Hindawi
Mobile Information Systems
Volume 2020, Article ID 8861947, 15 pages
https://doi.org/10.1155/2020/8861947

Research Article

Multiaccess Edge Computing Empowered Flying Ad Hoc Networks with Secure Deployment Using Identity-Based Generalized Signcryption

Muhammad Asghar Khan,[1] **Insaf Ullah**,[2] **Shibli Nisar**,[3] **Fazal Noor**,[4] **Ijaz Mansoor Qureshi**,[5] **Fahimullah Khanzada**,[6] **Hizbullah Khattak**,[2] **and Muhammad Adnan Aziz**[7]

[1]*Hamdard Institute of Engineering & Technology, Islamabad 44000, Pakistan*
[2]*Department of Information Technology, Hazara University, Mansehra, Pakistan*
[3]*Department of Electrical Engineering, National University of Sciences and Technology (NUST), Islamabad 44000, Pakistan*
[4]*Department of Computer Science and Information Systems, Islamic University of Madinah, Madinah 400411, Saudi Arabia*
[5]*Department of Electrical Engineering, Air University, Islamabad 44000, Pakistan*
[6]*Descon Engineering Limited, Lahore, Pakistan*
[7]*Department of Electronic Engineering, ISRA University, Islamabad 44000, Pakistan*

Correspondence should be addressed to Muhammad Asghar Khan; khayyam2302@gmail.com

Received 20 April 2020; Revised 19 May 2020; Accepted 2 June 2020; Published 1 July 2020

Academic Editor: Vishal Sharma

A group of small UAVs can synergize to form a flying ad hoc network (FANET). The small UAVs are, typically, prone to security lapses because of limited onboard power, restricted computing ability, insufficient bandwidth, etc. Such limitations hinder the applicability of standard cryptographic techniques. Thus, assuring confidentiality and authentication on part of small UAV remains a far-fetched goal. We aim to address such an issue by proposing an identity-based generalized signcryption scheme. The lightweight security scheme employs multiaccess edge computing (MEC) whereby the primary UAV, as a MEC node, provides offloading to the computationally fragile member UAVs. The scheme is based on the concept of the hyperelliptic curve (HEC), which is characterized by a smaller key size and is, therefore, suitable for small UAVs. The scheme is robust since it offers confidentiality and authentication simultaneously as well as singly. Formal as well as informal security analyses and the validation results, using the Automated Validation for Internet Security Validation and Application (AVISPA) tool, second such notion. Comparative analysis with the existing schemes further authenticates the sturdiness of the proposed scheme. As a case study, the scheme is applied for monitoring crops in an agricultural field. It has been found out that the scheme promises higher security and incurs lower computational and communication costs.

1. Introduction

Unmanned Aerial Vehicles (UAVs) have earned recognition in multiple domains owing to their versatile applications for surveillance, agriculture, health services, traffic monitoring, inspection, public safety, etc. [1]. Multiple small UAVs, as a flying ad hoc network (FANET), can combine and accomplish the assigned tasks efficiently in an autonomous manner [2, 3]. In FANETs, small interconnected UAVs synergize and exchange data with one another and with the ground stations [4]. They are characterized by high mobility, easy deployment, and self-organizing behavior [5]. However, such distinctive features, for efficient and effective deployment, demand the compliance of stringent guidelines [6]. For instance, it is mandatory to assure security and Quality of Service (QoS) when choosing a FANET system for on-time data communication services. Moreover, the networks must deploy an efficient networking architecture complemented by an efficient security scheme in order to allow a reliable exchange of information between UAVs and the ground stations.

FANETs can either be deployed independently or they can be integrated with the traditional networks via satellite or cellular communication links. The topic allures experts from the industry as well as academia. Most of the relevant research studies propose to integrate multiple-UAV systems with the traditional networks to assure Quality of Service (QoS), unhampered security, and sustained reliability. Therefore, it is imperative to identify loopholes in existing solutions. This can pave the way for solutions that support high throughput and a secure data communication regime. The envisioned Fifth Generation (5G) of wireless cellular communication systems is expected to offer higher capacity, enhanced data rate, and lower latency [7]. Besides, 5G offers multiaccess edge computing (MEC) architecture, which is characterized by cloud computing functionalities. Thus, 5G, when integrated into a UAV environment, by leveraging MEC, can relieve the resource-constrained UAVs from processing the computational tasks. Instead, the computationally intensive tasks will be offloaded to the edge of the network.

Generally, the small UAVs are not designed with security considerations and are, therefore, prone to security and privacy pitfalls [8]. UAV's sensing portion is also worth consideration. For instance, in the worst case, a sensor might transmit wrong information and that can result in UAVs making erroneous decisions. Similarly, the case of the faulty sensor is far more sinister. A damaged sensor can severely hamper the UAV's attempt to obtain information and might result in an event of a crash. Furthermore, a strong communication link is essential to allow the exchange of information between a UAV and a Base Station. An insecure and vulnerable link, on the other hand, is susceptible to attacks [9]. The concerns of confidentiality and authentication can be addressed by employing encryption and digital signature, respectively. And, in case both the attributes are desired, a hybrid version, the sign-then-encrypt approach, is utilized mostly.

However, the stringent constraints associated with a flying ad hoc network (FANET), such as limited onboard energy and limited computing capability, do not permit complex cryptographic operations. Moreover, undertaking computationally intensive tasks may result in slow response time which can, in turn, deteriorate the performance of FANETs. Fortunately, such deficiencies can be resolved by employing an amalgamated scheme, named "signcryption" [10]. It is a public key cryptosystem that performs the function of encryption and digital signature simultaneously. It is far more efficient and cost-effective than each of the alternates, i.e., encryption and digital signature. To simplify the key management process and to allow flexibility, Han et al. [11] presented an extension of the signcryption scheme, i.e., generalized signcryption (GSC). Not only does GSC offer encryption and digital signature in one go, but it also has the option to offer them separately, if demanded. Such feature is helpful in case either of the two key attributes, confidentiality or authenticity, is required.

In the public key cryptosystems, two basic approaches, Public Key Infrastructure (PKI) and Identity-Based Cryptography (IBC), are used to authenticate public keys [12]. In the PKI environment, it is crucial to ensure a trustworthy unforgeable link between the identity of the participant and its public key. This further stipulates the need for a signature Certificate Authority (CA) that assigns the link a unique signature. In the certification stage, the CA bounds the public key as the identity of a participant with certificates. The Public Key Infrastructure (PKI) approach encounters issues with certificate distribution and storage. On the other hand, an identity-based cryptosystem is used to reduce the cost of public key management [13]. In ID-based systems, a trusted third party named private key generator (PKG) computes private keys from a master secret and users' identity information. It then distributes these private keys to the users participating in the scheme. This eradicates the necessity for certificates as used in a conventional PKI.

The security and efficiency of the aforementioned security schemes are based on computationally hard problems. The RSA cryptography [14, 15] is based on a large factorization problem, which utilizes a large key, parameter certificate, and the identity stretches as much as 1024 bits [16]. This is not suitable for resource-constrained networks, or FANETs, because small UAVs lack onboard processing resources. Furthermore, bilinear pairing is 14.31 times worse than RSA [17], due to huge pairing and map-to-point function computation. In order to eliminate the discrepancies accompanying RSA and bilinear pairing, a new type of cryptography called the elliptic curve was introduced [18]. The elliptic curve cryptography is characterized by smaller parameter size, smaller public/private key size, smaller identity, and smaller certificate size. Moreover, unlike bilinear pairing and RSA, the security hardiness and efficiency of the elliptic curve cryptography scheme are based on 160-bit small keys [19]. The 160-bit key is, still, not suitable for and affordable by resource-hungry devices such as small UAVs. Thus, the hyperelliptic curve, a more modern version of the elliptic curve cryptography, was proposed [20]. The hyperelliptic curve uses an 80-bit key, identity, and certificate size and, at the same time, promises the security features assured by the elliptic curve, bilinear pairing, and RSA [21, 22]. Therefore, the hyperelliptic curve is a cogent choice for energy-constrained devices.

1.1. Authors' Motivation and Contributions. To reap the extensive benefits of multi-UAV systems, the underlying technical challenges need to be addressed. For instance, the small UAVs have limited onboard energy, which restricts the flying time to a specified period and the UAV's limited computational capability does not permit complex cryptographic operations. Therefore, there is a need to harness a state-of-the-art communication architecture with a lightweight security mechanism, which can, significantly, stabilize the battery lifetime, offer limited computation cost, and provide better connectivity.

