A Lightweight Authentication Protocol for 5G Cellular Network Connected Drones

Siyu Chen, Shujie Cui(✉), and Joseph Liu

Faculty of Information Technology, Monash University, Melbourne, Australia
csiy0001@student.monash.edu, {shujie.cui,joseph.liu}@monash.edu

Abstract. Drones are being diversely used in various areas due to their low price. Most of the use cases demand a secure and reliable wireless communication infrastructure to ensure the quality of service. Such demand boosts the deployment of drones in 5G cellular network. The ground base station (BS) is the main component associated with drones in the 5G cellular network. However, the BS in 5G currently broadcasts the system information message without authentication protection. This poses serious security concerns as the system information message will be used to build connection between the BS and cellular devices. Particularly, adversaries can masquerade as BSs, connect drones, and obtain the data captured by them. Although some attacks have been prevented due to the recent enhancements for 5G cellular protocols, the root vulnerability for the bootstrap phase between drones and the BS still existed and not fixed yet.

In this work, we consider a scenario where drones are used in a sport venue to capture the match and 5G cellular network is used to disseminate the live stream. To protect drones from fake BSs, we adopt and optimise the authentication protocol proposed by Singla *et al.* in [26]. Basically, we modify its architecture by deploying aerial balloon drone BSs over the sport venues to provide more reliable communication service. Moreover, we optimise the verification process in order to reduce the computation overhead on drones. We implemented a prototype of the protocol and evaluated its performance. The experiment results show our authentication protocol is practical to be adopted.

Keywords: Drones · 5G security · Multi-tier architecture · Authentication protocol · Elliptic curve cryptography

1 Introduction

Since the first commercial drone, or unmanned aerial vehicle (UAV), was introduced at CES 2010 by Parrot, drones have been adopted to undertake various services, such as delivery [20], filming movies [28], and post-disaster rescue [12], due to their reasonable price and diverse uses. To ensure quality of the services

X. Yuan et al. (Eds.): QShine 2021, LNICST 402, pp. 129–143, 2021.
https://doi.org/10.1007/978-3-030-91424-0_8

provided by drones, those emerging usages of drones demand a secure and reliable wireless communication infrastructure for control commands and information dissemination. On the one hand, the drones need to get time critical control and safety commands to maintain the flight operations. On the other hand, the drones have to disseminate collected data so as to pertain their mission. For instance, in a surveillance operation, drones need to transmit real time video to the ground station/remote pilot, and the underlying transmission medium should be able support high data rates (often higher in full HD video transmission or wireless backhauling).

Utilizing the cellular network for positioning, navigation, and communication of drones has gained significant interest in recent years, as it provides an effective solution for establishing reliable wireless connectivity with ground cellular Base Stations (BSs) [29]. Specifically, due to the rising adoption of 5G and the need for real-time systems, the global Cellular-Connected (CC) drone market is expected to generate $592.1 million in 2023 [23].

In this work, we consider the usage of 5G CC drones in sport venues for live stream. Basically, the drones are equipped with cameras to capture the real-time sport event and the components for 5G connection. Using small drones with cameras in a stadium would explore an advanced perspective that never seen before with the new vantage points and breathtaking views. By connecting drones with 5G cellular network, which is about 3 times faster than generic WiFi on average, drones can transfer high-resolution video signal more efficiently (up to 8k) [27]. The audience can get an immersive and high-quality live broadcast experience.

Since the communication between drones and 5G BSs are wireless in nature, different kinds of attacks, such as replay, man-in-the-middle, impersonation, privileged insider and password guessing are possible in our scenario. A major risk of a drone is getting out of the control due to malicious masquerade attacks. An adversary could create a fake BS nearby the stadium and induce CC drones to connect it and make them becomes rogue drones. In the worst case, the adversary might send malicious commands to compromised drones to interrupt the sport events, ask them to forward live stream to unsubscribed entities, or steer them to destroy assets or injure athletes and audience [18]. It is necessary to design a secure authentication scheme for drones to authenticate the messages from the BS, especially the broadcast system information message that used to set connection between drone and BS. Moreover, considering the CC drone has relatively low computation ability and battery life [19], the authentication protocol cannot induce heavy communication and computation overhead to the drones.

In [26], Singla *et al.* design a lightweight authentication protocol to secure the initialization connection between 5G network BSs and cellular devices. However, their protocol cannot be applied into our scenario directly. On the one hand, compared with 4G, 3G and 2G cellular networks, 5G base-stations use much higher frequency radio waves (e.g., millimeter waves) to offer faster communication but with much smaller coverage area. The sport venues are typically located in urban area and surrounded with high-rise buildings, which affects the

connection between drones and the 5G network. Whereas, the live stream of sport events has strong requirement for the stability of the communication. On the other hand, the computation run in drones should be more lightweight than that run in other type of cellular devices, like smartphones. The reason is that a sport match in a sport venue, such as football match, usually takes several hours, and during the match the drones have to keep flying in the air to record the match, which is much more power-consuming than other devices. Any significant computation overhead will decrease the endurance of the CC drone. The computation overhead on drones required by the protocol should be reduced in order let the drones work for longer period.

