Security Threats and Cellular Network Procedures for Unmanned Aircraft Systems: Challenges and Opportunities

Aly Sabri Abdalla and Vuk Marojevic

Abstract

Researchers and standardization bodies have raised concerns about using legacy cellular networks for supporting unmanned aerial vehicle (UAV) operations. Different from traditional user equipment (UE), an unmanned aircraft system (UAS)-capable UE — UAV-UE or controller-UE — needs additional network security measures to ensure safe airspace operation. This article introduces the security requirements and threats with respect to three major themes: authentication and authorization, location information veracity and tracking, and command and control signaling. We present the 3GPP reference architecture for network connected UASs, the new application functions of the 5G core network, and the 5G security mechanisms and procedures for meeting the established requirements. Three 5G core application functions supporting UASs facilitate the interworking between the 3GPP network and the UAS traffic management, delivering location reports, validating UAS subscriptions, and matching UAS IDs with their respective UE IDs, among others. We identify opportunities for UAS network security research and recommend critical security features and processes to be considered for standardization. We conclude that while the 5G standard introduces important security mechanisms, more security research and benchmarking are needed for cellular networks to support secure and scalable real-time control of UAVs and the emerging applications enabled by them.

Introduction

The unmanned aircraft system (UAS) technology development and market penetration has led to research and development on cellular connected unmanned aerial vehicles (UAVs). UAVs are considered as future cellular network users for receiving command and control (C2) and other services. They may also provide network support to extend coverage, increase capacity, or enhance security of 4G, 5G, and future 6G networks [1].

A UAS consists of a UAV and its controller (UAV-C). Secure communications and networking is critical for safe UAV operation. This includes the confidentiality protection of identifiers (IDs), spoofing immunity, and various levels for the integrity and privacy preservation of UAS control and data links [2]. UAS researchers have started to investigate cyber threats and vulnerabilities of cellular connected UAS nodes. For example, [3] and Alladi *et al.* [4] propose a physically unclonable function scheme for lightweight mutual authentication between UAVs and the 5G base station with unique and secure session keys for each session. Bansal *et al.* [5] develop a scalable authentication protocol using *K*-means clustering. Li *et al.* [6] present an elliptic curve cryptography authentication scheme to preserve the ID and authenticate the UAV and ground base station with low computational cost.

The threat model has shifted since sophisticated software radio hardware and software became widely available. Targeted wireless attacks to cellular networks, such as eavesdropping, jamming, and spoofing of control and data channels, can be implemented with open source software and commercial off-the-shelf hardware investments [7]. Recent experiences have shown that many UAS nodes and their communications systems are insecure, and that communications can be interrupted and intercepted, and nodes hijacked by means of software and radio signaling [8, 9] It has been reported that a 4G- enabled telemetry device mounted on an existing UAS is vulnerable to different types of attacks [10]. Information can be captured, modified, or injected, giving hackers complete control over the UAV [11]. Attackers can also force the deauthentication of UAS nodes and lure them to authenticate with fake systems [12].

Various standards committees have raised concerns about the security of cellular connected UAVs. One of these is the P1945 group of the IEEE Standards Association that defines the framework for structuring the low altitude airspace for UAV operations. One of its working groups is dedicated to the identification and authentication of UAS nodes. The Third Generation Partnership Project (3GPP) Technical Report (TR) 33.854, version 17.1.0, studies the security aspects of network-connected UAVs to identify key issues and solutions.

In light of rising security challenges of network-connected UASs, we identify three core security themes, present the UAS security mechanisms of the 5G cellular network architecture, and identify open research problems. More precisely, we discuss the security requirements for network access, location reporting, and C2 signaling

Digital Object Identifier:
10.1109/MCOMSTD.0003.2100108

The authors are with Mississippi State University-Starkville, USA.

via cellular networks for UAV and UAV-C users, identify the major threats to these critical UAS communications services, and present the 3GPP architecture and the specific procedures to protect the service availability and integrity.

The rest of the article is structured as follows. The next section introduces the network security requirements and threats around three major themes: UAS authentication and authorization (A&A), location information veracity and tracking, and C2 signaling integrity. We then present the 3GPP network architecture, interfaces, and 5G core (5GC) application functions (AFs) supporting UAS operations. Following that, we illustrate the 3GPP security mechanisms and procedures that rely on the 5GC AFs and their interconnections with other network functions (NFs) for meeting the above security requirements. Then we identify opportunities for UAS cellular network security research and recommend critical security features and processes to be considered as standardization work items. The final section provides the concluding remarks.

Security Requirements and Potential Threats

This section identifies the security requirements and potential threats to the UAS A&A, location information reporting, and C2 signaling.

UAS A&A

Security Requirements: The network must be able to identify the UAV and UAV-C and distinguish their network access from that of regular user equipment (UE). There are two types of IDs defined for a particular UAV node. The designated civil aviation authority (CAA) level UAV ID, which is assigned by the UAS service supplier (USS) or the UAS traffic management (UTM), is employed for remote identification and tracking (RID&T). The 3GPP UAV ID is used for recognizing the UAV; it provides the necessary credentials for the UAV to become an authorized UE and gain access to 3GPP services. The core network needs to match the CAA-level UAV ID to the 3GPP UAV ID.

An additional factor that must be taken into consideration to preserve a fully authenticated and authorized process is the pairing between the UAV and UAV-C that takes place at the USS/UTM. The result of this pairing process must be communicated to the network.

UAS A&A is the prerequisite for overruling the UAV-C in case of suspicious access. Consequently, any connection established by the UAS nodes must be authenticated and authorized by the network differently than the regular UAV-C, UAV, or UE. The network must follow certain policies regarding the unsuccessful A&A to prevent the registration and to cancel illegitimate protocol data unit (PDU) sessions.