Motivated by such objectives, for FANETs, the authors, here, suggest an identity-based generalized signcryption scheme. The very scheme makes use of multiaccess edge computing (MEC) and is based on a much advanced version of the elliptic curve, i.e., the hyperelliptic curve (HEC). HEC

is characterized by a smaller key size and, at the same time, promises security comparable to that of the counterparts, i.e., elliptic curve, bilinear pairing, and modular exponentiation. Incorporation of HEC reduces power consumption and improves the device's performance, thereby making it suitable for a wide range of devices, ranging from sensors to UAVs.

Some of the salient features signifying the contribution of our research work, in this paper, are as follows:

(i) We introduce a new architecture for flying ad hoc networks (FANETs) leveraging multiaccess edge computing (MEC) facility, where the primary UAV acts as a MEC node in order to provide computational offloading services for the member UAVs having limited local computing capabilities

(ii) We propose an efficient and provably secure identity-based generalized signcryption scheme for the architecture using the concept of a hyperelliptic curve

(iii) The proposed scheme is potent enough to thwart attacks, both known and unknown, and the validation results using the Automated Validation for Internet Security Validation and Application (AVISPA) tool second such notion

(iv) Moreover, upon doing a comparative analysis with the extant schemes, it is revealed that our proposed scheme is superior, particularly, in terms of computational and communication costs

1.2. Structure of the Paper. The rest of the paper is organized as follows. In Section 2, we provide a brief about the related work. Foundational concepts of the research work are presented in Section 3. Section 4 is dedicated to present the two system models, i.e., network model and threat model. In Section 5, we explain the salient features of the proposed scheme. Informal security analysis is provided in Section 6. Section 7 presents the practical deployment of the proposed scheme. For performance evaluation, the proposed scheme is compared with the existing schemes in Section 8. Section 9 contains a brief about a case study in which the scheme is applied for precision agriculture. Finally, Section 10 concludes the work.

2. Related Work

2.1. UAV-Enabled Multiaccess Edge Computing. Owing to the promising features of on-demand communication services and flexible deployment, UAV-enabled multiaccess edge computing capabilities have received much attention in recent years. So far, various studies have been conducted to examine the usability of edge computing for UAVs [23, 24]. However, the studies do not address the topic of security. Garg et al. [25] aimed to answer the surveillance-related concerns by proposing a framework based on probabilistic data structures. The framework treats UAVs as intermediate aerial nodes that offer a cyberthreat detection mechanism complemented with a real-time analysis. Four major elements of the framework are as follows: UAV, dispatcher, aggregator, and edge devices. The UAV is responsible for capturing and validating the data. The processing tasks in the edge computing devices are scheduled by the dispatcher. The aggregator assures the secure transmission of data. And, the edge devices analyze the data.

In [26], the authors extend the concept of network slicing to the case of UAV-based 5G network deployment and investigate the feasibility of a backhaul of an aerial node utilizing a UAV. The LTE signals are monitored to evaluate the suitability of UAVs in two scenarios: network capacity enhancement and increasing network coverage.

The methodology proposed by Christian et al. [27] increases the system reliability and reduces the end-to-end source-actuator latency. Their work intends to broaden the 5G network edge by making the FANET UAVs fly close to the monitoring layer. For enhanced operations, the UAVs follow a policy of mutual help and are accoutered with MEC facilities. However, the work fails to address the issue of the limited battery duration of the MEC-UAVs. In [28], the authors proposed a UAV edge-cloud computing model that utilizes a UAV swarm to provide the users real-time support. The end data are stored in the cloud server. In [29], the authors presented an architectural design of a slice orchestrator that enables new application models where the Internet of Things related functions can be applied on small Unmanned Aerial Vehicles, thus paving the way for implementing these functions on the edge network.

2.2. Security Mechanisms in Flying Ad Hoc Networks. The primary security mechanisms for FANETs emphasize authenticity, confidentiality, and integrity of data via cryptography. A well-designed data protection mechanism can significantly reduce the probability of the data get compromised, irrespective of the devilish technique involved. There are a few studies dedicated to investigating the data protection issues for UAV Networks. In a secure communication scheme proposed by He et al. [30], the requirement of an online centralized authority is waived off. The UAVs manage the area themselves and the authorized devices can obtain a broadcast key. The scheme is characterized by employing hierarchical identity-based broadcast encryption and a pseudonym mechanism, whereby the devices can, anonymously, broadcast the encrypted messages and decrypt the legal ciphertext. The work done seconds the notion that the very scheme, satisfactorily, addresses the four important security concerns: confidentiality, authentication, partial privacy preservation, and resistance to Denial of Service (DoS) attacks. However, it inherits a restriction in the registration phase, i.e., the concern of finding a hash value's preimage persists.

Three communication scenarios have been described by Won et al. [31, 32] to propose cryptographic protocols for drones and smart objects. The first scenario, i.e., one-to-one, implies a certificateless signcryption tag key for facilitating an authenticated key agreement and for providing nonrepudiation and user revocation. One-to-many, or the second scenario, enables a UAV to broadcast privacy-

sensitive data to multiple smart objects using a certificateless multirecipient encryption scheme. The third scenario is termed "many-to-one" and is characterized by UAVs capable of collecting data from multiple smart objects. However, for such protocols [31, 32], transmitting encrypted messages and assuring privacy simultaneously are too difficult to undertake. Such novel cryptographic mechanisms are efficient and secure. However, they are supposed to be used in group communication where nodes are of equal computational capability. In 2019, Asghar et al. [33] proposed a blind signature scheme for flying ad hoc networks in a certificateless setting. The scheme is suitable for authentication; however, it does not offer confidentiality and authentication simultaneously.

2.3. Identity-Based Generalized Signcryption Schemes. Lal et al. [34], in 2008, introduced the first identity-based generalized signcryption scheme and proposed a security model for it. However, Yu et al. [13] pointed out that the security model presented by Lal et al. [34] scheme is incomplete and proposed a new scheme, which is efficient in terms of computation and is secure. Later, in 2011, Kushwah et al. [35] simplified the security model introduced by Yu et al. [13] and proposed a more efficient identity-based generalized signcryption scheme. Wei et al. [36], in 2015, presented an identity-based generalized signcryption scheme, which demonstrated to be secure enough in the random oracle model. Shen et al. [37], in 2017, proposed an identity-based generalized signcryption scheme in the standard model. Nevertheless, the proposed scheme is based on bilinear pairing that is computationally expensive. In 2019, Waheed et al. [38] analyzed the work done by Wei et al. [36] and suggested an improved scheme that is far more secure and cost-effective. Lastly, in 2019, Zhou et al. [39] proposed an identity-based combined public key scheme for signature, encryption, and signature (IBCSESC). Under the premise of ensuring the confidentiality, integrity, authentication, and nonrepudiation of data, the combined cryptosystem reduces the key management work, saves storage space, and offers decreased computational consumption.

3. Preliminaries

3.1. Hyperelliptic Curve Cryptography (HECC). HECC is the advanced form of elliptic curve cryptography (ECC), and it is used to exchange keys and facilitate secure communications between two parties with very small size keys and incur lower computational and communication costs. For instance, an encryption activity done using RSA with a 1024-bit key and ECC with a 160-bit key is equivalent in performance to HECC encryption with an 80-bit key [40].

Suppose that $\mathfrak{F}q$ is a predetermined set and presume ∂ as the genus of $h\varepsilon c$ having order as $\partial \geq 2$. Let $(v), f(v) \in \mathfrak{F}q\,[v]$, deg $(h(v)) \leq \partial$, and $f(v)$ is a monic-polynomial having deg $(f(v)) = 2\partial + 1$. Thus, $h\varepsilon c$ of genus $\partial \geq 2$ over $\mathfrak{F}q$ is set of points $(v,)$ $\mathfrak{F}q * \mathfrak{F}q$ as shown in

$$h\varepsilon c\colon w^2 + (v)w = f(v). \tag{1}$$

It forms the divisors which are the formal sum of finite integers like $d = \sum x_i z_i$ where $x_i \in \mathfrak{F}q$ and $z_i \in h\varepsilon c$. Further, it forms a Jacobian group $\mathfrak{F}_{h\varepsilon c}(\mathfrak{F}q)$ having the following order:

$$(\sqrt{t} - 1)^{2\partial} \leq \mathcal{J}_{h\varepsilon c}\mathfrak{F}_q \leq (\sqrt{t} + 1)^{2\partial}. \tag{2}$$

3.2. Hyperelliptic Curve Discrete Logarithm Problem ($h\varepsilon c - dl$P). Assume that d is the divisor that is publicly available in the network and $\mathscr{L}$ is a randomly picked private number from $\mathfrak{F}_t$. Upon recovering $\mathscr{L}$ from $d_1 = d$, $\mathscr{L}$ is said to be ($h\varepsilon c - dl$P).

4. System Models

To elaborate on the operation and applicability of the proposed scheme, two models are used.

