An Efficient and Secure Certificate-Based Access Control and Key Agreement Scheme for Flying Ad hoc Networks

Muhammad Asghar Khan, Insaf Ullah, Neeraj Kumar, Omar Sami Oubbati, I Qureshi, Fazal Noor, Fahim Ullah

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2021.3055895, IEEE Transactions on Vehicular Technology

An Efficient and Secure Certificate-Based Access Control and Key Agreement Scheme for Flying Ad-hoc Networks

Muhammad Asghar Khan, Insaf Ullah, Neeraj Kumar, Omar Sami Oubbati, Ijaz Mansoor Qureshi, Fazal Noor and Fahim Ullah

***Abstract*—The evolution of Flying Ad-hoc Networks (FANETs) marks the paradigm shift from a single large drone to multiple small drones linked together in an ad-hoc fashion. To maintain the Quality of Service (QoS) in the multi-hop networking schema, FANETs utilize the available resources efficiently. However, due to open wireless boundary and high mobility of the drones, the FANETs are vulnerable to malicious nodes that can penetrate the network and, thus, pose serious security threats, particularly at the Medium Access Control (MAC) layer. Such susceptibility compromises the network security and privacy and harms the information exchange operation within the network. The attacker can either transmit a large number of reservation requests to waste the bandwidth, listen to the control messages, conduct power-efficient jamming or falsify the information to manipulate the network control. Therefore, secure access control and a key agreement mechanism are required. The mechanism must utilize the two phases, i.e., node authentication and key agreement, to counter the aforementioned attacks. Our contribution, in this paper, is a certificate-based access control and key agreement scheme, which is based on the technique of Hyperelliptic Curve Cryptography (HECC) and employs a collision-resistant one-way cryptographic hash function. In order to assess the viability and performance of the proposed scheme, we analyze it using formal security analysis techniques, such as the Real-Or-Random (ROR) model and Automated Validation of Internet Security Protocols and Applications (AVISPA) tool. The scheme is also evaluated using the informal security analysis technique, or the non-mathematical approach. The results obtained from both analyses affirm the superiority of our proposed scheme.**

***Index Terms*—Flying Ad-hoc Networks (FANETs), Drones, Security, Access Control, Key-Agreement, AVISPA.**

I. Introduction

Flying Ad-hoc Networks (FANETs) provide a decentralized communication mechanism that evolves due to coordination between a group of small drones [1],[2]. Although a FANET system is characterized by an ad-hoc mechanism, some of its features distinguish it from the predecessor ad-hoc networks, such as Mobile Ad-hoc Networks (MANETs) and Vehicular Ad-hoc Networks (VANETs). For instance, the nodes in a FANET system have higher mobility than those in VANETs and MANETs. Certainly, FANET nodes can either be static, particularly in the relaying network purposes or dynamic, where FANET nodes have ample freedom of movement and are agile enough to move and rotate in the three-dimensional (3D) space [3]. Such distinctive attributes make FANETs a suitable choice for time-limit and mission-critical tasks. However, on the other hand, it inherits challenges in terms of security and privacy [4],[5]. Thus, the participating drones in a FANET system should, in addition to handling the requests securely, maintain the integrity, and ensure an uninterrupted availability.

Efficient and secure communication among the drones, for the network layer, has received ample attention from the researchers. The research endeavors, however, have barely explored the security facet at the Medium Access Control (MAC) layer. The pivotal role played by the MAC layer cannot be ignored as it allows easy access to the broadcast radio channel [6],[7]. There are a few solutions in the existing literature that suggest exploring new and efficient MAC communication mechanisms for drones [8]. So far, system optimization for improved efficiency and fair common channel access has remained the primary aim of the existing solutions. However, the problem of security lapse is not well investigated.

Typically, the design consideration of small drones rarely addresses the security dimensions. Therefore, small drones are susceptible to cyber intrusions and physical attacks [9],[10],[11],[12],[13],[14]. For instance, merely granting the adversary access to the network can result in irreparable damages. The adversary can waste bandwidth by transmitting multiple reservation requests. Also, the attacker can listen to the control messages, resort to power-efficient jamming or falsify the information [15]. The inherent physical constraints arising due to limited on-board energy and limited computing capability, further exacerbate the situation. Moreover, a drone can become a luring target when hovering over a hostile environment.

In a FANET environment, the participating drones interact using IEEE 802.11, IEEE 802.15.4, and other notable wireless

M.Khan is with ISRA University and Hamdard Institute of Engineering & Technology, Islamabad, Pakistan (e-mail: khayyam2302@gmail.com).

I.Ullah is with Hamdard Institute of Engineering & Technology, Islamabad, Pakistan (e-mail: insafktk@gmail.com).

N.Kumar is with CSED, Thapar Institute of Engineering and Technology, Patiala, India (e-mail: Neeraj.kumar@thapar.edu).

O.Oubbati is with the Electronics Department, University of Laghouat, Algeria (e-mail: s.oubbati@lagh-univ.dz).

I.Qureshi is with the Electrical Engineering Department, Air University, Islamabad, Pakistan (e-mail: imqureshi@mail.au.edu.pk).

F.Noor is with the Faculty of Computer Science and Information Systems, Islamic University of Madinah (e-mail: mfnoor@gmail.com).

F.Ullah is with Descon Engineering Limited, Lahore, Pakistan (e-mail: fahimullahk@gmail.com).

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2021.3055895, IEEE Transactions on Vehicular Technology

communication standards. Such wireless communication standards not only provide connectivity, but also offer a communication link that is light-weight and cost-effective [16],[17]. Such standards usually rely on the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) protocol. Therefore, the decision to transmit energy is conditional upon the scenario when a legitimate node occupies a wireless medium. In the worst-case scenario, when a jammer throngs the same channel, data packets might collide and cause significant degradation in the network performance. It is observed that the issue of CRC (cyclic redundancy check) persists during packet collision. The sender attempts to re-transmit the lost packets, or the corrupted packets. Thus, the packet collision qualifies as a DoS attack. To prevent suchlike untoward incidents from happening, there is a need to design a secure, computationally efficient, and cost-effective authentication scheme for FANETs.

A. Research Motivation and Contributions

Superb efforts have been made to address the underlying challenges on the way to ensure optimum usage of FANETs. The limitations of constrained on-board vitality and restricted computational ability severely hamper such efforts. The drones are, therefore, restricted from flying for long intervals and from performing complex cryptographic tasks. This constraint requires efficient security mechanisms that can stabilize the battery lifetime and incur lower computational and communication costs. We aim to meet the objectives mentioned above and do so by coming forth with an efficient scheme that is certificate-based and aggregates access control and key agreement. The efforts, particularly, add additional security attributes to the Medium Access Control (MAC) layer. Salient features of our research work are as follows:

- We approach the concept of Hyperelliptic Curve Cryptography (HECC) to come forth with certificate-based access control and key agreement scheme. This supplements the work done by Das et al. [51], Malani et al. [53], and Odelu et.al [54]. An evident benefit of a hyperelliptic curve is its compactness since it requires an 80-bit key, which is way smaller than that needed by elliptic curve.
- The proposed scheme is analyzed using formal and informal analysis techniques. It demonstrates to be sturdy enough to thwart attacks. For carrying out the formal analysis, the methodologies of AVISPA [55] and ROR [52] are used.
- To improve efficiency, we propose a dual-radio strategy that caters to the demands of low power and high data rate operations. The proposed approach harnesses the robust features of each of the two options: the high-speed data transmission rate of IEEE 802.11; and the low-power consumption characteristics of IEEE 802.15.4.
- A detailed comparative analysis has been carried out to evaluate the feasibility in terms of computational costs, security features, and functionalities. The findings manifest the superiority of the proposed scheme, as compared to the existing solutions.

B. Organization of the Paper

The manuscript is structured section-wise. The related work is portrayed in Section II. A commentary about the system models is presented in Section III. The proposed scheme is exhibited in Section VI. Security analyses, both formal and informal, are discussed in Section V. The AVISPA tool is used for formal security verification and the findings are presented in Section VII. A comparative analysis is presented in Section VII. Section VIII, the final section, offers a succinct conclusion.

II. Related work

This section presents a literature review that comprises of three main subsections: the first subsection explains security schemes in FANETs, the second subsection describes security schemes at MAC layer, and the third subsection presents access control and key-agreement schemes.

A. Security Schemes in Flying Ad-hoc Networks

Uninterrupted communication plays a vital role in a FANET environment, since it is the primary pre-requisite for enabling the applications that require continuous connectedness. Therefore, the deficiencies that result in security lapses, reduced efficiency and lower reliability, need to be addressed [18]. The existing security mechanisms for FANETs, primarily, deal with authenticity, confidentiality and data integrity. The issue of data protection has, so far, remained unaddressed. Incorporating efficient data protection schemes in a FANET environment can offer a strong defense against the intrusions. In [19],[20] the authors aim to counter the broadcast storm problem that occurs in FANETs. In [21] the authors propose a secure group key establishment protocol that assists drones to form groups within the network. The protocol, however, focuses on the main goal ignoring the issues encountered in the transmission stage, such as a hidden terminal, exposed terminal and proximity problems.

A blind signature scheme for FANETs in a certificateless setting, primarily for authentication, has been proposed by Khan et al. in [22]. The scheme, however, does not accommodate the provision of confidentiality and authentication in one go. Therefore, the key-encapsulated certificateless signcryption scheme proposed by Khan et al. in [23] is characterized by offering confidentiality as well as authentication in a simultaneous manner. Still, neither of the schemes addressed the issue of coping with threats, both known as well as unknown, at the MAC layer.

B. Security Schemes at Medium Access Control layer

The research efforts on the topic of wireless MAC security have, so far, remained limited to addressing the concomitant threats in isolation. For instance, from the existing literature, studies undertaken so far focus on following issues: Denial of Service (DoS) attacks to jam the system [24],[25],[26],[27],[28],[29]; transmitting bogus requests to the reserve channels [30],[31],[32],[33]; falsifying information at the communication feedback point(s) [34]; sleeping-based MAC [35],[36],[37],[38] that is vulnerable especially in case an attacker knows the MAC layer information [39]; and

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2021.3055895, IEEE Transactions on Vehicular Technology

energy DoS attacks [40],[41]. Reportedly, there is no research attempt aimed at addressing the issue of multiple threats originating at the same time. Therefore, the system remains vulnerable to attackers, who can launch multiple attacks. Moreover, other security requirements of FANETs, such as integrity, confidentiality and non-repudiation etc., have also not been given due consideration. Therefore, the need to ponder over and formulate a newer security scheme has further intensified. The very scheme must be able to cope with multiple security challenges. The approaches considered as a reference in our study aim to enhance the security and privacy features of the network. By presenting a solution that addresses the security requirements in a holistic manner, our proposed approach takes such research to a new level.

