INL/CON-21-61518-Revision-0

A Proxy Signature-Based Drone Authentication in 5G D2D Networks

April 2021

Mai A. Abdel-Malek, Kemal Akkaya, Ahmed S. Ibrahim, Arupjyoti Bhuyan

Changing the World's Energy Future

INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC

INL/CON-21-61518-Revision-0

A Proxy Signature-Based Drone Authentication in 5G D2D Networks

Mai A. Abdel-Malek, Kemal Akkaya, Ahmed S. Ibrahim, Arupjyoti Bhuyan

April 2021

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

A Proxy Signature-Based Drone Authentication in 5G D2D Networks

Mai A. Abdel-Malek*, Kemal Akkaya*, Arupjyoti Bhuyan† and Ahmed S. Ibrahim*,
*Dept. of Electrical and Computer Engineering, Florida International University, Miami, FL 33174
Email: {mabde030,kakkaya,aibrahim}@fiu.edu
†INL Wireless Security Institute, Idaho National Laboratory, Idaho Falls, ID 83401
Email: arupjyoti.bhuyan@inl.gov

***Abstract*—5G is the beginning of a new era in cellular communication, bringing up a highly connected network with the incorporation of the Internet of Things (IoT). To flexibly operate all the IoT devices over a cellular network, Device-to-Device (D2D) communication standard was developed. However, IoT devices such as drones utilizing 5G D2D services could be a perfect target for malicious attacks as they pose several safety threats if they are compromised. Furthermore, there will be heavy traffic with an increased number of IoT devices connected to the 5G core. Therefore, we propose a lightweight, fast, and reliable authentication mechanism compatible with the 5G D2D ProSe standard mechanisms. Specifically, we propose a distributed authentication with a delegation-based scheme instead of the repeated access to the 5G core network key management functions. Hence, a legitimate drone is authorized by the core network via offering a proxy signature to authenticate itself to other drones. We implemented the proposed protocol in ns-3 that supports 5G D2D-based communication. We also conducted computational calculations on the RaspberryPi3 IoT device to mimic the drone calculation process and delays. The results demonstrate that the proposed protocol is lightweight and reliable.**

***Index terms*—** 5G security, authentication, D2D, drones, delegation, proxy signature.

I. Introduction

The anticipated 5G cellular network will integrate the Internet of Things (IoT) features and services toward a highly connected and informative communication experience [1]. From this context, the 5G network will not depend on the stationary infrastructure only but also mobile/IoT nodes. Such IoT nodes include sensors and drones for better on-site data collection and end-user experience. IoT devices are usually deployed in non-traditional environments, where cellular access may not always be possible, and thus, a device-to-device (D2D) direct communication ability is significant. For instance, drones need direct communication for data exchange between other drones and/or road-side units (RSU). The LTE Advanced/LTE-A, along with 5G, incorporate a D2D communication standard to allow User Equipment (UEs) in the same area to communicate together. This standard is called Proximity-based Services (ProSe) D2D, which provides several features that may be deployed jointly or independent of each other [2].

However, with all the expected data sensing and collection that IoT devices will bring to the future 5G networks, this will also create massive security breaches for malicious attacks. IoT devices, such as drones, are vulnerable to various security threats due to their limited resources. For instance, a malicious drone can act as a legitimate relay or a gateway to a set of drones and collect critical data from those drones. Therefore, drone security mechanisms during D2D communication need to be carefully designed to meet the application requirements and ensures safe communication. While there exists some recent research work for addressing the drone security challenges, these approaches are mainly designed for ad-hoc wireless networks, which would bring additional messages and overhead to the cellular network core [3], [4], [5]. On the other hand, the LTE-A ProSe services have their own customized security standards and a full key exchange protocol to secure D2D communication [2]. However, this standard does not apply to newly developed 5G ProSe. Its security extensions are still under development, which opens a wide area for research and contribution. It is important to note that even if the existing 4G ProSe security solution is adapted to the 5G network, there will still be high traffic toward the core network. Because of the 4G ProSe continuous access to the key management function server within the core network.