4.1. Network Model. We devise a novel architecture for a flying ad hoc network (FANET), constituted by UAVs, with a multiaccess edge computing (MEC) facility that makes use of the Fifth Generation (5G) wireless communication technology on backhaul and the Wi-Fi technology on fronthaul, as shown in Figure 1. The 5G and Wi-Fi wireless technologies are enabled on MEC-UAV in order to link it with the Macro Base Station (MBS) and to provide a hotspot service over the M-UAVs. The M-UAVs are connected with each other via a Wi-Fi link. The primary reason behind opting for such a hybridized approach is to utilize the prominent features of both technologies. This ends up in the resulting solution being of low cost, low power, high range, and high speed. A huge bandwidth is required when linking the Macro Base Stations with the core network. The proposed architecture involves the UAVs connected together via either of the two classes: monitoring UAV (M-UAV), responsible for performing the monitoring function from an assigned zone; and multiaccess edge computing UAV (MEC-UAV), utilizing MEC to handle a set of M-UAVs connected to it. It is the load generated by an M-UAV that acts as a decisive factor when assigning M-UAV(s) to a MEC-UAV, or the primary UAV. In the maneuver, each of the MEC-UAVs is equipped with Raspberry PI (RPI) powered with a 1.5 GHz 64-bit quad-core ARM Cortex-A72 processor [41].

4.2. Threat Model. The proposed scheme employs the Dolev-Yao (DY) threat model [42]. The model indicates that an untrustworthy nature prevails between the end-point entities and that there is an insecure open channel between the parties. Thus, for an attacker, it eases the task to eavesdrop and delete/modify the exchanged messages. Far worse is the scenario when a drone, while hovering over a hostile area, is physically captured and the data is compromised. Recently, the widely accepted "Canetti and Krawczyk's adversary model (CK-adversary model)" [43] becomes the "current de facto standard model in modeling authenticated key exchange protocols." According to the CK-adversary model,

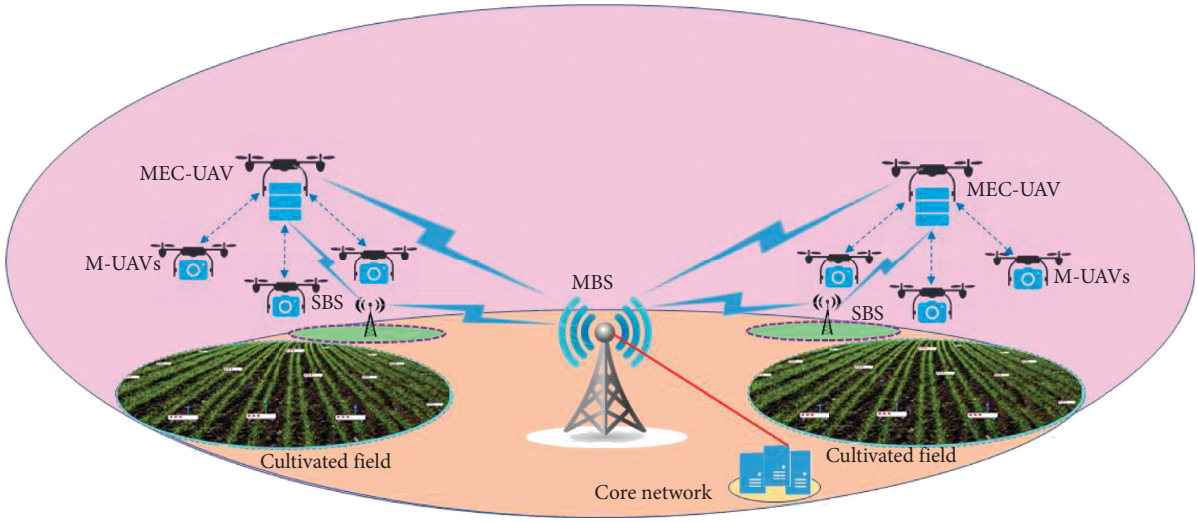

Figure 1: Multiaccess edge computing empowered FANET architecture of the proposed scheme when applied for monitoring.

"the adversary can not only deliver the messages (as in the DY model), but can compromise the secret credentials, secret keys and session states a well, particularly, when stored in the insecure memory." Therefore, it becomes an essential requirement that "the leakage of some forms of secret credentials, such as session ephemeral secrets or secret key, should minimally effect the secrecy of the communicating participants" [33].

5. Proposed Identity-Based Generalized Signcryption Scheme

5.1. Syntax of Identity-Based Generalized Signcryption Scheme. A formal model of identity-based generalized signcryption scheme consists of the following four algorithms [13, 37]: setup, key extraction, generalized signcryption, and generalized unsigncryption. The notations used in the proposed scheme are illustrated in Table 1.

(i) *Setup.* In the setup phase, the private key generation (PKG) generates the public parameters, randomly selects their master private key, and computes the master public key with the input of security parameter.

(ii) *Key Extraction.* When each of the participated contestants transmits their respective identities (ID_{ps}) to the PKG, PKG generates the private (A_{pc}) and public (B_{pc}) keys for each of them and delivers them using the private network.

(iii) *Generalized Signcryption.* The sender performs this process for producing generalized signcryption of a message (m). It initially takes the input parameter such as the identity of the sender and receiver (ID_{cs}, ID_{cr}), message (m), the private key of the sender (A_{cs}), the public key of the receiver (B_{cr}), and a fresh nonce (n_{cs}).

(iv) *Generalized Unsigncryption.* The receiver performs this process for recovering a message (m) and verifying generalized signcryption text ψ. It takes the input parameter like generalized signcryption text ψ, the identity of the sender and receiver (ID_{cs}, ID_{cr}), the private key of the receiver (A_{cr}), the public key of the receiver(B_{cr}), and the public key of the sender (B_{cs}).

5.2. Construction of the Proposed Identity-Based Generalized Signcryption Scheme. It includes the following four subphases [13, 37]:

Setup: in this phase, the private key generation (PKG) center performs essential steps. It

(a) Selects a security parameter κ
(b) Selects a hyperelliptic curve (HEC) of genus 2
(c) Selects a parameter q where the length is equivalents to 80 bits
(d) Selects a finite field f_q, where its order is q
(e) Selects a divisor D of the order q
(f) Selects two one-way hash function, i.e., h_a and h_b
(g) Selects a number uniformly for its private key as $\delta \in [1, 2, \ldots, (q-1)]$
(h) Computes its public key as $\Lambda = \delta.D$
(i) Produces all the public parameter param $E = [q, h_a, h_{b,} f_q, \kappa, \Lambda, HEC, D]$ and publish them to the network

Key extraction: when each of the participating contestants transmits their identity (ID_{pc}) to the PKG, the PKG generates the private and public keys by utilizing the performing the following computations:

(a) It computes private key for identity (ID_{pc}) as $A_{pc} = \delta \cdot h_a(ID_{pc}) \bmod q$
(b) It computes public key for identity (ID_{pc}) as $B_{pc} = A_{pc}.D$
(c) It delivers the pair of the public and private keys (B_{pc}, A_{pc}) to the participating contestants with its identity (ID_{pc}) by using the private network

Table 1: Notations used in the proposed algorithm.

S.NO	Symbol	Definition
1	$h\varepsilon c$	Hyperelliptic curve
2	κ	Security parameter
3	PKG	Private key generation center
4	q	A large prime number with length equivalents to 80 bits
5	$\mathfrak{F}q$	A finite field of the order q
6	h_a, h_b.	Hash functions
7	δ	Master private key of PKG
8	Λ	Master public key of PKG
9	E	Public parameter param
10	ID_{cs}	Identity sender
11	ID_{cr}	Identity receiver
12	A_{cs}	Private key of the sender
13	A_{cr}	Private key of the receiver
14	B_{cs}	Public key of the sender
15	B_{cr}	Public key of receiver
16	η, m	Ciphertext and plain text
17	n_{cs}	A fresh nonce
18	β	Encryption and decryption key
19	e_β, d_β	Encryption and decryption through β
20	$\psi = (\partial, \sigma, \eta, \Delta)$	Generalized signcryption text for the receiver
21	//	Used for concatenation
22	$\perp\!\!\!\perp$	Used for error

Generalized signcryption: given a message (m), the private key of the sender (A_{cs}), the public key of the receiver (B_{cr}), the identity of the sender and receiver (ID_{cs}, ID_{cr}), and a fresh nonce (n_{cs}), the sender performs this process for producing generalized signcryption by undertaking the following steps

