Efficient Authentication of Drones to mmWave Wireless Mesh Networks in Post-Disaster Scenarios

Mai A. Abdel-Malek*, Kemal Akkaya*, Nico Saputro†, and Ahmed S. Ibrahim*
*Dept. of Electrical and Computer Engineering, Florida International University, Miami, FL 33174, USA
Emails: {mabde030, kakkaya, aibrahim}@fiu.edu
†Dept. of Electrical Engineering, Parahyangan Catholic University, Bandung, Jawa Barat 40141, Indonesia
Email: nico@unpar.ac.id

***Abstract*—Unmanned Aerial Vehicles (UAVs), or drones, are increasingly being utilized for public safety circumstances including post-disaster recovery of destroyed communication infrastructure. For instance, drones are temporarily positioned within an affected area to create a wireless mesh network among public safety personnel. To serve the need for high-rate video-based damage assessment, drone-assisted communication can utilize high-bandwidth millimeter wave (mmWave) technologies such as IEEE 802.11ad. However, short-range mmWave communication makes it hard for optimally-positioned drones to be authenticated with a centralized network control center. Therefore and assuming that there are potential imposters, we propose two lightweight and fast authentication mechanisms that take into account the physical limitations of mmWave communication. First, we propose a drone-to-drone authentication mechanism, which is based on proxy signatures from a control center. Accordingly, any newly joining drone can authenticate itself to an exist one rather than attempting to authenticate to the out-of-reach control center. Second, we propose a drone-to-ground authentication mechanism, to enable each drone to authenticate itself to its associated ground users. Such authentication approach is based on challenge-response broadcast type, and it is still utilizing fast proxy signature approach. The evaluation of the proposed authentication mechanisms, conducted using NS-3 implementation of IEEE 802.11ad protocol, show their efficiency and practicality.**

***Index terms*—** Authentication, drones, millimeter wave, mesh network, proxy-signature.

I. Introduction

In a post-disaster circumstances such as hurricanes and earthquakes, the communication and power infrastructures could be damaged, disconnecting affected communities from the rest of the world. Restoring communication network is vital for damage assessment and to start the recovery process. To address the need for rapid post-disaster recovery, public safety agencies and local governments are currently considering the deployment of Unmanned Aerials Vehicles (UAVs), commonly known as drones which will act as relays among people in affected areas as well as with local authorities.

Generally, drone-assisted communication network can be based on a cellular infrastructure, having a number of base stations, or wireless mesh gateways [1], [2]. Recently, there have been multiple research works focusing on optimally-positioning drones to satisfy capacity and coverage requirements. Some of these works have utilized the high-bandwidth millimeter-wave (mmWave) spectrum band [3], [4], [5] to be able to support the required high-rate for video-based post-disaster damage assessment communication. Such works mostly focused on performance and connectivity issues. Security threats are under-explored, which can become relevant particularly in the post-disaster scenarios. For instance, as drones are commodity Internet of Things (IoT) devices, they can be easily obtained and deployed to maliciously eavesdrop the network. As the main focus of authorities and people will be to facilitate aid efforts, security will not be a priority as in the case of regular communication networks.

Authentication is particularly challenging in drone-assisted mmWave communication, given the short-range limitation of communication over mmWave spectrum band. More precisely, not all drones, which are optimally-positioned according to coverage or capacity constraints, will have direct communication link with the centralized authentication entity. Instead, drones will be connected among each other through multi-hop mesh network. Therefore, there is a need to have drone-based short-range authentication mechanisms, and this is the main motivation of this paper. Particularly, two different drone-based authentication challenges are considered in this paper.

The first scenario focuses on the initial joining of a drone to the mesh network. In that case, each drone that hoovers at a given position needs to authenticate itself to a control center (CC) and all other drones, if any, as these will communicate with each other during data relaying. As pointed out earlier, a remote authentication with a control center may not be viable for all drones due to short range mmWave characteristic. Furthermore, a drone-to-all drones authentication is not efficient in terms of time and battery consuming as it will require every combination of drones to connect with each other and perform mutual authentication. Therefore, we opt for a delegation authentication called proxy signature, where the proxy signer signs a message using a secret key of the original signer [6], [7]. Proxy signature provides data security and user privacy, while not increasing computational loads.