In this paper, we target the security challenges aforementioned in such a way that conjunct into the 5G D2D ProSe standard. One of the most popular IoT devices that can utilize 5G services are drones, wherefore, we customize our solution in the drone application context. Nevertheless, our model can also apply to other IoT devices in different domains, such as medical and vehicular networks. We assume having a swarm-of-drones where only one of them is within the cellular coverage (i.e., acting as a data relay) and others establish D2D links with this leader drone. The leader drone acts as a UE-to-Network Relay between the 5G core network and all other drones in the swarm. We propose mutual authentication of leader drone and others in the swarm. Given the resource limitations of drones, it is substantial that we provide an efficient and lightweight solution for scalability purposes.

As opposed to following an approach similar to 4G ProSe security standards where there is a requirement to have access to the network core, we opt for a solution that will minimize the message exchanges among the drones and the core network. To achieve the above objectives, we propose a delegation-based authentication using *proxy signatures*. A proxy signature enables a party to delegate its authentication

credentials to other parties while still providing the same security services as digital signatures (i.e., source authentication and message integrity). Specifically, the proxy signer signs a message using a secret key of the original signer and its own private key [6], [7]. Our solution is similar to the existing OpenID [8] type authentication mechanisms. In the sense that they rely on an OpenID server, which issues identities to be presented as evidence (i.e., like a proxy signature) for authentication. However, we do not want to access this server each time, in our case, since we would like to minimize the number of messages.

Therefore, after the mandatory 5G registration phase, we add a delegation phase, in which we assign a delegation warrant and proxy parameters. Those delegation parameters are used to derive the proxy signature keys for the authentication process. Then, we follow the existing ProSe device discovery model where a drone detects other drones in the network for D2D communication. The ProSe discovery model has two options: Model A and Model B. In Model A, a drone announces its existence in the network, wherein in Model B, each drone sends a discovery message to the nearest drones. Our proposed authentication protocol would work for both models. The authentication process is integrated into the discovery phase by attaching a drone's proxy signature and verifying it by the receiving drones.

We assessed our scheme through implementation with the NS-3 5G network simulator under the D2D communication model [9]. For a realistic assessment of computations times for the proxy signature keys, we performed all the computations on a Raspberry-Pi3 IoT device. We also set a baseline comparison to the 4G ProSe security standard. Our results show an overall much lower device authentication delay compared to this baseline.

The rest of the paper is organized as follows. The related works are summarized in Section II. Then, the system and attack models are described in Section III. The proposed authentication scheme is introduced in Section IV. The evaluation and the security analysis are in Section V. Finally, concluding remarks are provided in Section VI.

II. Related Work

In this section, we summarize the literature for drone and cellular D2D authentication. Several works attempted to develop practical and effective solutions for drone authentication in wireless networks. For instance, in [10], the authors propose a lightweight authentication scheme for the internet of drones deployment utilizing an efficient one-way cryptographic hash function. Other authors employed the elliptic curve certificate (ECC) for a legal drone digital identity proof as in [11]. A survey on variant state-of-the-art solutions to tackle security and privacy challenges in D2D communication spanning across a variety of D2D prospects is provided in [12]. In [13], the authors proposed a new blockchain-based secure framework for data management among a group of drones. Most of those works aforementioned are general-purpose drone authentication for any network and does not apply to our case of D2D communication in 5G.

Finally, in [14], the authors proposed a designated verified proxy blind signature scheme for drone network based on ECC that provides efficient computation. The assumptions and architecture in this work are different from our case and focus solely on computation calculations. Blind proxy signature is a proxy signature mechanism designed to maintain user privacy, and hence, it only has the original signer signature and not the delegated/proxy signer itself. A powerful device authentication proxy signature should have information about the proxy signer along with the original signer.

III. Preliminaries

A. System Model

We assume a drone-to-drone communication model under a 5G cellular infrastructure network. The drones can communicate directly through D2D communication. Moreover, all drones are initially registered as UE devices through the Security Anchor Function (SEAF)/Access & Mobility Management Function (AMF) in the network core for proper cellular communication. Hence, the primary 5G authentication protocols are executed for all the drones before any communication attempts throughout the network. One of the drones, *leader drone*, will act as a *UE-to-Network relay* to the 5G core network. The described communication model for the proposed 5G D2D drone communication is in Fig. 1. Each drone i is assumed to have a pair of public and private asymmetric keys: y_i and x_i respectively.

