A Proxy Signature-Based Swarm Drone Authentication With Leader Selection in 5G Networks

MAI A. ABDEL-MALEK, KEMAL AKKAYA, ARUPJYOTI BHUYAN, AND AHMED S. IBRAHIM

1Department of Electrical and Computer Engineering, Florida International University, Miami, FL 33174, USA
2Idaho National Laboratory, INL Wireless Security Institute, Idaho Falls, ID 83415, USA
3Department of Electrical and Computer Engineering, Virginia Tech, Blacksburg, VA 24061, USA

Corresponding author: Ahmed S. Ibrahim (aibrahim@fiu.edu)

ABSTRACT Drones are imperative for the 5G architecture as a mobile source to expand network coverage and support seamless services, particularly through enabling device-to-device (D2D) communication. Such deployment of drones in D2D settings raises various security threats in drone communication. While the existing D2D communication security standard within the 4G cellular architecture may address some of these issues, the standard includes heavy traffic toward the network core servers. If this security standard is to be adopted in the 5G D2D security services with the same traffic load, it may negatively impact the 5G network performance. Therefore, this paper proposes a lightweight proxy signature-based authentication mechanism for a swarm of drones compatible with the 5G D2D standard mechanisms. This paper proposes a distributed delegation-based authentication mechanism to reduce the traffic overhead toward the 5G core network. In this scheme, the legitimate drones are authorized as proxy delegated signers to perform authentication on behalf of the core network. Furthermore, we propose a mechanism to elect and relocate a new leader relay drone from the existing drone swarm. We implemented the proposed authentication algorithm in the 5G D2D-based communication package over NS-3 while performing the computational calculations on a RaspberryPi3 device to mimic the drone calculation process and delays. The performance of the proposed authentication shows a promising reduction in the authentication time and shows lightweight and reliable compatibility.

INDEX TERMS 5G security, authentication, D2D, drones, delegation, proxy signature.

I. INTRODUCTION

The next-generation cellular communication starting with 5G, has a ubiquity architecture, including a vast number of Internet of things (IoT) devices such as drones. Such devices are traditionally deployed in ad hoc mesh networks with limited to no cellular communication capabilities. Accordingly, this structure requires a suitable device-to-device (D2D) direct communication protocol to allow smooth data exchange between such devices (drones) and the cellular network infrastructure such as base stations and roadside units (RSU).

The cellular network structure starting with the LTE Advanced/LTE-A, comprises a D2D communication standard named Proximity-based Services (ProSe) to allow direct communication between User Equipments (UEs). The ProSe standard provides several features that may be deployed jointly or independent of each other [1]. However, this D2D connection can only be between two UEs or devices within 5G/LTE coverage. Since drones act as base stations or relays with no data of their own, they do not fall under D2D. Hence, the need for multi-hop communication to extend their coverage further, and then, a leader/co-leader drone with direct communication to the 5G base station needs to exist.

Nevertheless, drone deployment raises various security threats, which can go unnoticed and thus underexplored by focusing on the 5G network’s performance aspects. As limited resources devices, drones are exposed to several security threats due to limited processing capabilities and hence low-security measurements. Accordingly, drones pose an adequate target for various malicious attacks. Those security threats increase the need for authentication and security
mechanisms that can adequately eliminate suspicious drones. Recent research works tackle drone security aspects that are merely designed for ad hoc mesh networks [2], [3], which, if applied to the cellular network structure, will add to the cellular network overhead burden. Fortunately, the newly added D2D ProSe services have a designated security mechanism with a full key exchange protocol [1]. Nevertheless, the ProSe security extension for the 5G standard remains undergoing development, which unfolds enormous research opportunities. Moreover, the existing 4G ProSe security solution involves extensive communication toward the core network, which is not desirable with the 5G network dynamicity.

In this work, we propose a lightweight, stand-alone security mechanism for IoT devices represented by drones to be deployed along with the 5G ProSe standard with no extra overhead to the core network. We assume a swarm of drones within the 5G cellular network, where a leader drone from the swarm is responsible for the communication between the rest of the swarm drones and the 5G core network by acting as a UE-to-Network Relay. We further assume a co-leader drone to temporarily perform the leader drone’s responsibilities in case of an unresponsive leader drone and until assigning a new leader drone. Given the resource limitations of drones, we propose a lightweight, reliable, and efficient mechanism that serves scalability purposes.

We propose an authentication mechanism that opts for a delegation solution that maintains a minimum communication overhead toward the core network. We further tackle drone communication reliability by providing a replacement procedure for leader drone failure. The proposed authentication mechanism is based on proxy signature delegation, where the core network delegates the leader drone as its proxy signer to execute authentication between drones. A proxy signature enables an original signer (i.e., Core network) to delegate its authentication credentials to a proxy signer (i.e., drones) to provide services on its behalf [4], [5].

We propose adding a delegation phase right after the 5G registration phase. The delegation warrant and related keys are prepared and assigned to the drones to derive their unique proxy signature. The next step follows the ProSe device discovery stage, where drones detect each other and form a D2D network. The ProSe discovery has two models, A and 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 proxy signature authentication process is integrated into the ProSe discovery phase, compatible with Models A and B.

Moreover, we propose a distributed election-based leader drone selection mechanism for updating and relocating a new leader drone if failed or compromised. The swarm drones select the most eligible drone in the swarm to replace the failed leader drone based on its location and power consumption pattern. We assessed our scheme through both security and performance analysis. We present a security analysis and a revocation mechanism for the proposed proxy signature authentication mechanism if they are compromised. We then demonstrate our authentication scheme efficiency by implementing it on the NS-3 5G network simulator with the cellular D2D library [6]. The computations calculations are performed on a Raspberry-Pi IoT device for realistic drone processing assessment. Moreover, we select the 4G ProSe security standard for comparison purposes as a comparison baseline. Our proposed authentication scheme shows an overall better performance with a low authentication delay and better scalability than the baseline.