C. Access Control and Key-Agreement Schemes

A novel authentication and key agreement (AKA) scheme have been proposed by Semal et al. in [42] between users and nodes. The scheme makes use of hash function and bitwise XOR operation. It does not require a gateway node and is suitable for resource-constrained nodes. The scheme, however, was prone to man-in-the-middle and node impersonation attacks. Further, it lacked the capability to trace the users and to conceal the identification. Later, a new AKA scheme proposed by Farash et al. addressed and proposed viable solutions to the very issues in [43] Afterwards, Amin et al. [44] highlighted the deficiencies in the work of Farash et al. [43] and proposed an AKA scheme based on smart card. The significant shortcomings addressed in [44], for instance, included disposition to temporary information attack, off-line password guessing attack and user impersonation attack etc. However, the claim was dismissed by Jiang et al. [45] who identified plausible weaknesses, such as smart card loss attack and off-line password guessing attack, in [43].

Challa et al. [46] came forth with a new signature-based AKA scheme based on elliptic curve cryptography. Compared to its predecessors, the approach is characterized by increased communication and computation overhead. Wazid et al. [47] proposed a novel lightweight user AKA scheme for deploying an Internet of Drones (IoD) setup. The proposed scheme relied on one-way cryptographic hash functions and bitwise XOR operations. However, the proposed scheme fails to provide a session key agreement. To overcome such deficiency, Zhang et al. [48] proposed an improved alternate.

Li et al. [49] designed an access control mechanism that is based on an identity-based access control (IBAC) model and uses bilinear pairing operations. The mechanism paves ways for a sender-receiver connection whereby the sender, from a certificate-less cryptography (CLC) environment, can link up and transmit a message to a receiver, who is in the identity-based cryptography (IBC) environment. For implementation, the mechanism demands a gateway node between the two IoT smart devices, and it also incurs high costs.

The efficient access control protocol scheme proposed by Luo et al. [50] relies on IBC and bilinear pairing to link up with a smart device having different system parameters. The scheme demands a separate gateway node and is not economical. Further, the two-phase approach proposed by Das et al. [51], Malani et al. [53] and Odelu et al. [54] aims for a secure communication scenario between two sensing nodes. It involves node authentication, key agreement and the concept of elliptic curve cryptography. An apparent drawback of such scheme is the hefty costs We aim to address the aforesaid deficiencies and, as a coping mechanism, propose a certificate-based access control scheme for FANETs. The scheme is based on hyperelliptic curve and demonstrates to be far more secure and efficient. Another important feature is the compactness of its key size (80 bits), which is half as much required by the elliptic curve (160 bits).

III. SYSTEM MODELS

Two models, i.e. network model and threat model, have been utilized to demonstrate the applicability of the proposed scheme.

A. Network Model

There are "n" drones, where $n \geq 2$ as shown in Fig.1. The drones are categorized into either of the two groups: Sensor Drone (S-Drone) and Gateway Drone (G-Drone). Drones from both the groups are placed in the geographical clusters that collectively make up the mission area. Each of the drones, from both G-Drones and S-Drones, are assigned a unique ID. A cluster has fixed number of drones out of which there must be a G-Drone that is linked to the ground station. A drone has following three layers: physical layer (bottom part), data link layer (middle part) and upper layer (top port). The IEEE 802.15.4 (ZigBee) system is installed on Sensor Drones (S-Drones). Gateway Drones (G-Drones) leverage both the radio technologies i.e. IEEE 802.15.4 (ZigBee) and IEEE 802.11a (Wi-Fi). In this way, the features promised by IEEE 802.11a (high-speed data transmission) and IEEE 802.15.4 (low-power consumption) are utilized by the proposed system. The process of network formation kicks off as soon as a drone lifts off. Here, the drones are, supposedly, fed the information about neighbor's zone ID, location, altitude and speed etc. Further, the information does include the height sensors, IMU, GPS unit and the flight controller etc. The associated drones are interlinked together using the discovery function, which makes use of the beacon signals. Transmission of data between the S-Drones and G-Drones is accomplished using IEEE 802.15.4 at the frequency of 2.4 GHz. On the other hand, the data is routed between G-Drones and the ground station using IEEE 802.11a at the frequency of 5 GHz. An immediate pay off of the scheme is lower computational cost on the ground station since it only retains the information directed to it.

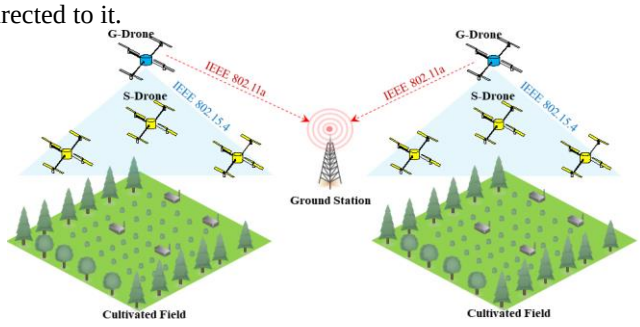

Fig.1. Network model

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2021.3055895, IEEE Transactions on Vehicular Technology

B. Threat Model

Dolev-Yao (DY) model is employed, which entails an insecure channel communication and an untrustworthy nature between the parties [56]. Thus, the malicious attacker can easily eavesdrop and tamper the exchanged messages. The worst-case scenario, for instance, might involve seizing a drone, that is hovering, and then compromising its data. The prevalent "Canetti and Krawczyk's adversary model (CK-adversary model)" is, reportedly, the de facto standard for modelling the authenticated key exchange protocols. The CK-adversary model entails that the adversary can also hack the secret credentials, secret keys and the session states.

Therefore, it has become an essential requirement that "the leakage of some forms of secret credentials, such as session ephemeral secrets or secret key, should have the minimum possible consequence on the secrecy of other secret credentials of the communicating participants" [58].

IV. PROPOSED SCHEME

This section is dedicated to present the proposed scheme, which is based on hyperelliptic curve (HEC) and utilizes the one-way cryptographic hash function. The proposed approach is composed of following four steps i.e., Setup, Drones Registration, Drones Access Control Process and New Drone Addition Phase. Each of the steps is explained as follows.

A. Setup

The setup step is executed by the certifier's authority ($\mathcal{C}_{rs}\mathcal{A}$). The prime intention is to generate private and public keys. Further, a public parameter set is prepared in this step. The following sequence is followed for performing such computations.

1. $\mathcal{C}_{rs}\mathcal{A}$ first choose d_{rs} from the set $\{1,2,3,\ldots\ldots,n-1\}$ as his private key.
2. It computes the public key as follows: $w_{rs} = d_{rs}.D$, where, D is the divisor on a hyper elliptic curve.
3. It selects the hash function $\hbar$, which has the capacity to avoid collisions and is characterized by irreversibility.
4. It selects the public parameter set as: $\eta = (w_{rs}, D, n, \hbar)$ and publishes it.

B. Drones Registration

The drone registration step takes into consideration all of the deployed drones, $\mathcal{DRN}_u$. It is supposed that the authority, $\mathcal{C}_{rs}\mathcal{A}$, wants to register them, in the offline manner. The process proceeds in the following sequence:

1. For each $\mathcal{DRN}_u$, $\mathcal{C}_{rs}\mathcal{A}$ selects an identity ID_u and a private key, a_u, from the set $\{1,2,3,\ldots\ldots,n-1\}$
2. It computes the public ID_u using the following relation: $b_u = a_u.D$
3. It selects f_u from $\{1,2,3,\ldots\ldots,n-1\}$ and computes the value of X_u as: $X_u = (f_u + a_u).D$
4. It calculates the certificate for ID_u as: $Cr_u = w_{rs} + (f_u + a_u)\hbar(ID_u \| X_u)$.
5. In the final step, $\mathcal{C}_{rs}\mathcal{A}$ pre-loads the identity set $(ID_u, Cr_u, b_u, a_u, X_u)$ to the memory of $\mathcal{DRN}_u$.

TABLE I
SYMBOLS AND THEIR DESCRIPTIONS

S. No	Symbol	Descriptions
1	$\mathcal{C}_{rs}\mathcal{A}$	certifier's authority
2	d_{rs}	private key of $\mathcal{C}_{rs}\mathcal{A}$
3	w_{rs}	public key of $\mathcal{C}_{rs}\mathcal{A}$
4	D	Divisor of hyper elliptic curve
5	n	A large prime number as $n \leqslant 2^{80}$
6	$\hbar$	Collision resistant hash function
7	η	public parameter set
8	$\mathcal{DRN}_u$, $\mathcal{DRN}_v$	Two communicating drones
9	ID_u	Identity of $\mathcal{DRN}_u$
10	ID_v	Identity of $\mathcal{DRN}_v$
11	a_u	Private key of $\mathcal{DRN}_u$
12	a_v	Private key of $\mathcal{DRN}_v$
13	b_u	Public key of $\mathcal{DRN}_u$
14	b_v	Public key of $\mathcal{DRN}_v$
15	Cr_u	Certificate of $\mathcal{DRN}_u$
16	Cr_v	Certificate of $\mathcal{DRN}_v$
17	NON_{eu}	A nonce which is encrypted by $\mathcal{DRN}_u$
18	NON_{euv}	A nonce which is encrypted by $\mathcal{DRN}_v$
19	$\mathcal{DRN}_{new}$	Represents new drone
20	ID_{new}	Identity of $\mathcal{DRN}_{new}$
21	a_{new}	Private key of $\mathcal{DRN}_{new}$
22	b_{new}	Public key of $\mathcal{DRN}_{new}$
23	Cr_{new}	Certificate of $\mathcal{DRN}_{new}$

C. Drones Access Control Process

Assume that two drones, say $\mathcal{DRN}_u$ and $\mathcal{DRN}_v$, wish to interconnect for having a key establishment mechanism. To undertake the process, there are four phases.

Phase # 1. If $\mathcal{DRN}_u$ wants to establish a key with $\mathcal{DRN}_v$, the actions are performed as follows:

- It chooses ε_u from $\{1,2,3,\ldots\ldots,n-1\}$
- It computes $\Omega_u = \varepsilon_u.D$
- It selects a fresh nonce N_u
- It encrypts the NON_{eu} *and* ID_u as $NON_{eu} = E_{b_v}(N_u, ID_u)$
- It computes $\Lambda_u = Cr_u + \hbar(ID_u \| Cr_u \| b_u \| X_u)(\varepsilon_u + a_u)$ as a signature on ε_u
- Finally, it dispatches the key $\Psi_1 = (NON_{eu}, \Omega_u, \Lambda_u, b_u, X_u, Cr_u)$ to $\mathcal{DRN}_v$ via open network.