(a) It selects a number in an irregular manner as $\varphi \in [1, 2, \ldots, (q-1)]$ and calculates $\Delta = \varphi \cdot D$
(b) It calculates $\beta = \varphi \cdot B_{cr} \cdot ID_{cr}$
(c) It computes $\eta = e_\beta(m//ID_{cs}//ID_{cr}//n_{cs})$
(d) It calculates $\sigma = h_b(m//ID_{cs}//ID_{cr}//n_{cs})$
(e) It computes $\partial = (ID_{cr} \cdot \varphi - \sigma \cdot \Delta \cdot A_{cs} \cdot ID_{cs}) \bmod q$
(f) It produces the final generalized signcryption text for the receiver as $\psi = (\partial, \sigma, \eta, \Delta)$

Generalized unsigncryption: given a generalized signcryption text $\psi = (\partial, \sigma, \eta, \Delta)$, the private key of the receiver (A_{cr}), the public key of sender and receiver (B_{cs}, B_{cr}), and the identity of the receiver (ID_{cr}), the sender performs this process for verifying the signature, and recovering a plain text (m) by undertaking the following steps:

(a) It computes $\beta = \partial \cdot B_{cr} + ID_{cs} \cdot \Delta \cdot \sigma \cdot B_{cs} \cdot A_{cr}$
(b) It decrypts $(m//ID_{cs}//ID_{cr}//n_{cs}) = d_\beta(\eta)$
(c) It computes $\sigma^\wedge = h_b(m//ID_{cs}//ID_{cr}//n_{cs})$
(d) It compares $\sigma^\wedge = \sigma$, if holds, then accept ψ otherwise generate the error symbol $\perp\!\!\!\perp$

Note that, in the above algorithm, if $ID_{cs} = \text{null}$ and $ID_{cr} \neq \text{null}$, then generalized signcryption proceeds in an encryption process. If $ID_{cr} = \text{null}$ and $ID_{cs} \neq \text{null}$, then generalized signcryption will run in the signature mode. And, if $ID_{cs} \neq \text{null}$ and $ID_{cr} \neq null$, then generalized signcryption will run in signcryption mode.

5.3. Correctness. The receiver can compute the decryption key as

$$\begin{aligned}
\beta = {} & \partial.B_{cr} + ID_{cs} \cdot \Delta \cdot \sigma \cdot B_{cs}.A_{cr}, \\
& (ID_{cr} \cdot \varphi - \sigma \cdot \Delta \cdot A_{cs} \cdot ID_{cs}) \cdot B_{cr} + ID_{cs} \cdot \Delta \cdot \sigma \cdot B_{cs} \cdot A_{cr}, \\
& (ID_{cr} \cdot \varphi - \sigma \cdot \Delta \cdot A_{cs} \cdot ID_{cs}) \cdot B_{cr} + ID_{cs} \cdot \Delta \cdot \sigma \cdot B_{cs} \cdot A_{cr}, \\
& (ID_{cr} \cdot \varphi \cdot B_{cr} - \sigma \cdot \Delta \cdot A_{cs} \cdot ID_{cs} \cdot B_{cr}) + ID_{cs} \cdot \Delta \cdot \sigma \cdot B_{cs} \cdot A_{cr}, \\
& (ID_{cr} \cdot \varphi \cdot B_{cr} - \sigma.\Delta \cdot A_{cs} \cdot ID_{cs} \cdot B_{cr}) + ID_{cs} \cdot \Delta \cdot \sigma \cdot A_{cs} \cdot D \cdot A_{cr}, \\
& (ID_{cr} \cdot \varphi \cdot B_{cr} - \sigma \cdot \Delta \cdot A_{cs} \cdot ID_{cs} \cdot B_{cr}) + ID_{cs} \cdot \Delta \cdot \sigma \cdot A_{cs} \cdot B_{cr}, \\
& (ID_{cr} \cdot \varphi \cdot B_{cr} - \sigma \cdot \Delta \cdot A_{cs} \cdot ID_{cs} \cdot B_{cr}) + ID_{cs} \cdot \sigma \cdot \Delta \cdot A_{cs} \cdot B_{cr}, \\
& ID_{cr} \cdot \varphi \cdot B_{cr} = \beta,
\end{aligned} \tag{3}$$

and it verifies ψ as it computes $\sigma\wedge = h_b(m//ID_{cs}//ID_{cr}//n_{cs})$ and compares $\sigma^\wedge = \sigma$. In case of equality, it accepts ψ and else generates the error symbol $\perp\!\!\!\perp$.

6. Informal Security Analysis

This section is dedicated to spotlight the proposed scheme's contribution in upholding basic security including resistance to replay attack, confidentiality, integrity, and unforgeability. Each of the characteristics is briefly analyzed in the following sections.

6.1. Confidentiality. The proposed scheme ensures confidentiality. In case an intruder wants to steal the original contents of a message or the secret key, he/she must have beforehand information about the key as $\beta = \varphi \cdot B_{cr} \cdot B\,ID_{cr}$. In order to determine β, it is required to compute φ from $\Delta = \varphi.D$, which is the discrete log problem in the hyperelliptic curve.

6.2. Replay Attack. The scheme offers replay attack resistance. Each session implies a fresh key (β) and a nonce (n_{cs}) i.e., $\eta = e_{\beta}(m//ID_{cs}//ID_{cr}//n_{cs})$. Therefore, it is, literally, not possible for an intruder of a session to penetrate another session with the same session key. Besides, the receiver is required to run a check for ascertaining the freshness of a message at every instance of reception. An obsoleteness, if spotted, renders the message useless.

6.3. Integrity. The sender takes the "hash value" of the message before sending the message, i.e.,: $\sigma = h_b(m//ID_{cs}//ID_{cr}//n_{cs})$. The "hash" exhibits a property of being an irreversible function. For the confirmation if either of the ciphertexts is altered or not, the receiver performs the following steps: it first decrypts $(m//ID_{cs}//ID_{cr}//n_{cs}) = d_{\beta}(\eta)$ and computes $\sigma^{\wedge} = h_b(m//ID_{cs}//ID_{cr}//n_{cs})$. After it compares $\sigma^{\wedge} = \sigma$, if it holds, then it accepts ψ; otherwise, it generates the error symbol $\perp\!\!\!\perp$.

6.4. Unforgeability. In our proposed scheme, if the intruder tries to generate a valid signature, then he/she is, first of all, required to compute $\partial = (ID_{cr} \cdot \varphi - \sigma \cdot \Delta \cdot A_{cs} \cdot ID_{cs})$, and to do so, the intruder needs to find φ from $\Delta = \varphi \cdot D$ and A_{cs} from $B_{cs} = A_{cs} \cdot D$. This equates to solving two hard problems with commensurate efforts. Thus, it is ensured that our designed approach offers resistance against the signature forging attack.

7. Deployment of the Proposed Scheme

In this phase, we provide the practical deployment of our proposed technique in the UAVs network for precision agriculture that involves monitoring of crop health in a cultivated field. The proposed scheme includes three subphases that are initializations, registration, and data transmission and verification, respectively.

7.1. Initialization. Figure 2 illustrates the initialization process, in which the PKG first calls the setup algorithm; i.e., it first selects a security parameter κ, picks a hyperelliptic curve (HEC) of the genus, chooses a parameter q where the length is equivalent to 80 bits, selects a finite field f_q, where its order is q, picks a divisor D of order q, select two one-way hash functions, i.e., h_a and h_b, chooses a number uniformly for its private key as $\delta \in [1, 2, \ldots, (q-1)]$, computes its public as $\Lambda = \delta \cdot D$, produces all the public parameter $E = [q, h_a, h_b, f_q, \kappa, \Lambda, HEC, D]$, and published it to the network. Note that, in this subphase, we used ID_{mec}, ID_{mbs}, and ID_{m-uav} for the identity of MEC-UAV, MBS/SBS, and M-UAV.

7.2. Registration. Figure 3 illustrates the registration process in which the PKG first calls the key extraction algorithm; i.e., when each of the participated contestants transmits its identity (ID_{pc}) to the PKG, then PKG generates the private and public keys as follows: it computes the private key for identity (ID_{pc}) as $A_{pc} = \delta \cdot h_a(ID_{pc}) \bmod q$, and then it computes public key for identity (ID_{pc}) as $B_{pc} = A_{pc} \cdot D$ Finally, PKG delivers the pair of public and private keys (B_{pc}, A_{pc}) to the participated contestants with its identity (ID_{pc}) by using the private network.note; in this subphase, we used (A_{mec}, B_{mec}), (A_{mbs}, B_{mbs}), and (A_{m-uav}, B_{m-uav}) for the private and public keys of MEC-UAV, MBS/SBS, and M-UAV.