Our contributions in this paper can be summarized as follows,

- We propose a drones’ D2D authentication mechanism that can be integrated within the 5G D2D ProSe discovery phase.
- We propose a new distributed mechanism to update and relocate a new leader drone in case of failure or compromise without interrupting the swarm drone communication.
- We implemented and tested in a realistic 5G architecture environment.

It is worth noting that our work here is a continuation of our previous work in [7], where we proposed a proxy signature-based authentication for drones’ secure D2D communication compatible with the 5G D2D ProSe standard mechanisms. In our previous work, we only assumed Model A for ProSe discovery for our experiments, and there was no procedure for replacing a compromised leader drone.

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 IV. The proposed authentication scheme is introduced in Section V. The evaluation and the security analysis are in Section VII. Finally, concluding remarks are provided in Section VIII.

II. RELATED WORK
This section summarizes the literature for drone and cellular D2D authentication.

III. DRONES AUTHENTICATION
A. DEVICE AUTHENTICATION
Since drone deployment increases security risks, recent research aims to design lightweight authentication protocols that do not burden the drones. For instance, in [3], the authors proposed an Elliptic Curve Cryptography (ECC)-based device identity proofing mechanism for drone authentication. In [8], an authentication mechanism based on Machine Learning (ML) algorithms for autonomous IoT systems. In [9], the authors proposed a lightweight key-based mutual authentication between anonymous UAVs through the shared ground station. The authors in [10] presented an adaptation of 2 authentication strategies for wireless sensor networks (WSN), one is a key agreement authentication, and the second is an ECC-based privacy-aware two-factor authentication protocol. Those aforementioned approaches can add undesirable traffic toward the 5G core network traffic. For a 5G-UAV enabled system, a cross-domain block
chain-assisted authentication using a multi-signature contract is proposed in [11].

Therefore, some new direction in drone authentication is delegation-based digital signature algorithms, such as the proxy signature algorithm. There have been multiple works that recite different proxy signature approaches for various purposes [12]–[14]. For instance, in [15], the authors proposed a blind ID-based partial delegation with warrant proxy signature is proposed to provide the anonymity of users. Also, in [16], the authors proposed an ECC-based proxy blind signature for drone networks. The blind-ID-based proxy signature does not have any information about the drone ID as a delegated signer to maintain anonymity. Nevertheless, this algorithm does not fit our authentication purposes and can lead to malicious drone attacks. Moreover, a robust proxy signature algorithm should have information about the proxy signer as much as it has for the original signer. Thus, in [17], a short certificate-based proxy signature is proposed with a low computational cost to overcome the integrity attacks on vehicular networks. Also, in [18], the authors proposed a new scheme to mitigate partial attacks not considered by the identity-based proxy signature. Our proposed authentication here utilizes the certificate-based proxy signature in Kim, Park, and Won’s proxy signature scheme [19]. In our proposed model, we propose employing the proxy signature concept for a unique Drone-enabled 5G network scenario as a lightweight solution for required mutual authentication. In particular, we propose a drones’ D2D authentication mechanism that can be integrated within the 5G D2D ProSe discovery phase. Our contribution in this work arises from the Drone-enabled 5G network setup and the integration of the concept within the current 5G ProSe standard. This work is also related to our previous work in [20], we proposed a proxy signature-based device authentication for drones in post-disaster situations.

B. D2D AUTHENTICATION

A survey on variant state-of-the-art solutions to tackle security and privacy challenges in D2D communication spanning a variety of D2D prospects is provided in [21]. An overview of the benefits of intelligent D2D communication in the IoT ecosystem is presented in [22], where the authors focused on the routing state-of-the-art. Algorithms can achieve intelligent D2D communication in the IoT. In [23], the authors proposed a new blockchain-based secure framework for data management among a group of drones. In [24], the authors proposed a Body Area Network Device-to-device Authentication using Natural gAit (BANDANA). The BANDANA algorithm enables secure spontaneous pairing of devices worn on the same body. In [25], the authors proposed propose new D2D authentication protocols with a secure initial key establishment using ciphertext-policy attribute-based encryption (CP-ABE). In [26], the authors proposed a secure and robust ECC-based multi-server authentication framework using a Physically Unclonable Function (PUF) for D2D communication. A novel multichannel authentication for the autonomous D2D using optical camera communication (OCC) was proposed in [27] to leverage the limited reachability of OCC for ensuring security. The proposed scheme in [27] executes the Diffie-Hellman key exchange in an OCC channel, which is an optical link between a light source such as an LED light and a camera. Moreover, the recent D2D authentication research direction is based on blockchain smart contracts. Blockchains allow data to be stored based on integrity checks using various cryptographic techniques and achieving a consensus and tempering-proof data content. In [28], the authors designed a smart contract-based blockchain-envisioned authenticated key agreement mechanism for IoT-enabled devices. Most of those works aforementioned are general-purpose drone authentication for any network and do not apply to our case of D2D communication in 5G. The authors in [29] proposed a lightweight elliptic-Elliptic-curve-based authentication scheme using PKI (FHEEP) in D2D communication. In [30], the authors investigated the direct D2D communications between user equipments in the LTE-advanced cellular networks. A quick and safe handover authentication scheme to D2D out-band controlled communication mobility situations in the 5G-WLAN heterogeneous networks were presented in [31]. Also, [32] introduced a blockchain-based architecture for 5G-enabled drone communications.

C. LEADER NODE SELECTION

Many wireless communication applications require a leader node selection process to help with the communication hierarchy [33]–[35]. In [34], [35] the election algorithms depend on extrema finding algorithms that elect a node with the maximum identifier from among a set of candidate nodes. In [36], the authors proposed a population protocol for leader election using polylogarithmic memory states per node. In [37], the authors proposed a low complexity message optimal algorithm for the problem of leader election in the presence of intermittent link failures. In [38], the authors present a framework for selecting a set of leader agents to minimize the system’s convergence time. Also, in [39] and [40], the authors presented an optimization problem for finding the set of leaders that maximizes network coherence and ensures coverage for a leader-follower consensus system. Moreover, to minimize the mean-square deviation from consensus, the authors in [41] developed an efficient algorithm for selecting leaders in large, stochastically forced consensus networks. To address the leader selection algorithm for routing protocols in WSN, the authors in [42] proposed a leader selection algorithm to enhance the network lifetime to a greater extent. A systematic communication model to control the UAV-swarm using a master-slave network architecture and select the UAV leader dynamically is proposed in [43].