Therefore in this paper, we first propose a proxy-based scheme for drone-to-drone authentication, where we delegate one of the drones to sign the authentication warrant on behalf of a CC to reduce the communication time and energy. In this

The work of Ahmed Ibrahim is supported in part by the National Science Foundation under award number CNS-1618692.

978-1-7281-8298-8/20/$31.00 ©2020 IEEE

way, we ensure that authentication of a newcomer drone with one of the existing drones would suffice as it represents others in the network through the proxy features.

The second scenario, considered in this paper, focuses on the problem of trust among the deployed drones and the ground nodes. A drone may act as an imposter to deceive ground nodes. Therefore, there is a need for authentication of drones to ground nodes. In this paper, we aim to find an efficient way of authentication between a drone and its associated ground nodes, which is based on group authentication that reduces the overhead of the process significantly. Thus, we propose adapting a broadcast-based group authentication scheme where a simple challenge-response authentication is followed. The signed messages in the broadcast utilizes the proxy signature of the CC.

We implemented the two proposed authentication schemes in NS-3 network simulator by utilizing an underlying IEEE 802.11ad communication environment that enables mesh networking among the ground nodes and drones. We implemented other baselines to compare with our approaches and assessed the overhead that comes with authentication. The results indicate that our mmwave-based authentication approaches can significantly reduce the authentication time and energy consumption.

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

II. Related work

Since drones are vulnerable to several kind of attacks, drone authentication is studied within the context of message authentication. For instance, in [8], the authors propose a lightweight authentication and key agreement scheme for internet of drones deployment utilizing an efficient one-way cryptographic hash functions. Our goal in this paper is not message authentication as we aim to perform device authentication. For device authentication, there has been some other studies. In [9], the authors proposed an elliptic curve (ECC) digital certificate as the identity proof of the legal drone toward drone network identity authentication. Such an identity can easily be replayed or regenerated in a post-disaster scenario. Moreover, a machine learning (ML) mechanism for authentication in autonomous IoT systems is studied in [10]. This assessment is done for different ML algorithms by computing and reporting the precision and recall rates for each algorithm. This approach will not work in a post-disaster scenario since the training needs to be done in advance.

There has been multiple works for different proxy signature approaches for different purposes [6]. A short certificate base proxy signature is proposed in [11] with a low computational cost to overcome the integrity attacks on vehicular networks. In [12], a blind ID-based partial delegation with warrant proxy signature is proposed, where ID-based proxy is to provide the anonymity of users. In [13], the authors proposed a new scheme to mitigate partial attacks not considered by the identity-based proxy signature. While our work utilizes proxy signature concept like these studies, its proposed protocols are very much different where the goal is to authenticate drones to an existing network.

III. System and Attack Models

A. System Model

We assume a post-disaster scenario where most of the cellular base-stations and cable/DSL infrastructure have been damaged and not functioning. To enable communication among citizens and emergency crew, we assume that certain number of drones could be deployed within a neighborhood in order to form a temporary ad hoc wireless mesh network among user smart phones/laptops or WiFi routers in their homes. We assume these drones can act semi-autonomously to make their own decisions once deployed. For providing high bandwidth multimedia communications, we assume these drones are capable of supporting mmWave communications such as IEEE 802.11ad standard which operates at the 60GHz frequency. We assume each user (ground) node has installed an emergency client application in advance that can be used in the aftermath of a disaster where there is no Internet access. We assume that there is a control center (CC) maintained by public-safety personnel, which can send drones to the region of interest to form a wireless mesh network where these drones serve as relay nodes to ground user nodes as shown in Fig. 1. One of the drones can act as a gateway that can connect to the CC using a wide area communication standard such as LoRa [14].