Phase # 2. Here, after the receiving the key Ψ_1, $\mathcal{DRN}_v$ performs the following computations:

- It decrypts N_u, $ID_u = D_{a_v}(NON_{eu})$ and checks for the freshness of N_u
- It checks for certificate of the source drone by applying the condition:

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2021.3055895, IEEE Transactions on Vehicular Technology

$(w_{rs} + X_u.h(ID_u \| X_u)) \stackrel{?}{=} Cr_u.D.$

- It attempts to verify the signature and, to do so, it checks for the relation: $(Cr_u.D + (\Omega_u + b_u).h(X_u \| \Omega_u \| Cr_u \| b_u \| NON_{eu})) \stackrel{?}{=} \Lambda_u.D$
- If the signature is valid, it computes the value of Ω_v using the following relation:
  $\Omega_v = \varepsilon_v.D$, where ε_u belongs to $\{1,2,3,\ldots\ldots,n-1\}$
- It computes Λ_v using the following relation: $\Lambda_v = Cr_v + h(ID_v \| Cr_v \| b_v \| X_v)(\varepsilon_v + a_v)$
- It performs the following calculations:
  $Y_{uv} = \varepsilon_v.\Omega_u = \varepsilon_v.\varepsilon_u.D$
  $\mu_{uv} = a_v.b_u = a_v.a_u.D$
- It computes the value of NON_{euv} using the relation $NON_{euv} = E_{b_u}(N_u, N_v)$
- It finds out the value of session key, to be shared with DRN_u, from the relation $K_{uv} = h(ID_u \| NON_{euv} \| Y_{uv} \| \mu_{uv} \| ID_v)$
- Here, K_{uv} can be verified since $VK_{uv} = h(NON_{euv} \| K_{uv})$
- Finally, DRN_v transmits Ψ_2, where $\Psi_2 = (NON_{euv}, \Omega_v, \Lambda_v, b_v, X_v, Cr_v, VK_{uv}, ID_v)$, to DRN_u via open network.

Phase # 3. In this phase, after receiving Ψ_2, DRN_u proceeds with the computations as follows.

- It first decrypts $(N_u, N_v) = D_{a_u}(NON_{euv})$ and checks for the freshness of N_v
- It checks for certificate of the source drone and ascertains for applicability of the following condition: $(w_{rs} + X_v.h(ID_v \| X_v)) \stackrel{?}{=} Cr_v.D$
- It verifies the signature by checking for the applicability of the following condition:
  $(Cr_v.D + (\Omega_v + b_v).h(X_v \| \Omega_v \| Cr_v \| b_v \| NON_{euv})) \stackrel{?}{=} \Lambda_v.D$
- It performs following calculations: $Y_{uv}^{\bullet} = \varepsilon_u.\Omega_v = \varepsilon_u.\varepsilon_v.D$ and $\mu_{uv}^{\bullet} = a_u.b_v = a_u.a_v.D$
- It computes the value of NON_{euv} using the relation: $NON_{euv} = E_{b_v}(N_u, N_v)$
- It finds out the value of session key using the relation:
  $K_{uv}^{\bullet} = h(ID_u \| NON_{euv} \| Y_{uv}^{\bullet} \| \mu_{uv}^{\bullet} \| ID_v)$
- At this step, $K_{uv}^{\bullet}$ can be verified since $VK_{uv}^{\bullet} = h(NON_{euv} \| K_{uv}^{\bullet})$
- Finally, DRN_u transmits $\Psi_3 = (NON_{euv}, VK_{uv}^{\bullet})$ to DRN_v via open network

Phase # 4. Here, after the receiving Ψ_3, DRN_v proceeds with the computations as follows.

- It decrypts $(N_u, N_v) = D_{a_v}(NON_{euv})$ and checks if N_u is fresh
- In case if N_u is found to be anew, it calculates VK_{uv}^{**} using the relation:
  $VK_{uv}^{**} = h(NON_{euv} \| K_{uv})$
- It also checks if the relation $VK_{uv}^{**} \stackrel{?}{=} VK_{uv}^{\bullet}$ holds true
- The following equality can also be authenticated: $VK_{uv} \stackrel{?}{=} VK_{uv}^{\bullet}$

D. New Drone Addition Phase

This phase involves addition of a new drone DRN_{new} after establishment of a network. DRN_{new} includes $C_{rs}A$ in an offline manner. The process proceeds stepwise as follows:

- For DRN_{new}, $C_{rs}A$ choses an identity ID_{new} and assigns a private key a_{new} from $\{1,2,3,\ldots\ldots,n-1\}$
- It computes public identity ID_{new} using the relation: $b_{new} = a_{new}.D$.
- It selects f_{new} from $\{1,2,3,\ldots\ldots,n-1\}$ and performs the following computation:
  $X_{new} = (f_{new} + a_{new}).D$
- It calculates certificate for the identity ID_{new} using the relation:
  $Cr_u = w_{rs} + (f_{new} + a_{new})h(ID_{new} \| X_{new})$
- Finally, $C_{rs}A$ pre-loads the set $(ID_{new}, Cr_{new}, b_{new}, a_{new}, X_{new})$ to the memory of DRN_{new}

V. SECURITY ANALYSIS

Definition 1 (Collision-Resistant Cryptographic One-Way Hash Function): A ''collision-resistant cryptographic one-way hash function'' h: $\{0, 1\}^* \rightarrow \{0, 1\}^n$ is a ''deterministic mathematical function that produces a fixed length output string of n bits against a variable length input string''.

Definition 2 (Hyper elliptic curve Discrete logarithm problem (HECDLP)): The HECDLP is a hard problem in which the attacker attempts to extract f from the relation $L=f.D$, where f is the uniformly selected number from$\{1,2,3,\ldots\ldots,n-1\}$.

A. Formal Security Analysis Through ROR Model

The widely-accepted "Real-Or-Random (ROR) model" [52] has been used to prove the existence of semantic security (secret key security) in the proposed scheme (ACKA-FANETs). Under the ROR model, it is assumed that there exists an intruder A aiming to target a drone D^S during communication at a stage S^{Th}. In the proposed scheme, the drone D^S is represented by the variables DRN_u and DRN_v. The variables DRN_u^S and DRN_u^U are used to depict S^{Th} and U^{Th} occurrences of DRN_u and DRN_v respectively. The queries to be initiated by the intruder A, that can harm the operations, can be classified as follows:

1. **Execute query**: The execute query allows the intruder A to capture the transmitted messages while the communication link is being established between DRN_u and DRN_v.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2021.3055895, IEEE Transactions on Vehicular Technology

2. **Reveal query***:* The reveal query is intended to disclose the secret key established between $\mathcal{DRN}_u$ and $\mathcal{DRN}_v$.
3. **Test query:** In the test query the intruder $\mathcal{A}$ requests the drone $\mathcal{D}^S$ for a secret key. The drone $\mathcal{D}^S$reverts with a probabilistic result $\mathcal{C}$, where $\mathcal{C}$ denotes the randomly-chosen bits.

We also make it clear that a hash function is used for a random oracle, which is accessible to the intruder $\mathcal{A}$ as well as other connected drones. By applying Theorem 1, explained in the following para, we demonstrate that our proposed scheme has a robust and effective secret key security mechanism.

Theorem 1. Suppose the intruder $\mathcal{A}$, operating in a polynomial time $\mathcal{T}$, intends to break the security of a secret key using the games G_x, G_y and G_z. Here, the variables $|\hbar ash|, \mathcal{Q}_{hash}$ and $Ad_{\mathcal{A}}^{HECDLP}(\mathcal{T})$ represent the size of irreversible hash function $\hbar(.)$, the number of hash queries and the non-negligible winning advantages for $\mathcal{A}$ respectively. The pay-off that prompts the intruder $\mathcal{A}$ to jeopardize the secret key security between $\mathcal{DRN}_u$ and $\mathcal{DRN}_v$ in the access control step of the designed $ACKA$ scheme can be written as:

$$Ad_{\mathcal{A}}^{ACKA-FANETs}(\mathcal{T}) \leqslant {\mathcal{Q}_{hash}}^2 / |\hbar ash| + 2.\, Ad_{\mathcal{A}}^{HECDLP}(\mathcal{T}).$$

Proof. We prove the existence of semantic security (secret key security) in our proposed ACKA scheme. The security is based on equations 1 – 5. Here, it is being ascertained whether the ACKA scheme can shield against the secret key exposure attack or not. To do so, three games are considered. The winning advantage for the intruder $\mathcal{A}$ is given as:

$$Ad_{\mathcal{A},\, G_x,\, G_y, \text{and } G_z}^{HECDLP} = prob\,[wins_{\mathcal{A}}^{G_x,\, G_y, \text{and } G_z}].$$

***Game G_x*:** In game G_x, the intruder $\mathcal{A}$ employs the working capacity of the ROR model to attack and disturb the proposed $ACKA$ scheme. While the game is being initiated, the bit $\mathcal{C}$ is chosen uniformly. The following output is obtained:

$$Ad_{\mathcal{A}}^{ACKA-FANETs}(\mathcal{T}) = |2.\, Ad_{\mathcal{A},\, G_x,\, G_y, \text{and } G_z}^{HECDLP} - 1| \quad (1)$$

***Game G_y*:** In game G_y, the intruder $\mathcal{A}$ makes use of the "execute query" to tap the communication between $\mathcal{DRN}_u$ and $\mathcal{DRN}_v$. The activity takes place during the access control step of the proposed $ACKA$ scheme. The prime intention is to break the secret key security by capturing Ψ_1, Ψ_2 and Ψ_3. As a next step, $\mathcal{A}$ checks whether the secret key $\mathcal{K}_{uv}$, obtained from the communication between $\mathcal{DRN}_u$ and $\mathcal{DRN}_v$, is original or randomly selected. It does so to the reveal and test queries. Therefore, the secret key $\mathcal{K}_{uv}$, between $\mathcal{DRN}_u$ and $\mathcal{DRN}_v$, can be produced as follows:

$$\{\mathcal{K}_{uv} = \hbar(\, ID_u \| \, NON_{euv} \| \, \Upsilon_{uv} \| \, \mu_{uv} \| \, ID_v) = \hbar(\, ID_u \| \, NON_{euv} \| \, \Upsilon_{uv}^{\bullet} \| \, \mu_{uv}^{\bullet} \| \, ID_v)\}$$

To carry on the activity, $\mathcal{A}$ needs to know the following unknown values:

ε_u representing the randomly generated number $\mathcal{DRN}_u$;
ε_v representing the randomly generated number $\mathcal{DRN}_v$;
a_u representing the private key $\mathcal{DRN}_u$; and
a_v representing the private key $\mathcal{DRN}_v$.