IV. PRELIMINARIES

A. 5G PROSE STANDARD

Both 4G and 5G cellular standards have a D2D communication mode that allows UEs to form a D2D network for
direct communication purposes. The current D2D standards for 4G and 5G are 3GPP ProSe standards (TS 33.303) [1] and (TR 23.752) [44], respectively. ProSe standard allows 4G/5G devices to detect each other and communicate directly. Moreover, the ProSe standard involves ProSe discovery and ProSe direct communication modes for two or more ProSe-enabled UEs. The 5G (TR 23.752) ProSe [44] 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. The ProSe standard has two models of discovery: Model A and Model B. In Fig. 1(a) Model A, the UE-network relay announces its presence, while in Fig. 1(b) Model B, the UE/drone sends a discovery message to the nearest nodes.

- **5G ProSe UE-to-Network Relay**: A UE that provides functionality to support connectivity to the network for Remote UEs. Based on our network model, we focus on this case, where the leader drone represents the UE-to-Network relay (shown in Fig. 2). However, our approach can also work for the Direct Discovery mode.

The current 4G ProSe security standard [1] allows the ProSe-enabled UEs to create the D2D communication with one or more UE functioning as a UE-network relay for other ProSe-enabled UEs. Any UE desires to use the ProSe services have to be registered to the ProSe Function and then acquire a Key Request to ProSe Key Management Function (PKMF) residing within the 4G core, which issues a symmetric key with an ID (i.e., PKUK ID). Therefore, all ProSe-enabled UEs 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, there is still no finalized security standard for the 5G standard yet [44].

## B. PROXY SIGNATURES

In this work, we rely on Kim, Park, and Won’s (KPW) proxy signature scheme [19]. The KPW model is a warrant-based proxy signature where the proxy key pair depends on the proxy signer’s private key. Therefore, the proxy signer’s identity is protected using the node’s authentic key pair \((x_i, y_i)\). The KPW is considered a robust proxy signature model since it identifies both the original signer’s identity through a warrant \(w_i\) signed by its private key and the proxy signer’s identity through its private key. Once a proxy signer creates its unique proxy signature, it can never repudiate his/her signature as no other node can replicate it.

The proxy signature mechanism allows a Node B to authenticate itself to other nodes on behalf of the original signer A using the proxy signature keys \(x_p\) and \(y_p\). 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 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 \(s_A = x_A h(m_w, r_A) + K_A\), 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 \(g^{s_A} = y_A h(m_w, r_A) r_A\), it then generates the proxy signature keys as follows:

\[
\begin{align*}
    x_p &= s_A + h(m_w, r_A) x_B \\
    y_p &= (y_A y_B)^{h(m_w, r_A)} r_A
\end{align*}
\]  

## C. SYSTEM MODEL

For our system model, we consider a 5G cellular network with drones connected as UEs through the 5G Authentication procedure (EAP-AKA or EAP TLS). Hence, all drones are initially registered as UE devices through the Security Anchor Function (SEAF)/Access & Mobility Management Function (AMF) in the 5G core network. All the drones have a unique digital identity (DID) enforced by the Federal Aviation Administration (FAA) [45]. We further assume that drones communicate directly through D2D communication by activating the ProSe services. We further assume that one of the drones is recognized as a leader drone, which will perform as a UE-to-Network relay. The described communication model for the proposed 5G D2D drone communication is presented in Fig. 3, where each drone \(i\) is assumed to have a pair of public and private asymmetric keys: \(y_i\) and \(x_i\) respectively.

## D. ATTACK MODEL

We assume the following threats to the drones:

1. **Malicious Leader/swarm Drone**: We consider a malicious drone that broadcasts messages to other drones claiming to be a UE-network relay for them to collect private data.
2. **Replay Attack**: We consider a malicious drone spoofing the communication between legitimate drones to maliciously transmit a repeated or delayed signature to verify itself to the leader drone.
3. **Message Integrity and Modification Attack**: We consider a MiTM node attempts to alter the authentication message or compromise its content.

## V. DRONE AUTHENTICATION PROTOCOL IN 5G PROSE

The 4G ProSe security standard procedure can be time-consuming and introduce additional message overhead, especially with the massive number of devices expected with the 5G network. Therefore, we propose a new lightweight security model for drone authentication over the 5G ProSe services that will not add additional message exchange load. Our proposed authentication procedure minimizes the number of exchange messages with the 5G core network.

Specifically, we propose a proxy signature-based device authentication where the drones are authorized from the core network by delegation to identify each other. The leader
drone first broadcasts its unique proxy signature, then other drones, who wish to join the swarm, reply with their proxy signature, as shown in Fig. 4. In all those authentication messages, the original signer is the 5G core network (i.e., the elements that will replace PKMF in 4G) without the actual need to exchange messages upon each new drone attachment. We provide the details of this process in the following subsections.

### A. REGISTRATION AND DELEGATION PHASE

The drones, as a part of the 5G network, are registered and then authenticated through the 5G-AKA authentication [46]. Then, the drones’ digital IDs are validated, and the proposed delegation phase is initiated for the D2D communication. A specific slice function designated for drone authentication is triggered when a device with a drone ID is registered to the network function operator. The delegation phase in our proposed authentication algorithm is where all the authorized drones are provided with the delegation parameters for creating the proxy signature keys. The delegation parameters are acquired from the Authentication Authorization and Access Server (AAA-S) in the 5G core network, as shown in Fig. 5.

As described in Section IV-B, the AAA-S prepares the delegation warrant and its delegation keys for a drone $D_i$, then signs it with its private key $x_c$. The delegation keys are generated as follows,

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

where, $h()$ is a collision resistant hash function. Then, the AAA-S creates a unique warrant $w_i$ for each drone $D_i$ signed

![Figure 1. ProSe direct discovery exchange messages between ProSe enabled UEs.](image)
by the delegation keys \( (r_i, s_i) \), as follows:

\[
w_i = S(r_i, s_i),
\]

where \( S() \) is a digital signature function. Note that this warrant is specific to drone \( D_i \) as it uses the \( (r_i, s_i) \).