7.3. Data Transmission and Verification. Figure 4 illustrates the data transmission and verification of the proposed scheme. In this phase, MEC-UAV performs the following process for generating a signcrypted ciphertext: it first selects a number in an irregular manner as $\varphi \in [1, 2, \ldots, (q-1)]$ and calculates $\Delta = \varphi \cdot D$. It also calculates $\beta = \varphi \cdot B_{mbs} \cdot D_{mbs}$ and computes $\eta = e_{\beta}(m//ID_{mec}//ID_{mbs}//n_{mec})$. Then, it computes $\sigma = h_b(m//ID_{mec}//ID_{mbs}//n_{mec})$ and $\partial = (ID_{mbs} \cdot \varphi - \sigma \cdot \Delta \cdot A_{mec} \cdot ID_{mec}) \bmod q$. Finally, it sends ψ to MBS/SBS using an open network. Upon reception of ψ MBS/SBS, it performs the verification and decryption process as follows: it computes $\beta = \partial \cdot B_{mbs} + ID_{mec} \cdot \Delta \cdot \sigma \cdot B_{mec} \cdot A_{mbs}$ and decrypts $(m//ID_{mec}//ID_{mbs}//n_{mec}) = d_{\beta}(\eta)$. It also computes $\sigma^{\wedge} = h_b(m//ID_{mec}//ID_{mbs}//n_{mec})$ and compares $\sigma^{\wedge} = \sigma$; if it holds, then, it accepts ψ; otherwise, it generates the error symbol $\perp\!\!\!\perp$.

In the above process, if ID_{mec} = null and $ID_{mbs} \neq$ null, then MEC-UAV performs the encryption process. If ID_{mbs} = null and $ID_{mec} \neq$ null, then MEC-UAV performs the signature method. If $ID_{mbs} \neq$ null and $ID_{mec} \neq$ null, then MEC-UAV performs the signcryption mode.

8. Performance Comparison

This section equates the performance of the proposed scheme with the existing counterparts suggested by Yu et al.'s scheme [13], Kushwah et al.'s scheme [35], Wei et al.'s scheme [36], Shen et al.'s scheme [37], and Zhou et al.'s scheme [39].

8.1. Computational Cost. For evaluating the effectiveness, the proposed scheme is compared with five existing schemes proposed by Yu et al. [13], Kushwah et al. [35], Wei et al. [36], Shen et al. [37], and Zhou et al. [39]. The major findings obtained from the comparison are depicted in Table 2. The five existing schemes utilize elliptic curve scalar multiplication and bilinear pairings, both of which are costlier options. Therefore, we apply the hyperelliptic divisor multiplication. From the observations, it has been revealed that the time taken for processing a single scalar multiplication varies considerably: Elliptic Curve Point Multiplication (ECPM), 0.97 ms; bilinear pairing, 14.90 ms; pairing-based point multiplications, 4.31 ms; and modular exponentiation, 1.25 ms [44]. In order to measure the performance of the proposed scheme, the Multiprecision Integer and Rational Arithmetic C Library (MIRACL) [12] is used. It tests the runtime of the basic cryptographic operations for about 1000 times. For testing the simulation results, a workstation

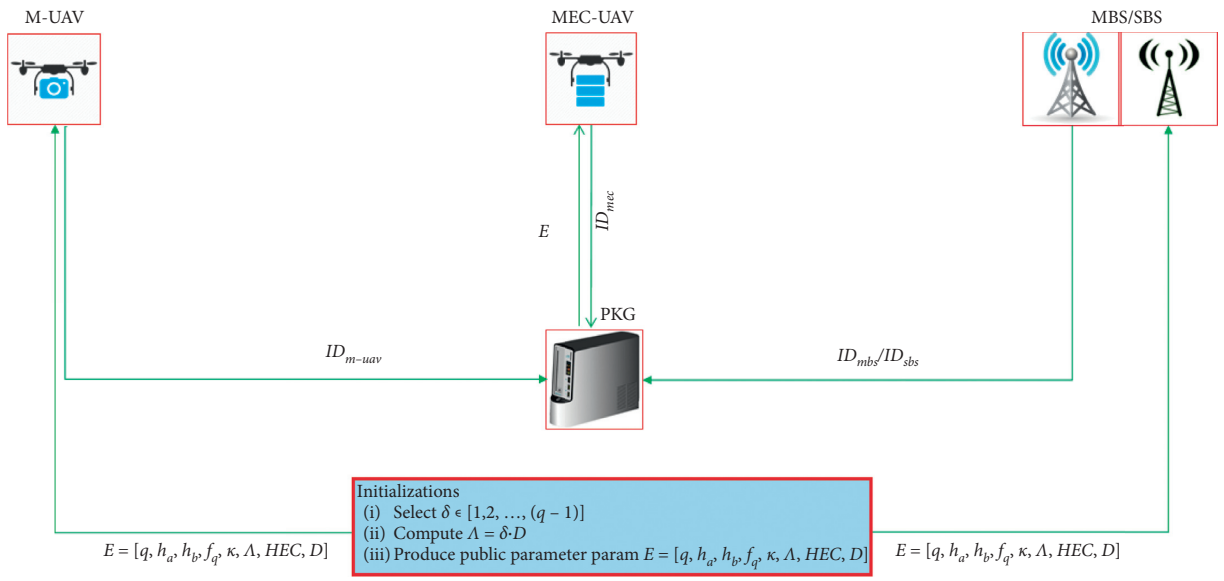

Figure 2: Initialization phase.

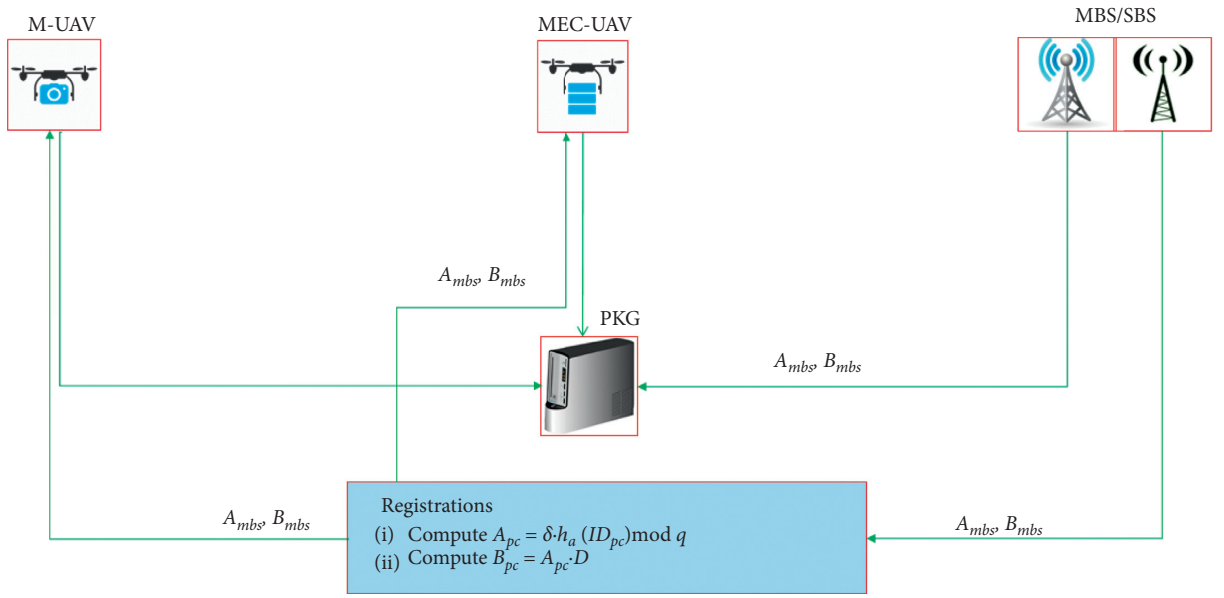

Figure 3: Registration phase.

having the following specifications is used: Intel Core i7-4510U CPU @ 2.0 GHz, 8 GB RAM, and Windows 7 Home Basic 64-bit Operating System [42]. Owing to a smaller key size of 80 bits, the Hyperelliptic Curve Divisor Multiplication (HCDM) is assumed to be of 0.48-millisecond duration [45, 46].

From the findings in Tables 2–4 and Figure 5, it is evident that our approach is far more efficient in terms of computational costs.

8.2. Communication Cost. This section is dedicated to discuss the comparison results in the perspective of communication costs. The proposed approach is compared with the existing five schemes presented by Yu et al. [13], Kushwah et al. [35], Wei et al. [36], Shen et al. [37], and Zhou et al. [39]. In the comparative analysis, the variables used along with the respective values are shown in Table 5 [40].

It is assumed that each of the schemes has associated communication costs as shown in Table 6.

From Figure 6, it is evident that a decision to opt for our proposed scheme results in a significant reduction in the associated communication costs. Table 7 depicts the percentage reduction in communication costs.