In this paper, we adapt the authentication protocol proposed in [26] to allow drones to authenticate 5G BSs. Moreover, we modify the protocol in two aspects in order to make it suitable for our scenario. Specifically, to address the first problem, we deploy an aerial balloon drone over the sport venue to provide the BS service, *i.e.,* broadcast system information messages and collect live streaming to and from the drones under its coverage. Compared with the ground BS outside of the sport venue, our aerial balloon drone BS has much better coverage and is much closer to the drones working within the venue. Moreover, this deployment can increase signal quality and reduce signal attenuation. By doing so, the drones can connect to the 5G network more easily and stable, and the live stream can be transmitted with better guarantee. Moreover, we optimise the protocol to reduce the computation overhead in drones. Precisely, we simplify the signature verification process on drones. Our experiment results show the protocol is practical for our scenario.

2 Preliminary

This section briefly describes the architecture of our protocol for stadium live stream (Fig. 1). We also introduce the basic building block for our proposed protocol, hierarchical identity-based signatures (HIBS).

2.1 Multi-tier Drone in 5G Cellular Network

Our architecture consists of three main components: 5G core network (5GC), next-gen radio access network (Next-gen RAN), and CC drones. In the following, we will mainly discuss the components involved in the authentication protocol.

5GC. 5GC manages several components that provide service to CC drones. Our protocol mainly involves the 5GC Private Key Generator (5GC-PKG) and the Access and mobility Management Function (AMF). 5GC-PKG is a new component introduced by our scheme. It generates private-public key pair for the AMF. The functionality of AMF is similar to the mobility management entity (MME) in the 4G network [14]. Its core function in our scenario is to manage BSs, including the ground BSs and the aerial BS balloon drone. Specifically, AMF generates private-public key pairs for BSs under its coverage.

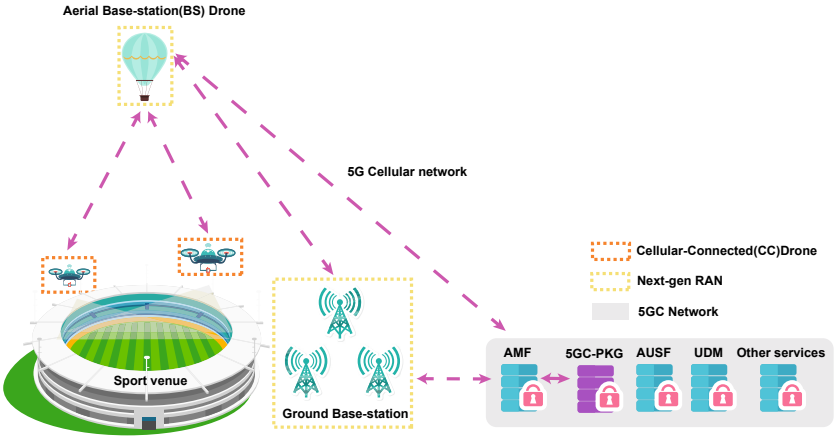

Fig. 1. The architecture of our protocol in 5G cellular network

Next-Gen RAN. It consists of the ground BSs and aerial BS balloon drones at its coverage. In our scenario, the aerial BS balloon drone is in charge of receiving the video signal from CC drones and transferring data for live stream purpose. It also directly controls the CC drones below its coverage by sending commands. The BS balloon drone needs to broadcast the Master Information Block (MIB) message and the System Information Blocks type 1 (SIB1) message to CC drones at regular intervals. MIB and SIB1 messages are the most important information that will enable further communication between the CC drone and the BS balloon drone. Precisely, MIB contains the necessary parameters required to decode SIB1, and SIB1 contains the essential parameters for setting the connection. The connection between a CC drone and the aerial BS balloon drone will be secure as long as the MIB and SIB1 messages are authenticated. Therefore, in our protocol the CC drones only need to verify SIB1 messages broadcast from the BS balloon drone.

CC Drones. They access the 5G cellular network using the Universal Subscriber Identity Module (USIM) card, which is provisioned by a cellular network operator. It contains a 5G Subscription Permanent Identifier (SUPI) [9], which also known as the International Mobile Subscriber Identifier (IMSI) in 4G LTE and 3GPP cellular network. Once CC drones received the broadcast messages from the BS balloon drone, they would verify the information by using our HIBS scheme. Also, our CC drones would be mainly responsible for high-resolution video recording in a sport venue and send the stream to aerial BS balloon drone through the secure communication channel.

2.2 Hierarchical Identity-Based Signatures

Notation. p and q are primes. We define a group $\mathbb{Z}_q$ and a finite field $\mathbb{F}_p$ for HIBS and use an elliptic curve (EC) over $\mathbb{F}_p$ as $E(\mathbb{F}_p)$. P is the generator points on $E(\mathbb{F}_p)$. $x \leftarrow S$ defines a random x is selected from a set S uniformly. $\|$ is denoted as string concatenation. $x \times P$ is represented elliptic curve scalar multiplication and all operations for EC utilise an additive notation. We use a hash function $H_1 : \{0,1\}^{i_1} \rightarrow \mathbb{Z}_q$, where i_1 denotes the identity space.

The hierarchical identity-based signatures [8] eliminates the requirement for certificates. It is a generalization of identify-based cryptography that deploys multiple PKGs in tree structure. Precisely, the upper-trier PKG generates the private key for lower-tier entities. In our scheme, we use a 2-tier hierarchical architecture, where 5GC-PKG is the root PKG and generates keys for AMFs, and AMFs are the lower-trier PKGs that generate keys for aerial balloon BS drones. Every entity has a position the tree. The identifies of 5GC-PKG, AMF and the aerial balloon BS drone are ID_0, ID_1, and ID_2, respectively. Specifically, we define $\mathbf{ID}_s = (ID_1, ..., ID_s)$, which is a set of identities of the entities lead up to ID_s, from the node directly following the root. We formally define the HIBS in the following.