Potential Threats: A weak UAS authentication process can grant access to an untrusted UAV or UAV-C to receive UAS services. This can cause leakage of critical data such as UAS system capabilities, location, and encryption keys. Unauthorized UAVs may attempt to imitate the behavior of legitimate UAVs to launch man-in-the-middle or replay attacks [13]. An unauthorized node that is able to obtain the credentials of authorized nodes could then inject false data. In a surveillance scenario, for example, an unauthorized UAV may deliberately alter and provide false data (e.g., altered pictures or video streams).

A fake USS/UTM may inject messages to the UAS nodes that affect UAV flight operations with the possibility of UAV hijacking. A malicious radio node may continuously jam the communications channels to cause bandwidth saturation, hinder the A&A process of legitimate UAS nodes requesting network access, or cause denial of service of already authenticated nodes.

Location Information Veracity and Tracking

Security Requirements: The UAV is required to inform the USS/UTM about its location using one of several forms of location information, including the absolute position, for example, the global navigation satellite system (GNSS) coordinates, or the relative position, such as the cell ID or tracking area coordinates. The reported location information may be used by the USS/UTM to define the optimal set of actions needed to ensure safe aerial operations. The reporting of location information can be verified using UAS application layer mechanisms such as the network RID. It is preferred that the position reporting for both the UAV/UAV-C and the USS/UTM is accomplished leveraging network-assisted positioning mechanisms and that the network forwards the estimated location information to the USS/UTM as supplementary data when it is requested.

There are already various location services that can be used by the UAV or UAV-C in the evolved terrestrial radio access network (RAN) or next generation RAN (NG-RAN). These include the network-assisted GNSS, downlink positioning, enhanced cell ID, terrestrial beacon system, reference signal time difference, and observed time difference of arrival.

Potential Threats: The location information can be compromised through spoofing attacks causing false location reports that may mislead the USS/UTM in its airspace management decisions. False location data can lead to costly cyber-physical or kinetic attacks that, for example, steer the UAV toward unauthorized or prohibited airspace, deceive the maneuver strategy to create air conflicts, or confuse authorities or pilots about the location of UAVs. Location spoofing attacks can be carried out by external means through a fake GNSS or cell ID transmitter [9].

C2 Signaling Integrity

Security Requirements: C2 signaling is used to control the UAV through a controller, which can be the UAV-C, USS/UTM, or another trusted authority. C2 communications can be classified as direct, network-assisted, and UTM-navigated [2]. It is critical to preserve reliable and available C2 communications in spite of radio condition variations, different traffic situations, and unpredictable events, which can be addressed by means of selecting or switching to the appropriate C2 communications mode. For example, when a UAV approaches beyond visual line of sight (BVLoS) or the direct communications link between the UAV and UAV-C becomes unstable, a seamless switch from direct to network-assisted C2 should happen while maintaining the highest security standards.

An additional factor that must be taken into consideration to preserve a fully authenticated and authorized process is the pairing between the UAV and UAV-C that takes place at the USS/UTM. The result of this pairing process must be communicated to the network.

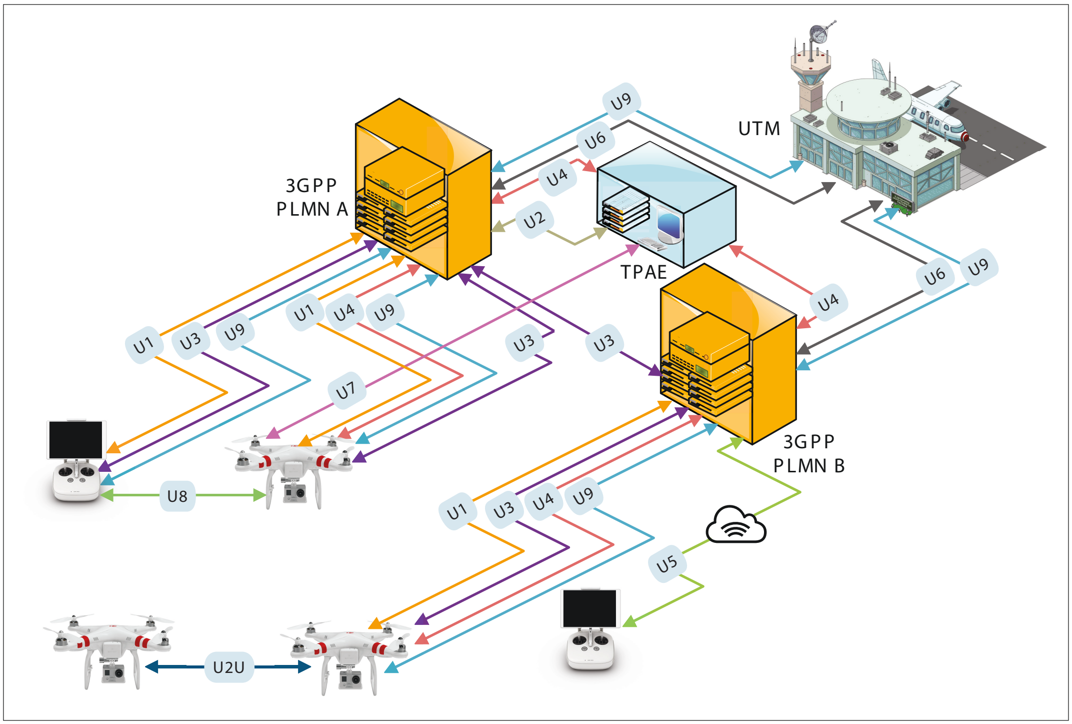

Figure 1. The 3GPP interfaces for cellular network connected UASs. PLMN: public land mobile network; TPAE: third party authorized entity; UTM: UAS traffic management.