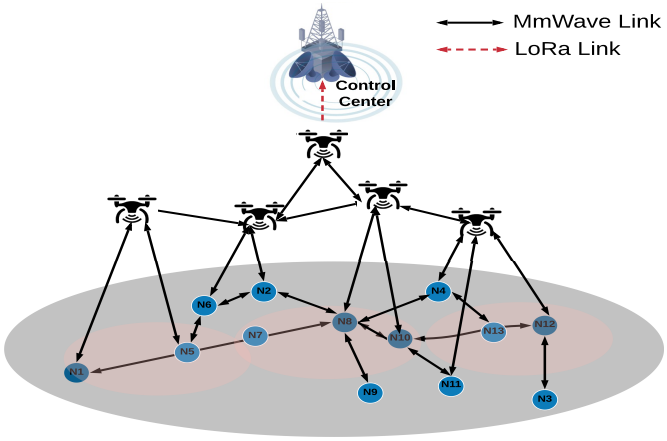

Fig. 1. Envisioned adhoc wireless mesh network of drones and ground users.

B. Attack Model

We assume that there may be malicious drones as they are deployed externally but the ground nodes will be trusted. The drones do not collude and there is time synchronization among the nodes. The following attacks are considered:

- A malicious drone can act as an imposter and become part of the wireless mesh network. Once becoming a mesh node, a malicious drone may not honor routing and forwarding

(i.e., block messages, change the messages, etc.) or it can be just passive to collect private information coming from ground users.

- Without becoming part of the wireless mesh network, a malicious drone can broadcast message to ground nodes claiming to be a gateway for them. In such cases, private user data can be collected from the ground users.

IV. Proposed Authentication Schemes

The drone authentication problem with the presence of new drones and ground users to form a IEEE 802.11ad-based wireless mesh network can be divided into two sub-problems: (1) the mutual authentication among drones for new and legitimate drone deployment; and (2) the drone-to-ground nodes authentication. Our proposed idea of the authentication scheme is based on proxy delegation from the CC for both cases. As such, rather than allowing each drone pair to mutually authenticate each other, we follow a more efficient approach where authentication with any of the drones would suffice. Given the nature of mmWave links, this process will not only be much faster but also enable energy-efficiency in terms of drone movement. To enable this delegation, we utilize proxy signature concept [15]. Basically, the motivation comes from the fact that one can designate a proxy to sign messages on behalf of him/herself. The delegation can be in different forms but eventually the signature from the proxy can be traced back to the original signer for verification. In our case, we will utilize the signature as an indication for device (source) authentication. We propose that the CC will designate the drones as its proxies so that the drones can authenticate themselves to the post-disaster wireless mesh network as new devices. The details proposed approaches are discussed next.

A. Registration Phase

Basically, the first step in the network formation is the *registration phase* where the ground nodes within the envisioned mesh network are determined. To this end, the control center will designate an *observer drone*, D_0, which will hoover above the region of interest to collect information from the interested ground nodes. Specifically, the observer drone D_0 broadcasts a message that includes its public key Pub_{D0}, its unique pseudonym ID_{D0}, and the CC's certificate, $cert_{cc}$. The observer drone then collects the responses from any ground node which would like to become part of this mesh network. Note that the emergency client application on a ground node comes pre-installed with the public key of a certificate authority (CA) that can be used to verify any signature coming from the CC. Through this client app, any ground node, G_j will send a reply message that includes its unique ground node ID ID_{Gj}, public key Pub_{Gj}, its location, and its received signal strength indicator (RSSI) value. At the end, all the collected ground node info will be sent to the control center using LoRa by the observer drone. Based on the collected data, the CC optimally computes the number of $(M-1)$ new drones that need to be deployed and the best M locations for these new drones and the observer drone to maximize the communication throughput and enhance the link qualities by utilizing some of the existing solutions [16].

B. Delegation Phase

Before the CC releases the additional $(M-1)$ drones to these locations, it performs some initial configurations to these drones first simply by manually accessing the drones and installing the needed parameters for creation of a proxy signature as used in [15]. To enable this, we assume that each drone D_i, $i = 1, 2, ..., (M-1)$ has a pair of public-private key $(Pub_{D_i}, Priv_{D_i})$.