When the very four values are known to the intruder $\mathcal{A}$, its probability to win reduces significantly. Hence, it is difficult to distinguish between $Game\ G_x$ and $Game\ G_y$ as depicted in the following relation:

$$Ad_{\mathcal{A},\, G_x}^{HECDLP} = Ad_{\mathcal{A},\, G_y}^{HECDLP} \quad (2)$$

***Game G_z*:** In game G_z, by exploiting the hash query, the intruder $\mathcal{A}$ can launch an aggressive attack against the proposed $ACKA$ scheme. In Ψ_1, Ψ_2 and Ψ_3 the values such as $\mathcal{CR}_u, \Lambda_u, \Lambda_v, \mathcal{CR}_v, \mathcal{VK}_{uv}$ and $\mathcal{VK}_{uv}^{\bullet}$ are protected through a collision resistant/one way hash function. Also, it is worth mentioning that even if the intruder is successful in capturing Ω_u and Ω_v, it would be impracticable to generate the following two keys:

1) $\{\Upsilon_{uv} = \varepsilon_v.\, \Omega_u = \varepsilon_v.\varepsilon_u.D = \Upsilon_{uv}^{\bullet} = \varepsilon_u.\, \Omega_v = \varepsilon_u.\varepsilon_v.D\}$
2) $\{\mu_{uv} = a_v.\, \mathcal{B}_u = a_v.a_u.D = \mu_{uv}^{\bullet} = a_u.\, \mathcal{B}_v = a_u.a_v.D\}$

It is difficult to perform the aforementioned computations because of the following two reasons:

1) In order to find out values of the involved variables, such as $\varepsilon_v, \varepsilon_u, a_v$ and a_u, cumbersome $HECDLP$ calculations are required.
2) The collision resistant property of hash function obstructs an attempt to find the values of ε_v, ε_u, a_v, and a_u from Λ_u and Λ_v

Even if the intruder $\mathcal{A}$ performs the hash query, no collision occurs. Also, it is difficult to distinguish between $Game\ G_y$ and $Game\ G_z$. Therefore, due to $HECDLP$ and owing to the concept of birthday paradox, the following output is obtained:

$$|Ad_{\mathcal{A},\, G_y}^{HECDLP} - Ad_{\mathcal{A},\, G_z}^{HECDLP}| \leqslant {\mathcal{Q}_{hash}}^2 / 2|\hbar ash| + Ad_{\mathcal{A}}^{HECDLP}(\mathcal{T}) \quad (3)$$

When $\mathcal{A}$ performs all of the possible queries and once it guesses the bit $\mathcal{C}$, it also performs the reveal and test query. This results in the following output:

$$Ad_{\mathcal{A},\, G_y}^{HECDLP} = 1/2 \quad (4)$$

From equations (1) and (2), we obtain the following output:

$$1/2\, Ad_{\mathcal{A}}^{ACKA-FANETs}(\mathcal{T}) = |Ad_{\mathcal{A},\, G_x,}^{HECDLP} - 1/2\,| = |Ad_{\mathcal{A},\, G_y,}^{HECDLP} - 1/2\,| \quad (5)$$

Similarly, making use of equations (1), (2) and (3) leads to the following output:

$$1/2\, Ad_{\mathcal{A}}^{ACKA-FANETs}(\mathcal{T}) = |Ad_{\mathcal{A},\, G_y}^{HECDLP} - Ad_{\mathcal{A},\, G_z}^{HECDLP}| \leqslant {\mathcal{Q}_{hash}}^2 / 2|\hbar ash| + Ad_{\mathcal{A}}^{HECDLP}(\mathcal{T}) \quad (6)$$

Multiplying equation (6) by "2" results in the following equation:

$$Ad_{\mathcal{A}}^{ACKA-FANETs}(\mathcal{T}) = |Ad_{\mathcal{A},\, G_y}^{HECDLP} - Ad_{\mathcal{A},\, G_z}^{HECDLP}| \leqslant {\mathcal{Q}_{hash}}^2 / |\hbar ash| + 2.\, Ad_{\mathcal{A}}^{HECDLP}(\mathcal{T})$$

B. Informal Security Analysis

1) Man-in-the-Middle Attack: Suppose the intruder $\mathcal{A}$ intends to alter the message Ψ_1, being transmitted between the drones $\mathcal{DRN}_u$ and $\mathcal{DRN}_v$. The message Ψ_1 comprises of multiple parameters and is given as:

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2021.3055895, IEEE Transactions on Vehicular Technology

$\Psi_1 = (\text{NON}_{eu}, \Omega_u, \Lambda_u, \mathcal{b}_u, \mathcal{X}_u, \mathcal{Cr}_u)$

Thus, to be successful in its malicious attempt, the intruder $\mathcal{A}$ will need to estimate the values of Λ_u and NON_{eu}:

$\Lambda_u = \mathcal{Cr}_u + \mathcal{h}(ID_u \| \mathcal{Cr}_u \| \mathcal{b}_u \| \mathcal{X}_u)(\varepsilon_u + a_u)$

$\text{NON}_{eu} = E_{\mathcal{b}_v}(\text{N}_u)$

In other words, $\mathcal{A}$ must have the values of ε_u, a_u , and a_v, which can only be obtained from the following relations: $\Omega_u = \varepsilon_u . D$; $\mathcal{b}_u = a_u . D$ and $\mathcal{b}_v = a_v . D$. Performing such mathematical manoeuvre is impracticable since it is equivalent to solving the hyper elliptic curve discrete logarithm problem three times. Therefore, our scheme proves to be sturdy enough to resist the Man-in-the-Middle Attacks.

2) Drone Impersonation Attack: Suppose the intruder $\mathcal{A}$ attempts to impersonate $\mathcal{DRN}_v$ in order to generate the following message:

$\Psi_2 = (NON_{euv}, \Omega_v, \Lambda_v, \mathcal{b}_v, \mathcal{X}_v, \mathcal{Cr}_v, \mathcal{VK}_{uv}, ID_v)$

Such attempt will, in turn, demand extensive computations in order to generate the variables Λ_v, $\mathcal{VK}_{uv}$ and NON_{euv}. The mathematical relations along with the inherent calculation requirements are given as follows:

1. $\Lambda_v = \mathcal{Cr}_v + \mathcal{h}(ID_v \| \mathcal{Cr}_v \| \mathcal{b}_v \| \mathcal{X}_v)(\varepsilon_v + a_v)$

For Λ_v to execute such equation, it is essential for to extract the values of ε_v and a_v from the relations $\Omega_v = \varepsilon_v . D$ and $\mathcal{b}_v = a_v . D$ respectively.

2. $\mathcal{VK}_{uv} = \mathcal{h}(NON_{euv} \| \mathcal{K}_{uv})$

Here, to approach the value of $\mathcal{VK}_{uv}$, $\mathcal{A}$ is required to solve the following equation: $\mathcal{K}_{uv} = \mathcal{h}(ID_u \| NON_{euv} \| Y_{uv} \| \mu_{uv} \| ID_v)$. This, in turn, demands calculation to generate Y_{uv} and μ_{uv} using the relations $Y_{uv} = \varepsilon_v . \Omega_u$ *and* $\mu_{uv} = a_v . \mathcal{b}_u$ respectively.

3. $NON_{euv} = E_{\mathcal{b}_u}(N_u, N_v)$

In case of the variable NON_{euv}, $\mathcal{A}$ will need to have the value of a_u, which can be obtained by utilizing the equation $\mathcal{b}_u = a_u . D$.

In short, if the intruder $\mathcal{A}$ attempts to pose as $\mathcal{DRN}_v$, complex mathematical operations are required. Such mathematical maneuvers are equivalent to computing the hyper elliptic curve discrete logarithm problem for up to five times. This is infeasible. Therefore, the proposed ACKA scheme offers protection from the Drone impersonation attacks.

3) Replay Attack: We assume that the intruder $\mathcal{A}$, with the aim of intercepting communication between $\mathcal{DRN}_u$ and $\mathcal{DRN}_v$, attempts to capture and then replay the message, Ψ_1:

$\Psi_1 = (\text{NON}_{eu}, \Omega_u, \Lambda_u, \mathcal{b}_u, \mathcal{X}_u, \mathcal{Cr}_u)$

To proceed ahead, $\mathcal{A}$ will be required to compute the value of $\text{NON}_{eu} = E_{\mathcal{b}_v}(\text{N}_u)$. However, to do so, the value a_v needs to be extracted from the relation $\mathcal{b}_v = a_v . D$. The same process needs to be repeated in case replay is demanded for Ψ_2 and Ψ_3.

Here, again, performing such computational effort is equivalent to solving the hyper elliptic curve discrete logarithm problem, which is far too complex to be resolved by the intruder $\mathcal{A}$. Therefore, the proposed scheme guarantees protection from the Replay Attack.

4) Mutual Authentication: The proposed scheme provides mutual authentication. Suppose if $\mathcal{DRN}_u$ dispatches the Ciphertext $\Psi_1 = (\text{NON}_{eu}, \Omega_u, \Lambda_u, \mathcal{b}_u, \mathcal{X}_u, \mathcal{Cr}_u)$ to $\mathcal{DRN}_v$. After receiving the key Ψ_1, $\mathcal{DRN}_\text{v}$ performs the following computations:

- It decrypts $N_u = D_{a_v}(NON_{eu})$ and checks for the freshness of N_u
- It checks for certificate of the source drone by applying the condition: $(w_{rs} + \mathcal{X}_u . \mathcal{h}(ID_u \| \mathcal{X}_u)) \stackrel{?}{=} \mathcal{Cr}_u . D$.
- It attempts to verify the signature and to do so, it checks for the relation: $(\mathcal{Cr}_u . D + (\Omega_u + \mathcal{b}_u) . \mathcal{h}(\mathcal{X}_u \| \Omega_u \| \mathcal{Cr}_u \| \mathcal{b}_u \| NON_{eu})) \stackrel{?}{=} \Lambda_u . D$

In case of valid signature, the proposed scheme achieves mutual authentications.