Potential Threats: The ability to eavesdrop, monitor, or otherwise attack C2 communications between the UAS peers is a security risk that must be suppressed to ensure the safety and integrity of aerial operations. Uncertainty in the security measures for C2 links makes the system vulnerable to control deficiencies that can lead to operations failures or UAVs being hijacked. Smart attackers can target and take advantage of the switching process between C2 modes and exploit the security vulnerabilities of the least protected mode. A combined eavesdropping and jamming attack can be conducted over the C2 links, where the jammer downgrades the quality of service and triggers the process of switching from one C2 mode to another. The eavesdropper may then intercept the control messages and use this information to further attack the system.

3GPP Network Architecture for UASs

This section introduces the 3GPP reference architecture for supporting UAS operations.

Interfaces for Cellular Networked UASs

3GPP considers a UAS as a UAV and UAV-C pair, where each will be authorized as an individual UE in the network. The 3GPP work items aim to provide a network architecture that enables control plane (CP) and user plane (UP) communications services for UASs and provide wireless connectivity between the UAS and non-3GPP aviation entities, such as the USS or UTM for BVLoS operation. The USS/UTM is responsible for providing various functions supporting safe and secure operations. These functions include C2 services, CAA services, telematics, UAS-generated data, RID, authorization, enforcement, and regulation of UAS operations. The USS/UTM can be integrated in the 3GPP framework as an AF, operating as a CP NF or as an application server in the data network.

There are external entities that can monitor UAVs, track UAV data, and control UAVs. These fall under the umbrella of the third party authorized entity (TPAE), which can be an application server in the data network. C2 packets may thus be exchanged between the UAV and the UAV-C, UTM, or TPAE for UAV control. Figure 1 illustrates the network interfaces for UASs. They were introduced in 3GPP TR 23.754, version 17.1.0, and are described below.

U1: Carries control signals for the 3GPP network to identify, authenticate, authorize, and track the UAV and UAV-C

U2: Facilitates RID&T of the UAV through the TPAE

U3: Transports C2 packets between the UAV-C and the UAV through the cellular network

U4: Enables C2 signaling and RID&T between the UAV and the TPAE

U5: Transports C2 packets between the UAV and the UAV-C, where the UAV-C is connected to a non- 3GPP network

U6: Facilitates identification, authorization, and tracking of the UAV and UAV-C by the USS/UTM

U7: Carries the RID that is broadcast by the UAV to entities outside the scope of 3GPP

U8: Characterizes C2 signaling links via non-3GPP networks

U9: Supports various USS/UTM operational functions, such as networked RID, C2 signaling, UAV authentication, authorization, and tracking

U2U: Establishes the RID broadcast channel among UAVs

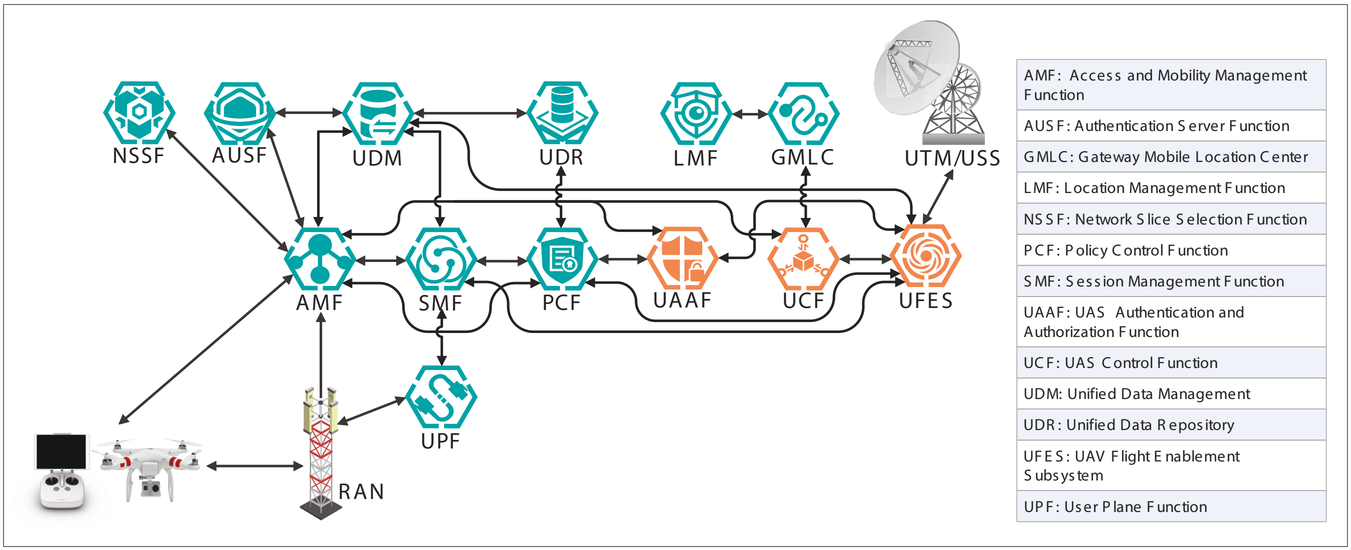
NSSF
AUSF
UDM
UDR
LMF
GMLC
UTM/USS
AMF
SMF
PCF
UAAF
UCF
UFES
UPF
RAN
AMF: Access and Mobility Management Function
AUSF: Authentication Server Function
GMLC: Gateway Mobile Location Center
LMF: Location Management Function
NSSF: Network Slice Selection Function
PCF: Policy Control Function
SMF: Session Management Function
UAAF: UAS Authentication and Authorization Function
UCF: UAS Control Function
UDM: Unified Data Management
UDR: Unified Data Repository
UFES: UAV Flight Enablement Subsystem
UPF: User Plane Function

Figure 2. The 5GC integrating three UAS AFs.