8.3. Security Functionalities. Here, the proposed scheme is compared with the existing schemes in terms of security functionalities. Table 8 lists the comparison outcomes based

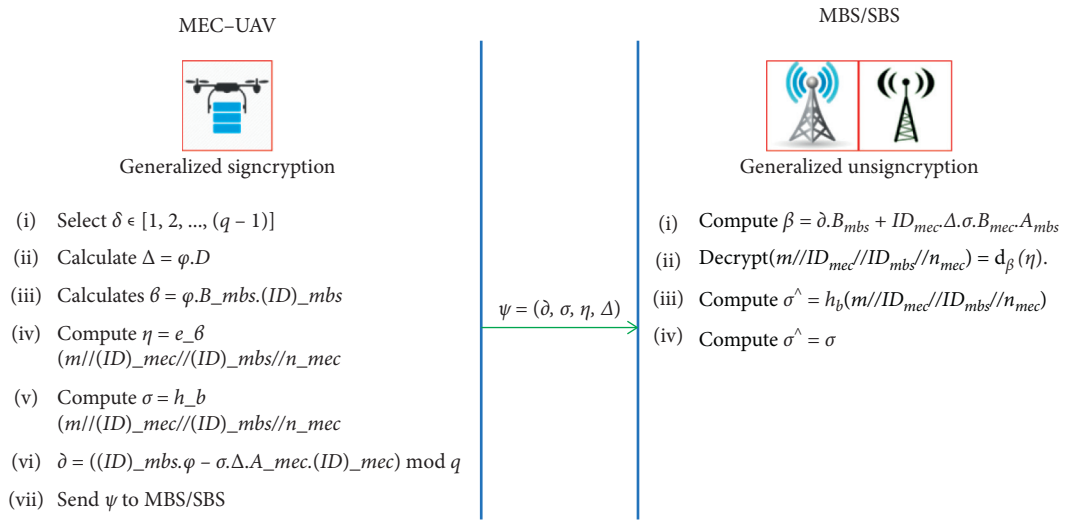

Figure 4: Data transmission and verification phase.

Table 2: Computational cost.

Schemes	Generalized signcrypt	Generalized unsigncrypt	Total
Yu et al.'s scheme [13]	4bpm + 1bp + 1mexp	1bpm + 3bp + 3mexp	5bpm + 4bp + 4mexp
Kushwah et al.'s scheme [35]	5bpm + 2mexp	4bpm + 2bp + 3mexp	9bpm + 2bp + 5mexp
Wei et al.'s scheme [36]	9bpm + 1bp + 7mexp	2bpm + 4bp	11bpm + 5bp + 7mexp
Shen et al.'s scheme [37]	2bpm + 6mxp	5bpm + 2mexp	7bpm + 8mexp
Zhou et al.'s scheme [39]	3bpm + 1bp	1bpm + 2bp	4bpm + 3bp
Proposed	6 hm	5 hm	11 hm

hm = hyperelliptic curve divisor multiplication, em = elliptic curve scalar multiplication, bp = bilinear pairing, bpm = pairing-based point multiplications, mexp = modular exponentiation.

Table 3: Computational cost in milliseconds.

Schemes	Generalized signcrypt (ms)	Generalized unsigncrypt (ms)	Total (ms)
Yu et al.'s scheme [13]	33.39	58.38	86.23
Kushwah et al.'s scheme [35]	24.05	50.79	74.84
Wei et al.'s scheme [36]	62.44	68.22	130.66
Shen et al.'s scheme [37]	16.12	24.05	40.17
Zhou et al.'s scheme [39]	27.83	34.11	61.94
Proposed	2.88	2.40	5.28

Table 4: Percentage improvement in computational cost.

Schemes	Total computational cost of extant scheme (x) (%)	Total computational cost of proposed scheme (y) (%)	z (using the formula**) (%)
Yu et al.'s scheme [13]	86.23	5.28	93.87
Kushwah et al.'s scheme [35]	74.84	5.28	92.94
Wei et al.'s scheme [36]	130.66	5.28	95.95
Shen et al.'s scheme [37]	40.17	5.28	86.85
Zhou et al.'s scheme [39]	61.94	5.28	91.47

** Percentage change, $z = x - y/x * 100$.

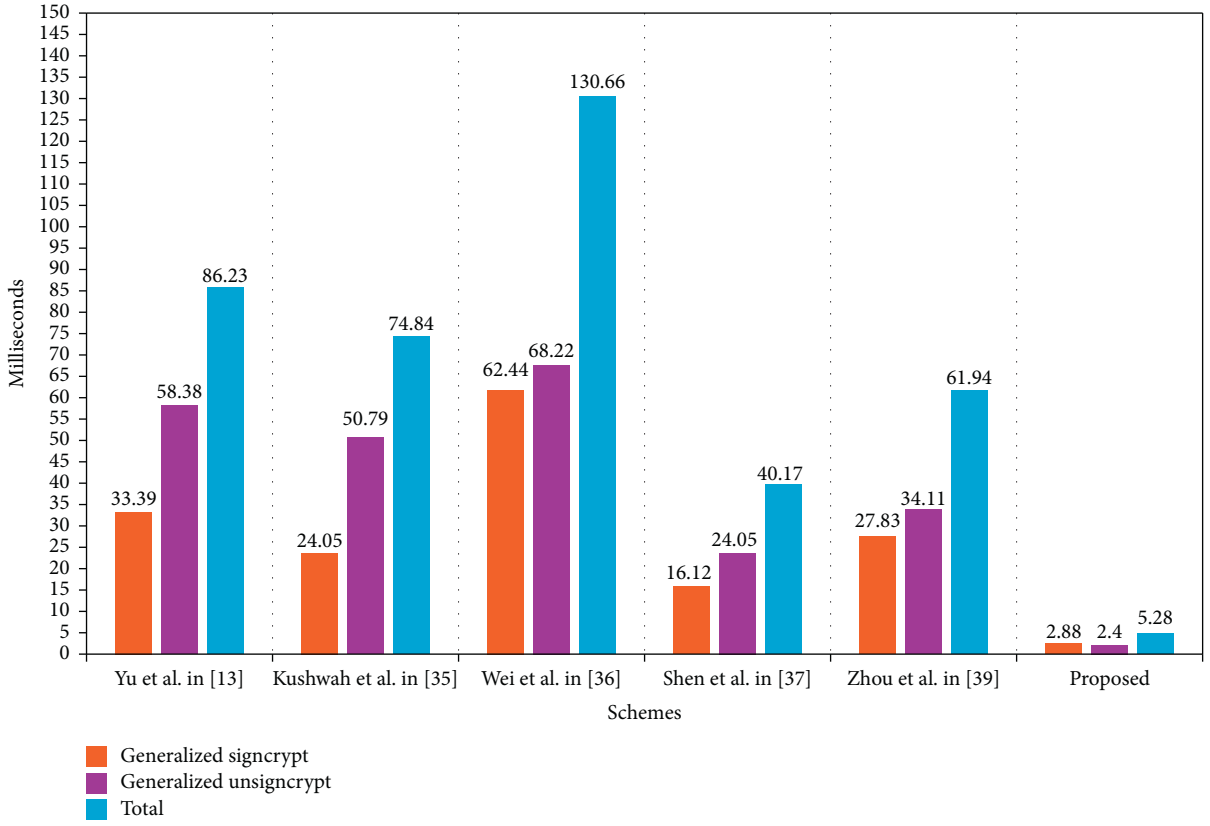

Figure 5: Computational cost (in ms).

Table 5: Variables used for a communication cost comparison.

Variable	Value (bits)
$\|S\|$	1024
$\|Z_q\|$	160
$\|Z_n\|$	80
$\|H\|$	512
$\|m\|$	1024
$\|W\|$	1024

Table 6: Communication cost.

Schemes	Communication cost
Yu et al.'s scheme [13]	$\|S\| + \|m\|$
Kushwah et al.'s scheme [35]	$\|S\| + \|m\|$
Wei et al.'s scheme [36]	$7\|S\| + \|m\|$
Shen et al.'s scheme [37]	$4\|S\| + \|m\|$
Zhou et al.'s scheme [39]	$\|S\| + \|m\|$
Proposed scheme	$3\|Z_n\| + \|m\|$

on the following security parameters: unforgeability, integrity, replay attack, and formal analysis. From the table, it can be seen that none of the existing schemes offer a replay attack.

9. Flying Ad Hoc Network-Based Precision Agriculture: A Case Study

To further assess the practicability, the proposed scheme is applied to a precision agriculture case that involves FANETs for monitoring the health of the crops. Small UAVs are used to capture the images, which are, in the next step, processed to extract useful information. Values from the Normalized Difference Vegetation Index (NDVI) are computed to differentiate healthy plants from the nonhealthy ones. This is done by measuring the chlorophyll content. It further helps in the localization of the area under stress. The images captured by the M-UAVs are transferred to the MEC-UAV, which, utilizing the onboard microcontroller, generates the respective tasks to be carried on by the Decision Support Engine (DSE). For value addition and versatility, the M-UAVs can have additional gadgets, such as cameras, IMU, sensors, and GPS units. The web portal contains a variety of services such as visualization of historical/real data, NDVI mapping, and the correlation functionality.