The delegation tuple of \( (w_i, r_i, s_i, y_c) \), where \( y_c \) is the AAA-S public key, is sent securely to the drone \( D_i \). Moreover, the leader drone \( D_l \) as a UE-to-Network relay receives a similar delegation tuple of \( (w_l, r_l, s_l, y_c) \), where \( w_l \) is a special warrant indicating the leader duties.

**B. DISCOVERY AND DEVICE AUTHENTICATION PHASE**

The next phase is the drone discovery phase to find other ProSe enabled drones and the leader drone (i.e., UE-to-Network relay) for D2D connection. The second part of Fig. 5(a) and Fig. 5(b) show the 5G ProSe D2D discovery process for Model A and Model B, respectively. Each drone (leader or not) attaches its proxy signature message within the discovery messages for both Model A and Model B. Any ProSe enabled drone receiving the discovery message replies by attaching its own proxy signature. The detailed proxy signature authentication mechanism is explained in the following subsections.

1) LEADER DRONE AUTHENTICATION

The leader drone authentication phase in Fig. 5 shows the detailed message exchange protocol for our proposed proxy signature authentication.

- Based on the delegation tuple, the proxy signature keys for the leader drone are generated as follows,

\[
\begin{align*}
xp_l &= s_l + h(w_l, r_l)x_l, \\
yp_l &= (y_c y_l)^{h(w_l, r_l)} r_l
\end{align*}
\]

(4)

- The leader timestamped proxy signature message is created as follows,

\[
\sigma_l = S(t_l, xp_l),
\]

(5)

where \( t_l \) is a timestamp nonce using its private key \( xp_l \).

- The leader drone \( D_l \) broadcasts this proxy signature (blue dotted message in Fig. 5) 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:

\[
V(t_l, \sigma_l, (y_c y_l)^{h(w_l, r_l)} yp_l) \equiv True,
\]

(6)

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

2) SWARM DRONES PROXY SIGNATURE-BASED AUTHENTICATION

In response to the leader’s broadcasted proxy signature, each ProSe enabled drone in the vicinity replies with its proxy signature message to be authenticated to the leader drone. The swarm drone authentication phase in Fig. 5 shows the authentication message details for any drone in the swarm.

- Any drone \( D_i \) generates its proxy signature keys, as follows,

\[
\begin{align*}
xp_i &= s_i + h(w_i, r_i)x_i, \\
yp_i &= (y_c y_i)^{h(w_i, r_i)} r_i
\end{align*}
\]

(7)

Note that the proxy keys are based on asymmetric keys. There is no shared symmetric key used in this proposed authentication model.
**FIGURE 5.** Proxy signature exchange messages within 5G Core and the involved drones.
Next, each drone prepares a signed nonce with its timestamped proxy private key, \(xp_i\), as follows:

\[
\sigma_i = S(t_i, xp_i)
\]  

(8)

After receiving the leaders broadcast signature message, \(D_l\) then sends its 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:

\[
V(t_i, \sigma_i, (y_i, yp_i))^{h(w_i, y_i)} yp_i = True,
\]  

(9)

where \(V()\) is a digital signature verification algorithm. After both the leader drone and the swarm drones validate each other proxy signature authenticity, the authenticated drones are ready to start the ProSe D2D communication.

### 3) SECURE COMMUNICATION SETUP

In order to start a secure D2D communication, a shared symmetric key \(K_s\) is used. The symmetric key is used to encrypt communication between the drones in the swarm. Then, \(K_s\) will be shared between the drones after the authentication process is done. The symmetric key \(K_s\) is updated periodically to ensure integrity. This key is used for message encryption, authentication, and integrity. We do not discuss these details as message authentication is beyond our scope.

### C. LEADER DRONE REPLACEMENT PROCESS

We propose a backup process to select a new leader drone if the leader drone is compromised or has communication instability, as shown in Fig. 6. The drone compromising detection is based on the received signal strength indicator (RSSI) level for jamming detection, the message delivery time for Man-in-The-Middle (MiTM) attack, and the number of lost messages for Denial-of-Service (DoS) attack [47]. We assume that once all the drones are authenticated, they are trusted. Thus, there will not be any suspicious activity from any of the drones, and therefore, the leader election is only triggered based on unresponsive behavior. The leader drone re-selection process is triggered after a swarm drone fails to connect to the leader drone for a specific period. Then, the detection of the unresponsive behavior is by all swarm drones within the neighborhood. The swarm drone then announces the leader drone’s unresponsive behavior to other drones in the swarm to release the leader drone from leadership responsibilities. Then, for the new leader drone selection, we propose a distributed selection-based replacement process between the drones in the swarm where all the drones participate in the leader drone selection decision. Each swarm drone \(i\) that fits leader drone aspects based on a stability score will announce itself to other swarm drones as a possible leader drone candidate by reusing the ProSe broadcasting discovery message. The stability score (SS) is based on the distance from the leader drone position, proximity, stability, and authenticity record. The SS value is calculated as follows,

\[
SS_i = \alpha BL_i + \gamma D_{i,l} \geq SS_L,
\]  

(10)

where \(\alpha\) and \(\gamma\) are selection percentage parameters depending on network preference. Also, \(BL_i\) and \(D_{i,l}\) are the candidate drone battery level and the distance between the candidate drone \(i\) and the existing leader drone. Also, \(SS_L\) is the stability score threshold for a drone to be a leader drone candidate. Each drone updates this stability value through communication with its neighbors. Once received a broadcast copy from all the \(C\) candidates, each drone processes and compares the SS value for each candidate drone and chooses the drone with the highest score to be the next leader drone \(k\). All the exchange messages between the authenticated drones
FIGURE 7. Leader drone replacement exchange messages.

are encrypted using $K_s$ for integrity purposes. Finally, the next selected leader drone $k$ announces itself as the next leader drone based on the selection operation and then relocates to the leader drone position to resume communication. The detailed exchange message of the proposed model is shown in Fig. 7.