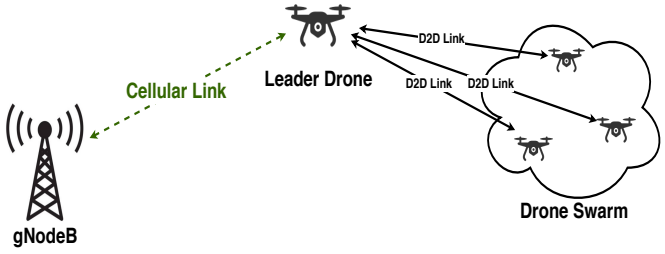

Fig. 1. Assumed drone communication model.

B. Background on Proxy Signatures

We utilize Kim, Park and Won's proxy signature scheme [15], where a proxy key pair depends on the signer private key for authentic information on the proxy signer's identity. Hence, in this model, the proxy signer's identity is protected using the node's authentic key pair (x_i, y_i). This is considered a strong proxy signature since it represents both original signer's in the form of a *warrant* w_i and proxy signer's signatures (i.e., the node's private-public key pair (x_i, y_i)). Once a proxy signer creates a valid proxy signature, no one can ever repudiate his/her signature.

To further elaborate on this scheme, let the 5G core network (i.e., the original signer) be node A and the under authentication drone (i.e., the proxy signer) be node B. First, node A generates a random number K_A from a g generator of multiplicative subgroup Z_q^* with order of large prime q,

and hence, $K_A \in Z_q^*$. Then, node A computes two proxy parameters $r_A = g^{K_A}$ and $s_A = x_A h(m_w w, r_A) + K_A$, where x_A is A's private key, $h()$ is a collision resistant hash function and m_w is A's signed warrant. The tuple (r_A, s_A) is A's signature for m_w, where (m_w, r_A, s_A) has to be sent secretly to node B. Next, once node B verifies the received tuple as $g^{s_A} \stackrel{?}{=} y_A^{h(m_w w, r_A)} r_A$, it then generates the proxy signature keys as follows:

$$\begin{aligned} x_p &= s_A + h(m_w, r_A) x_B \\ y_p &= (y_A y_B)^{h(m_w, r_A)} r_A \end{aligned} \tag{1}$$

This means, Node B can authenticate itself to other nodes on behalf of the original signer A using the proxy signature keys x_p and y_p.

C. Background on 5G ProSe Standard

4G and 5G Cellular networks allow UEs to establish independent D2D connections for data exchange. For 4G and 5G networks the current D2D standard is 3GPP ProSe standards (TS 33.303) [2] and (TR 23.752) [16], respectively. The ProSe is a D2D standard allowing LTE/5G devices to detect each other and to communicate directly. The ProSe standard comprises the ProSe discovery and the ProSe Direct Communication, which enables establish communication paths between two or more ProSe-enabled UEs. The 5G (TR 23.752) ProSe [16] defines the following functions for D2D communication:

- **5G ProSe Direct Discovery**: A procedure employed by a ProSe-enabled UE to discover other ProSe-enabled UEs in its vicinity by using only the capabilities of the two UEs with New Radio (NR) technology.
- **5G ProSe UE-to-Network Relay**: A UE that provides functionality to support connectivity to the network for Remote UE(s). Based on our network model, we focus on this case, as shown in Fig. 1, where the leader drone represents the UE-to-Network relay. However, our approach can also work for the Direct Discovery mode.

The current 3GPP ProSe standards (TS 33.303) under the 4G ProSe [2], includes the ability to use a UE node as a UE-network relay as well as connection establishment with it requires an in-advance key exchange process. The nodes which will use ProSe services first needs to register with ProSe Function and then make a *Key Request* to ProSe Key Management Function (PKMF), both of which are unique units residing within the 4G core [2]. PKMF will issue a symmetric key with an ID (i.e., PKUK ID). Similarly, when a node acting as UE-network relay is contacted by a remote UE, it will need to make another *Key Request* to the PKMF for getting the same symmetric key corresponding to the PKUK ID. Hence, both nodes will agree on the same symmetric key and can move on to authenticate each other. Although the security mechanism for the ProSe is well defined for 4G/LTE, there is still no finalized security standard for the 5G standard yet [16].

D. Attack Model

We assume the following threats to the drones:

1) *Malicious Leader Drone*: A malicious drone can broadcast messages to other drones claiming to be a UE-network relay for them. In such cases, private data is collected from the drones.
2) *Replay Attack*: A malicious drone sniffs the communication between other legitimate drones to maliciously transmit a repeated or delayed signature to verify itself to the leader drone.