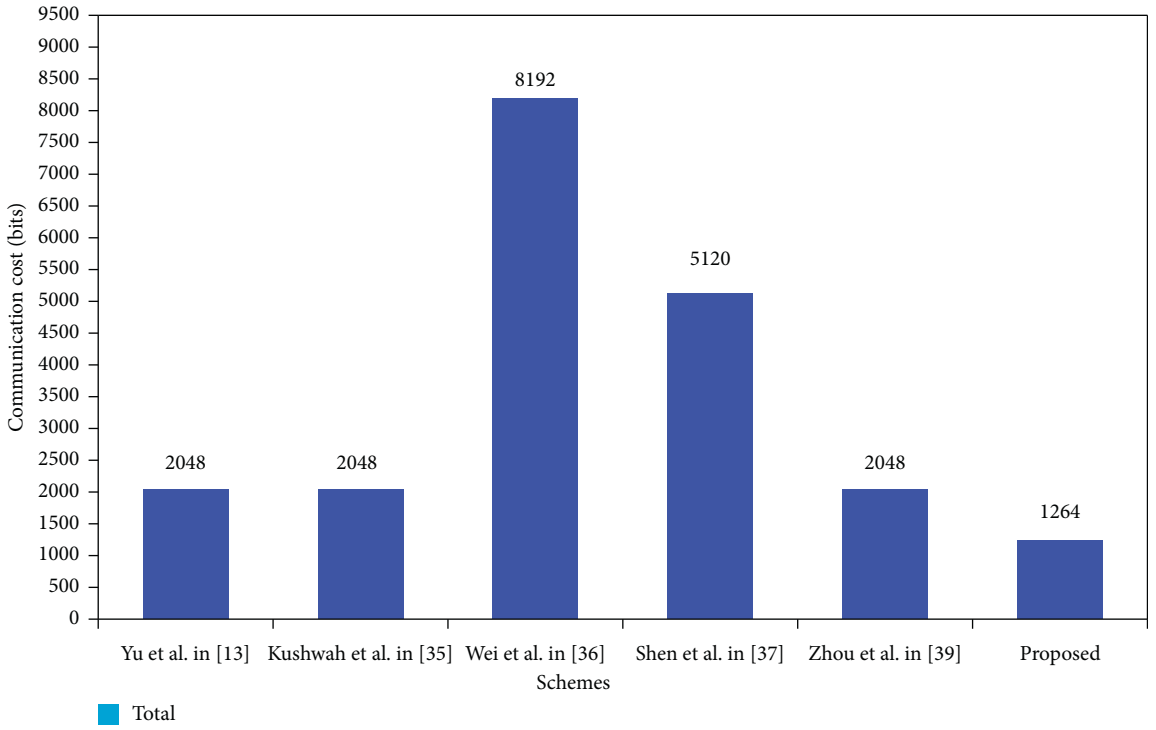

Figure 6: Total communication cost (in bits).

Table 7: Percentage reduction in communication cost.

Scheme	Equation for evaluating reduction	Resulting reduction in communication cost (%)
Yu et al.'s scheme [13]	$(\|S\| + \|m\|) - (3\|Z_n\| + \|m\|)/(\|S\| + \|m\|)$	38.28
Kushwah et al.'s scheme [35]	$(\|S\| + \|m\|) - (3\|Z_n\| + \|m\|)/(\|S\| + \|m\|)$	38.28
Wei et al.'s scheme [36]	$(7\|S\| + \|m\|) - (3\|Z_n\| + \|m\|)/(\|S\| + \|m\|)$	84.57
Shen et al.'s scheme [37]	$(4\|S\| + \|m\|) - (3\|Z_n\| + \|m\|)/(\|S\| + \|m\|)$	75.31
Zhou et al.'s scheme [39]	$(\|S\| + \|m\|) - (3\|Z_n\| + \|m\|)/(\|S\| + \|m\|)$	38.28

Table 8: Comparison with relevant existing schemes.

Schemes	Security functionalities				
	Informal				Formal
	U	I	C	RA	FA
Yu et al.'s scheme [13]	✓	✓	✓	✗	✗
Kushwah et al.'s scheme [35]	✓	✓	✓	✗	✗
Wei et al.'s scheme [36]	✓	✓	✓	✗	✗
Shen et al.'s scheme [37]	✓	✓	✓	✗	✗
Zhou et al.'s scheme [39]	✓	✓	✓	✗	✗
Proposed	✓	✓	✓	✓	✓

U: unforgeability, I: integrity, RA: replay attack, FA: formal analysis. The symbol ✓ satisfies the security functionality; ✗ does not satisfy the security functionality.

10. Conclusions

There is an evolving trend of combining multiple small UAVs, as a flying ad hoc network (FANET), to cater to the needs of future applications that demand autonomy and pervasiveness. However, the small UAVs inherent limited onboard energy and restricted computational capability. Such limitations hinder their deployment for longer time-

```
role
role_Mecuav(Mecuav:agent, Mbssbs:agent, Bmec:public_key, Bmbs:public_key, SND, RCV:channel(dy))
played_by Mecuav
def=
        local
        State:nat, Add:hash_func, Phii:text, Idmec:text, Delta:text, Idmbs:text, Nmec:text,M:text, Encrypts:hash_func, Beeta:
symmetric_key
        init
           State := 0
        transition
           1. State = 0 /\ RCV(start) = |> State' : = 1 /\ SND(Mecuav.Mbssbs)
           2. State = 1 /\ RCV(Mbssbs.{Nmec'}_Bmbs) = |> State' : = 2 /\ Idmbs' : = new() /\ Phii' : = new() /\ Delta' : = new() /\ Idmec' :
 = new() /\ Beeta' : = new() /\ M' : = new() /\ secret(M',sec_2,{Mecuav}) /\ witness(Mecuav, Mbssbs,auth_1,M') /\
SND(Mecuav.{Encrypts(M'.Nmec'.Idmec'.Idmbs')}_Beeta'.{Add(Idmec'.Phii'.Delta'.Phii'.Idmbs')}_inv(Bmec))
end role
```

Algorithm 1: High-level protocol specification language (HLPSL) code for the MEC-UAV role.

```
role
role_Mbssbs(Mecuav:agent, Mbssbs:agent, Bmec:public_key,Bmbs:public_key,SND,RCV:channel(dy))
played_by Mbssbs
def=
        local
        State:nat,Add:hash_func, Phii:text, Idmec:text, Delta:text, Idmbs:text, Nmec:text,M:text, Encrypts:hash_func, Beeta:
symmetric_key
        init
           State := 0
        transition
           1. State = 0 /\ RCV(Mecuav.Mbssbs) = |> State' : = 1 /\ Nmec' : = new() /\ SND(Mbssbs.{Nmec'}_Bmbs)
           6. State = 1 /\ RCV(Mecuav.{Encrypts(M'.Nmec.Idmec'.Idmbs')}_Beeta'.{Add(Idmec'.Phii'.Delta'.Phii'.Idmbs')}
_inv(Bmec)) = |> State' : = 2 /\ request(Mbssbs, Mecuav, auth_1, M') /\ secret(M',sec_2,{Mecuav})
end role
```

Algorithm 2: High-level protocol specification language (HLPSL) code for MBS role.

```
role session1(Mecuav:agent, Mbssbs:agent, Bmec:public_key, Bmbs:public_key)
def=
        local
           SND2, RCV2, SND1, RCV1: channel(dy)
        composition
           role_Mbssbs(Mecuav, Mbssbs,Bmec, Bmbs,SND2,RCV2) /\ role_Mecuav(Mecuav, Mbssbs, Bmec, Bmbs, SND1, RCV1)
end role
role session2(Mecuav:agent, Mbssbs:agent, Bmec:public_key, Bmbs:public_key)
def=
        local
           SND1, RCV1:channel(dy)
        composition
           role_Mecuav(Mecuav, Mbssbs,Bmec, Bmbs, SND1, RCV1)
end role
```

Algorithm 3: High-level protocol specification language (HLPSL) code for Sessions role.

intervals and complex cryptographic operations. Addressing such deficiency, in this article, utilizing the concept of the hyperelliptic curve (HEC), we propose an efficient lightweight security scheme, called identity-based generalized signcryption. The scheme is based on multiaccess edge computing (MEC). The HEC approach is

```
role environment()
def=
        const
        hash_0:hash_func, bmec:public_key,alice:agent,bob:agent, bmbs:public_key,const_1:agent, const_5:public_key,const_9:
public_key,auth_1:protocol_id,sec_2:protocol_id
        intruder_knowledge = {alice, bob}
        composition
           session2(i, const_1,const_5,const_9) /\ session1(alice, bob, bmec, bmbs)
end role
goal
        authentication_on auth_1
        secrecy_of sec_2
end goal
environment()
```

Algorithm 4: High-level protocol specification language (HLPSL) code for environment role.