After the leader drone selection process, the authentication process is triggered again for the leader drone to start its rule. The new leader drone is assumed to buffer any packets from other drones in the swarm until reaching the assigned leader position.

VI. SECURITY ANALYSIS
This section discusses the proposed scheme security analysis to demonstrate our proposed scheme’s effectiveness.

A. PROXY KEY REVOCATION
A key revocation procedure exists for any key-based cryptosystem or authentication mechanism to terminate the keys in case of expiration or compromisation. Proxy revocation is the declaration of the proxy signature and the attached warrant to be obsolete and not valid anymore. We propose that the AAA-S in the core network can revoke $y_p$, which is the public proxy key of any proxy drone or a leader drone. Upon the signature validation step, each drone will also check whether the received proxy signature is in a proxy revocation list. This revocation check applies to every drone in the network; hence, both the leader drone and other drones need to check whether the key is revoked or not. The AAA-S can report the revoked drone’s delegation warrant, $w_i$, and private keys to the Certificate Authority (CA) to add it to the CRL list. Then, the certificate ID is designated to report the revoked public-private keys for the compromised drones and append the corresponding delegation warrant to the end of the Certificate ID, CertificateID||$w_i$. However, in this case, the drone cannot communicate in any other network again until obtaining new private keys from the CA.

B. FORMAL SECURITY ANALYSIS
To formally prove the effectiveness of our proposed mutual authentication, we use Burrows, Abadi, and Needham (BAN) logic [49]. The BAN logic is a formal security proof based on the evolution of beliefs of the trusted parties involved in the authentication protocols following the exchanges between the different engaged entities. BAN logic proof provides accurate security analysis and excludes possible attacks for newly introduced authentication protocols based on exchanged messages during the authentication process. In the following subsections, we provide the detailed notations and terms for BAN logic and then provide our proposed authentication formal proof based on BAN logic.

1) BAN LOGIC TERMS AND NOTATIONS
BAN logic defines authentication protocols based on three entities, participants (A and B), keys (K), and messages (X). Based on those terms, the protocol is translated using the following notations and formulas in Table 1. Based on notations in Table 1, the BAN logic defines the following BAN logic postulate rules for authentication schemes’ security reliability proofing.
1) **Message Meaning Rule:** 
\[ A|\equiv A \rceil \hat{X}, A \rceil [X] |\sim 1 \]
2) **Belief Rule:** 
\[ A|\equiv X, A|\equiv Y \]
3) **Jurisdiction Rule:** 
\[ A|\equiv [X], A|\equiv X \]
4) **Freshness Rule:** 
\[ A|\equiv [X], A|\equiv [Y] \]
5) **Nonce Verification Rule:** 
\[ A|\equiv [X], A|\equiv B|\equiv \neg X \]

2) **DRONE AUTHENTICATION PROTOCOL FORMAL SECURITY PROOF**

We start the formal security analysis of our proposed security mechanism by declaring the security goals (SG) of our mechanism as follows,
- **SG1:** \( D_s \equiv D_t \equiv AAA-S. \)
- **SG2:** \( D_s \equiv D_t \equiv AAA-S. \)
- **SG3:** \( D_s \equiv D_t \equiv yp \)
- **SG4:** \( D_s \equiv D_t \equiv yp \)

Moreover, we assume the following BAN logic-based initial assumption,
- **IA1:** \( D_t \equiv AAA - S. \)
- **IA2:** \( D_t \equiv AAA - S \Rightarrow w_1. \)
- **IA3:** \( D_t \equiv AAA - S \Rightarrow w_1. \)
- **IA4:** \( D_t \equiv AAA - S \Rightarrow w_1. \)
- **IA5:** \( D_t \equiv D_t \Rightarrow yp. \)
- **IA6:** \( D_t \equiv D_t \Rightarrow yp. \)

Then, we can write our proposed authentication messages in the BAN logic form as follows,

We first start by the leader drone authentication analysis, BLM1: \( D_t \leftarrow (t, \sigma_i, yp), \sigma_i = S(t, xp_i) \) (Eq. 5). Then, based on the initial assumption IA1, IA2, and the BAN message meaning rule, we get the following:

- **BLM2:** \( D_s \equiv D_t \sim \sigma_i. \)
  By applying the BAN freshness rule, we get BLM3.
- **BLM3:** \( D_s \equiv D_t \equiv \sigma_i. \) Applying the BAN jurisdiction rule, we get BLM4.
- **BLM4:** \( D_s \equiv \sigma_i. \) Next, we apply the Nonce verification rule to get BLM5.
  - **BLM5:** \( D_s \equiv D_t \leftrightarrow yp \rightleftharpoons D_t. \) Based on BLM5, then the SG3 is achieved.

Similarly, for the swarm drone authentication analysis,

- **BLM6:** \( D_t \leftarrow (t, \sigma_i, yp), \sigma_i = S(t, xp_i) \) (Eq. 8). Then, based on the initial assumption IA3, IA4, and the BAN message meaning rule, we get the following:
  - **BLM7:** \( D_s \equiv D_t \sim \sigma_i. \)
    By applying the BAN freshness rule, we get BLM8.
  - **BLM8:** \( D_s \equiv D_t \equiv \sigma_i. \) Applying the BAN jurisdiction rule, we get BLM9.
  - **BLM9:** \( D_s \equiv \sigma_i. \) Next, we apply the Nonce verification rule to get BLM10.
    - **BLM10:** \( D_s \equiv D_t \leftrightarrow yp \rightleftharpoons D_t. \) Based on BLM10, then the SG4 is achieved. Finally, based on IA1, IA3, BLM5, and BLM10, security goals SG1 and SG2 are achieved. Hence, all our proposed authentication security goals are achieved.

**C. INFORMAL SECURITY ANALYSIS**

The security analysis of our proposed authentication model is qualified to sustain the following security issues,

1) **Authentication of Source:** During the delegation phase, the drones are assigned with the network core (original signer) warrant and delegation parameter. Therefore, during the drone authentication stage, the verifier drone can verify the delegation source. Thus, the proposed scheme proves the authentication of the source.