Definition 1 (Hierarchical Identity-based Signatures). *A hierarchical identity-based signature scheme is defined as* $HIBS = \{Setup, Extract, Sign, Verify\}$.

- $(sk, mpk, params) \leftarrow Setup(1^k)$. *Given the security parameter k, the 5GC-PKG chooses the master secret key sk, computes system parameters params and its master public key mpk. Only the 5GC-PKG knows the sk, and params and mpk will be publicly available.*
- $(sk_{ID_s}, \boldsymbol{Q}_{ID_s}) \leftarrow Extract(\boldsymbol{ID}_s, sk_{ID_{s-1}}, \boldsymbol{Q}_{ID_{s-1}})$. *Given identity tuple* $\boldsymbol{ID}_s = (ID_1, ..., ID_s)$ *at level s, and the commitment value* $\boldsymbol{Q}_{ID_{s-1}}$ *the private key* $sk_{ID_{s-1}}$ *of the entity at depth of* $s-1$*, it returns the private key for the entity* ID_s *and its commitment value tuple* $\boldsymbol{Q}_{ID_s} = (Q_{ID_1}, ..., Q_{ID_s})$.
- $\sigma \leftarrow Sign(m, sk_{ID})$. *Given private key* sk_{ID}*, message m, and it outputs a signature sigma.*
- $r \leftarrow Verify(m, \sigma, \boldsymbol{ID}_s, \boldsymbol{Q}_{ID_s})$. *It takes message m, signature* σ*,* $\boldsymbol{ID}_s$*,* $\boldsymbol{Q}_{ID_s}$ *as input, and returns* $r = 1$ *or* $r = 0$ *to represent the signature is valid or not, respectively.*

3 Overview of Our Solution

3.1 Threat Model

In this work, we consider the widely-knowledge Dolev-Yao threat model where the adversary could inject, drop, or modify messages sent by legitimate entities through the public radio channel. We consider the adversary targets at attacking CC drones. In particular, an adversary could inject and tamper the messages

sent by the legitimate aerial BS drone, and masquerade as a BS and induce the CC drone to connect it. For example, the adversary can create a fake BS and force the CC drones to connect it over legitimate one by controlling the radio signal strength [14]. Then, the adversary can send malicious commands to CC drones and ask them to forward the living stream to an unsubscribed entity. Moreover, the adversary can mount different attacks on CC drones, such as man-in-the-middle, replay [16], and bidding down [25] attacks. However, the adversary can not physically tamper or access the legitimate aerial BS balloon drone, CC drones or 5GC infrastructure. It can not also access their private keys stored in BS drone or CC drones.

3.2 Scope of Our Solution

Our scheme enables CC drones to authenticate their upper-tier BS balloon drone before establishing a connection by verifying the SIB1 messages broadcast from the BS balloon drone. We do not consider DoS attacks, such as forcing the CC drone to disconnect our original network and registering to a fake BS using an RF jammer [7]. We also do not consider the passive eavesdropping attack [9] on the communication between the CC drone and the BS balloon drone.

Moreover, our scheme is envisioned for sport venues using drones for transmitting video data. Indeed, our scheme can be extended to many other scenarios, such as deployment in disaster relief. For instance, if an earthquake happens in an area and local architectures have been destroyed, CC drones can provide cellular network support to the survivor immediately below its coverage [19]. It can also record the video for the site condition and transmission to the ground control station and help to search for survivors.

Lastly, our solution can be extended to a 4G LTE or lower protocol cellular network with minimal modifications. This allows our system to become more flexible and increase its commercial competitiveness.

3.3 Overview of Our Protocol

Our authentication protocol allows CC drones to authenticate the aerial BS balloon drone's identity by verifying the SIB1 messages sent by it. Our authentication protocol is basically built based on top of the HIBS scheme, and it consists of 3 layers of components: 5GC-PKG, AMF, and BS balloon drone. We supply a high-level overview of our proposed authentication protocol.

The 5GC-PKG generates its private-public key pairs(PK_{5GC}, sk_{5GC}) at the initialisation phase. Its public key PK_{5GC} is pre-installed inside the USIM of all CC drones during their registration. The AMF sends its identifier AMF_ID and key generation request periodically to 5GC-PKG and receives (sk_{AMF}, PK_{AMF}, ID_{AMF}) from 5GC-PKG. ID_{AMF} is a concatenation of expire timestamp for its key-pair and AMF_ID. Similarly, the BS balloon drone sends a key generation request and NCI_ID to the AMF and receives (PK_{BSD}, sk_{BSD}, ID_{BSD}). ID_{BSD} is a concatenation of the expiration timestamp for its key pair and NCI_ID. The BS balloon drone uses its assigned sk_{BSD} to sign the SIB1 message and

generates the signature $Sign\{SIB_1\}$. The BS balloon drone sends $Sign\{SIB_1\}$, PK_{AMF}, ID_{AMF}, ID_{BSD}, and PK_{BSD} to CC drone. Then, the CC drone utilizes obtained information to verify the signature, timestamps of key pairs for the BS balloon drone and the AMF. If the timestamps are still valid and verification is successful, the CC drone would connect to the BS balloon drone.

