Security Use-Cases for Countering Threats of CLA and UAV in 6G*

Kijung Bong†
ICT
University of Science & Technology
Korea
bkj8797@gmail.com

Jonghyun Kim*
Cyber Security Research Division
Electronics and Telecommunications Research Institute
Korea
jhk@etri.re.kr

ABSTRACT

Recently [1], 6G mobile communication technology has been actively researched and faces issues about security and privacy. The various technologies and applications to be used in 6G will bring new security issues. Among the technologies, CLA and UAV have a ripple effect that can cause severe damage to the entire network. In particular, in case of the UAV base station, there are various security points such as devices, software and communications to be considered. In this paper, the security use-cases and threats scenarios of both CLA and UAV in 6G environment are described. Initially, the major threats that can occur in each environment are described through system architecture and communication process. Afterwards, the security use-cases are described in consideration of the threats and characteristics of each environment respectively. Finally, the attacks and security use-cases of each environment are depicted as the respective scenarios.

CCS CONCEPTS

• **Security and privacy** → **Network security**; Mobile and wireless security

KEYWORDS

6G, Mobile Communication Security, 6G Security, CLA, UAV

1 INTRODUCTION

Fast and innovative changes have been made from first-generation (1G) mobile communication technology to current fifth-generation (5G) mobile communication technology. Currently, research and standardization work for high-quality 5G technology are being actively conducted. Meanwhile, 6G mobile communication technology research is also being conducted in Korea, Europe, Finland, United States, and Japan. In 6G, new technologies and applications that did not exist and not used before will be implemented for a higher level of user experience beyond 5G.

However, new security and privacy issues emerge accordingly. For example, CLA (Closed Loop Automation) will be used as a core function of Network Management Automation solution in 6G. If a security threats is posed to CLA, it can cause severe damage to the availability of the entire network. Furthermore, flying base station using UAV (Unmanned Aerial Vehicle) will be implemented in 6G. It means that physical security, drone communication security, base station communication security, etc. should be considered.

Not only security issues in CLA and UAV, there are various security issues to be considered in other technologies used in 6G environments. The paper focuses on CLA and UAV, which may incur severe risks among 6G technologies, and presents potential security threats, security use-cases and scenarios in CLA and UAV environments.

In Section 1, the trends and security considerations of 6G mobile communication technologies are briefly described. In Section 2, the related standards and papers are introduced. In Section 3, the security threats of CLA and UAV in 6G environments are described. In Section 4, the security use-cases for countering the threats dealt with in Section 3 are described. In Section 5, the attacks and security use-cases scenarios of CLA and UAV in 6G environments are described. Finally, the paper concludes in the final section.

2 RELATED WORKS

Use-cases and capability of UAV are introduced in 3GPP [1]. Pre-conditions, post-conditions and service flows of each use-cases are described. Especially, some cases deal with the detailed values related to KPIs.

UAV Systems connectivity, Identification and Tracking processes are introduced by 3GPP [2]. Initially, the standard defines a mechanism that tracks and identifies a UAV/UAV-C. Afterwards, authorization/authentication process is described. Especially, communication procedures in EPS and 5GS environments are described.

ACM ICEA '21, December 28–29, 2021, Jinan, China

ACM ISBN 978-1-4503-9160-3/21/12..$15.00
https://doi.org/10.1145/3491396.3506556

UAS (Unmanned Aerial System) service and architectural key issues/solutions over 3GPP systems are introduced by 3GPP [3]. Initially, the standard defines architectural requirements for an efficient UAS system. Afterwards, overall evaluation of key issues and solutions is done. Especially, various communications on the UAV(UAS) system are described.

C. Benzaid, et al. [4], introduces potential threats and security measures in ZSM (Zero touch network and Service Management). In the paper, the ZSM attack surfaces such as Open API, CLA, Intent-Based Interfaces are defined. Moreover, attack scenarios and applicable mitigation mechanisms in such environment are proposed.