5G Core Application Functions

Enhancements to the core network are necessary for supporting UAS operations and ensuring service availability, integrity, and authorization. 3GPP introduces three AFs that are integrated into the 5GC specifically for supporting UASs. These are highlighted in Fig. 2 and introduced below. The next section will further elaborate how these and other 5GC functions of Fig. 2 will interact to implement critical network security procedures.

UAV Flight Enablement Subsystem (UFES): The UFES serves as a single interface to the USS/UTM. Principally, it performs the USS/UTM discovery and selection without requiring other 3GPP network nodes. The USS/UTM selection is based on the CAA-Level UAV ID, which provides RID&T information to the TPAE/USS/UTM that may be monitoring the UAV. The UFES supports the delivery of the external UAV ID as the 3GPP UAV ID to the USS/UTM, and can retrieve relevant subscription information from the unified data management (UDM) and receive policy control information from the policy control function (PCF). It determines a PDU session for the UAV operation through the session management function (SMF) to transmit operation updates from the USS containing the updated authorized UAV and UAV-C pairing information.

UAS A&A Function (UAAF): The UAAF assists with the A&A of UAS nodes over the UP. A UAV originating A&A request is transferred to the UAAF through the access and mobility management function (AMF). It includes the UAV ID, the UAV application ID, and the served USS/UTM ID. The UAAF validates the UAV subscription, and appends relevant subscription and application information from the PCF to be sent to the USS/UTM via the UFES.

UAS Control Function (UCF): The UCF is operated by the public land mobile network (PLMN) serving the UAV/UAV-C. It invokes the gateway mobile location center (GMLC) procedures for obtaining the location of the UAV or the UAV-C upon receiving a request from the USS/UTM via the UFES, while triggering the AMF for registration information related to the served node. The UCF is also responsible for matching the UAV/UAV-C ID provided by the UTM/USS with the corresponding UE ID and for transferring the CAA-level UAV ID to the USS/UTM. The UCF determines the 5GC NF to be invoked for supporting the interworking between the 5GC and the USS/UTM.

3GPP Security Solutions

This section introduces the 3GPP approach to prevent many of the previously described security threats. Specifically, we discuss the 3GPP procedures to secure access, location information, and C2 signaling.

UAS A&A

Figure 3 presents the 3GPP workflow for UAS A&A. It involves the UAAF, which validates the subscription information of the UAV and UAV-C and assists with the A&A processes of the USS/UTM. The procedure is described below.

The primary A&A is performed between the UAV/UAV-C and the 5G network just like for a regular UE through the PLMN UE ID (i.e., the subscription permanent ID) and the corresponding credentials (Step 1). A PDU session is established between the UAV/UAV-C and the UAAF for enabling UAS-specific A&A message exchanges with a default policy that prevents any traffic from the UAV/UAV-C except the traffic destined for the UAAF (Step 2). The UAV/UAV-C initiates the A&A request with the UAAF as UP data while providing the UAV/UAV-C identity, USS/UTM identity if already known, and application level information (Step 3).

The UAAF in continuation requests the relevant subscription information of the UAV/UAV-C from the PCF with the assistance of the binding support function (BSF), which binds the UAV/UAV-C AF request to the PCF (Step 4). After receiving the subscription information, the UAAF checks its validity for aerial subscription. If the check is successful, the UAAF determines the USS/UTM serving the UAV/UAV-C based on the provided information in Step 3 and the stored list of valid USS/UTM IDs. The 3GPP UAV ID that is obtained from the BSF is added to the CAA-Level UAV-ID and forwarded to the USS/UTM together with the application level information. The UFES

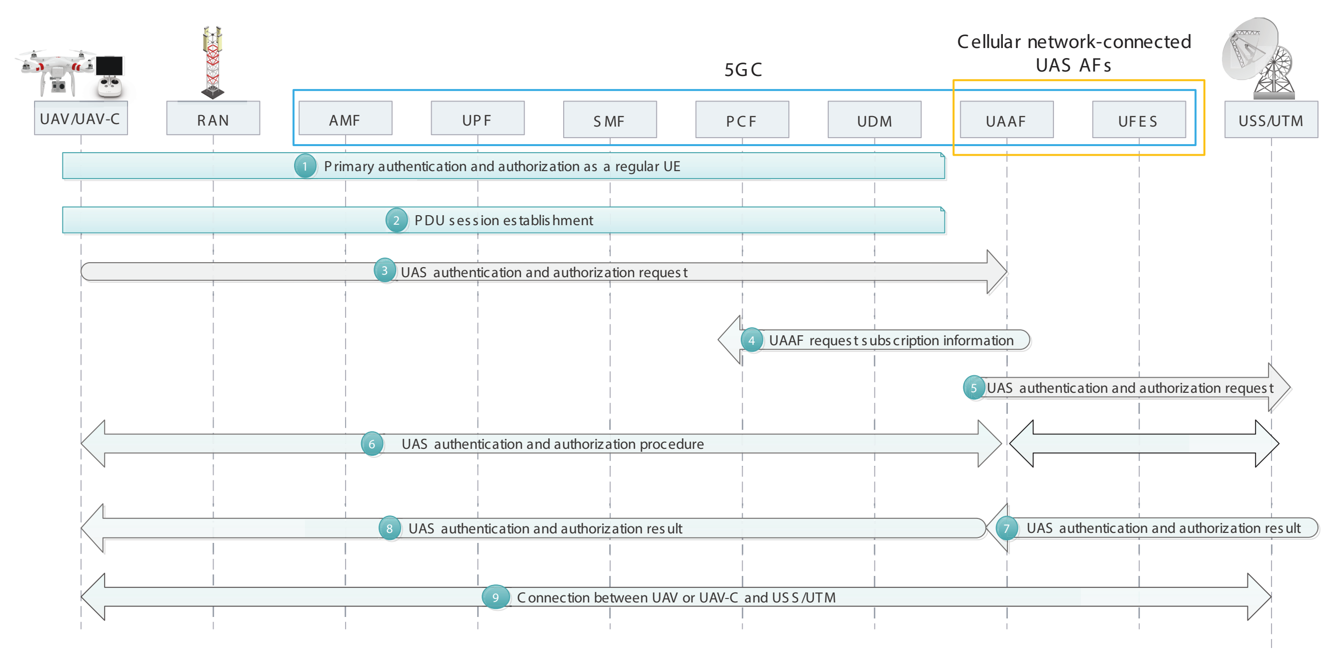
UAV/UAV-C
RAN
5GC
AMF
UPF
SMF
PCF
UDM
Cellular network-connected UAS AFs
UAAF
UFES
USS/UTM
1 Primary authentication and authorization as a regular UE
2 PDU session establishment
3 UAS authentication and authorization request
4 UAAF request subscription information
5 UAS authentication and authorization request
6 UAS authentication and authorization procedure
8 UAS authentication and authorization result
7 UAS authentication and authorization result
9 Connection between UAV or UAV-C and USS/UTM