5) Ephemeral Secret Leakage (ESL) Attack: Suppose the intruder $\mathcal{A}$ wants to generate the following session key:

$\mathcal{K}_{uv} = \mathcal{h}(ID_u \| NON_{euv} \| Y_{uv} \| \mu_{uv} \| ID_v)$ *or* $\mathcal{K}_{uv}^{\bullet} = \mathcal{h}(ID_u \| NON_{euv} \| Y_{uv}^{\bullet} \| \mu_{uv}^{\bullet} \| ID_v)$

In order to do so, it is essential for $\mathcal{A}$ to find out values of the following variables: $Y_{uv} = \varepsilon_v . \Omega_u$; $\mu_{uv} = a_v . \mathcal{b}_u$; $Y_{uv}^{\bullet} = \varepsilon_u . \Omega_v$ and $\mu_{uv}^{\bullet} = a_u . \mathcal{b}_v$. However, an attempt aimed at finding such values further stipulate the values of $\varepsilon_v, a_v, \varepsilon_u$, and a_u, which is equivalent to computing the hyper elliptic curve discrete logarithm problem four times. Thus, it can be concluded that the proposed scheme is resistant to the Ephemeral Secret Leakage (ESL) attacks as well.

6) Malicious Drone Deployment Attack: In this case, let's assume that the intruder $\mathcal{A}$, in an established network, makes an attempt to deploy a fake drone $\mathcal{DRN}_{fake}$. $\mathcal{A}$ proceeds as follows:

a. It chooses a fake identity, ID_{fake}, and a random private key, a_{fake}
b. It computes the public identity, ID_{fake}: $\mathcal{b}_{fake} = a_{fake} . D$
c. It selects $\mathcal{f}_{fake}$ and computes $\mathcal{X}_{fake}$: $\mathcal{X}_{fake} = (\mathcal{f}_{fake} + a_{fake}) . D$
d. It calculates the certificate for ID_{fake} as: $\mathcal{Cr}_{fake} = w_{fake} + (\mathcal{f}_{fake} + a_{fake}) \mathcal{h}(\text{ID}_{fake} \| \mathcal{X}_{fake})$
e. Finally, it pre-loads the set $(\text{ID}_{fake}, \mathcal{Cr}_{fake}, \mathcal{b}_{fake}, a_{fake}, \mathcal{X}_{fake})$ to the memory of $\mathcal{DRN}_{fake}$

However, in reality, to generate a genuine certificate for the fake drone $\mathcal{DRN}_{fake}$, the intruder must have the value of a_u, which can be obtained from the relation $\mathcal{b}_u = a_u . D$. Unfortunately, manipulating the very relation is as hard as computing an HECDLP. Therefore, in addition to other features, our solution protects the system from Malicious Drone Deployment Attacks.

7) Anonymity Preservation: Anonymity is preserved in our scheme. The Ciphertext i.e. $\Psi_1 = (\text{NON}_{eu}, \Omega_u, \Lambda_u, \mathcal{b}_u, \mathcal{X}_u, \mathcal{Cr}_u)$ does not contains drone identity directly. $\mathcal{A}$ can only extract ID_u from $\Lambda_u = \mathcal{Cr}_u + \mathcal{h}(\text{ID}_u \| \mathcal{Cr}_u \| \mathcal{b}_u \| \mathcal{X}_u)(\varepsilon_u + a_u)$. In order to get access to drone identity, random number ε_u and the private key a_u of $\mathcal{DRN}_\text{u}$ will be required. For that $\mathcal{A}$ will need to compute hyperelliptic curve discrete logarithmic problem twice. Further, it is hard to recover ID_u from

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2021.3055895, IEEE Transactions on Vehicular Technology

$\hbar(\mathrm{ID}_u \| \mathcal{Cr}_u \| \mathcal{b}_u \| \mathcal{X}_u)$, because of the one-way property of hash function. Thus, from the above debate it has been cleared that the proposed scheme ensures anonymity.

8) Resistance against Cloning Attack: In this particular attack, $\mathcal{A}$ can physically capture the drone device and copy the secret. However, this attack is not be possible in the proposed scheme due to the updating of secret key for each session.

9) Resistance against De-synchronization Attack: During the communication between sender and receiver, $\mathcal{A}$ can preclude the synchronized updating of the secret information. To prevent such attack, the receiver drone has the capacity of storing the old messages with their nonce in the database. Here, if $\mathcal{A}$ sends the cipher text $\Psi_1 = (\mathrm{NON}_{eu}, \Omega_u, \Lambda_u, \mathcal{b}_u, \mathcal{X}_u, \mathcal{Cr}_u)$ to the receiving drone, then the receiver drone decrypts the value NON_{eu} such as $N_u = D_{a_v}(NON_{eu})$ and check freshness of N_u. In this way, the receiver drone can avoid a *de-synchronization attack*.

10) Resistance against DoS Attack

The scheme is secured against the DoS attack. For example, if $\mathcal{DRN}_\mathrm{v}$ transmits Ψ_2, where $\Psi_2 = (NON_{euv}, \Omega_v, \Lambda_v, \mathcal{b}_v, \mathcal{X}_v, \mathcal{Cr}_v, \mathcal{VK}_{uv}, ID_v)$, to $\mathcal{DRN}_\mathrm{u}$, then recalling *phase #3* : after receiving Ψ_2, $\mathcal{DRN}_u$ proceeds with the series of computations as follows. It first decrypts $(N_u, N_v) = D_{a_u}(NON_{euv})$ and checks for the freshness of N_v and certificate of the source drone respectively to ascertains the applicability of the following condition: $(\mathcal{w}_{rs} + \mathcal{X}_v.\hbar(ID_v \| \mathcal{X}_v)) \stackrel{?}{=} \mathcal{Cr}_v.D$, and finally verifies the signature by checking for the applicability of the following condition:

$$(\mathcal{Cr}_v.D + (\Omega_v + \mathcal{b}_v).\hbar(\mathcal{X}_v \| \Omega_v \| \mathcal{Cr}_v \| \mathcal{b}_v \| NON_{euv})) \stackrel{?}{=} \Lambda_v.D$$

However, the aforementioned computation is hard for $\mathcal{A}$ to extract information for DoS attack.

VI. FORMAL SECURITY VERIFICATION USING AVISPA SIMULATION STUDY

The algorithms A1 and A2 succinctly portrays the manner the proposed scheme is implemented. Both Gateway Drones (G-Drones) and Ground Station (GS) use High-level protocol specification language (HLPSL). For running the simulation, we use a Hair Workstation having following specifications: Intel (R) Core TM i3-4010U @ 1.70 GHz, Windows 8.1 64-bit OS, Oracle VM Virtual Box (V 5.2.0.118431) and SPAN (V SPAN-ubunti-10.10-light_1). The algorithms A3 and A4 were used to carry out the execution tests, keeping in view OFMC and CL-AtSe back-ends, in order to evaluate the system's sturdiness to attacks. The simulations excluded SATMC and TA4SP as they are not compatible with bitwise XOR operations. A strong monitoring mechanism is also required and therefore, the back-ends surveil the probability of man-in-the-middle attack(s). The SPAN (Specific Protocol Animator for AVISPA) tool is also used for simulation purposes. The results, including the outcomes obtained from OFMC and AtSe, depicted in Fig. 2 and Fig.3, demonstrate the effectiveness of the proposed scheme.

Algorithm A1 High-level protocol specification language (HLPSL) code for Drone_u

```
role
role_Drnu(Drnu:agent,Drnv:agent,Bu:public_key,Bv:public_key,SN
D,RCV:channel(dy))
played_by Drnu
def=
   local
   State:nat,Nu:text,Nv:text,Xu:text,Idu:text,Cru:text,Eu:text,Xv:text,
Idv:text,Crv:text,Hash:hash_func,Ev:text
   init
      State := 0
   transition
      1. State=0 /\ RCV(start) =|> State':=1 /\ SND(Drnu.Drnv)
      2. State=1 /\ RCV(Drnv.Drnu) =|> State':=2 /\ Nu':=new() /\
SND(Drnu.{Nu'}_Bv)
      4. State=2 /\ RCV(Drnv.{Nu.Nv'}_Bu) =|> State':=3 /\
Eu':=new() /\ Xu':=new() /\ Cru':=new() /\ Idu':=new() /\
SND(Drnu.{Hash(Idu'.Cru'.Xu').Eu'}_inv(Bu))
      6. State=3 /\ RCV(Drnv.{Hash(Idv'.Crv'.Xv').Ev'}_inv(Bv)) =|>
State':=4
end role
```

Algorithm A1 High-level protocol specification language (HLPSL) code for Drone_v

```
role
role_Drnv(Drnv:agent,Drnu:agent,Bu:public_key,Bv:public_key,SN
D,RCV:channel(dy))
played_by Drnv
def=
   local
   State:nat,Nu:text,Nv:text,Xu:text,Idu:text,Cru:text,Eu:text,Xv:text,
Idv:text,Crv:text,Hash:hash_func,Ev:text
   init
      State := 0
   transition
      1. State=0 /\ RCV(Drnu.Drnv) =|> State':=1 /\ SND(Drnv.Drnu)
      3. State=1 /\ RCV(Drnu.{Nu'}_Bv) =|> State':=2 /\ Nv':=new()
/\ SND(Drnv.{Nu'.Nv'}_Bu)
      5. State=2 /\ RCV(Drnu.{Hash(Idu'.Cru'.Xu').Eu'}_inv(Bu)) =|>
State':=3 /\ Ev':=new() /\ Xv':=new() /\ Crv':=new() /\ Idv':=new() /\
SND(Drnv.{Hash(Idv'.Crv'.Xv').Ev'}_inv(Bv))
end role
```

Algorithm A3 High-level protocol specification language (HLPSL) code for Sessions role

```
role session1(Drnv:agent,Drnu:agent,Bu:public_key,Bv:public_key)
def=
   local
      SND2,RCV2,SND1,RCV1:channel(dy)
   composition
      role_Drnv(Drnv,Drnu,Bu,Bv,SND2,RCV2) /\
role_Drnu(Drnu,Drnv,Bu,Bv,SND1,RCV1)
end role

role session2(Drnu:agent,Drnv:agent,Bu:public_key,Bv:public_key)
def=
   local
      SND1,RCV1:channel(dy)
   composition
      role_Drnu(Drnu,Drnv,Bu,Bv,SND1,RCV1)
end role
```

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2021.3055895, IEEE Transactions on Vehicular Technology