CLA based on the ZSM architectural framework are introduced by ETSI [5]. Initially, the standard introduces CL within the ZSM framework, from both functional and deployment perspectives and specifies Closed Loop-specific requirements. Afterwards, the standard deals with the details of closed-loop automation enablers and specification of management service relevant to closed loops.

Security guidelines of 5G communication system are introduced in ITU-T [6]. In the standard, potential threats and security capabilities for each domain in 5G systems are described. Especially, the detailed attack scenarios and security use-cases for specific threat are depicted in the appendix.

M. Mozaffari, et al. [7], introduces key barriers, consideration and potential solutions of commercial usage of UAV. Moreover, measures for enhancing capabilities of UAV in cellular network, such as RS-based handover are described. Finally, various considerations and communications (e.g., A2G communication) in beyond low-altitude UAV environment is described.

P. Porambage, et al. [8] introduces security and privacy to be considered in 6G environment. Security attacks and possible defense mechanisms on applications and domain in 6G environment are described. Especially, security challenges and security measures of CLA and UAV are included. Besides, standardization and project across the world are introduced.

V. -L. Nguyen, et al. [9] also introduces security and privacy to be considered in 6G environment. In particular, domains of the 6G environment were classified by layer and security and privacy issues are described. Moreover, the attack scenarios and security use-cases are described for some threats.

3 SECURITY THREATS

3.1 Security Threats of CLA in 6G

The clause 3.1 deals with the potential security threats to be considered in the CLA environment. The CLA architecture in 6G environments are described in clause 3.1.1 below. In addition, the components and overall procedure of the CLA architecture are presented. Security threats in the CLA architecture are described in clause 3.1.2 below.

3.1.1 Overview of CLA Architecture in 6G. CLA is one of the fundamental technologies for the network management automation solutions. CLA performs network monitoring and maintenance through the overall procedure; Data Collection, Analysis, Decision, Execution. In addition, it performs network self-optimizing through the communication cycling. It evaluates the real-time network status, traffics and resource availability without the operator's manual work, and conducts optimal measures accordingly. In 6G environments, the real-time monitoring and optimization measures for the ultra-large traffics are needed. Furthermore, the real-time response to failures of the infrastructure resources is also needed. For this reason, in 6G, the CLA-based network management automation solutions are expected to be applied for the network management on RAN, Core Network. ETSI ZSM (Zero touch network and Service Management) is a representative model of the network management automation solutions based on the CLA[4][5]. The overall framework of ZSM is depicted in Fig. 1.

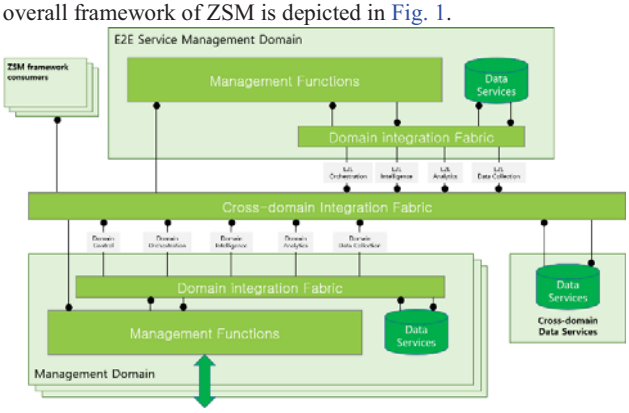

Figure 1: ETSI - ZSM(Zero touch network and Service Management) Framework [4][5]

There are four main stages in the Closed Loop of ZSM[5]. In the **Monitoring stage**, data is transmitted in a form that can be stored and analyzed from one or more sources. In the **Analysis stage**, the insights are derived based on data, and the cause of the event is analyzed. In the **Decision stage**, it is determined what action to take on the issues detected in the analysis stage. In the **Execution stage**, the workflows determined in the decision stage for the managed entity are executed. Importantly, each stage is an abstract stage, so one process may proceed in several steps, or more than one process may be combined. There are the detailed domains involved in each process, and the closed loop automation is implemented by the mutual communication between them.