2) **Identifiable:** The construction of the proposed authentication scheme is warrant and private key-based. Therefore, any drone can identify both the original signer and the proxy signer. Thus, identifiability is satisfied.

3) **Message Integrity:** The authentication message alteration can result in a rejected authentication in the verification stage in Eq. (9) and Eq. (6). Any malicious drone \( D_m \) attempts to create its own proxy signature message can not obtain the core network delegation tuple required for legitimate proxy signature keys. Therefore, the proxy signature message integrity is achieved.

4) **Prevention of Misuse:** The scope of the message is only comprised of the warrant, and therefore, the drone (proxy signer) can not sign an illegal document. Our proposed D2D drone authentication utilizes delegation parameters provided only by the core network. An authorized drone provides a unique proxy signature message based on the core network delegation parameters to be a part of the drone swarm. Therefore, the proposed scheme prevents the misuse of proxy signing.

5) **Strongness:** During the verification process, the verifier’s secret key is needed. Thus, any entity other than the designated verifier (the drone) is incapable of verifying the validity of the message signature pair. Thus, any entity other than the designated verifier (drone) is incapable of verifying the validity of the message signature pair. Hence, the proposed scheme is strong against the resilience of various types of attacks.

6) **Modification Attack:** The warrant comprises the message scope, and verification needs the secret key of the core network. Thus, during verification, message alteration will not be successful. Thus, the proposed scheme prevents modification attacks.

7) **Replay Attack:** Any illegitimate node attempting to catch and redirect a legitimate drone \( D_t \) proxy signature, \( (t_i, \sigma_i, w_i, yp_i, y) \), the signature will not pass the verification at Eq.(6). Similarly, for any attempt of a replay attack of the leader drone broadcast message, the signature will not pass the verification at Eq.(6). Therefore, our proposed authentication mechanism is resilient against any replay attacks.

8) **Impersonation Attack:** Due to the correctness of verification and that it is based on several parameters
from both the signer drone (proxy signer) and the core network (original signer), the impersonation attack cannot be successful.

9) **MiTM Attack:** To prevent MiTM attacks, authentication of source, identifiability, and unforgeability should be satisfied. Since the proposed authentication scheme satisfies all these aforementioned properties, an eavesdropper cannot alter the message signature pair. Hence, the proposed scheme prevents the MiTM attack.

VII. PERFORMANCE ANALYSIS

This section presents the evaluation results to demonstrate our proposed scheme’s effectiveness.

A. EXPERIMENT SETUP

Our implementation setup is done using the NS-3 5G network simulator, which has recently implemented a 5G RAN module [50] with the ProSe D2D library in [6]. In this setup, we created 2 UE nodes representing a leader drone and a swarm drone to test our proposed authentication mechanism. We used a Raspberry-Pi3 IoT device (Raspberry Pi OS Lite, an 8GB microSD card) for the authentication calculation and proxy signature keys generation. We also added a server node representing the AAA-S as the core network delegation authority. We repeated the experiment for the ProSe discovery modes for both Model A and Model B, where there was a negligible change between the two models. The system parameters for the NS-3 simulation used in the experiments are listed in Table 2.

B. METRICS AND BASELINES

We assess the efficiency of our proposed authentication mechanism using the total authentication time as an evaluation parameter. The total authentication time includes all the communication and computation delays during the authentication message exchange process. Moreover, we consider the 4G ProSe D2D security standard as a centralized baseline for comparison.

C. PERFORMANCE RESULTS

1) DRONE COMPUTATIONAL OVERHEAD

Table 3 shows the computational processing delays that drones experience during our proposed proxy signature authentication exchange messages. Our proposed authentication mechanism’s total computational processing delay, including all parameters and signature calculations, is 2.012 msec. Therefore, the computational processing complexity is lightweight and drone processing friendly.

2) COMMUNICATION DELAY

Table 4 displays the communication delays experienced during the proposed authentication mechanism, which sums to a total of 6.35 msec. After adding the total computation processing delay, our proposed authentication mechanism’s total authentication time is 8.362 msec. However, the ProSe security standard total authentication time is 1.5 times higher than our proposed delegated-based authentication mechanism.

3) AUTHENTICATION SCALABILITY

We investigate the scalability of our proxy signature authentication mechanism over the current ProSe security standard. Table 5 shows the total number of messages sent and received for each approach. As can be seen, our proposed proxy-based approach is much more energy-efficient compared to the ProSe security standard.

4) IMPACT OF DRONES DISTANCE

We explore the variation in total authentication time depending on physical layer aspects. In Fig. 8, we investigate the effect of the distance between the drones on the total required authentication time. We compare the 4G-ProSe authentication mechanism if to be used in the 5G network and our proposed Proxy Signature authentication. Longer distance means higher path loss, especially with the 5G mmWave communication (28 GHz); the path loss drops faster than the 4G traditional 2.4 GHz communication, making the communication time more noticeable. We notice that our
TABLE 5. Total # of authentication messages.

| # of Drones | LTE ProSe Security Standard | Proposed Proxy Signature |
|-------------|----------------------------|--------------------------|
|             | TX | RX | TX | RX |
| 2           | 6  | 4  | 1  | 2  |
| 4           | 12 | 8  | 1  | 4  |
| 6           | 18 | 6  | 1  | 6  |
| 8           | 24 | 16 | 1  | 8  |
| 10          | 30 | 20 | 1  | 10 |

FIGURE 8. TCP re-transmissions overhead for different N.

TABLE 6. Authentication delay under varying background traffic.

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

Proxy Signature authentication is more efficient and scalable than the existing 4G-based ProSe authentication model.

5) IMPACT OF BACKGROUND TRAFFIC DELAY
We implemented an uplink and downlink background traffic through the leader drone while simultaneously starting our proxy authentication mechanism. We set the background traffic’s packet transmissions frequency parameter at 1 msec. Table 6 shows a maximum total communication delay of 0.8 µsec at 40 background nodes. Therefore, the impact of high background traffic is negligible with no extra delay overhead.