Algorithm A3 High-level protocol specification language (HLPSL) code for Sessions role

```
role environment()
def=
   const
   hash_0:hash_func,bu:public_key,bob:agent,alice:agent,bv:public_
key,const_1:agent,const_2:public_key,const_3:public_key,auth_1:pro
tocol_id,sec_2:protocol_id
   intruder_knowledge = {alice,bob}
   composition
      session2(i,const_1,const_2,const_3) /\ session1(bob,alice,bu,bv)
end role

goal
   authentication_on auth_1
   secrecy_of sec_2
end goal
environment()
```

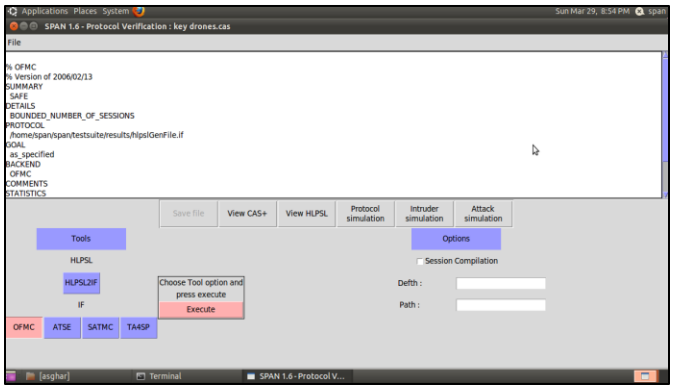

Fig.2. Simulation results for on-the-fly model-checker (OFMC

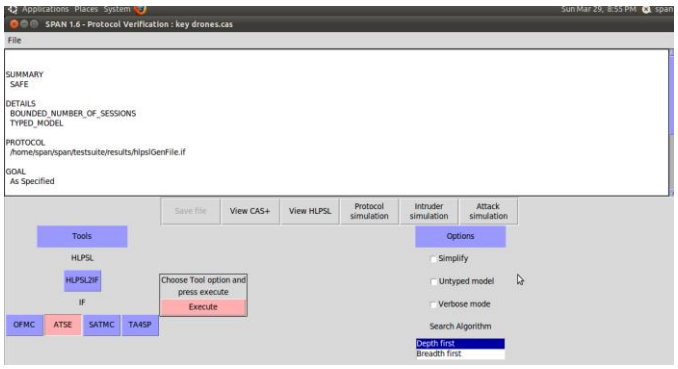

Fig.3. Simulation results for AtSe.

VII. COMPARATIVE ANALYSIS

Section VII is dedicated to present a comparative analysis of the proposed solution. Here, the proposed scheme is compared with the work done by Das et al. [51], Malani et al. [53], Semal et al. [42] and Odelu et al. [54].

A. *Computational Cost*

In this subsection, the proposed scheme is compared with the schemes proposed by Das et al. [51], Malani et al. [53], Semal et al. [42] and Odelu et al. [54]. The key results obtained from the comparison are shown in Table II to determine the effectiveness of the proposed scheme. The existing schemes either utilize elliptic curve scalar multiplication or bilinear pairings, both of which are more costly computational options. Therefore, we apply the hyperelliptic divisor multiplication. It has been shown from the results that the time it takes for a single scalar multiplication to be processed differs significantly: elliptic curve point multiplication (ECPM), 0.97 milliseconds; bilinear pairing, 14.90 ms; pairing-based point multiplication, 4.31 ms and modular exponentiation, 1.25 ms [59]. MIRACL, or Multi-precision Integer and Rational Arithmetic C Library, is used to assess the performance of the proposed scheme [60]. The library applies a large number of tests, up to 1000, on basic cryptographic operations. An Intel Core i7-4510U CPU having 2.0 GHz processor, 8 GB RAM and Windows 7 is used to run the simulations [59]. The Hyperelliptic Curve Divisor Multiplication (HCDM) is believed to be 0.48 milliseconds in duration [22],[23] due to a smaller key size of 80-bits. It is clear from the results in Table II and Table III that our method is much more effective in terms of the cost of computing, as shown in Fig. 4.

TABLE II
COMPARISON COMPUTATIONAL COSTS

Schemes	$\mathcal{DRN}_u$/device cost	$\mathcal{DRN}_v$/device cost	Total
Das *et al* [51]	6 em	6 em	12 em
Malani *et al* [53]	6 em	6 em	12 em
Semal *et al* [42]	2 $\mathcal{bp}m$	1$\mathcal{bp}$+3$mexp$	2 $\mathcal{bp}m$ +1$\mathcal{bp}$+3$mexp$
Odelu *et al* [54]	6 em	6 em	12 em
Our	6 $\mathcal{hm}$	6 $\mathcal{hm}$	12 $\mathcal{hm}$

Where,

$\mathcal{hm}$ = hyperelliptic curve divisor multiplication
em = elliptic curve scalar multiplication
$\mathcal{bp}$ = bilinear pairing
$\mathcal{bp}m$ = pairing-based point multiplications
$mexp$ = modular exponentiation

TABLE III
COMPARISON OF COMPUTATIONAL COSTS (IN MILLISECONDS)

Schemes	$\mathcal{DRN}_u$/smart IoT device	$\mathcal{DRN}_v$/smart IoT device	Total (in milliseconds)
Das *et al* [51]	5.28	5.28	10.56
Malani *et al* [53]	5.28	5.28	10.56
Semal *et al* [42]	8.62	18.65	27.27
Odelu *et al* [54]	5.28	5.28	10.56
Proposed	2.88	2.88	5.76

B. *Communication Cost*

This subsection is aimed at discussing the comparison results from the perspective of communication costs. The proposed approach is compared with the existing schemes presented by Das et al. [51], Malani et al. [53], Semal et al. [42] and Odelu et al. [54]. In comparative analysis, the variables used, along with the respective values, are depicted in Table V and illustrated in Fig 5.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2021.3055895, IEEE Transactions on Vehicular Technology

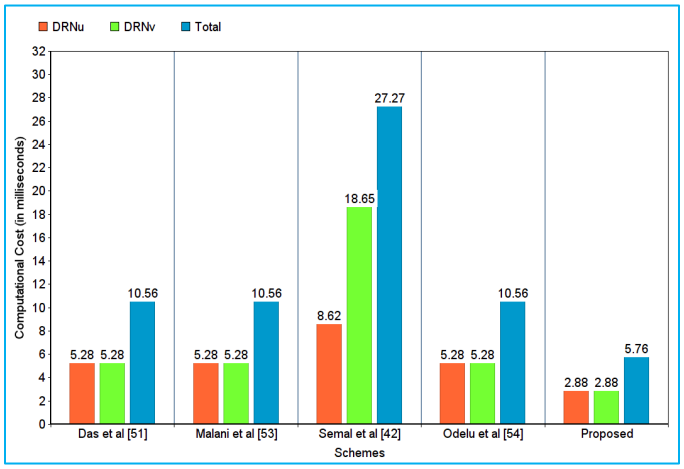

Fig.4. Computational cost (in ms)

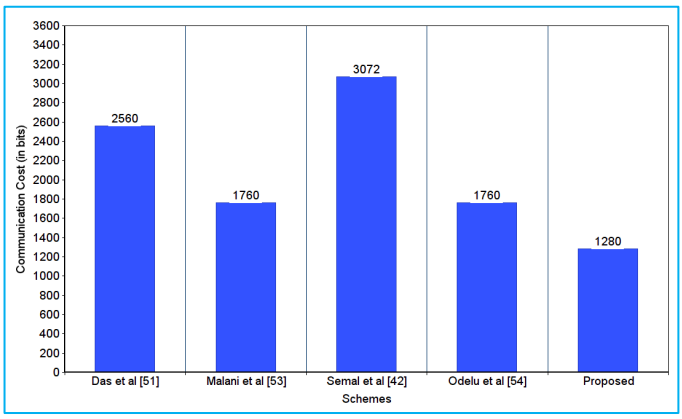

Fig.5. Communication cost (in bits)

TABLE IV
COMPARISON OF COMMUNICATION COSTS (IN BITS)

Variable	Value
$\|\mathbb{G}\|$	1024 bits
$\|\mathcal{Z}_q\|$	160 bits
$\|\mathcal{Z}_n\|$	80 bits

From Table V, it is evident that opting for our proposed scheme results in significant reduction in the associated communication costs.

TABLE V
COMPARISON OF COMMUNICATION COSTS

Schemes	No. of messages	Total (in bits)
Das *et al* [51]	$16\|\mathcal{Z}_q\|$	2560
Malani *et al* [53]	$11\|\mathcal{Z}_q\|$	1760
Semal *et al* [42]	$3\|\mathbb{G}\|$	3072
Odelu *et al* [54]	$11\|\mathcal{Z}_q\|$	1760
Proposed	$16\|\mathcal{Z}_n\|$	1280

C. Storage Requirement

In this subsection, we analyze the storage requirement of the proposed scheme with the existing counterpart presented by Das et al. [51], Malani et al. [53], Semal et al. [42] and Odelu et al. [54]. The computed values are shown in Table VI. In the proposed scheme using a hyperelliptic curve (HEC), we consider identity, certificate, public key, and private key. The NIST standard key size for hyper elliptic curve is 80-bits, 160-bits for an elliptic curve, and 1024 bits for bilinear pairing.

TABLE VI
COMPARISON OF STORAGE REQUIREMENT

Schemes	Approximate size (in bits)
Das *et al* [51]	640
Malani *et al* [53]	640
Semal *et al* [42]	3072
Odelu *et al* [54]	320
Proposed	320

D. Comparison of Security Attributes

This section is dedicated to present a comprehensive comparison of the proposed scheme with the existing schemes, primarily within the context of security functionalities. A brief comparison is depicted in Table VII. It can be observed from the table that none of the existing schemes address the Cloning, DoS and De-synchronization attacks.

TABLE VII
COMPARISON OF SECURITY ATTRIBUTES

Security Attributes	Das *et al* [51]	Malani *et al* [53]	Semal *et al* [42]	Odelu *et al* [54]	Proposed
RA	✓	✓	✓	✓	✓
MIA	✓	✓	✓	✓	✓
MA	✓	✓	✓	✓	✓

DIA	✓	✓	×	✓	✓
DoSA	✓	✓	✓	✓	✓
PCA	✓	✓	×	✓	✓
FVA	✓	✓	×	✓	✓
FSA	✓	✓	✓	✓	✓
RCA	×	×	×	×	✓
DoSA	×	×	×	×	✓
DA	×	×	×	×	✓
AP	✓	✓	✓	✓	✓
ECA	✓	✓	✓	✓	✓

Legend: *RA*: replay attack; *MIA*: man-in-the-middle attack; *MA*: mutual authentication; *DIA*: device impersonation attack; *MDA*: malicious device deployment attack; *DoSA*: Denial-of-Service attack; *FVA*: formal security verification using AVISPA tool; *FSA*: formal security analysis; *CA*: Cloning Attack ; *AP*: anonymity preservation; *DA: De-synchronization Attack; EAC*: ESL attack under the CK-adversary model. Symbol: ✓ satisfy the security functionality, ×: does not satisfy the security functionality.