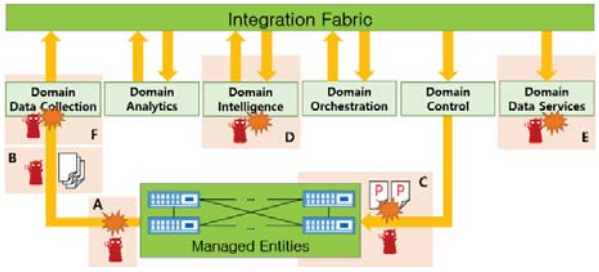

Figure 2: Security Threats on CLA Architecture [4]

3.1.2 Security Threats in CLA Architecture. The potential security threats in the CLA environment are as follows (the CLA model is based on ETSI ZSM framework). Fig. 2 shows the security threats in CLA architecture.

First, the Man-in-the-Middle attack can occur during the communication between domains. For example, there are packet eavesdropping/modification and dropping threats by attackers. The attackers obtain the entity information or the network information by eavesdropping on transmitted messages. Moreover, the attackers manipulate them to change or hide the notifications and the attribute values for a specific event. The threat corresponds to A in Fig. 2.

In addition, the packet crafting and fake notification attacks can occur by fake entity. Due to the nature of a closed loop with continuous feedback, it can degrade the QoS of the entire network. Also, large amounts of data can be injected into the loop, resulting in denial of service. The threat corresponds to B in Fig. 2.

Finally, in the closed loop coordination environment, the conflict of CL instances and the QoS degradation can occur due to the priority issue of CLs and the replay attacks. For example, the attacker can cause a collision between CLIs (Closed Loop Instances) by manipulating their priorities. Furthermore, the network is not optimized by replaying the actions transmitted to the managed entity, which can lead to QoS degradation of the entire network. The threat corresponds to C in Fig. 2.

Besides, the following major threats exist; threats on AI/ML model inside the closed loops, threats on the closed loop data storages and DoS/DDoS to specific entities. The threats correspond to D~F in Fig. 2.

3.2 Security Threats of UAV in 6G

The clause 3.2 deals with the potential security threats to be considered in the UAV environment. The UAV system in 6G environments is briefly described in clause 2.2.1 below. In addition, the components of UAV system are presented. The security threats in the UAV base station system are described in clause 2.2.2 below.

3.2.1 Overview of the UAV System. In 6G, the UAV System is expected to be used as a base station. The UAV System is an unmanned aerial vehicle system such as a drone. It includes the UAS that manages the UAV/UAV-Controller and the USS (UAV Service Supplier)/UTM (UAV Traffic Management) that manage the UAS. Additionally, entities and functions such as the UAE (UAS Application Enabler), the UCF (UAV Control Function), the SEAL (Service Enabler Architecture Layer), etc. are included. Fig. 3 briefly shows the overall architecture of the UAV(UAS) model in 3GPP System[3].

In 6G, the UAV system will be used as a base station in the form of placing base station hardware on the UAV or adding software function. As the moving base station is realized, it can be particularly used in the specific situations or areas. For example, it can be used in the areas that traffic is rapidly increasing (e.g., the sports stadiums where games are held) or the areas that are not serviceable (e.g., the disaster areas).

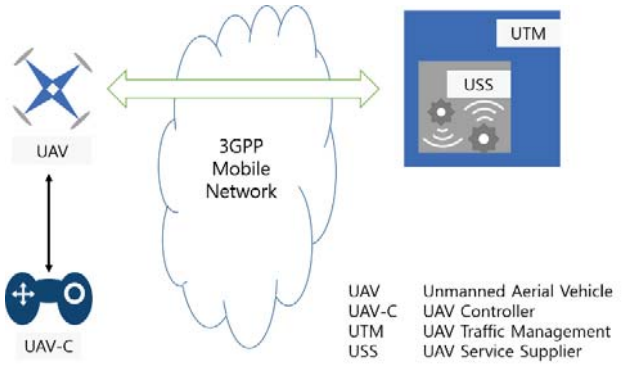

Figure 3: The UAV(UAS) Model in 3GPP System[3]

3.2.2 Security Threats in the UAV System. Threats can occur in various scenarios and environments such as the UAV devices, the UAS communication and the authentication/authorization processes. Fig. 4 shows one scenario of them, the reporting of UAV events process. The major threats in the UAV System are as follow.