6) LEADER DRONE SELECTION OVERHEAD
The delays experienced during the new leader drone selection process between the swarm drones depend on 2 factors; one is the number of candidate drones, and the second is the time to relocate the selected leader drone physically. The number of exchanged messages between the swarm drone equals the number of candidates C, as each drone broadcasts its announcing message. The drone relocation time depends on the distance between the newly selected leader drone and the assigned location and the drone speed to the new position. Assuming an average drone speed of 50 mph, ≈ 81 km/h, and an average distance between the new leader drone and its assigned location of 150 m, the average relocation time is 6.71 sec. The dominating delay for the new leader drone selection is from the drone’s physical relocation. However, due to the buffering capabilities offered by the new leader until reaching its assigned position, there was no packet lost during this drone relocation process.

VIII. CONCLUSION
We proposed a reliable authentication mechanism compatible with the 5G D2D ProSe standard mechanisms for the communication within the drones’ swarm. The proposed authentication is distributed-based authentication with a delegation-based scheme instead of the repeated access to the 5G core network. We proposed a delegation-based proxy signature authentication mechanism that reduces the drones’ communication overhead toward the core network. The drones are proposed to get authenticated to each other and toward a UE-to-Network relay leader drone through delegation digital signature. Moreover, we proposed a leader drone replacement process to overcome the unresponsive leader drone situations. Moreover, we introduced a revocation mechanism for the proposed proxy signature keys and the delegation warrants if expired or compromised. We evaluated our proposed authentication scheme through the NS-3 5G D2D communication module for communication delay and a Raspberry Pi 3 for computational processing. Our results evaluation indicated a lightweight, efficient, and, more importantly, scalable compared to the 4G ProSe security standard.

REFERENCES
[1] Technical Specification Group Services and System Aspects: Proximity-Based Services (ProSe); Security Aspects, document TS 33.303 V16.0.0 Technical Specification (Release 16), 3GPP, 2020.
[2] 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 Things J., vol. 6, no. 2, pp. 3572–3584, Apr. 2019.
[3] 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 Proc. Int. Conf. Netw. Netw. Appl. (NAN), Oct. 2019, pp. 379–384.
[4] M. L. Das, A. Saxena, and D. B. Phatak, “Algorithms and approaches of proxy signature: A survey,” Dec. 2006, arXiv:cs/0612098.
[5] W.-B. Lee and C.-K. Yeh, “A new delegation-based authentication protocol for use in portable communication systems,” IEEE Trans. Wireless Commun., vol. 4, no. 1, pp. 57–64, Jan. 2005.
[6] M. Diouf. (Jun. 2017). mmWave Cellular Network Simulator. [Online]. Available: https://github.com/makhtardiouf/d2d
[7] M. A. Abdel-Malek, K. Akkaya, A. Bhuyan, and A. S. Ibrahim, “A proxy signature-based drone authentication in 5G D2D networks,” in Proc. IEEE 93rd Veh. Technol. Conf. (VTC-Spring), Apr. 2021, pp. 1–7.
[8] M. Karimi-buki, M. Aibin, Y. Lai, R. Khan, R. Norfield, and A. Hunter, “Drones’ face off: Authentication by machine learning in autonomous IoT systems,” in Proc. IEEE 10th Annu. Ubiquitous Comput., Electron. Mobile Commun. Conf. (UEMCON), Oct. 2019, pp. 0329–0333.

[9] T. Alladi, N. Naren, G. Bansal, V. Chamola, and M. Guizani, “SecAuDiAV: A novel authentication scheme for UAV-ground station and UAV-UAV communication,” IEEE Trans. Veh. Technol., vol. 69, no. 12, pp. 15068–15077, Dec. 2020.

[10] M. Rodrigues, J. Amaro, F. S. Osorio, and B. R. L. J. C. Kalinka, “Authentication methods for UAV communication,” in Proc. IEEE Symp. Comput. Commun. (ISCC), Jun. 2019, pp. 1210–1215.

[11] B. Liu, K. Yu, C. Feng, and K.-K. R. Choo, “Cross-domain authentication for 5G-enabled UAVs: A blockchain approach,” in Proc. 4th ACM MobiCom Workshop Drone Assist. Wireless Commun. 5G Beyond (DroneCom). New York, NY, USA: Association for Computing Machinery, 2021, pp. 25–30, doi: 10.1145/3477090.3481053.

[12] T. Li, Y. Onodera, Y. Nakayama, and D. Hisano, “Multi-channel nature schemes, revisited,” in Proc. IEEE Internet Things J., 2021, pp. 25–30, doi: 10.1145/3477090.3481053.

[13] W.-B. Lee and C.-K. Yeh, “A new delegation-based authentication protocol for use in portable communication systems,” IEEE Trans. Wireless Commun., vol. 4, no. 1, pp. 57–64, Jan. 2005.

[14] H. Wang and J. Pieprzyk, “Efficient one-time proxy signatures,” in Proc. Int. Conf. Theory Appl. Cryptol. Secur. Berlin, Germany: Springer, Nov. 2003, pp. 507–522.

[15] F. Zhang and K. Kim, “Efficient id-based blind signature and proxy signature for bilinear pairings,” in Proc. Australas. Conf. Inf. Secur. Privacy. Berlin, Germany: Springer, Jul. 2003, pp. 312–323.

[16] L. He, J. Ma, R. Mo, and D. Wei, “Designed verifier proxy blind signature scheme for unmanned aerial vehicle network based on mobile edge computing,” Secur. Commun. Netw., vol. 2019, pp. 1–12, Apr. 2019.

[17] G. K. Verma, B. B. Singh, N. Kumar, and D. He, “CB-FS: An efficient short-certificate-based proxy signature scheme for UAVs,” IEEE J. Sel. Areas Commun., vol. 14, no. 1, pp. 621–632, Mar. 2020.

[18] W. Liu, Y. Mu, G. Yang, and Y. Tian, “Strong identity-based proxy signature schemes, revisited,” Wireless Commun. Mobile Comput., vol. 2018, pp. 1–11, Aug. 2018.

