

[24] 3GPP TS 29.503, *5G System; Unified Data Management Services*.\

[25] 3GPP TS 29.244, *Interface between the Control Plane and the User Plane (N4)*.