VIII. CONCLUSION

In Flying Ad-hoc Networks (FANETs), multiple small drones are supposed to interconnect and accomplish the assigned tasks autonomously, in an efficient manner. However, the associated stringent constraints on part of the small drones, such as limited on-board energy, restricted computing capability and insufficient bandwidth etc., hinder their ability to perform complex cryptographic operations. Further, a slow response time and a deteriorated performance is the immediate aftermath of bidding to carry out computationally intensive tasks. Our work aimed to counter such drawback by offering an efficient key agreement scheme in the certificate-based settings. Hyperelliptic curve, a much-advanced version of elliptic curve, is employed to come forth with the solution. The proposed scheme is characterized by a multitude of advantages. For instance, it has a smaller key size, incurs lower computational, as well as communication, costs and offers superior security. Further, the scheme is capable of hindering malicious attacks. The resistance characteristic is further endorsed by the results obtained from a detailed security analysis that includes formal analysis, using ROR model and the widely-accepted AVISPA tool, as well as an informal analysis. Therefore, the proposed scheme caters to ever increasing needs of the resource-constrained small drones. It is reckoned that incorporation of the very scheme for FANETs will pave way for further realization of a reliable FANET communication arena.

REFERENCES

[1] I. Bekmezci, O. K. Sahingoz, and S¸amil Temel, "Flying ad-hoc networks (FANETs): A survey," *Ad Hoc Netw*., vol. 11, no. 3, pp. 1254–1270, 2013.

[2] F. Noor, M.A. Khan, A. Al-Zahrani, I. Ullah, and K.A. Al-Dhlan, "A Review on Communications Perspective of Flying Ad-Hoc Networks: Key Enabling Wireless Technologies, Applications, Challenges and Open Research Topics," *Drones*, vol.4, no.65, pp.1-14, 2020.

[3] A. Guillen-Perez and M.-D. Cano, ''Flying ad hoc networks: A new domain for network communications,'' *Sensors*, vol. 18, no. 10, pp.1-23, 2018.

[4] Lv, Zhihan. "The Security of Internet of Drones," *Computer Communications*, vol. 148, pp. 208–214, 2019.

[5] N. M. Rodday, R. D. O. Schmidt, and A. Pras, ''Exploring security vulnerabilities of unmanned aerial vehicles,'' in *IEEE/IFIP Netw. Oper. Manage. Symp. (NOMS)*, pp. 993–994, IEEE, 2016.

[6] F. Khan, A. Rehman, A.Yahya, M.A. Jan, J. Chuma, Z. Tan, and K. Hussain, "A Quality of Service-Aware Secured Communication Scheme for Internet of Things-Based Networks," *Sensors*, vol. 19, no. 4321, pp.1-18, 2019.

[7] B. Alzahrani, O. S. Oubbati, A. Bernawi, A. Atiquzzaman, D. Alghazzawi, "UAV assistance paradigm: State-of-the-art in applications and challenges," *Journal of Network and Computer Applications*, vol. 166, no.102706, pp.1-44, 2020.

[8] G. Choudhary, V. Sharma, and I. You, "Sustainable and secure trajectories for the military internet of drones (IoD) through an efficient medium access control (mac) protocol," Comput. *Electr. Eng.*, vol. 74, pp. 59–73, 2019.

[9] C. Lin, D. He, N. Kumar, K. R. Choo, A. Vinel and X. Huang, "Security and Privacy for the Internet of Drones: Challenges and Solutions," in *IEEE Communications Magazine*, vol. 56, no. 1, pp. 64-69, 2018.

[10] Y. Zhi, Z. Fu, X. Sun, and J. Yu, "Security and Privacy Issues of UAV: A Survey," *Mobile Netw Appl*, vol. 25, pp. 95-101, 2019.

[11] Y. Guo, M. Wu, K. Tang, J. Tie, and X. Li, "Covert Spoofing Algorithm of UAV Based on GPS/INS-Integrated Navigation," *in IEEE*

Transactions on Vehicular Technology, vol. 68, no. 7, pp. 6557-6564, 2019.

[12] A. Eldosouky, A. Ferdowsi, and W. Saad, "Drones in Distress: A Game-Theoretic Countermeasure for Protecting UAVs Against GPS Spoofing," in *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 2840-2854, 2020.

[13] C.G. L. Krishna, and R.R. Murphy, "A review on cybersecurity vulnerabilities for unmanned aerial vehicles*," 2017 IEEE International Symposium on Safety, Security and Rescue Robotics (SSRR)*, Shanghai, pp. 194-199, 2017.

[14] S.P. Arteaga, L.A.M. Hernández, G.S. Pérez, A.L.S. Orozco, and L.J.G Villalba, "Analysis of the GPS Spoofing Vulnerability in the Drone 3DR Solo," in *IEEE Access*, vol. 7, pp. 51782-51789, 2019.

[15] M.A. Khan, I. Ullah, S. Nisar, F. Noor, I.M. Qureshi, and F. Ullah, "Multi-access Edge Computing (MEC) Enabled Flying Ad-hoc Networks with Secure Deployment using Identity Based Generalized Signcryption," *Mobile Information System*, vol.2020, no. 8861947, ,pp.1-15, 2020.

[16] M.A. Khan, I.M. Qureshi, and F.A. Khanzada, "Hybrid Communication Scheme for Efficient and Low-Cost Deployment of Future Flying Ad-Hoc Network (FANET)," *Drones*, vol.3, no.16, pp,1-20, 2019.

[17] M. A. Khan, A. Khalid and F. Khanzada, "Dual-Radio Dual-Band Configuration for Flexible Communication in Flying Ad-hoc Network (FANET)," *2019 International Conference on Communication Technologies (ComTech)*, Rawalpindi, Pakistan, IEEE, pp. 108-113, 2019.

[18] L. Gupta, R. Jain and G. Vaszkun, "Survey of Important Issues in UAV Communication Networks," in *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1123-1152, 2016.

[19] S. Z. Arnosti, R. M. Pires and K. R. L. J. C. Branco, "Evaluation of cryptography applied to broadcast storm mitigation algorithms in FANETs," *2017 International Conference on Unmanned Aircraft Systems (ICUAS)*, Miami, FL, USA, pp. 1368-1377, 2017.

[20] R. M. Pires, A. S. R. Pinto and K. R. L. J. C. Branco, "The Broadcast Storm Problem in FANETs and the Dynamic Neighborhood-Based Algorithm as a Countermeasure," in *IEEE Access*, vol. 7, pp. 59737-59757, 2019.

[21] N. Islam, M. K. Hossain, G. G. M. N. Ali and P. H. J. Chong, "An expedite group key establishment protocol for Flying Ad-Hoc Network (FANET)," *2016 5th International Conference on Informatics, Electronics and Vision (ICIEV)*, Dhaka, pp. 312-315, 2016.

[22] M.A. Khan, I.M. Qureshi, I. Ullah, S. Khan, F. Khanzada, F. Noor, "An Efficient and Provably Secure Certificateless Blind Signature Scheme for Flying Ad-Hoc Network Based on Multi-Access Edge Computing," *Electronics*, vol. 9, no. 30, pp. 1-22, 2020.

[23] M.A. Khan et.al. "Efficient and Provably Secure Certificateless Key-Encapsulated Signcryption Scheme for Flying Ad-Hoc Network," *IEEE Access*, vol. 8, pp. 36807-36828, 2020.

[24] Z. Liu, H. Liu, W. Xu, and Y. Chen, "Exploiting jamming-caused neighbor changes for jammer localization," *Parallel and Distributed Systems*, IEEE Transactions on, vol. 23, no. 3, pp. 547–555, 2012.

[25] W. Xu, W. Trappe, and Y. Zhang, "Channel surfing: defending wireless sensor networks from interference," in IPSN '07: Proceedings of the 6th international conference on Information processing in sensor networks. New York, NY, USA: ACM, pp. 499–508, 2007.

[26] R. Gummadi, D. Wetherall, B. Greenstein, and S. Seshan, "Understanding and mitigating the impact of rf interference on 802.11 networks," in SIGCOMM '07: Proceedings of the 2007 conference on Applications, technologies, architectures, and protocols for computer communications. New York, NY, USA: ACM, pp. 385–396, 2007.

[27] J. H. Reed and M. Lichtman, Letter Response to FirstNet Conceptual Network NOI (Docket No. 120928505250501; RIN 0660XC002), Nov. 2012.

[28] S.-Y. Chang, Y.-C. Hu, and N. Laurenti, "Simple MAC: a jamming resilient MAC-layer protocol for wireless channel coordination," *in Proceedings of the 18th annual international conference on Mobile computing and networking*, ser. Mobicom '12, pp. 77–88,2012.

[29] S.-Y. Chang, Y.-C. Hu, J. Chiang, and S.-Y. Chang, "Redundancy offset narrow spectrum: countermeasure for signal-cancellation based jamming," in Proceedings of the 11th ACM international symposium on Mobility management and wireless access, ser. MobiWac '13. New York, NY, USA: ACM, pp. 51–58, 2013.

[30] J. Bellardo and S. Savage, "802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions," in USENIX Security Symposium, August 2003.

[31] Y. Hu, A. Perrig, and D. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks," Wireless Networks, vol. 11, no. 1, pp. 21–38, 2005.

[32] R. Negi and A. Rajeswaran, "DoS attacks on a reservation-based MAC protocol," in IEEE ICC, 2005.

[33] V. Gupta, S. Krishnamurthy, and M. Faloutsos, "Denial of Service Attacks at the MAC Layer in Wireless Ad Hoc Networks," in MILCOM, vol. 2, pp. 1118–1123, 2002.

[34] Y.-C. Tung, S. Han, D. Chen, and K. G. Shin, "Vulnerability and protection of channel state information in multiuser mimo networks," in Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, ser. CCS '14. New York, NY, USA: ACM, pp. 775–786, 2014.

[35] J. Manweiler and R. Roy Choudhury, "Avoiding the rush hours: Wifi energy management via trafc isolation," in *Proceedings of the 9th International Conference on Mobile Systems, Applications, and Services*, ser. MobiSys '11. New York, NY, USA: ACM, pp. 253–266, 2011.