4 Protocol Description

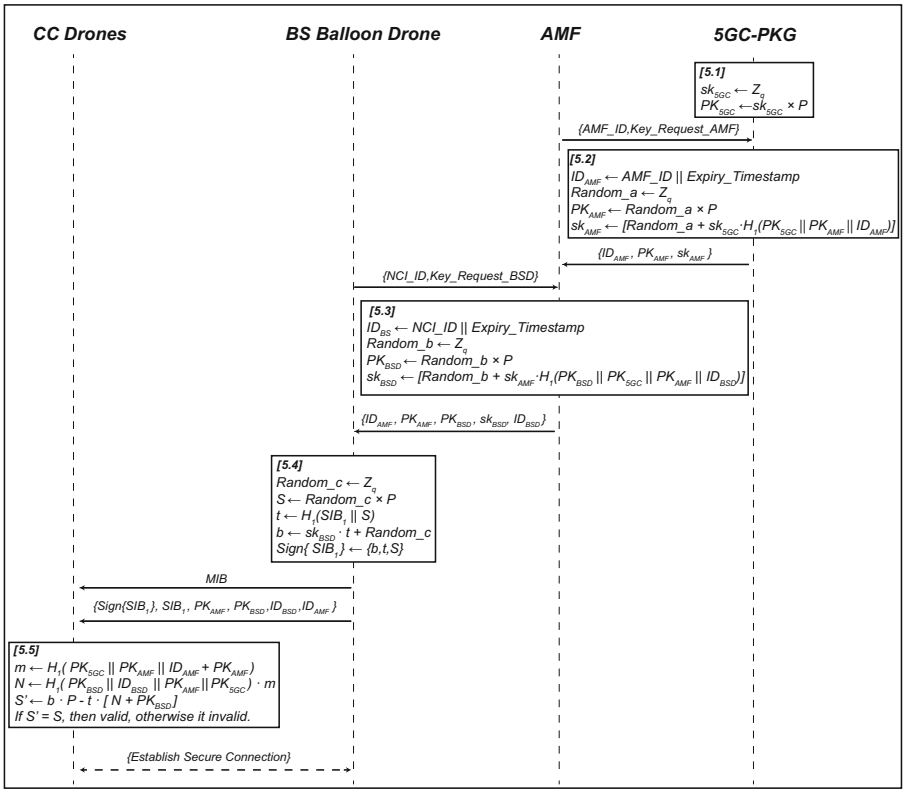

Fig. 2. Our proposed protocol for multi-tier drone system in 5G cellular networks

In this section, we first present the key management mechanism. Second, we give the way to prevent relay attack. Finally, we describe our authentication protocol for different phases. The specific computation performed by each entity and the communication between entities are shown in Fig. 2.

Key Management. We assign different validity period time for each generated private-public key pair of each entity instead of using complicated key revocation techniques. For example, we can set one year validity time for 5GC-PKG's key pair, and set one day for AMFs' keys. Both the 5GC-PKG and the AMFs are located in the 5G core network which are generally carefully protected, thus they cannot be tampered with easily and we can set longer period of validity for their keys. In contrast, the BS balloon drones are much easier to be attacked. We assign a shorter validity time, such as 5 min, for their keys. These validity periods for each entity's key pair can be configured by the network operator based on the situation.

Relay Attack Countermeasure. Our protocol provides mechanisms against illegitimate BSs by allowing the CC drone to authenticate the SIB1 messages. However, the adversary can eavesdrop on such messages and re-transmit them to CC drones. This relay attack can induce CC drones to connect the illegitimate BS.

To prevent relay attack, we propose to bind time to the SIB1 messages broadcast from the aerial BS balloon drone. Specifically, we append two additional fields to the broadcast SIB1 message: T_{sign} denotes when the SIB1 message is being signed; $\triangle T$ denotes the validity period of our signature, and it is location dependent. If CC drones start to verify the SIB1 message at time T_v, the message is valid if $T_v - T_{sign} < \triangle T$. A successful fake BS attack requires to relay the SIB1 message within $\triangle T$ time of T_{sign}. However, to determine an appropriate $\triangle T$ value requires taking account of location-dependent signal interference, which is hard to estimate due to environmental dynamics. Our idea is to measure the maximum time the SIB1 message taken from the legitimate BS balloon drone to CC drones and the minimum time required for a fake BS to execute a successful relay attack, and define them as t_{min} and t_{max}, respectively. t_{max} value must be larger than t_{min} as the fake BS requires an extra round of transmission. $\triangle T$ should be in (t_{min}, t_{max}), i.e., $t_{min} < \triangle T < t_{max}$. We leave a better solution to our future work.