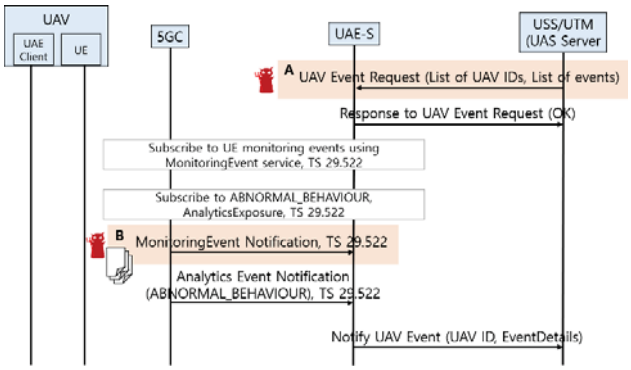

Figure 4: Security Threats of UAV System (example: reporting of UAV events process) [3]

First, the Man-in-the-Middle attack can occur in the process of exchanging information between the UAV/UAS and the USS/UTM. The attacker can eavesdrop on communication between the UAV/UAS and the USS/UTM, modify or drop messages. In particular, the communication may include critical information such as a UAV ID, a UAS ID, a Remote ID and a plurality of UE IMSIs. The threat corresponds to A in Fig. 4.

In addition, the notification/request/response message snipping attack and the fake message transmission attack can occur. Transmitting fake messages can severely affect to the UAV mobility and communication. Above all, transmitting a large number of messages can cause DoS/DDoS attacks and serious damage to the networks. The threat corresponds to B in Fig. 4.

Besides, the following major threats exist; eavesdropping or skipping the authentication/authorization process, takeover the UAV controller during UAV/UAV-C switching, and obtaining the UE information in the cell stored in the UAV device.

4 SECURITY USE-CASES

4.1 Security Use-cases of CLA in 6G

In clause 3.1, potential security threats of CLA to be considered in 6G environments are described. With regards to security threats, the core security use-cases that should be considered in the CLA environment are as follows.

Integrity of data and mutual authentication between entities. The encrypted communication, the integrity checks of data and the authentication of source must be guaranteed. Especially, PKI (Public Key Infrastructure) can be applied. In PKI, communication between entities is proved using the issued certificate. The CA (Certificate Authority) which issues certificates, is able to located in the uppermost network that manages CLIs.

AI/ML model security. Security measures countering the data poisoning and evasion attack should be applied to AI/ML models inside the CLA. In particular, the sufficient adversarial training should be performed at the training process.

DoS/DDoS detection and protection on domain and managed entities. Each domain should configure a white list-based network to receive data only through the fabric or managed entities. The list of allowed sources depends on the network topology and operator's judgement. Moreover, additional DoS/DDoS protection solutions should be applied to each managed entities and Domain Data Collection, since they are vulnerable due to the various data sources. For example, a method of installing an API gateway or setting a traffic threshold can be applied.

Replay protection. A timestamp or sequence number must be attached to the packets delivered to Domain Data Collection and delivered from Domain Control.

Access control of storage. Access control should be applied to the objects accessing storages, such as the management domain storage and the cross-domain storage. The Authentication/ authorization of the objects is essential, especially the authorization through a Role-based Access Control (RBAC) for the authenticated objects.

Redundancy. In Preparation for the packet dropping/ modification attacks and the line failure, a redundant structure should be applied. Especially, a redundancy of the link related to the Domain Data Collection and the Domain Control is essential. It can be not only a security measure for the technical attack, the system failure and the human error, but also works the load balancing.

4.2 Security Use-Cases of UAV in 6G

In clause 3.2, potential security threats of the UAV in 6G environments are described. With regards to the security threats, the core security use-cases that should be considered in the UAV environment are as follows.