FIGURE 3. The 3GPP workflow for UAV/UAV-C A&A.

facilitates the communications between the UAAF and the USS/UTM (Step 5).

If the information sent to the USS/UTM in the previous step is insufficient for A&A, the UAAF relays additional messages between the UAV/UAV-C and the USS/UTM through the UFES (Step 6). The A&A result becomes transparent and is provided to the UAAF. If the authentication is successful, the USS/UTM may provide application specific information to be used for secure communications. If the authentication is unsuccessful, the USS/UTM may inform the UAAF about the possible measures to be taken, such as terminating the PDU session established in Step 2 (Step 7). The UAAF relays the result to the UAV/UAV-C through the 5GC and RAN (Step 8). If the result of Step 6 is successful, the UAAF also informs the SMF to modify the PDU session established in Step 2 with the authenticated identities of the UAV/UAV-C such that the UAV/UAV-C can communicate with the USS/UTM beyond the limitations of the initial PDU session (Step 9).

The requirements for cellular-enabled UAV communications are defined in 3GPP Technical Specifications (TSs) 22.125, version 17.6.0. These specifications, among others, establish that the end-to-end latency shall be between 40 ms and 1 s, depending on the control mode and UAV speed. The end-to-end latency for C2 signaling over a 5G network has been measured as 30 ms [14]. A&A needs to be established beforehand and can initially be done before UAV takeoff. The total time for authenticating a UE with the 5GC takes 22 ms according to 3GPP TS 33.501, version 17.7.0. This corresponds to Step 1 of Fig. 3. We estimate the total time for completing the A&A Steps 1–9 to be between 22 and 154[1] ms. The UAS authentication delay can be further reduced by advancing core network technologies, leveraging mobile edge computing, caching, and optimized integration of access-stratum and non-access-stratum implementations, among others.

LOCATION INFORMATION VERACITY AND TRACKING

Figure 4 presents the 3GPP workflow for the secure exchange of location information. This workflow involves the UCF which is responsible for the location verification and for tracing the information of the UAV and UAV-C to provide trustful location reporting to the USS/UTM. The workflow is described below.

The process starts with the primary A&A process of the UAS node as a UE in the 5G network followed by the A&A with the USS/UTM to validate the aerial subscription as previously described and illustrated in Fig. 3 (Step 1). The 5G system establishes the PDU session for location information and tracking data exchange and validation between the UAV/UAV-C and the USS/UTM (Step 2). The UAS node sends the flight operation permission request as UP data to the UTM. This request may include the UAV identity, its current location, planned trajectory, and so forth (Step 3).

The USS/UTM initiates the location request and verification procedures by communicating with the UCF through the UFES. The location information request includes the CAA-level UAV ID (Step 4). After receiving the request, the UCF activates the location services AFs of the 5GC through the GMLC to trigger the location verification procedures and obtain the location information of the UAV and UAV-C by following the location procedures defined in 3GPP TS 23.273, version 17.7.0 (Step 5). The GMLC therefore invokes a service operation request in the UDM to obtain the privacy settings of the target node (UAV or UAV-C). The UDM returns the network address of the serving AMF (Step 6). The GMLC communicates with the location management function (LMF) to select the network-assisted positioning method that relies on the NG-RAN location measurements. The serving base station obtains and returns the position information via the AMF. The LMF then calculates the location

[1] With four steps in Fig. 3 similar in complexity to Step 1 and four smaller steps, we estimate the upper bound to be 7–22 ms.