4.1 5GC-PKG Initialisation Phase

During the initialization phase, the 5GC-PKG chooses a random value from $\mathbb{Z}_q$ as its private key sk_{5GC} and generates $sk_{5GC} \times P$ as its public key PK_{5GC} (as shown in Eq. 1). The 5GC-PKG is mainly responsible for generating the private-public key pairs for AMFs of a particular network operator. As mentioned, we also set a validity period for PK_{5GC} and sk_{5GC} in the 5G cellular network such as one year. PK_{5GC} is pre-installed in USIM [9,14] of the CC drones along with the expiry date, which waits to be refreshed once the connection has been established. When its public-private key pair expires, the 5GC-PKG updates and refreshes its new key pair and then delivers its new public key to lower-tier parties. This communication procedure can be executed using a confidential and integrity protection channel among each entity in the system.

$$sk_{5GC} \leftarrow \mathbb{Z}_q, PK_{5GC} \leftarrow sk_{5GC} \times P \tag{1}$$

4.2 AMF Key Generation

AMF gets its key pair from 5GC-PKG by sending a key generation request and its identifier AMF_ID to 5G-PKG. After getting the request from AMF, 5GC-PKG computes $PK_{AMF} \leftarrow Random\_a \times P$, where $Random\_a$ is randomly sampled from $\mathbb{Z}_q$. AMF's private key sk_{AMF} is generated based on sk_{5GC} and PK_{5GC}. Meanwhile, sk_{AMF} should be specific to PK_{AMF} and ID_{AMF}. Therefore, as shown in Eq. 3, sk_{5GC}, PK_{5GC}, PK_{AMF} and ID_{AMF} are all involved in the generation of sk_{AMF}. Once the 5GC-PKG generates private-public key pair for the AMF, it delivers ID_{AMF}, sk_{AMF}, PK_{AMF} to the AMF. When the AMF receives the key pair from 5GC-PKG, it first verifies the expiry timestamp embedded in AMF_ID. This procedure can ensure that the AMF receives valid private-public key pair for itself. We also set a validity period such as 24 h for PK_{AMF} and sk_{AMF} in the AMF component. If the key pairs expire, the AMF will request a new pair of key.

$$Random\_a \leftarrow \mathbb{Z}_q, PK_{AMF} \leftarrow Random\_a \times P \tag{2}$$

$$sk_{AMF} \leftarrow [Random\_a + sk_{5GC} \cdot H_1(PK_{5GC} \| PK_{AMF} \| ID_{AMF})] \tag{3}$$

4.3 BS Balloon Drone Key Generation

The AMF serves the BS balloon drones under its tracking area. The BS balloon drone first sends the key generation request to AMF. The AMF chooses a random value $Random\_b$ from $\mathbb{Z}_q$ and takes $Random\_b \times P$ as the BS balloon drone's public key PK_{BSD}. The secret key sk_{BSD} for BS balloon drone is derived from $Random\_b$, ID_{BSD}, PK_{BSD}, PK_{5GC}, and PK_{AMF} (Eq. 5). The AMF sends ID_{AMF}, PK_{AMF}, PK_{BSD}, sk_{BSD}, ID_{BSD} to the BS balloon drone. The BS balloon drone's key pair also has a validity period, such as 5 min. The ID_{BSD} concatenates the expiration timestamp for its key-pair and BS balloon drone's NCI_ID, so the BS balloon drone verifies the validity period time of its public-private keys by checking the timestamp. A BS balloon drone might under the tracking areas of multiple AMFs [24], thus it can send key generation requests to multiple AMFs. The BS balloon drone can only keep one of the key pairs and discard the other key pairs from AMFs, and it also can keep all the key pairs until they expire.

$$Random\_b \leftarrow \mathbb{Z}_q, PK_{BSD} \leftarrow Random\_b \times P \tag{4}$$

$$sk_{BSD} \leftarrow [Random\_b + sk_{AMF} \cdot H_1(ID_{BSD} \| PK_{BSD} \| PK_{5GC} \| PK_{AMF}] \tag{5}$$

4.4 Message Signing at BS Balloon Drone

For signing a SIB1 message, the BS balloon drone first randomize SIB1 by concatenating it with a random EC point S. Second, the randomized SIB1 is hashed into t with the hash function H_1, and it signs over the hash value t with its private key sk_{BSD}, rather than the original or the randomized SIB1, and get b (see Eq. 7). The final signature consists of b, t, and S. Later on, it broadcasts the signature along with the SIB_1, ID_{BSD}, PK_{BSD}, ID_{AMF} and PK_{AMF} to CC drones. Once the CC drones receive those broadcast messages, they use HIBS to verify the signature.

$$Random\_c \leftarrow \mathbb{Z}_q, S \leftarrow Random\_c \times P \tag{6}$$

$$t \leftarrow H_1(SIB_1 \| S), b \leftarrow sk_{BSD} \cdot t + Random\_c \tag{7}$$

$$Sign\{SIB_1\} \leftarrow (b, t, S) \tag{8}$$

4.5 Signature Verification at CC Drones

Finally, CC drones verify the signature with obtained messages. Recall that, the CC drone receives PK_{5GC}, PK_{AMF}, ID_{AMF}, ID_{BSD} and PK_{BSD} from the upper layer. First, the CC drone checks the identity ID_{AMF} and ID_{BSD} and the expiry timestamps embedded in them. If all the public keys are valid, the CC drone will verify the signed SIB1 message, and the details are shown in Eq. 9–12. In the verification phase, the keys of all the entities in upper layers are involved, which means only when all the keys of the entities in upper layers are valid, the verification could pass.

$$m \leftarrow H_1(ID_{AMF} \| PK_{AMF} \| PK_{5GC}) + PK_{AMF} \tag{9}$$

$$N \leftarrow H_1(PK_{BSD} \| ID_{BSD} \| PK_{AMF} \| PK_{5GC}) \cdot m \tag{10}$$

$$S' \leftarrow b \cdot P - t \cdot [N + PK_{BSD}] \tag{11}$$

$$S' \stackrel{?}{=} S \tag{12}$$

Notably, we optimise the verification process on CC drones compared with the protocol proposed by Singla et al. [26]. Precisely, in our scheme, the BS Balloon Drone also sends the intermediate value S to the CC drone. During the verification phase, the CC drone just computes S' with the messages received from the BS Balloon Drone in the same way as the generation of S, including the signed message b, and verifies if $S = S'$. By doing so, our scheme saves a step of computing a hash value compared with [26].