As part of this proxy signature, the CC creates a *warrant* w_{Di} for each D_i by signing the drone's public key with its private key $Priv_{cc}$: $w_{Di} = \mathbf{S}(Pub_{Di}, Priv_{cc})$, where **S()** is any digital signature function. Then, a pair of *CC delegation keys* (r_i, s_i) is created for drone D_i as follows: Let g be a generator of a multiplicative subgroup of Z_p^* with order p. The CC chooses a random number $k_i \in_R Z_p^*$ and calculates these keys:

$$\begin{aligned} r_i &= g^{k_i}, \\ s_i &= Priv_{cc}\mathbf{H}(w_{D_i}, r_i) + k_i, \end{aligned} \tag{1}$$

where, $\mathbf{H}()$ is a collision resistant hash function.

Along with these keys, a *delegation message* of a tuple $(w_{D_i}, r_i, s_i, cert_{cc})$ is created and installed in each drone D_i, which can now create a *proxy public-private key pair* $(Pub_{Dproxy_i}, Priv_{Dproxy_i})$ using the info in the delegation message to sign any message on behalf of the CC as follows:

$$\begin{aligned} Priv_{Dproxy_i} &= s_i + \mathbf{H}(w_{D_i}, r_i) Priv_{D_i} \\ Pub_{Dproxy_i} &= (Pub_{cc} Pub_{D_i})^{\mathbf{H}(w_{D_i}, r_i)} r_i \end{aligned} \tag{2}$$

Since $Priv_{Dproxy_i}$ is only known by D_i, the proxy signature can be only created by a legitimate drone D_i. Note that the same process was used to create the proxy key pair of the observer drone D_0.

C. Drone-to-Drone Mutual Authentication

Once the drones go to their locations, each drone D_i initiates the authentication process by creating a timestamp nonce t_{Di}, and then signs this nonce with its proxy private key $Priv_{Dproxy_i}$: $\sigma_i = \mathbf{S}(t_{Di}, Priv_{Dproxy_i})$. D_i then broadcasts a proxy signature that contains the following tuple: $(t_{Di}, \sigma_i, w_{Di}, r_i, Pub_{Di})$. Any other drone, say D_j, within the vicinity will be able to verify this proxy signature by verifying whether the proxy signature is valid. This verification can be done by the following equation:

$$\mathbf{V}(t_{Di}, \sigma_i, (cert_{cc} Pub_{Di})^{\mathbf{H}(w_{D_i}, Pub_{D_i})} r_i) \stackrel{?}{=} True \tag{3}$$

where **V()** is a digital signature verification algorithm. Note that this process can happen simultaneously for every drone, which can save significant time. However, due to potential varying arrival times of drones to their locations, some drones may not receive these broadcasts on time. Therefore, the broadcasts from D_i should continue until the neighboring drone(s) such as D_j replies back with the same message but with a different timestamp. The timestamps are used to prevent

any replay attacks from malicious drones. This process is shown in Fig. 2. In this way, both drones are authenticated each other and can now become part of the mesh network.

Note that as long as a drone broadcasts a proxy signature, it can be authenticated with the rest of the drones without a need for individual authentications. This saves us time and energy in the context of the public safety application.

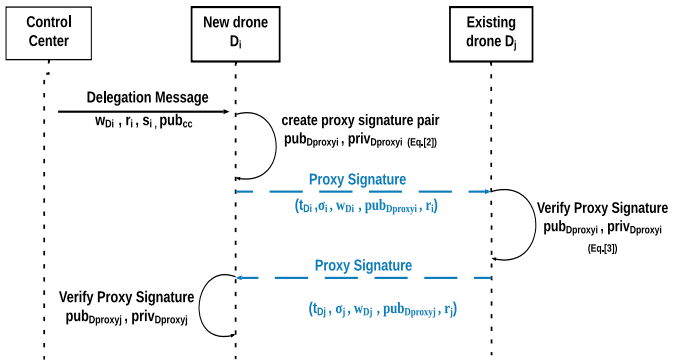

Fig. 2. Message exchanges among drones for mutual authentication.