[19] B. Lee, H. Kim, and K. Kim, “Strong proxy signature and its applications,” in Proc. SCIS, Jeju, Jan. 2001, pp. 603–608.

[20] M. A. Abdel-Malek, K. Akkaya, N. Saputro, and A. S. Ibrahim, “Efficient authentication of drones to mmWave wireless mesh networks in post-disaster scenarios,” in Proc. IEEE Global Commun. Conf. (GLOBECOM), Dec. 2020, pp. 1–6.

[21] 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 Commun. Surveys Tuts., vol. 19, no. 2, pp. 1054–1079, 2nd Quart., 2017.

[22] O. Bello and S. Zeadally, “Intelligent device-to-device communication in the Internet of Things,” IEEE J. Sel. Areas Commun., vol. 10, no. 3, pp. 1172–1182, Sep. 2016.

[23] 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 Trans. Veh. Technol., vol. 69, no. 8, pp. 9097–9111, Aug. 2020.

[24] D. Schürmann, A. Brüsch, S. Sigg, and L. Wolf, “BANDANA—Body area network device-to-device authentication using natural gait,” in Proc. IEEE Int. Conf. Pervasive Comput. Commun. (PerCom), Mar. 2017, pp. 190–196.

[25] H. Kwon, C. Hahn, D. Kim, K. Kang, and J. Hur, “Secure device-to-device authentication in mobile multi-hop networks,” in Proc. Int. Conf. Wireless Algorithms, Syst., Appl. Cham, Switzerland: Springer, 2014, pp. 267–278.

[26] K. Mahmood, S. Shamshad, M. Rana, A. Shafiq, S. Ahmad, M. A. Akrarn, and R. Amin, “PUF enable lightweight key-exchange and mutual authentication protocol for multi-server based D2D communication,” J. Inf. Secur. Appl., vol. 61, Sep. 2021, Art. no. 102900. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1224212621001277

[27] T. Li, Y. Onodera, Y. Nakayama, and D. Hisano, “Multi-channel authentication for secure D2D using optical camera communication,” in Proc. IEEE 19th Annu. Consum. Commun. Netw. Conf. (CCNC), Jan. 2022, pp. 858–863.

[28] A. Vangala, A. K. Sutrala, A. K. Das, and M. Jo, “Smart contract-based blockchain-envisioned authentication scheme for smart farming,” in Proc. IEEE Int. Conf. Mobile Things, vol. 8, no. 10, pp. 10792–10806, Jul. 2021.
M. A. Abdel-Malek et al.: Proxy Signature-Based Swarm Drone Authentication With Leader Selection in 5G Networks

M. A. Abdel-Malek received the B.Sc. degree (Hons.) from the Communications and Electronic Department, Faculty of Engineering, Alexandria University, Egypt, in 2013, the M.S. in wireless technology from Nile University (NU), Egypt, in 2016, and the Ph.D. degree from the Electrical and Computer Engineering Department (ECE), Florida International University (FIU). She was a Research Assistant at the Wireless Intelligent Networks Center (WINC), NU, and a Research Assistant at Virginia Tech-Middle East and North Africa (VT-MENA) for one year, from August 2015 to August 2016. She is currently a Postdoctoral Assistant with the Commonwealth Cyber Initiative (CCI), Virginia Tech (VT).

Kemal Akkaya (Senior Member, IEEE) received the Ph.D. degree in computer science from the University of Maryland, Baltimore County, in 2005. He joined the Department of Computer Science at Southern Illinois University (SIU) as an Assistant Professor, where he was an Associate Professor, from 2011 to 2014. He was a Visiting Professor at The George Washington University, in Fall 2013. He is a Full Professor with the Department of Electrical and Computer Engineering with a joint courtesy appointment with the School of Computer and Information Sciences, Florida International University. He leads the Advanced Wireless and Security Laboratory (ADWISE), ECE Department. He has published over 230 papers in peer reviewed journal and conferences. His current research interests include security and privacy, the internet of things, and cyber-physical systems. He received the “Top Cited” Article Award from Elsevier, in 2010. He is the EiC of Springer Computer Science Journal, an Area Editor of Elsevier Ad Hoc Network Journal and serves on the Editorial Board of IEEE COMMUNICATION SURVEYS AND TUTORIALS. He was the General Chair of IEEE Local Computer Networks (LCN) Conference 2018 and the TPC Chair for IEEE International Conference on Communications (ICC), Global Communications Conference (Globecom), International Conference on Network Protocols (ICNP), Conference on Computer Communications Workshops (INFOCOM), Local Computer Networks Conference (LCN), Wireless Communications and Networking Conference (WCNC), and ACM WiSec.

Arupjyoti (Arup) Bhuyan received the Ph.D. degree in engineering and applied sciences from Yale University. He has extensive industry experience in wireless communications. In October 2015, he joined INL, where he is the Technical Director of the INL Wireless Security Institute. His research interests include secure implementation of future generations of wireless communications with scientific exploration and engineering innovations across the fields of wireless technology, cybersecurity, and computational science. Specific goals are to lead and focus wireless security research efforts for 5G and Beyond with national impact, to secure communications for a nationwide unmanned aerial systems and for 5G spectrum sharing with distributed scheduling.

Ahmed S. Ibrahim received the B.S. and M.S. degrees in electronics and electrical communications engineering from Cairo University, Cairo, Egypt, in 2002 and 2004, respectively, and the Ph.D. degree in electrical engineering from the University of Maryland, College Park, MD, USA, in 2009. He was an Assistant Professor at Cairo University, a Wireless Research Scientist at Intel Corporation, and a Senior Engineer at Interdigital Communications Inc. He is currently an Assistant Professor with the Electrical and Computer Engineering Department, Florida International University (FIU), Miami, FL, USA. He was a recipient of the NSF CAREER Award, in 2022. His research interests include wireless systems, including drone-assisted millimeter wave communications, vehicular communications, and rethinking wireless networks through the lens of Riemannian geometry.

* * *