5 Performance Analysis

5.1 Experiment Setup

We implemented a prototype of our scheme in Python 3.7 [22] using Crypto 2.6.1 library [21]. The performance of each entity involved in the scheme was evaluated on a Macbook Pro laptop with 2.5 GHz 4-core Intel Core i7 processor and 16 GB 1600 MHz DDR3 memory.

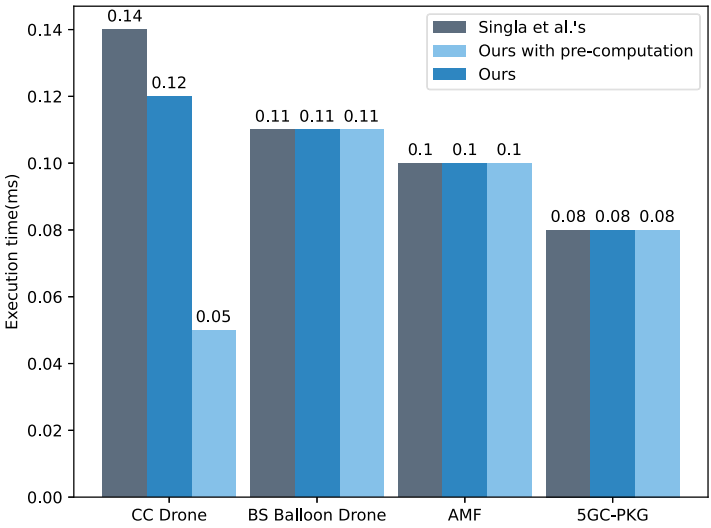

Fig. 3. Execution time for each entity in our proposed protocol

5.2 Computation Overhead

We evaluate the key generation time on 5GC-PKG and AMF, the signing time on the balloon drone BS, and the verification time on drones, and the results are shown in Fig. 3. All the results shown in Fig. 3 are the average of 10 times execution. For the test, we set the key size to 256-bit, which achieves 128-bit symmetric key security according to NIST recommendations [3]. From Fig. 3, we can see that, although the verification process on CC drones takes the longest time among all the entities, it only takes 0.12 ms to verify the signature, which is nearly negligible compared with the time of a sport match.

We also compare the performance of our scheme with the one proposed by Singla *et al.* in [26] in Fig. 3. We can see for the execution time in 5GC-PKG, AMF, and BS Balloon Drone, there is no big difference between the two schemes. However, the verification on CC drones of our scheme is more efficient due to our optimisation, which outperforms the verification of [26] by 14.3%.

We also optimize our proposed protocol by pre-computing the values of m and N at the CC drone. They can be pre-computed due to the fact that both m and N are independent on the SIB1 message, and they are derived from the public keys and identifies of AMF and BS balloon drone. As mentioned, the key pairs of each entity in our scheme have validity period. As long as all the keys involved in the computation of m and N are all valid, they will be the same and the CC drone can pre-compute them offline. When m and N are pre-computed, it only takes 0.05 ms to verify the signature from the BS balloon drone. In this case, the verification phase of our scheme outperforms [26] by 2.4×.

5.3 Communication Overhead

We also evaluate the communication volume for different phases of our protocol, and the result is shown in Table 1. For the authentication, the CC drone only receives 149 bytes from the BS balloon drone, which is a relatively low communication overhead for CC drones.

Table 1. Communication volume for our proposed protocol in different phases

Entity name	Communication volume (B)	Total (B)
AMF → 5GC-PKG	$AMF\_ID(7)$, $Key\_Request\_AMF(2)$	9
5GC-PKG → AMF	$ID_{AMF}(7)$, $PK_{AMF}(32)$, $sk_{AMF}(34)$	73
BS Balloon Drone → AMF	$NCI\_ID(5)$, $Key\_Request\_BSD(2)$	7
AMF → BS Balloon Drone	$ID_{AMF}(7)$, $PK_{AMF}(32)$, $PK_{BSD}(32)$, $sk_{BSD}(42)$, $ID_{BSD}(9)$	122
BS Balloon Drone → CC Drone	MIB(3), $Sign\{SIB_1\}(64)$, $SIB_1(2)$, $PK_{AMF}(32)$, $PK_{BSD}(32)$, $ID_{BSD}(9)$, $ID_{AMF}(7)$	149

The communication overhead between other entities is smaller as they only communicate for keys. The validity period of the private-public key for each entity can affect the communication volume the entities other than the CC drones. The shorter the valid time for private-public key pair for each entity, the more communication volume in a specific time. For example, suppose a BS balloon drone's private-public key is only valid for 5 min. In that case, it indicates that every 5 min passed, the BS balloon drone needs to repeat the key generation request to the AMF, so it requires to send the request 288 times for one day. However, if the key pair for the BS balloon drone is valid for 10 min, the communication volume for that phase would be half the amount compared with the valid period of 5 min.