Authentication of between UAS and USS/UTM. Kerberos authentication protocol can be used for the UAV/UAS proof in the USS/UTM. It can operate by deploying AS (Authentication Server) and TGS (Ticket Granting Service) in the core network, and issuing a TGT (Ticket Granting Ticket) to the UAV/UAS/UAE-client. The ticket validity period is as valid as the running time of the drone (related to the battery). Also, it must expire if the UAV is out of a specific range (e.g., a UTM scope, a Macro cell). As one of the representative security use-cases for the UAV system, Kerberos can be considered.

Confidentiality of identifiers and integrity of control messages. The lightweight encryption technology is essential on UAV since the UAV performs not only UAS system communication but also base station functions in 6G environment. Lightweight cryptography such as LEA (Lightweight Encryption Algorithm) and HIGHT (High Security and Light Weight) can be applied. Applying encryption to all data may be a burden on the UAV system. Therefore, a method of encrypting only the identifiers such as UAV ID and UAS ID should be considered. Moreover, modifications to UAV control-related communication (e.g., C2 Communication) can lead to a severe risk. For the reason, the integrity check of the control messages should be conducted. Integrity check can be implemented by applying MAC (Message Authentication Code) using the built-in key distributed in advanced.

Physical security of UAV storage system. In preparation for the UAV theft, the key hiding and protection techniques should be applied. Especially, the security for the side-channel attack is essential. The side-channel attacks such as spectre and rambleeds can occur, and the security measures such as OpenSSH can be applied. Also, the protection of critical data in the UAV device, such as UE information and IDs, should be considered.

DoS/DDoS detection and protection on UAS system. For the UAS system, a network should be configured based on a white list. The UAV system should only allow the communications with the USS/UTM, SEAL, etc. Information updating about the new UAS systems or the network-related changes can be conducted by receiving updated rules from the USS/UTM.

5 SCENARIOS OF SECURITY USE-CASES

The section 5 depicts scenarios according to the security threats and security use cases dealt with above. Use-cases scenarios in the CLA environment are described in clause 5.1 below. The security use-cases scenarios in the UAV environment are described in clause 5.2 below.

5.1 CLs Conflict Attack in Closed Loop Coordination Environments

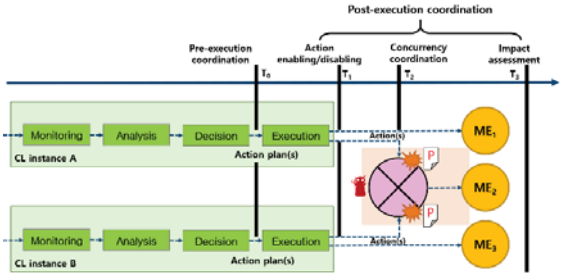

Figure 5: Scenario of CLs Conflict Attack [5]

Overview. Fig. 5 is a diagram showing the conflict attack between the CLs that can occur in a CLC (closed loop coordination) environment. In CLA environment, when an event occurs in the managed entities (such as VNFs), the appropriate action for the event is executed. The CLC refers to a multi-CLs environment and it may cause a conflict between the CLs when different actions are performed on the same managed entity. To prevent this, there is a priority-related attribute. However, by changing the value of the corresponding attribute, a conflict between the CLs can be caused.

Attack scenario. For the events occurring on the managed entities, messages for recovery are sent to the Domain Data Collection. After the analysis and decision stage for the corresponding message, action plans and the conflict detection are conducted during the pre-execution coordination process. After that, the CL instance that can execute the action on the same managed entity is determined using the value of the closedLoopPriority attribute. The attacker modifies the value of the closedLoopPriority delivered in the process, resulting in a conflict between the CLs. As a prerequisite for the attack, a specific managed entity malfunctions or fails. This may be unintended or caused by the attacker.

Consequence. The recovery of the managed entity that are malfunctioning is not properly taken due to the conflict between them. This leads to the QoS degradation or denial of service for the managed entity.