IV. Drone Authentication Protocol in 5G ProSe

A. Motivation and Overview

As described under the ProSe security standard, the authentication solution is time-consuming and introduces additional message overhead. The ProSe security standard further requires maintaining the state information about all the keys. As a result, following a similar approach will not be useful to IoT devices, which require a fast and scalable authentication mechanism. Therefore, in this paper, we propose a new model for the 5G standard, with no pre-messaging to sustain IoT devices that may be resource-constrained, such as drones.

In this way, we also minimize the message count to ensure scalability for the 5G Core and support an increased number of nodes.

Specifically, we propose a proxy signature-based device authentication where the leader drone first authenticates itself to the swarm of drones by only broadcasting a proxy signature. Hence, other drones in the swarm initiate the authentication to this leader drone by using a similar proxy signature to be ready for communication, as shown in Fig. 2. In both cases, the original signer of these proxy signatures is the 5G Core (i.e., the elements that will replace PKMF in 4G). Therefore, we allow the nodes to authenticate themselves to the PKMF existing within 4G through the leader drone. We provide the details of this process in the next subsections.

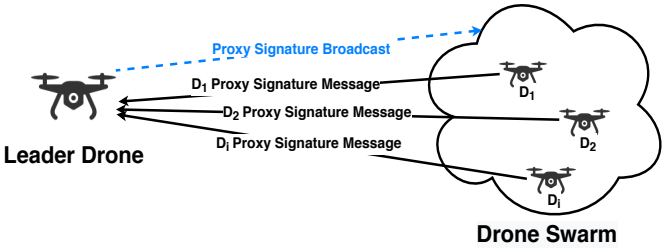

Fig. 2. Drones authentication messages.

B. Registration and Delegation Phase

After the drones are registered and authenticated through 5G authentication services (i.e., 5G-AKA [17] mechanism), they are checked against their digital drone IDs to initiate a delegation phase for D2D communication. A specific slice function is triggered based on the drone IDs kept in a list by the network function operator. In the delegation phase, all these drones receive the needed parameters for the proxy signature creation. Those parameters are fetched from a specific server

named Authentication Authorization and Access server (AAA-S) in the 5G core network, as shown in Fig. 3.

Let us assume that AAA-S has a private-public key pair (x_c, y_c). The proxy signature keys are created for a drone D_i by first generating a random number as a seed for the proxy signature parameters. The details of this process are as follows:

- Let g be a generator of a multiplicative subgroup of Z_p^* with order p. Then a random number $k_i \in_R Z_p^*$ is selected from this set.
- The proxy signature parameters are generated as follows:

$$\begin{aligned} r_i &= g^{k_i}, \\ s_i &= x_c h(w_i, r_i) + k_i, \end{aligned} \tag{2}$$

  where, $h()$ is a collision resistant hash function. In addition, as part of this proxy signature, the AAA-S creates a unique *warrant* w_i for each drone D_i, as follows:

$$w_i = \mathbf{S}(r_i, s_i), \tag{3}$$

  where **S()** is any digital signature function. Note that this warrant is specific to drone D_i as it uses the (r_i, s_i).
- Then, the delegation parameters (i.e., the proxy parameters, the warrant, and the core network public key) are sent securely to the drone D_i as a tuple of (w_i, r_i, s_i, y_c). We use the K_{SEAF} key produced during the 5G primary authentication for this encrypted communication.
- The leader drone D_l that will act as a UE-to-Network relay receives a similar uniquely created tuple of (w_l, r_l, s_l, y_c).

C. Discovery and Device Authentication Phase

The next phase after the registration and delegation phases is the discovery phase, where the drones can search for the other available UE-to-Network relay drones for D2D connection. This phase is done through the ProSe standard in the cellular network. The second part of Fig. 3 shows the 5G ProSe D2D discovery process. The ProSe standard has two models of discovery: Model A and Model B. In Model A, the UE-network relay announces its presence, while in Model B, the UE/drone sends a discovery message to the nearest nodes. Our proposed authentication protocol would work for both models. In discovery messages for both models, each drone (leader or not) attaches the proxy signature. Anyone who replies will attach its proxy signature as well. We explain this protocol in two parts below:

1) Leader Drone Authentication: The leader drone message exchange for the proposed proxy signature authentication protocol is shown in Fig. 3 under the leader drone authentication phase.