D. Drone-to-Ground Authentication

The next step in the formation of the proposed wireless mesh networks is to ensure that the ground nodes trust the newly joining drones. To this end, in this section, we propose a device authentication mechanism to legitimize the drones to the ground nodes in the network and avoid any illegitimate drone to communicate with these nodes in the context of the disaster applications. Given the nature of mmWave communications, we opted for a group authentication scheme where we can easily reach out to large number of nodes with a single message to not only achieve faster processing but also to eliminate any redundant messages as they can be easily lost. Note that authenticating nodes pair by pair is time and power-consuming for both the drones and the nodes in a disaster situation, particularly in the context of mmWave channel. To enable group authentication, we first need to divide the ground nodes in the clusters where a drone will be responsible to serve to each cluster as shown in Fig. 3. In order to enable this, each ground node should select a drone. When a drone does a broadcast, a ground node may hear from multiple of these drones depending on its location. We assume that the ground node will pick the drone whose message arrives first.

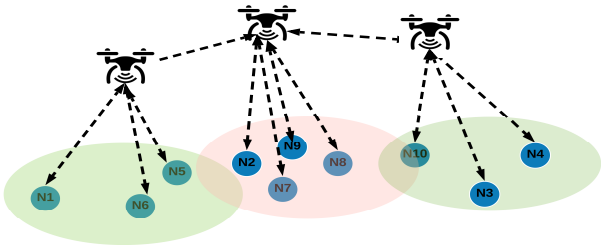

Fig. 3. Clustering of ground nodes to be served by a particular drone.

As the goal is to authenticate drones as entities that can be trusted by these ground nodes, we propose using a one-time challenge response protocol based on public-key cryptography. The motivation also comes from the fact that the ground nodes and the drones cannot agree on a symmetric key easily as this will introduce extra communication or other mechanisms that may not be suitable for disaster cases. Thus, we opt for a group-based challenge-response as we do not want to perform this process one-by-one with each ground node.

Nevertheless, we still rely on the proxy-signatures generated by the CC. The idea is to send a challenge to each ground node from their respective drone through a broadcast message. This challenge will include a proxy signature from the drone (i.e., delegated by the CC) that needs to be verified by each ground node. To this end, each drone D_i prepares and broadcast a proxy signature to its cluster that contains the following tuple:

$$D_i \rightarrow \forall nodes : (ID_{D_i}, t_i, w_{D_i}, \beta_i, cert_{CC}, Pub_{D_i}) \quad (4)$$

where $\beta_i = \mathbf{S}((ID_{Di}||w_{D_i}||t_i), Priv_{Dproxy_i})$ is a signed message consisting of drone ID, its warrant, and a timestamp t_i using the drone's proxy private key $Priv_{Dproxy_i}$.

On receiving this broadcast proxy signature, a ground node, G_j, first verifies the *warrant* to ensure that it is signed by the private key of the CC: $\mathbf{V}(Pub_{D_i}, w_{D_i}, cert_{cc}) \stackrel{?}{=} True$. Next, it verifies the proxy signature to ensure that it is signed by the proxy private key of drone D_i:

$$\mathbf{V}((ID_{Di}||w_{D_i}||t_i), \beta_i, (cert_{cc}Pub_{D_i})^{\mathbf{H}(w_{D_i}, r_i)} r_i) \stackrel{?}{=} True. \quad (5)$$

Note that it can also verify the signature of CC using CA's private key which was pre-installed.

V. Security and Performance Analysis

In this section, we first discussed the security analysis of the proposed schemes and then present the simulation results to demonstrate the effectiveness of the proposed scheme.

A. Security Analysis

In order to join the network, a legitimate drone D_i will need to show that it has a valid and unique pair of proxy key, which is created based on a unique pair of delegation key given by the CC to the drone D_i. A malicious drone D_m needs to broadcast a proxy signature message (either to other drones or ground nodes) that can be verified using the D_m's proxy public key. Since the delegation phase is conducted manually and securely prior the drones' release to the new location, D_m will not be able to create its pair of proxy key since it does not have the unique pair of delegation key. Hence, it cannot join and become part of the mesh network.