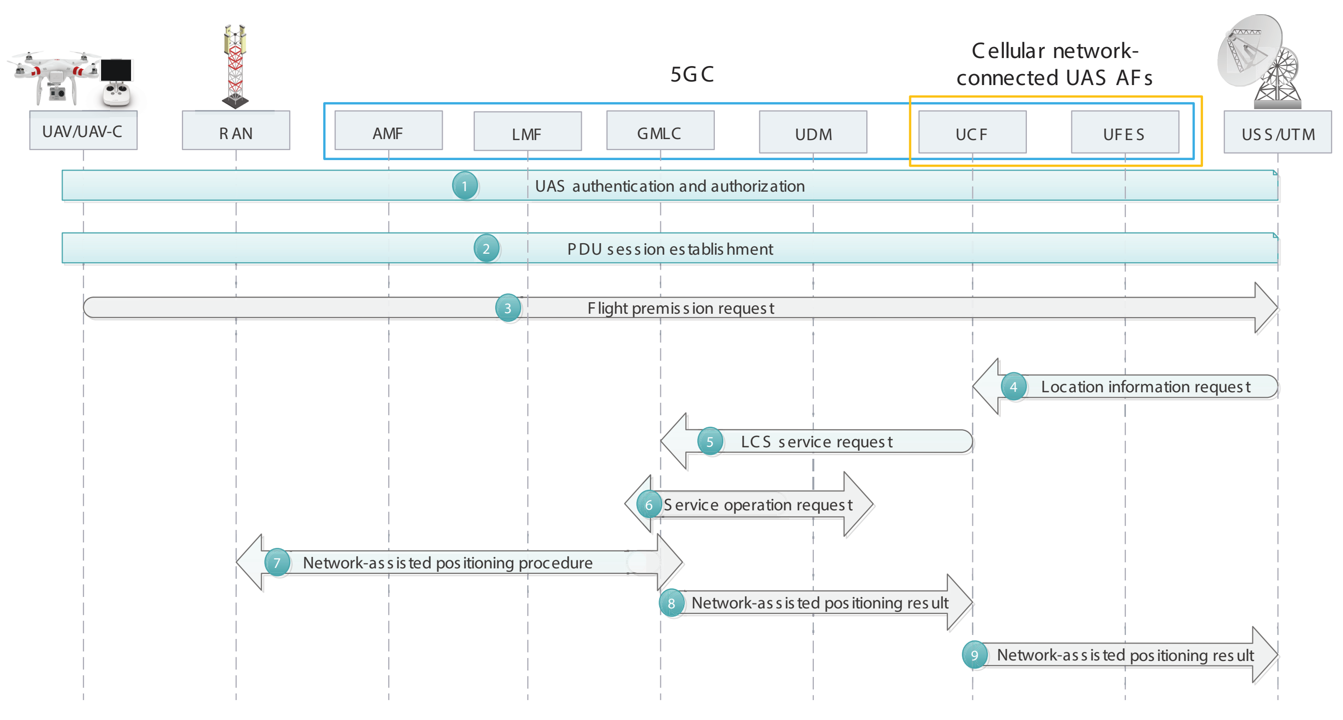
5GC
Cellular network-connected UAS AFs
UAV/UAV-C
RAN
AMF
LMF
GMLC
UDM
UCF
UFES
USS/UTM
1 UAS authentication and authorization
2 PDU session establishment
3 Flight premission request
4 Location information request
5 LCS service request
6 Service operation request
7 Network-assisted positioning procedure
8 Network-assisted positioning result
9 Network-assisted positioning result

FIGURE 4. The 3GPP workflow for UAV/UAV-C location information provisioning, verification, and tracking.

result and responds to the GMLC (Step 7). The obtained location measurement is transferred from the GMLC to the UCF (Step 8), which forwards it to the USS/UTM (Step 9). This information can be used to verify the location or flight behavior that the UAV reported as part of Step 3.

C2 Signaling Integrity

Figure 5 illustrates the 3GPP workflow for secure C2 communications link establishment between the UAV and its controller, which can be the UAV-C, TPAE, or USS/UTM. This procedure is an application programming interface based solution that facilitates a secondary authentication with the USS/UTM via the 5G data network authentication, authorization, and accounting server. The following steps are performed.

The primary authentication procedure is performed between the UAV/UAV-C and the 5G network for registering with the network as regular UEs (Step 1). A request message is sent from the UAV to the AMF for establishing the PDU session with the USS/UTM. This message includes the CAA-level UAV ID and data network name/single-network slice selection assistance information (DNN/S-NSSAI). The AMF uses the subscription information of the UAV and the DNN/S-NSSAI to determine the appropriate SMF (Step 2). The SMF performs a check on the applicability for requesting the UAV to perform the secondary authentication based on the supplied subscription information and the local policies (Step 3).

The SMF triggers the USS/UTM to initiate the API-based authentication process through a proxy A&A function implemented by the UAAF in the 5GC. The USS/UTM address can be resolved by the SMF with the obtained CAA-level UAV ID. The proxy A&A initiates communications with the USS/UTM through the UFES and sends the 3GPP UAV ID for performing the secondary authentication. If the process succeeds, the USS/UTM sends back a new assigned CAA-level UAV ID, authorization token, and any other essential information to the proxy A&A, which forwards the new credentials to the SMF (Step 4). The SMF then sends the PDU establishment session accept message to the UAV with the new credentials (Step 5).

An additional PDU session establishment request is initiated by the UAV. This request includes the new CAA-level UAV ID obtained from the secondary authentication process and the UAV-C identity for pairing; a pairing authorization request is sent to the USS/UTM. The USS/UTM informs the SMF of the authorized IP address of the UAV-C and instructs it to reconfigure the PDU session accordingly (Step 6). The PDU session establishment accept message is sent to the UAV, which then applies the new credentials and security parameters for future communications (Step 7). Secure application layer communications is now established for C2 between the UAV and the USS/UTM using the new security parameters (Step 8), and the UAV can initiate secure C2 communications with its UAV-C peer (Step 9).

Remaining Challenges and Future Directions

Various challenges remain for secure UAV operations through cellular networks. We identify the critical challenges and opportunities for research and future standardization.