- The leader drone D_l creates the proxy signature keys, (xp_l, yp_l), using the delegation parameters as follows:

$$\begin{aligned} xp_l &= s_l + h(w_l, r_l) x_l \\ yp_l &= (y_c y_l)^{h(w_l, r_l)} r_l \end{aligned} \tag{4}$$

- The leader drone then creates the following signature:

$$\sigma_l = \mathbf{S}(t_l, xp_l). \tag{5}$$

  where t_l is a timestamp nonce using its private key xp_l. Note that since xp_l is only known by D_l, the proxy signature can be only created by a legitimate D_l.
- The leader drone D_l broadcasts this proxy signature (blue doted message in Fig. 3) that contains the following tuple:

$$(t_l, \sigma_l, w_l, yp_l, y_l)$$

- Then, each drone D_i in the swarm receives the proxy signature and verifies the leader's proxy signature as follows:

$$\mathbf{V}(t_l, \sigma_l, (y_c y_l)^{h(w_l, y_l)} yp_i) \stackrel{?}{=} True, \tag{6}$$

  where **V()** is a digital signature verification algorithm.

2) Swarm Drones Proxy Signature-based Authentication: Next, in response to the leader's broadcast signature, the swarm drones send a reply to be authenticated to the leader drone. The swarm drones authentication to the leader drone is shown in Fig. 3 under the swarm drone authentication phase.

- Initially, each drone D_i creates the proxy signature keys, (xp_i, yp_i), using the delegation parameters as follows:

$$\begin{aligned} xp_i &= s_i + h(w_i, r_i) x_i, \\ yp_i &= (y_c y_i)^{h(w_i, r_i)} r_i. \end{aligned} \tag{7}$$

- Next, each drone prepares a signed nonce with its proxy private key, xp_i as follows:

$$\sigma_i = \mathbf{S}(t_i, xp_i). \tag{8}$$

- Next, after receiving the leaders broadcast message, the drone D_i then sends the proxy signature message that contains the following tuple: $(t_i, \sigma_i, w_i, yp_i, y_i)$ in its reply.
- Then, the leader drone D_l verifies this proxy signature, as follows:

$$\mathbf{V}(t_i, \sigma_i, (y_c y_i)^{h(w_i, y_i)} yp_i) \stackrel{?}{=} True, \tag{9}$$

  where **V()** is a digital signature verification algorithm.

Since both the leader drone and the drones in the swarm are already mutually authenticated, they can start message communication securely. The leader drone can create a symmetric key and send it to the other drones using its private key, to be used for message encryption, authentication, and integrity. We do not discuss these details as message authentication is beyond our scope.

D. Proxy key Revocation

Whenever asymmetric keys are used, there is a need for a key revocation mechanism if they are compromised. Revocation is the declaration for the existing proxy signature keys as obsolete (i.e., not valid anymore). We propose that the AAA-s in the core network can revoke y_p, which is the public proxy signature of a proxy drone B. Simultaneously