6 Related Work

Commercial Cellular-Connected Drones. Google Loon project [10] aims to provide cellular network connectivity in remote areas. It has been achieved by utilizing stratospheric balloons to replay radio communication links from ground stations to end user's devices. Facebook's project, called Aquila [17], built a drone BS at a high altitude and provided internet coverage below its flight path. Later on, Huawei wireless X Lab [11] initiated the Digital Sky Initiative in 2017 to investigate the specific use cases associated with multi-tier drones system in the cellular network. Those prototypes utilized multi-tier drones connected to terrestrial networks via an air-to-ground wireless link or a satellite link to provide the 3GPP cellular network or WiFi signal to ground users.

Authentication Methodologies. 3GPP specifications [1] proposed three authentication solutions to verify the authenticity of BSs. The first solution is to verify the system information (SI) messages with identity-based cryptography and using the keys provisioned by the cellular network operators or digital signatures. In this solution, the BS cannot be authenticated during the initialization registration process, and it can only authenticate the BS during cell re-selection. The second one is to use a certification authority (CA) [1], where the BS is assigned a certificate to sign its broadcast messages [5]. However, sending CA certificates can cause significant communication overhead. The last method is to sign the BS's broadcast messages using identity-based signature schemes, which are more lightweight than the CA-based solution. However, the recommended identity-based schemes, SM9 [6] and Boneh-Lynn-Shacham (BLS) [4], from IEEE standard require costly pairing computations on the CC drones.

Attack Mitigation. To address fake BS, many solutions, such as [1], suggest only sending broadcast messages after building a secure communication connection between BS and end devices. The secure communication connection provides integrity and confidentiality protection. However, the adversary still can mount bidding-down attacks where the end devices are forced to use older cellular network protocols, such as 4G LTE, 3G, or 2G. Another typical way utilises machine learning technologies [13,15] to collect and analyse surrounding cellular network signal from legitimate BSs, end devices, and other deployed hardware in the cellular network [16], and white-list trusted BSs. However, in those methods, the adversary can easily bypass such detection by using a legitimate device as a covert channel. Similarly, the scheme also gives in [2] collects numerous regional legitimate BSs' characteristics and builds a unique cell print for authentication.

Although some prevention mechanisms already developed in 4G LTE/3GPP, they are not practical for drones due to the heavy computation and communication overhead. In particular, the masquerade attack is still a problem in the 5G cellular network. It poses an obstacle to developing a secure multi-tier drone system in the 5G cellular network. Our proposed protocol allows the drones to detect fake BS and it is lightweight and efficient.

7 Conclusion and Future Work

We propose to use 5G cellular network connected drones to capture real-time live streaming in sport venues. To provide more stable network connection, we deploy an aerial balloon drone to provide the 5G base station service in our architecture. More importantly, we propose a lightweight and efficient authentication protocol to secure the connection between CC drones and the BS balloon drone so as to prevent fake BSs from stealing the live stream or sending malicious commands to drones. Our evaluation results shown that the proposed protocol has a relatively low communication and computation overhead.

For our future work, on the one hand, we will evaluate the performance of our protocol in real CC drones. On the other hand, we will optimise the protocol further to make it more lightweight. For instance, we will modify the protocol so that more computation can be processed offline for drones.

References

1. Specification number TR 33.809 version 0.8.0. In: Study on 5G security enhancements against false base stations. 3GPP (2020)
2. Alrashede, H., Shaikh, R.A.: IMSI catcher detection method for cellular networks. In: 2019 2nd International Conference on Computer Applications and Information Security (ICCAIS), pp. 1–6. IEEE (2019)
3. BlueKrypt: Cryptographic key length recommendation. https://www.keylength.com/en/4/. Accessed 14 June 2021
4. Boneh, D., Lynn, B., Shacham, H.: Short signatures from the Weil pairing. J. Cryptol. **17**(4), 297–319 (2004). https://doi.org/10.1007/s00145-004-0314-9
5. Boyd, C. (ed.): ASIACRYPT 2001. LNCS, vol. 2248. Springer, Heidelberg (2001). https://doi.org/10.1007/3-540-45682-1
6. Cheng, Z.: The SM9 cryptographic schemes. IACR Cryptol. ePrint Arch. 2017, 117 (2017). http://eprint.iacr.org/2017/117
7. Dabrowski, A., Pianta, N., Klepp, T., Mulazzani, M., Weippl, E.R.: IMSI-catch me if you can: IMSI-catcher-catchers. In: Jordan, C.N.P., Hahn, A., Butler, K.R.B., Sherr, M. (eds.) Proceedings of the 30th Annual Computer Security Applications Conference, ACSAC 2014, New Orleans, LA, USA, 8–12 December 2014, pp. 246–255. ACM (2014). https://doi.org/10.1145/2664243.2664272
8. Gentry, C., Silverberg, A.: Hierarchical ID-Based cryptography. In: Zheng, Y. (ed.) ASIACRYPT 2002. LNCS, vol. 2501, pp. 548–566. Springer, Heidelberg (2002). https://doi.org/10.1007/3-540-36178-2_34
9. Gharsallah, I., Smaoui, S., Zarai, F.: A secure efficient and lightweight authentication protocol for 5G cellular networks: Sel-aka. In: 2019 15th International Wireless Communications and Mobile Computing Conference (IWCMC), pp. 1311–1316. IEEE (2019)
10. Google loon project main page (2011). https://loon.com/. Accessed 23 April 2021
11. Mbbf2017 connected aerial vehicle live (2017). https://www.huawei.com/au/technology-insights/industry-insights/outlook/mobile-broadband/xlabs/use-cases/mbbf2017-connected-aerial-vehicle-live. Accessed 23 April 2021
12. Huo, Y., Dong, X., Lu, T., Xu, W., Yuen, M.: Distributed and multi-layer UAV network for the next-generation wireless communication (2018)
13. Hussain, S.R., Echeverria, M., Chowdhury, O., Li, N., Bertino, E.: Privacy attacks to the 4G and 5g cellular paging protocols using side channel information. In: 26th Annual Network and Distributed System Security Symposium, NDSS 2019, San Diego, California, USA, 24–27 February 2019. The Internet Society (2019)
14. Hussain, S.R., Echeverria, M., Singla, A., Chowdhury, O., Bertino, E.: Insecure connection bootstrapping in cellular networks: the root of all evil. In: Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks, WiSec 2019, Miami, Florida, USA, 15–17 May 2019, pp. 1–11. ACM (2019). https://doi.org/10.1145/3317549.3323402