[36] X. Zhang and K. G. Shin, "E-mili: Energy-minimizing idle listening in wireless networks," *IEEE Transactions on Mobile Computing*, vol. 11, no. 9, pp. 1441–1454, 2012.

[37] G. De Silva, B. Chen, and M. C. Chan, "Collaborative cellular tail energy reduction: Feasibility and fairness," in *Proceedings of the 17th International Conference on Distributed Computing and Networking*, ser. ICDCN '16. New York, NY, USA: ACM, pp. 25:1–25:10, 2016.

[38] M. Brownfeld, Y. Gupta, and N. Davis, "Wireless sensor network denial of sleep attack," in *Information Assurance Workshop, 2005. IAW '05. Proceedings from the Sixth Annual IEEE SMC*, pp. 356–364, 2005.

[39] D. Raymond, R. Marchany, M. Brownfeld, and S. Midkiff, "Effects of denial of sleep attacks on wireless sensor network mac protocols," in *Information Assurance Workshop, 2006 IEEE*, pp. 297–304,2006.

[40] D. Halperin, T. S. Heydt-Benjamin, B. Ransford, S. S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno, and W. H. Maisel, "Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses," in 2008 IEEE Symposium on Security and Privacy (sp 2008), pp. 129–142, 2008.

[41] S-Y. Chang, S.L. Kumar, Y-C. Hu, and Y. Park Y "Power-positive networking: wireless-charging-based networking to protect energy against battery DoS attacks," *ACM Trans Sensor Netw* 15(3):27, 2019.

[42] B. Semal, K. Markantonakis and R. N. Akram, "A Certificateless Group Authenticated Key Agreement Protocol for Secure Communication in Untrusted DRONE Networks," *2018 IEEE/AIAA 37th Digital Avionics Systems Conference (DASC)*, London, pp. 1-8, 2018.

[43] M. S. Farash, M. Turkanovi´c, S. Kumari, and M. H¨olbl, "an efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the internet of things environment," Ad Hoc Networks, vol. 36, pp. 152–176, 2016.

[44] R. Amin, S. H. Islam, G. Biswas, M. K. Khan, L. Leng, and N. Kumar, "Design of an anonymity-preserving three-factor authenticated key exchange protocol for wireless sensor networks," Computer Networks vol. 101, pp. 42–62, 2016.

[45] Q. Jiang, S. Zeadally, J. Ma, and D. He, "Lightweight three-factor authentication and key agreement protocol for internet-integrated wireless sensor networks, *IEEE Access*, vol. 5, pp. 3376–3392, 2017.

[46] S. Challa, M. Wazid, A. K. Das, N. Kumar, A. G. Reddy, E.-J. Yoon, and K.- Y. Yoo, "Secure signature-based authenticated key establishment scheme for future iot applications," *IEEE Access*, vol.5, pp. 3028–3043, 2017.

[47] 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 drone's deployment," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 3572–3584, 2019.

[48] Y. Zhang, D. He, L. Li et al., "A lightweight authentication and key agreement scheme for internet of drones," *Computer Communications*, 2020.

[49] F. Li, Y. Han, and C. Jin, ''Practical access control for sensor networks in the context of the Internet of Things,'' *Comput. Commun.*, vol. 89–90, pp. 154–164, 2016.

[50] M. Luo, Y. Luo, Y. Wan, and Z. Wang, ''Secure and efficient access control scheme for wireless sensor networks in the cross-domain context of the IoT,'' *Secur. Commun. Netw.*, vol. 2018, pp. 1–10, 2018.

[51] A. K. Das, M. Wazid, A. R. Yannam, J. J. P. C. Rodrigues and Y. Park, "Provably Secure ECC-Based Device Access Control and Key Agreement Protocol for IoT Environment," in *IEEE Access*, vol. 7, pp. 55382-55397, 2019.

[52] M. Abdalla, P. Fouque, and D. Pointcheval, ''Password-based authenticated key exchange in the three-party setting,'' in *Public Key Cryptography—PKC*. Les Diablerets, Switzerland: Springer, pp. 65–84, 2005.

[53] S. Malani, J. Srinivas, A. K. Das, K. Srinathan, and M. Jo. CertificateBased Anonymous Device Access Control Scheme for IoT Environment. IEEE Internet of Things Journal, vol.6, no. 6, pp. 9762–9773, 2019.

[54] V. Odelu, A. K. Das, K. R. Choo, N. Kumar and Y. Park, "Efficient and Secure Time-Key Based Single Sign-On Authentication for Mobile Devices," in *IEEE Access*, vol. 5, pp. 27707-27721, 2017.

[55] AVISPA. (2019). *Automated Validation of Internet Security Protocols and Applications*. [Online]. Available: http://www.avispa-project.org/

[56] D. Dolev and A. Yao, "On the security of public key protocols," IEEE Transactions on Information Theory, vol. 29, no. 2, pp. 198–208, 1983.

[57] R. Canetti and H. Krawczyk, "Universally Composable Notions of Key Exchange and Secure Channels," in *International Conference on the Theory and Applications of Cryptographic Techniques– Advances in Cryptology (EUROCRYPT'02)*, Amsterdam, The Netherlands, pp. 337–351, 2002.

[58] J. Srinivas, A. K. Das, N. Kumar, and J. P. C. Rodrigues, "Cloud Centric Authentication for Wearable Healthcare Monitoring System," *IEEE Transactions on Dependable and Secure Computing*, doi: 10.1109/TDSC.2018.2828306, 2018.

[59] C. X. Zhou, Z. Zhao, W. Zhou et al., "Certificateless key insulated generalized signcryption scheme without bilinear pairings," *Security and Communication Networks*, pp. 1-17, 2017.

[60] "Shamus Sofware Ltd. Miracl library," [Online]. Avalable : http://github.com/miracl/ MIRACL.

Muhammad Asghar khan is currently pursuing a Ph.D. degree in electronic engineering at the School of Engineering and Applied Sciences (SEAS), ISRA University, Islamabad. He is serving as a Lecturer with the Department of Electrical Engineering, Hamdard University, Islamabad. He is a reviewer for various journals published by IEEE, MDPI and EURASIP. His research interests include UAVs/Drones with a focus on networks, platforms, security, as well as applications and services.

Insaf Ullah received the Master's degree in Computer Sciences from the Department of Information Technology, Hazara University Manshera, Pakistan. He is currently pursuing Ph.D. in Computer Sciences from the same department. He is serving as a Lecturer with the Department of Computer Sciences, Hamdard University, Islamabad. His research interests include network security.

Neeraj Kumar received the Ph.D. degree in computer science and engineering from Shri Mata Vaishno Devi University, Katra, India. He is currently an Associate Professor with the Department of Computer Science and Engineering, Thapar University, Patiala, India. He has more than 300 technical research papers in leading journals such as the IEEE Transactions on Industrial Informatics, the IEEE Transactions on Industrial Electronics, the IEEE Transactions on Dependable and Secure Computing, the IEEE Transactions on Intelligent Transportation Systems, the IEEE TWPS, the IEEE Systems Journal, the IEEE Communications Magazine, the IEEE WCMAG, the IEEE NETMAG, and conferences. His research is supported from DST, TCS, and UGC. He has guided many students leading to M.E. and Ph.D. His research interests include mobile computing, parallel/distributed computing, multiagent systems, service-oriented computing, routing and security issues in mobile ad hoc, and sensor and mesh networks. He is recipient of best papers award from IEEE Systems Journal (2018) and IEEE ICC (2018). He is TPC Member/Technical committee members of various conferences and organized various workshops in ICC, and Globocom conferences.

Omar Sami Oubbati (Member, IEEE) is an Associate Professor at the Electronics department, University of Laghouat, Algeria and a Research Assistant in the Computer Science and Mathematics Lab (LIM) at the same university. He received his degree of Engineer (2010), M.Sc. in Computer Engineering (2011), M.Sc. degree (2014), and a PhD in Computer Science (2018), all from University of Laghouat, Algeria. From Oct. 2016 to Oct. 2017, he was a Visiting Student with the Laboratory of Computer Science, University of Avignon, France. His main research interests are in Flying and Vehicular ad hoc networks, Energy harvesting and Mobile Edge Computing, Energy efficiency and Internet of Things (IoT). He is the recipient of the 2019 Best Survey Paper for Vehicular Communications (Elsevier). He has actively served as a reviewer for flagship IEEE Transactions journals and conferences, and participated as a Technical Program Committee Member for a variety of international conferences, such as IEEE ICC, IEEE CCNC, IEEE ICCCN, IEEE WCNC, IEEE ICAEE, and IEEE ICAIT. He serves on the editorial board of Vehicular Communications Journal of Elsevier and Communications Networks Journal of Frontiersin. He has also served as guest editor for a number of international journals. He is a member of the IEEE and IEEE Communications Society.

Ijaz Mansoor Qureshi received Bachelor's, Master's and PhD degrees in Avionic Engineering (NED University of Engineering and Technology, Karachi, Pakistan), Electrical Engineering (Middle East Technical University, Ankara, Turkey) and High Energy Physics (University of Toronto, Ontario, Canada) respectively. He has to his credit a post-PhD experience stretching 27 years in various Pakistani higher education institutes of repute. He has supervised about 37 PhD thesis so far. At the moment, he is associated with the Electrical Engineering Department, Air University as Professor.

Fazal Noor received his B. Eng. and M. Eng. degrees in Electrical and Computer Engineering from Concordia University, Montreal, Canada in 1984 and 1986, respectively. He received his Ph.D. Engineering from McGill University, Montreal, Canada in 1993. Currently, he is a Professor with the Faculty of Computer and Information Systems (FCIS) at Islamic University of Madinah, Saudi Arabia. He has published numerous papers in various reputable international journals and conferences. He has been a reviewer for IEEE, Elsevier, Springer,

and various other journals. Currently, he holds the position of Vice Dean of Graduate Studies and Scientific Research at FCIS. He was Program Coordinator for Master of Computer Science program. He has received best faculty award in 2007. He has been a TPC member of many conferences. He is a fellow member of IAER. He has been QA evaluator for Computer Engineering program. His research interests are in AI, FANETS, Neural Networks, Embedded Systems, Signal Processing, Network Security, IoT, Optimization Algorithms, and Parallel and Distributed computing.

Fahim Ullah Khanzada holds Bachelor's degree in electronic engineering from Baluchistan University of Information Technology, Engineering and Management Sciences (BUITEMS), Quetta and Master's degree in Electrical Engineering from the University of Nottingham, Nottingham, UK. His experience encompasses academia, industry and standardization. He is presently associated with Descon Engineering Limited, Lahore, Pakistan.