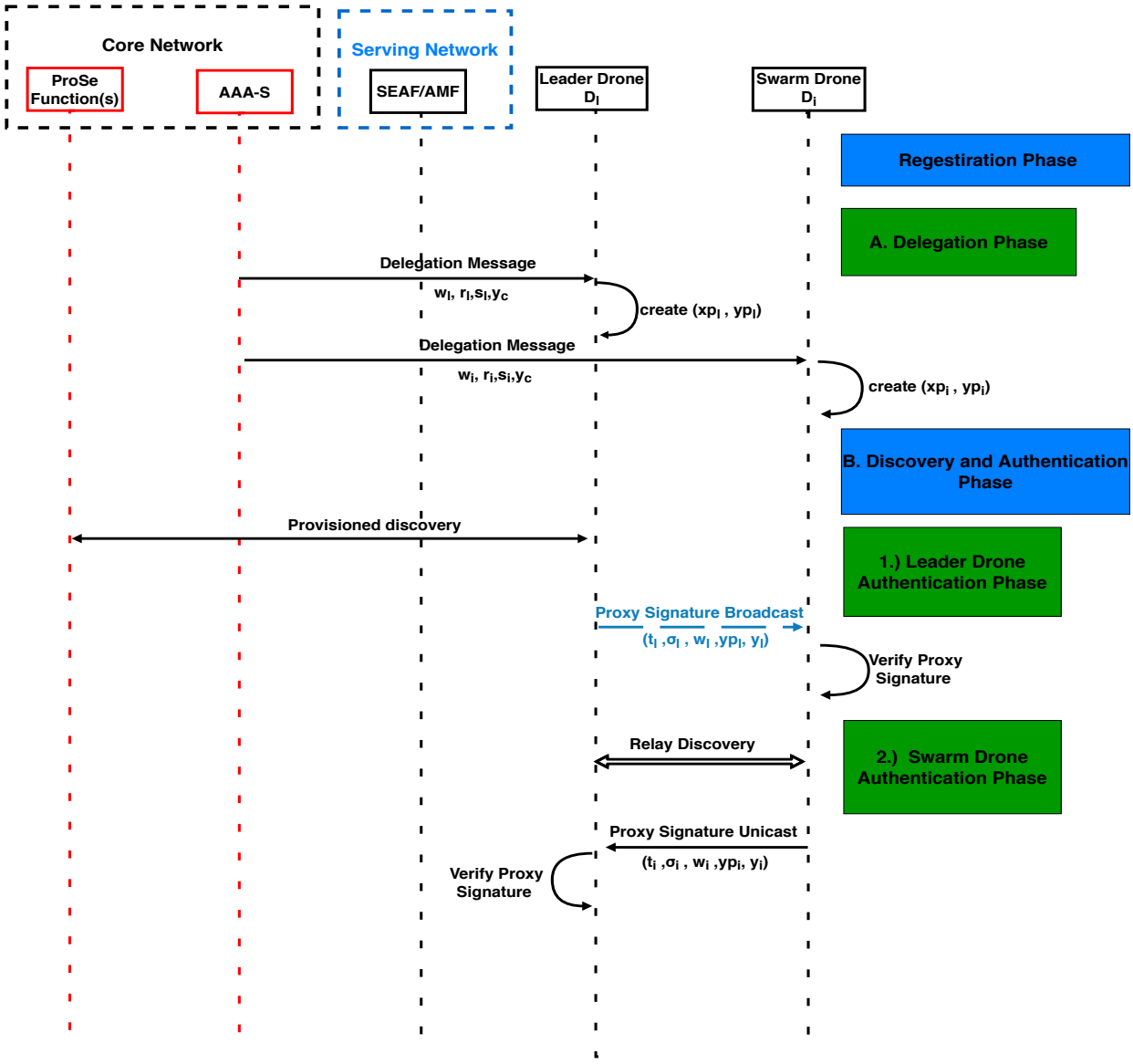

Fig. 3. Proxy Signature exchange messages within 5G Core and the involved drones.

as the leader drone verifying the proxy signature of B using its public proxy key y_p, it will also check whether this key is in a proxy revocation list. This revocation process is similar to the case of certificate revocation lists (CRLs) [18] in usual public-key systems.

V. Security and Performance Analysis

In this section, we first discuss the proposed scheme security analysis and then present the evaluation results to demonstrate our proposed scheme effectiveness.

A. Security Analysis

Here, we introduce how our authentication protocol address the attacks mentioned in Section III-D.

1) *Malicious Leader Drone*: Our proposed D2D drone authentication utilizes information distributed by the core network itself through delegation. Hence, to join the network, a legitimate leader drone D_l needs to show its valid and unique pair of proxy keys. The proxy keys are created based on the unique delegation parameters, r_l and s_l, given by the SEAF/AMF serving network to the drone D_l. Moreover, a malicious leader drone D_m needs to broadcast a proxy signature message that can be verified using the D_m's proxy public key. However, since the delegation phase is held securely before the drones' release to its location, D_m will fail to create its pair of the proxy keys since it does not have the unique delegation parameters.
2) *Malicious Swarm Drone*: Similar to leader drone, a legitimate swarm drone D_i will need to show that it has a valid and unique pair of proxy keys. Such proxy keys are created based on unique delegation parameters, r_i and s_i,

given by the SEAF/AMF serving network specifically to the drone D_i. As this will not be possible with a malicious drone, it will fail to authenticate itself to the leader drone.

3) *Replay Attack*: The protocol is also resilient against any replay or integrity attacks. Any adversary D_m that tries to impersonate a legitimate drone in the swarm D_i by performing a *replay attack* where it replays a captured message from D_i either for joining the network or claiming to be the leader drone. In both cases, D_m broadcasts the whole proxy signature of drone D_i, $(t_i, \sigma_i, w_i, yp_i, y_i)$. Let us assume a verifier node receives this broadcast for the first time. This proxy signature will not pass the verification using Eq. 9 due to stale timestamp value in the message. Similarly, for replay attack of the leader drone broadcast message, the signature will not pass the verification at Eq. 6 in the same manner.