Security Use-cases. The requests transmitted from the Fabric the action execution process in managed entity, encrypting communication or integrity checks should be applied. In particular, encrypted communication using TLS/SSL and IPSec should be applied to the communication between Fabric, Domain Control, shared managed entity, and managed entity. Additionally, the MAC-based message integrity check can be applied between each entity to prove that the attribute or action message has not changed.

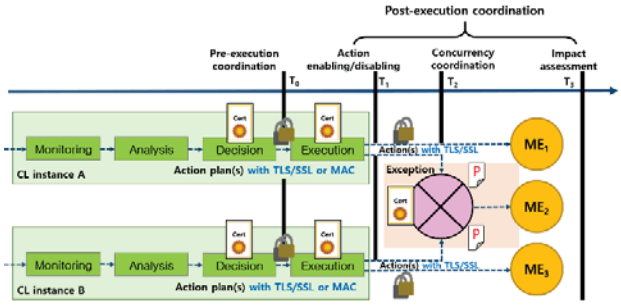

Figure 6: Security Use-cases of CLs Conflict Attack [5]

As a simple method, an exception handling can be applied in the case of a priority conflict. It can be implemented simply by configuring the static CL to be executed in the event of a priority conflict. As one of the representative security use-cases for CLA architecture, the PKI can be considered. The certificate can be used for the communication between the Domain and entities by deploying the CA on the uppermost network and issues the certificate. The security use-cases described above are depicted in Fig. 6.

5.2 Eavesdropping Attack in Network-assisted Positioning Provision to USS/UTM Process

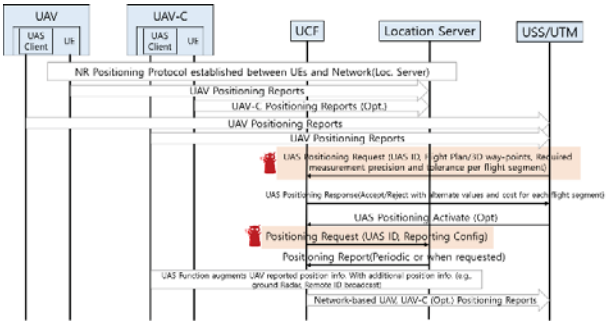

Figure 7: Scenario of Eavesdropping attack [3]

Overview. Fig. 7 is a diagram showing the eavesdropping attack that can occur during the network-assisted positioning provision to the USS/UTM process. In order to know the exact position of the UAV(UE), the USS/UTM uses the various types of UAV positioning information. In the process, positioning information of a specific UAV is exchanged between the UCF and USS/UTM, and the attackers can steal critical information exposed in the process.

Attack scenario. The connection between the UAV/UAV-C and LMS (Location Management Service) is established and the UAV/UAV-C transmits positioning reports to the LMS. In addition, the UAV/UAV-C also transmits reports to the USS/UTM. The USS/UTM combines positioning information transmitted directly from a UAV with 3GPP positioning information transmitted to the LMS. At this time, the positioning information is checked and enhanced using the UCF and information such as UAS ID and Flight Plan/3D way-points is exposed in the process. The attacker can obtain a UAS ID through the information and specify a UAS corresponding to the ID.

Consequence. The attacker can perform various authentication/ authorization by using the obtained UAS ID and location information of the corresponding UAS. For example, grouping or C2 Communication Cancellation between the UAV and UAV-C are possible, which can lead to various threats by a fake UAS.

Security Use-cases. First, a mutual authentication process between the UCF/LMS and USS/UTM is required before the UAV Positioning Request/Response process. It can be implemented through the mTLS-based mutual authentication and encrypted communication. However, when implementing a UAV system in the real environment, there may be issues such as lightweighting or the latency depending on the environment. Accordingly, a method of applying encryption only to the critical information (e.g., UAS ID) can be applied.