Encryption

The communications links between the UAV and the UAV-C are vulnerable to eavesdropping and other adversarial attacks. The encryption of signals transmitted between UAS nodes has not been standardized yet within the scope of the

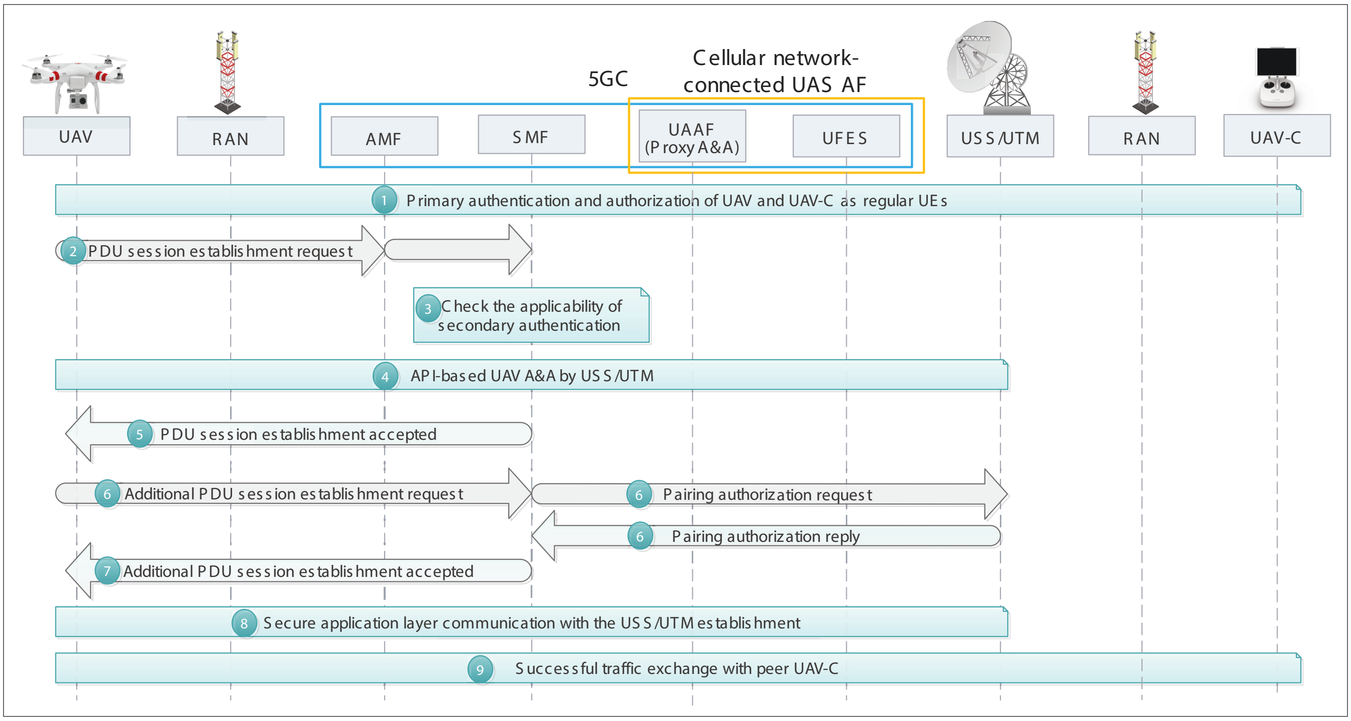
5GC
Cellular network-connected UAS AF
UAV
RAN
AMF
SMF
UAAF (Proxy A&A)
UFES
USS/UTM
RAN
UAV-C
1 Primary authentication and authorization of UAV and UAV-C as regular UEs
2 PDU session establishment request
3 Check the applicability of secondary authentication
4 API-based UAV A&A by USS/UTM
5 PDU session establishment accepted
6 Additional PDU session establishment request
6 Pairing authorization request
6 Pairing authorization reply
7 Additional PDU session establishment accepted
8 Secure application layer communication with the USS/UTM establishment
9 Successful traffic exchange with peer UAV-C

FIGURE 5. The 3GPP workflow to authenticate and authorize C2 communications between UAV and UAV-C over the 5G network.

3GPP, but there are efforts that address this problem as part of open source and commercial software projects. For example, the Paparazzi and DJI open source UAV projects have managed to implement encrypted protocols using Chacha20 with Poly1305 and 256-bit keys with advanced encryption standards, respectively [15]. It is critical to standardize and enforce encryption for all communications, including UAV/UAV-C originating or terminating data to prevent eavesdropping, location tracking, data breaches, and other attacks to privacy and integrity.

A&A Lifetime

3GPP has established revocation procedures to update the A&A parameters; however, it does not define a specific lifetime and when a revocation shall be triggered. It is triggered only when a node requests it. Attackers can take advantage of potentially long-lived authentication parameters as has been shown in 4G, where UEs can be tracked if their temporary IDs are not frequently changed. The A&A revocation process should be regularly triggered to maintain up-to-date status of the active UAS nodes and missions.

USS/UTM A&A

Most of the studied threat models and solutions target UAS nodes. The USS and UTM are the main components within the UAS framework where most of the authentication, authorization, and other related information about the UAV and UAV-C are stored and processed. The 3GPP specifications do not provide details on the USS/UTM authentication. It is rather assumed that the USS/UTM is a trusted node prior to authenticating UAS nodes with the network. This assumption may be exploited by an adversary to perform a variety of attacks, such as USS/UTM spoofing and requesting network services for unauthorized UAS missions. It is important to perform authentication checks of the USS and UTM.

Handover

Handover introduces system overhead and latency. The handover process needs to be robust and secure to avoid service disruption, especially for C2. The UTM, which authorizes UAS nodes and flight plans, may support the 3GPP network's handover processes for UAVs and the associated security mechanisms. Based on the flight path information or UAV mission, it may notify the network to trigger the transfer of the established security context from the current system that serves the UAV to the target system in advance of the expected handover. With the help of UAV network measurements, potential service outages may be anticipated to adjust flight plans or seamlessly switch alternative navigation mechanisms in a secure manner, including automatic flight by UTM and semi-autonomous navigation [2].