B. Experiment Setup

We simulated the proposed approach using the ns-3 5G network simulator, which has recently implemented 5G RAN module [19]. We also utilized the D2D implementation in [9] for a node to node communication between drones. We created 2 UE nodes representing the leader drone and one swarm drone, respectively. For our experiment, we added a server node representing the AAA-S for the proxy authentication computation. We selected Model A, where the leader announces itself first, then the others join. We also assume that the proxy signature parameters are pre-installed to the nodes. The system parameters for the NS-3 simulation used in the experiments are listed in Table I. We further used a Raspberry-Pi3 IoT device to mimic the drone's behavior for complexity convenience and realistic assessment.

TABLE I
SIMULATION PARAMETERS

Parameter	Value
Packet size	56 Byte
Data rate	30 Mb/sec
gNodeB distance	300 m
drone to drone distance	150 m
K_{SEAF} size	256 bit
Proxy Signature Hash Function	SipHash [20]

C. Metrics and Baselines

To assess the proposed authentication mechanism overhead, we consider the *total authentication time*, which includes all the communication and computation delays during the authentication process.

Moreover, as a baseline comparison to our proposed D2D authentication mechanism, we use the 4G ProSe D2D security as a centralized authentication model.

D. Performance Results

1) Drone Computational Overhead: The drones computational delay experienced through the proxy signature authentication are listed in Table II. As seen, the total processing delay for our proposed drone D2D authentication is 2.012 msec, which includes all the proxy signature parameters and keys calculations. These results indicate that the computational complexity is almost negligible.

TABLE II
COMPUTATIONAL OVERHEAD

Operation	Delay (msec)
SipHash Function	0.13
Proxy Private Key Creation xp_i&xp_l	1.02
Proxy Public Key Creation yp_i& yp_l	0.992
Total	**2.012**

2) Communication Delay: The communication delays experienced between the drones are listed in Table III. The total delay for the proposed proxy signature authentication communication delay is 6.35 msec. Hence, the total delay for the proposed authentication mechanism after adding the computation delay is 8.362 msec. In comparison, the ProSe mechanism with a total authentication time of 12.46 msec, while our proposed authentication mechanism is almost 33% faster. The reason for this delay is due to the 4G-based ProSe connection to the core network.

TABLE III
COMMUNICATION OVERHEAD

Approach	Connection	Delay(msec)
Proxy Signature	Discovery Phase	2.32
Proxy Signature	D2D Message Exchange	4.03
Proxy Signature	**Total Communication Delay**	**6.35**
4G-based ProSe	**Total Communication Delay**	**12.46**

3) Impact of Background Traffic Delay: We further investigate the impact of background traffic from other existing communication to the leader drone during the D2D drone authentication. We simulated an uplink and downlink background traffic over the leader drone simultaneously while starting the D2D proxy authentication. The traffic frequency at each background node is set to 1 msec intervals between packet transmissions. As shown in Table IV, the total authentication communication delay based on the background traffic up to 40 nodes is within 0.8 µsec. Hence, under background traffic, the additional delay is negligible, which means no extra delay overhead on the proposed authentication.

TABLE IV
AUTHENTICATION DELAY UNDER VARYING BACKGROUND TRAFFIC

Background Nodes	Delay (msec)
1	6.350012
10	6.350064
20	6.350207
40	6.35089

VI. CONCLUSION

This paper proposed a lightweight, fast, and secure drone authentication scheme for D2D communication under 5G networks. We designed the approach to be integrated easily into

the current D2D ProSe standard. We utilized proxy signatures to replace the need for a direct connection with the core. In this scenario, the nodes are authenticated through the authorized UE-to-Network relay node. We implemented the proposed authentication scheme using the NS-3 5G implementation for D2D communication. The evaluation of the authentication model indicated its efficiency and feasibility over the 4G Standard ProSe scheme.

VII. Acknowledgements

This work is supported by a grant from the Idaho National Lab Wireless Security institute (INL WSI).

References

[1] S. Li, L. Da Xu, and S. Zhao, "5g internet of things: A survey," *Journal of Industrial Information Integration*, vol. 10, pp. 1–9, 2018.