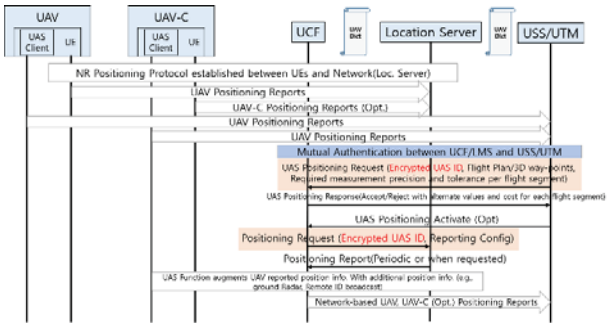

Figure 8: Security Use-cases of Eavesdropping Attack [3]

In addition, the temporary identifier, not sensitive IDs, can be used for the information exchange except for the authentication/ authorization process. There is a method of assigning a one-time identifier based on channel information when the UAV was activated. It can be used only for one life cycle of the UAS. In addition, there is a method of using a dictionary for the UAV located in a specific cell or scope. The USS/UTM and UCF/LMS have the same UAV dictionary and can communicate using an index mapped to the UAV ID. The security use-cases described above are depicted in Fig. 8.

6 CONCLUSIONS

6G research work is underway following 5G/B5G and the various technologies and security measures to be used in 6G environments are being discussed. This paper described the security use-cases for Closed Loop Automation and UAV base station that are predicted to have high risks or vulnerabilities among the technologies to be used in 6G environments. In the CLA environment, the mutual authentication between domain and infrastructure resource, the anomaly input data injection to closed loop and the conflict between CLs are introduced as the major security issues. In addition, the various and detailed security use-cases are described and a method of applying PKI is presented as one of the representative security scenarios. In the UAV environment, the eavesdropping on communication, the mutual authentication between UAV/UAS and USS/UTM, and the IDs exposed on communication are introduced as the major security issues. In addition, the various and detailed security use-cases are described and a method of applying Kerberos protocol is presented as one of the representative security scenarios. In relation to this research, the evaluation of vulnerability is able to be conducted in CLA and UAV environmental testbeds. In addition to CLA and UAV dealt with in this paper, the threats and security measures of the other 6G technologies should also be studied in the future.

ACKNOWLEDGMENTS

This work was supported by Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government (MSIT) (No.2021-0-00796, Research on Foundational Technologies for 6G Autonomous Security-by-Design to Guarantee Constant Quality of Security)

REFERENCES

[1] 3GPP. 2019. Technical Specification Group Services and System Aspects; Enhancement for Unmanned Aerial Vehicles; Stage 1. TR 22.829.
[2] 3GPP. 2021. Study on supporting Unmanned Aerial Systems (UAS) connectivity, Identification and tracking. TR 23.754.
[3] 3GPP. 2021. Study on application layer support for Unmanned Aerial Systems (UAS). TR 23.755.
[4] C. Benzaid and T. Taleb. 2020. ZSM Security: Threat Surface and Best Practices. IEEE Network Magazine, volume 34, pages 124-133. https://doi.org/10.1109/MNET.001.1900273
[5] ETSI. 2021. Zero-touch network and Service Management (ZSM); Closed-Loop Automation; Part 1: Enablers. GS ZSM 009-1.
[6] ITU-T SG 17. 2021. 4th Revised baseline text for X.5Gsec-guide: Security guidelines for 5G communication system. Study Period 2017. Contribution 1133
[7] M. Mozaffari, X. Lin, and S. Hayes. 2021. Towards 6G with connected sky: UAVs and beyond. arXiv:2103.01143. [Online]. https://arxiv.org/abs/2103.01143.
[8] P. Porambage, G. Gür, D.P.M. Osorio, M. Liyanage, A. Gurtov, M. Ylianttila. 2021. The roadmap to 6G security and privacy, IEEE Open J. Commun. Soc. https://doi.org/10.1109/OJCOMS.2021.3078081
[9] V. -L. Nguyen, P. -C. Lin, B. -C. Cheng, R. -H. Hwang and Y. -D. Lin. 2021. Security and privacy for 6G: A survey on prospective technologies and challenges, IEEE Communications Survey&Tutorials. https://doi.org/10.1109/COMST.2021.3108618