D_m may also try to impersonate a legitimate drone D_i by performing a *replay attack* where it replays a captured message from D_i either for joining the network or claiming as the gateway for ground nodes. In both cases, D_m broadcasts the whole proxy signature of drone D_i, $(t_{Di}, \sigma_i, w_{Di}, Pub_{DProxy_i}, Pub_{D_i})$. Let us assume a verifier node (either drone or ground node) X_k receives this broadcast for the first time. This proxy signature will not pass the verification using Eq. 3 due to stale timestamp value in the message. This applies to Eq. 5 in the same manner.

B. Experimental Setup

We used NS-3 [17] network simulator to performed the evaluations. We adopted the IEEE 802.11ad mmWave implementation described in [18] as the underlying communication for the drone-to-drone and drone-to-ground nodes communications. We used the following IEEE 802.11ad parameters for the experiments: *PHY Type* = DMG-MCS18, *Antenna Sector*=8, *Transmission Power*=10 dBm, and *Transmitter and Receiver gain*=23. The LoRa connection from observer drone to CC is also implemented using NS-3 LoRa module. The CC is assumed at 1km from the observer node. We used a Raspberry Pi IoT device to mimic constrained drone processing power and to measure the authentication times of the required cryptographic operations. These collected authentication times are then utilized in NS-3 to make a realistic simulation scenario. We used ECC for signatures. The key size is set to 260 bits.

N_D number of drones are placed to cover the whole area of interest. Each drone covers an area of 100×100 m^2. The ground node density in an area is varied in therms of the number of ground nodes. We used different number of ground nodes (i.e., $(10, 20, \cdots, 50)$) for the evaluations. The position of the ground nodes are randomly distributed. The drone is assumed to be placed in the specific location above the area with a varying altitude below 60m in such a way that it ensures the coverage of all ground nodes within the area.

C. Metrics and Baselines

To assess the performance, we considered the *total authentication time*, which includes all the communication and computation delays. In addition, we considered the energy metric for drones, which indicates the energy consumption for running the proposed approaches. To this end, we mainly counted the *number of messages* sent (TX) and received (RX) by all drones as computation energy is almost negligible compared to communication energy costs. To compare with our proposed approach, we considered some baselines as follows:

1) *Drone-to-Drone mutual authentication*: For this case, we considered a baseline approach where all the newcomer drones are authenticated to CC through the observer drone using multi-hop/ long-distance communication to the CC based on a challenge-response mechanism. This is referred to as *centralized authentication*. As a second baseline, we also considered our proxy approach but in a sequential manner where drones authenticate themselves in a sequence starting from the first neighbor of the observer drone using unicast messages. This approach is referred to as *sequential proxy signature* in the figures while our approach is shown as *parallel proxy signature*.
2) *Drone-to-ground node authentication*: For this case, as a baseline we considered a pairwise proxy authentication from a drone to each of the ground nodes using unicast messaging. This is referred to as *unicast-based proxy signature* in the figures. Moreover, we consider a traditional group authentication through the CC where the drone asks the observer drone to request a signed message from CC. The CC sends it back to drone via the observer, which then can broadcast it to the ground nodes in the cluster. This baseline is referred to as *centralized group authentication* in the figures. Our approach is labeled as *broadcast-based proxy signature*.

D. Performance Results

1) Drone-to-Drone Mutual Authentication results

Fig. 4 shows the authentication time plotted with the increasing number of drones for all approaches. As can be seen, our parallel proxy scheme can provide significant time savings compared to a centralized challenge-response approach and sequential proxy. With the increased number of drones, the reduction is almost doubled. This can be attributed to the fact that our approach performs authentications in parallel, thanks to consent from CC, which reduces the authentication time.