15. Jin, J., Lian, C., Xu, M.: Rogue base station detection using a machine learning approach. In: 28th Wireless and Optical Communications Conference, WOCC 2019, Beijing, China, 9–10 May 2019, pp. 1–5. IEEE (2019). https://doi.org/10.1109/WOCC.2019.8770554
16. Lilly, A.: IMSI catchers: hacking mobile communications. Netw. Secur. **2017**(2), 5–7 (2017). https://doi.org/10.1016/S1353-4858(17)30014-4
17. Maguire, Y.: Building communications networks in the stratosphere (2015). https://engineering.fb.com/2015/07/30/connectivity/building-communications-networks-in-the-stratosphere/. Accessed 23 April 2021
18. Mortimer, G.: Stadiums and arenas are keeping the good drones in, and the spies out with dedrone (2017). https://www.suasnews.com/2017/03/stadiums-arenas-keeping-good-drones-spies-dedrone/. Accessed 23 April 2021
19. Naqvi, S.A.R., Hassan, S.A., Pervaiz, H., Ni, Q.: Drone-aided communication as a key enabler for 5G and resilient public safety networks. IEEE Commun. Mag. **56**(1), 36–42 (2018). https://doi.org/10.1109/MCOM.2017.1700451
20. Nassi, B., Shabtai, A., Masuoka, R., Elovici, Y.: Sok - security and privacy in the age of drones: Threats, challenges, solution mechanisms, and scientific gaps. CoRR abs/1903.05155 (2019). http://arxiv.org/abs/1903.05155
21. Pycrypto 2.6.1. https://pypi.org/project/pycrypto/. Accessed 14 June 2021
22. Python 3.7.0. https://www.python.org/downloads/release/python-370/. Accessed 14 June 2021
23. Research, Markets: Global cellular-connected drone market analysis and forecast, 2020–2023 and 2030 (2020). https://www.globenewswire.com/en/news-release/2020/10/30/2117598/28124/en/Global-Cellular-Connected-Drone-Market-Analysis-Forecast-2020-2023-2030.html. Accessed 13 June 13 2021
24. Shaik, A., Borgaonkar, R., Park, S., Seifert, J.: On the impact of rogue base stations in 4G/LTE self organizing networks. In: Papadimitratos, P., Butler, K.R.B., Pöpper, C. (eds.) Proceedings of the 11th ACM Conference on Security and Privacy in Wireless and Mobile Networks, WiSec 2018, Stockholm, Sweden, 18–20 June 2018, pp. 75–86. ACM (2018). https://doi.org/10.1145/3212480.3212497
25. Shaik, A., Borgaonkar, R., Park, S., Seifert, J.: New vulnerabilities in 4G and 5G cellular access network protocols: exposing device capabilities. In: Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks, WiSec 2019, Miami, Florida, USA, 15–17 May 2019, pp. 221–231. ACM (2019). https://doi.org/10.1145/3317549.3319728
26. Singla, A., Behnia, R., Hussain, S.R., Yavuz, A.A., Bertino, E.: Look before you leap: Secure connection bootstrapping for 5g networks to defend against fake base-stations. In: Cao, J., Au, M.H., Lin, Z., Yung, M. (eds.) ASIA CCS 2021: ACM Asia Conference on Computer and Communications Security, Virtual Event, Hong Kong, 7–11 June 2021, pp. 501–515. ACM (2021)
27. Ullah, H., Nair, N.G., Moore, A., Nugent, C.D., Muschamp, P., Cuevas, M.: 5G communication: an overview of vehicle-to-everything, drones, and healthcare use-cases. IEEE Access **7**, 37251–37268 (2019). https://doi.org/10.1109/ACCESS.2019.2905347
28. Yang, G., et al.: A telecom perspective on the internet of drones: From LTE-advanced to 5G. CoRR abs/1803.11048 (2018)
29. Zeng, Y., Lyu, J., Zhang, R.: Cellular-connected UAV: potential, challenges, and promising technologies. IEEE Wirel. Commun. **26**(1), 120–127 (2019)