Blockchain for UAS Communications Security

The standards committees should investigate the use of blockchain and distributed ledger technologies to support the registration of UAS nodes with desirable characteristics such as non-repudiation and tunable trade-offs between operator privacy and public transparency. Blockchain can supplement flight data recording to ensure that the data exchange over the cellular network is secure, tamper-proof, and traceable for the entire UAS mission without human intervention.

Conclusions

Cellular communications networks are being considered to carry UAS data and control signals, and the corresponding interfaces and protocols are being standardized for emerging 5G networks.

This article has identified the UAS network security requirements, threats, the 3GPP architecture, interfaces, and security procedures, and the remaining research and standardization opportunities related to A&A, location information, and C2 signaling. Critical security features are enabled by the three 5GC AFs supporting UAS operations. The UFES performs the USS/UTM discovery and selection. It determines a PDU session for transmitting UAS operation updates. The UAAF validates UAS subscriptions and appends relevant subscription and application information to be sent to the USS/UTM. The UCF is responsible for delivering the UAV/UAV-C location reports upon request from the USS/UTM, matching the UAV/UAV-C ID with the respective UE ID, and transferring the CAA-level UAV ID to the UTM/USS as part of the authentication and location procedures. While the 5G standard introduces important security mechanisms, more security research and benchmarking are needed for cellular networks to support secure and scalable real-time control of UAVs and the emerging applications enabled by them.

Acknowledgment

This work was supported in part by the National Science Foundation under grant number CNS-1939334.

References

[1] A. S. Abdalla *et al.*, "UAV-Assisted Attack Prevention, Detection, and Recovery of 5G Networks," *IEEE Wireless Commun.*, vol. 27, no. 4, Aug. 2020, pp. 40–47.

[2] A. S. Abdalla and V. Marojevic, "Communications Standards for Unmanned Aircraft Systems: The 3GPP Perspective and Research Drivers," *IEEE Commun. Stds. Mag.*, vol. 5, no. 1, Mar. 2021, pp. 70–77.

[3] L. Wang *et al.*, "Security Threats and Countermeasures of Unmanned Aerial Vehicle Communications," *IEEE Commun. Stds. Mag.*, vol. 5, no. 4, 2021, pp. 41–47.

[4] T. Alladi *et al.*, "Drone-MAP: A Novel Authentication Scheme for Drone-Assisted 5G Networks," *Proc. IEEE INFOCOM Wksps.*, May 2021.

[5] G. Bansal and B. Sikdar, "Location Aware Clustering: Scalable Authentication Protocol for UAV Swarms," *IEEE Networking Letters*, 2021.

[6] Y. Li, X. Du, and S. Zhou, "A Lightweight Identity Authentication Scheme for UAV and Road Base Stations," *Proc. 2020 ACM Int'l. Conf. Cyberspace Innovation of Advanced Technologies*, Dec. 2020, pp. 54–58.

[7] V. Marojevic *et al.*, "Performance Analysis of a Mission-Critical Portable LTE System in Targeted RF Interference," *Proc. IEEE VTC-Fall*, Sept. 2017.

[8] K. Pärlin, M. M. Alam, and Y. Le Moullec, "Jamming of UAV Remote Control Systems Using Software Defined Radio," *Proc. 2018 IEEE Int'l. Conf. Military Commun. Info. Systems*, May 2018.

[9] X.-C. Zheng and H.-M. Sun, "Hijacking Unmanned Aerial Vehicle by Exploiting Civil GPS Vulnerabilities Using Software-Defined Radio," *Sensors and Materials*, vol. 32, no. 8, 2020, pp. 2729–43.

[10] Y. Zeng, R. Zhang, and T. J. Lim, "Wireless Communications with Unmanned Aerial Vehicles: Opportunities and Challenges," *IEEE Commun. Mag.*, vol. 54, no. 5, May 2016, pp. 36–42.

[11] D. Rudinskas, Z. Goraj, and J. Stankünas, "Security Analysis of UAV Radio Communication System," *Aviation*, vol. 13, no. 4, 2009, pp. 116–21.

[12] O. Westerlund and R. Asif, "Drone Hacking with Raspberry-Pi 3 and WiFi Pineapple: Security and Privacy Threats for the Internet-of-Things," *Proc. 2019 1st Int'l. Conf. Unmanned Vehicle Systems*, Oman), 2019.

[13] B. Bera, A. K. Das, and A. K. Sutrala, "Private Blockchain-Based Access Control Mechanism for Unauthorized UAV Detection and Mitigation in Internet of Drones Environment," *Elsevier Computer Commun.*, vol. 166, 2021, pp. 91–109.

[14] G. Makropoulos *et al.*, "Field Trial of UAV Flight with Communication and Control through 5G Cellular Network," *Proc. 2021 IEEE Int'l. Mediterranean Conf. Commun. Networking*, 2021, pp. 330–35.

[15] S. Iqbal, "A Study on UAV Operating System Security and Future Research Challenges," *Proc. IEEE 11th Annual Computing and Commun. Wksp. and Conf.*, Jan. 2021, pp. 759–65.

Biographies

ALY SABRI ABDALLA (asa298@msstate.edu) is a Ph.D. candidate in the Department of Electrical and Computer Engineering at Mississippi State University-Starkville. His research interests are scheduling, congestion control, and wireless security for vehicular ad hoc and UAV networks.

VUK MAROJEVIC (vuk.marojevic@msstate.edu) is an associate professor in electrical and computer engineering at Mississippi State University-Starkville. His research interests include resource management, vehicle-to-everything communications, and wireless security with application to cellular communications, mission-critical networks, and unmanned aircraft systems.