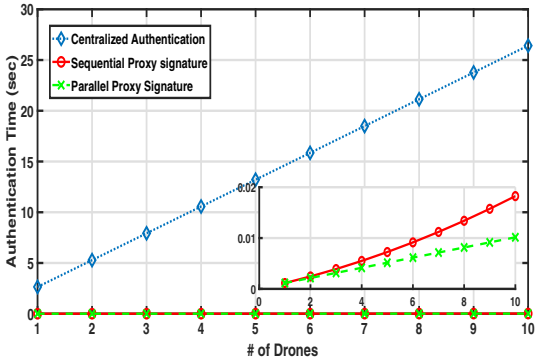

Fig. 4. Drone-to-Drone mutual authentication time under varying # of drones.

Table I shows the total number of messages sent and received for each approach. As can be seen, proxy-based approaches are much more energy-efficient. Parallel proxy approach reduces the transmission messages, TX more than 13 fold when the # of drones is 11 compared to centralized approach. Again this is due to elimination of the need to reach observer drone or CC for any authentication purposes. Moreover, the parallel proxy approach results in more received messages, RX, more than the sequential proxy signature as we broadcast the messages and more nodes can receive it. However, as TX energy cost is typically much higher than RX, parallel proxy approach is still more energy efficient as it almost halves the TX count.

TABLE I
TOTAL # OF MESSAGES FOR DRONE-TO-DRONE AUTHENTICATION.

	Centralized Authentication		**Sequential Proxy Signature**		**Parallel Proxy Signature**	
# of Drones	TX	RX	TX	RX	TX	RX
2	6	6	2	2	2	2
3	14	14	4	4	3	6
4	24	24	6	6	4	12
5	36	36	8	8	5	18
6	50	50	10	10	6	24
7	66	66	12	12	7	29
8	84	84	14	14	8	34
9	104	104	16	16	9	39
10	126	126	18	18	10	44
11	150	150	20	20	11	49

2) Drone-to-Ground Authentication Results

In this subsection, we present the performance of the authentication mechanism for Drone-to-Ground authentication.

We assessed the effect of different number of ground nodes on the drone-to-ground node authentication time. As seen in Fig. 5, the time for *Unicast-based Proxy Signature* increases linearly with the increasing number of ground nodes since in this mechanism the drone authenticates to each ground node separately. However, for our *broadcast-based proxy signature* approach, the authentication time stays stable even though the number of ground nodes increases. This is due to the fact that we use a broadcast-based approach where each ground node can become part of one of the existing clusters served by a drone. Increasing the number of nodes will only increase the size of a cluster yet the broadcast will still reach them in one message. Note that compared to these proxy cases, the *centralized group authentication* performs much worse due to the need for the long distance communication to the CC. Nonetheless, since each drone uses broadcasts, the authentication time is fixed.

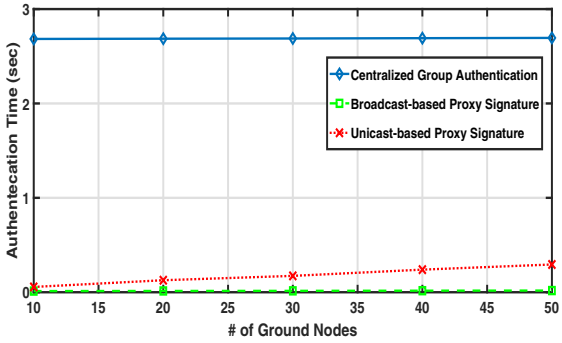

Fig. 5. Drone-to-Ground authentication time under varying # of ground nodes

Looking at the total number of messages exchanged, as seen in Table II, our approach requires a single transmission message from each drone while this will increase with the number of ground nodes in the unicast-based authentication. Moreover, a drone in centralized group authentication needs to reach the observer and the CC which increases the TX count. Given that RX count is similar for all approaches, our broadcast-based proxy approach consumes the least energy.

TABLE II
TOTAL # OF MESSAGES FOR DRONE-TO-GROUND AUTHENTICATION.