[2] 3GPP support office , "3rd generation partnership project; technical specification group services and system aspects; proximity-based services (ProSe); security aspects," 3GPP TS 33.303 V16.0.0 Technical Specification (Release 16), Tech. Rep., 2020.

[3] M. Wazid, A. K. Das, N. Kumar, A. V. Vasilakos, and J. J. P. C. Rodrigues, "Design and analysis of secure lightweight remote user authentication and key agreement scheme in internet of drones deployment," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 3572–3584, 2019.

[4] L. Teng, M. Jianfeng, F. Pengbin, M. Yue, M. Xindi, Z. Jiawei, C. Gao, and L. Di, "Lightweight security authentication mechanism towards uav networks," in *2019 International Conference on Networking and Network Applications (NaNA)*, 2019, pp. 379–384.

[5] M. Karimibiuki, M. Aibin, Y. Lai, R. Khan, R. Norfield, and A. Hunter, "Drones' face off: Authentication by machine learning in autonomous iot systems," in *2019 IEEE 10th Annual Ubiquitous Computing, Electronics Mobile Communication Conference (UEMCON)*, 2019, pp. 0329–0333.

[6] M. L. Das, A. Saxena, and D. B. Phatak, "Algorithms and approaches of proxy signature: A survey," *arXiv preprint cs/0612098*, 12 2006.

[7] W.-B. Lee and C.-K. Yeh, "A new delegation-based authentication protocol for use in portable communication systems," *IEEE Transactions on Wireless Communications*, vol. 4, no. 1, pp. 57–64, 1 2005.

[8] D. Recordon and D. Reed, "Openid 2.0: a platform for user-centric identity management," in *Proceedings of the second ACM workshop on Digital identity management*, 2006, pp. 11–16.

[9] M. Diouf, "mmWave cellular network simulator," https://github.com/makhtardiouf/d2d, Jun 2017.

[10] M. Wazid, A. K. Das, N. Kumar, A. V. Vasilakos, and J. J. P. C. Rodrigues, "Design and analysis of secure lightweight remote user authentication and key agreement scheme in internet of drones deployment," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 3572–3584, 2019.

[11] L. Teng, M. Jianfeng, F. Pengbin, M. Yue, M. Xindi, Z. Jiawei, C. Gao, and L. Di, "Lightweight security authentication mechanism towards uav networks," in *2019 International Conference on Networking and Network Applications (NaNA)*, 2019, pp. 379–384.

[12] M. Haus, M. Waqas, A. Y. Ding, Y. Li, S. Tarkoma, and J. Ott, "Security and privacy in device-to-device (d2d) communication: A review," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 2, pp. 1054–1079, 2017.

[13] B. Bera, S. Saha, A. K. Das, N. Kumar, P. Lorenz, and M. Alazab, "Blockchain-envisioned secure data delivery and collection scheme for 5g-based iot-enabled internet of drones environment," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 8, pp. 9097–9111, 2020.

[14] L. He, J. Ma, R. Mo, and D. Wei, "Designated verifier proxy blind signature scheme for unmanned aerial vehicle network based on mobile edge computing," *Security and Communication Networks*, vol. 2019, 2019.

[15] B. Lee, H. Kim, and K. Kim, "Strong proxy signature and its applications," in *Proceedings of SCIS*, vol. 2001, 1 2001, pp. 603–608.

[16] G. support office, "3rd generation partnership project; technical specification group services and system aspects; study on system enhancement for proximity based services (ProSe) in the 5G system (5GS)," 3GPP TR 23.752 V0.3.0 Technical Specification (Release 16), Tech. Rep., 2020.

[17] A. Koutsos, "The 5g-aka authentication protocol privacy," in *IEEE European Symposium on Security and Privacy (EuroS P)*, 2019, pp. 464–479.

[18] M. Myers, R. Ankney, A. Malpani, S. Galperin, and C. Adams, "X. 509 internet public key infrastructure online certificate status protocol-ocsp," RFC 2560, Tech. Rep., 1999.

[19] N. Wireless and the University of Padova, "mmWave cellular network simulator," https://apps.nsnam.org/app/mmwave/, Sep 2018.

[20] J.-P. Aumasson and D. J. Bernstein, "Siphash: a fast short-input prf," in *International Conference on Cryptology in India*. Springer, 2012, pp. 489–508.