	Centralized Authentication		**Unicast-based Proxy Signature**		**Broadcast-based Proxy Signature**	
# of Ground Nodes	TX	RX	TX	RX	TX	RX
10	5	14	10	10	1	10
20	5	24	20	20	1	20
30	5	34	30	30	1	30
40	5	44	40	40	1	40
50	5	54	50	50	1	50

VI. CONCLUSION

In this paper, we presented a fast and lightweight authentication mechanism for introducing drones to a post-disaster adhoc network with mmWave links. First portion of our approach authenticates drones to each other in short distances while the second focuses on authenticating the drones to ground user nodes. We utilized a proxy signature based authentication mechanism so that any newly joining drone can authenticate itself to any of the existing ones and vice versa by presenting a signature that can be traced back to a CC. The drone to ground authentication is also based on this proxy signature that comes as a challenge from the drone to ground users within a broadcast message. The proposed authentication mechanism is implemented and tested under NS-3 by utilizing mmWave channel from IEEE 802.11ad standard and relying on the computations from a Raspberry PI. The results shows that our proposed authentication is fast, reliable and more importantly scalable to larger ad hoc networks.

REFERENCES

[1] R. Bishop, "A survey of intelligent vehicle applications worldwide," in *Proceedings of the IEEE Intelligent Vehicles Symposium (Cat. No.00TH8511)*, 10 2000, pp. 25–30.

[2] B. Braunstein, T. Trimble, R. Mishra, B. Manoj, L. Lenert, and R. Rao, "Challenges in using distributed wireless mesh networks in emergency response," in *International ISCRAM Conference*, 5 2006, pp. 30–38.

[3] T. S. Rappaport, S. Sun, R. Mayzus, H. Zhao, Y. Azar, K. Wang, G. N. Wong, J. K. Schulz, M. Samimi, and F. Gutierrez, "Millimeter wave mobile communications for 5g cellular: It will work!" *IEEE Access*, vol. 1, pp. 335–349, 2013.

[4] X. Wu, C. X. Wang, J. Sun, J. Huang, R. Feng, Y. Yang, and X. Ge, "60-ghz millimeter-wave channel measurements and modeling for indoor office environments," *IEEE Transactions on Antennas and Propagation*, vol. 65, no. 4, pp. 1912–1924, 4 2017.

[5] W. Roh, J. Y. Seol, J. Park, B. Lee, J. Lee, Y. Kim, J. Cho, K. Cheun, and F. Aryanfar, "Millimeter-wave beamforming as an enabling technology for 5g cellular communications: theoretical feasibility and prototype results," *IEEE Communications Magazine*, vol. 52, no. 2, pp. 106–113, 2 2014.

[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] 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.

[9] 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.

[10] 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.

[11] G. K. Verma, B. Singh, N. Kumar, and D. He, "Cb-ps: An efficient short-certificate-based proxy signature scheme for uavs," *IEEE Systems Journal*, 7 2019.

[12] F. Zhang and K. Kim, "Efficient id-based blind signature and proxy signature from bilinear pairings," in *Australasian Conference on Information Security and Privacy*. Springer, 7 2003, pp. 312–323.

[13] W. Liu, Y. Mu, G. Yang, and Y. Tian, "Strong identity-based proxy signature schemes, revisited," *Wireless Communications and Mobile Computing*, vol. 2018, 2018.

[14] D. Magrin, M. Centenaro, and L. Vangelista, "Performance evaluation of lora networks in a smart city scenario," in *2017 IEEE International Conference on communications (ICC)*. ieee, 5 2017, pp. 1–7.

[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] M. A. Abdel-Malek, A. S. Ibrahim, M. Mokhtar, and K. Akkaya, "Uav positioning for out-of-band integrated access and backhaul millimeter wave network," *Physical Communication*, vol. 35, p. 100721, 8 2019.

[17] ns 3, "ns-3: network simulator 3," Release 3.24.1, 2016. [Online]. Available: http://www.nsnam.org/

[18] H. Assasa and J. Widmer, "Implementation and evaluation of a wlan ieee 802.11 ad model in ns-3," in *ACM Proceedings of the Workshop on ns-3*, 6 2016, pp. 57–64.