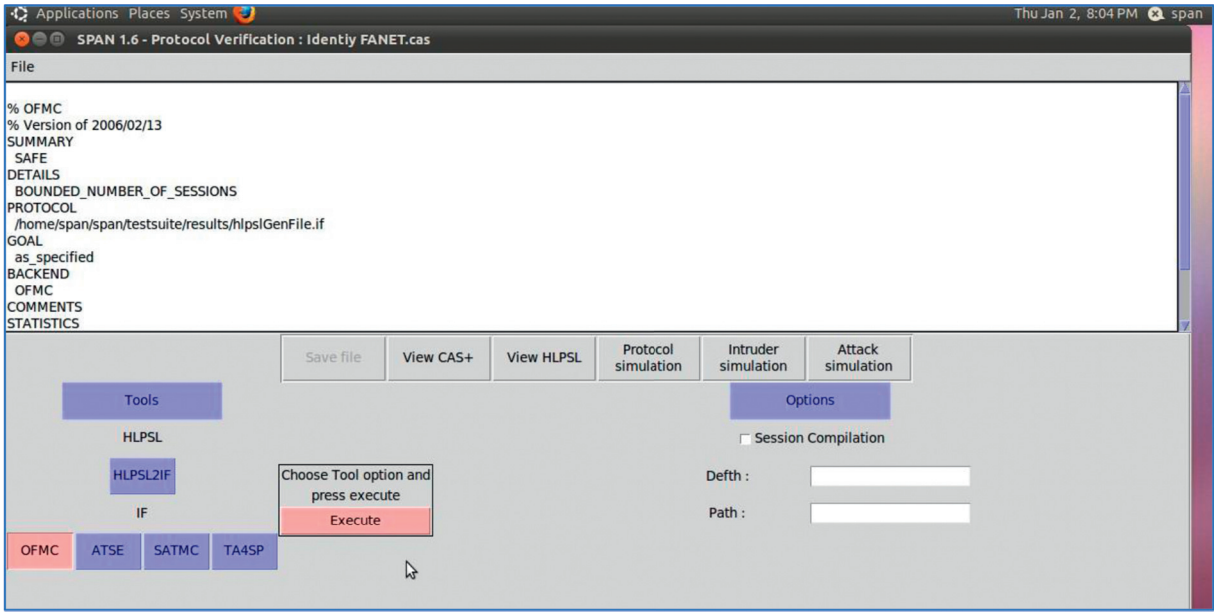

Figure 7: Simulation results for on-the-fly model-checker (OFMC).

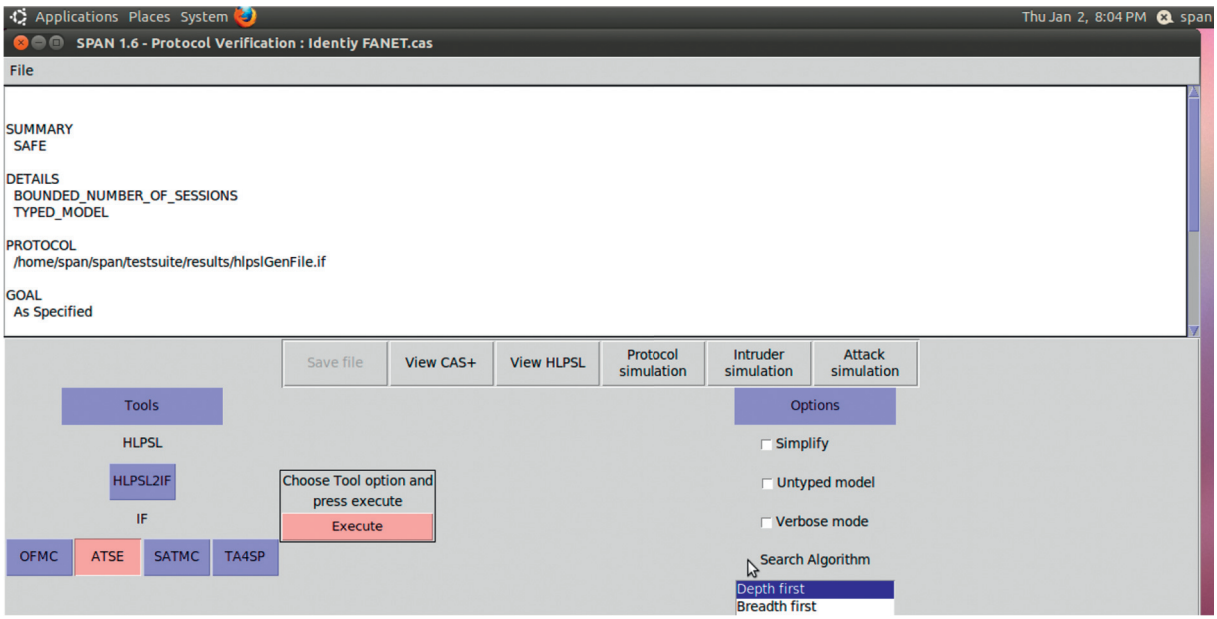

Figure 8: Simulation results for AtSe.

effective in generating small keys and is, therefore, suitable for low-computational devices such as small UAVs. Both formal and informal security analyses, using the AVISPA tool, demonstrate the potency of the proposed scheme in thwarting various known and unknown cyberattacks. Moreover, upon comparative analysis with the major existing counterparts, the scheme has demonstrated to be efficient in terms of computational and communication costs.

For our future work, we aim to complement the research work by including other aspects of formal analysis, such as the Real-Or-Random (ROR) model and Random Oracle Model (ROM). Moreover, we also intend to incorporate a computational offloading and scheduling mechanism, in which the M-UAVs will be able to offload and schedule the computing tasks to the MEC-UAV for improved processing power and faster execution.

Appendix

Implementation of Our Proposed Scheme in AVISPA

High-level protocol specification language (HLPSL) has been consulted to implement the proposed scheme for MEC-UAV and MBS. This has been illustrated in Algorithms 1 and 2. To run the simulations, a Haier Win8.1 PC computer workstation powered with an Intel (R) Core (TM) i3-4010U CPU @ 1.70 GHz and 64-bit Operating System was chosen. The software part of the setup is composed of Oracle VM Virtual Box (version: 5.2.0.118431) and SPAN (version: SPAN-Ubuntu-10.10-light_1). From Algorithms 3 and 4, the roles for session, goal, and environment have been executed to comply with the conventions. The execution test considers OFMC and CL-AtSe back ends for evaluating the system's susceptibility to attacks. The simulation results do not include the results of SATMC and TA4SP. It is because SATMC and TA4SP are not compatible with bitwise XOR operations. Another factor worthy of consideration is the requirement to monitor the execution of a specified protocol. Therefore, the back ends delegated the responsibility to check operations. In order to verify the Dolev-Yao (DY) model, the back ends also estimate the vulnerability of the system to man-in-the-middle attack [42]. The widely known web-tool SPAN (Specific Protocol Animator for AVISPA) is also used to simulate the proposed scheme. The results obtained from OFMC (Figure 7) and AtSe (Figure 8) further demonstrate the scheme's potency against replay and man-in-the-middle attacks.

Data Availability

All data generated or analysed during this study are included in this published article.

Conflicts of Interest

The authors declare no conflicts of interest with respect to the research, authorship, and/or publication of this article.

References

[1] M. A. Khan, B. A. Alvi, A. Safi, and I. U. Khan, "Drones for good in smart cities: a review," in *Proceedings of the 2018 International Conference on Electrical, Electronics, Computers, Communication, Mechanical and Computing (EECCMC*, pp. 1–6, Vaniyambadi, India, January 2018.

[2] E. Yanmaz, S. Yahyanejad, B. Rinner, H. Hellwagner, and C. Bettstetter, "Drone networks: communications, coordination, and sensing," *Ad Hoc Networks*, vol. 68, pp. 1–15, 2018.

[3] V. Sharma, "Advances in drone communications, state-of-the-art and architectures," *Drones*, vol. 3, no. 1, p. 21, 2019.

[4] O. S. Oubbati, M. Atiquzzaman, P. Lorenz, M. H. Tareque, and M. S. Hossain, "Routing in flying ad hoc networks: survey, constraints, and future challenge perspectives," *IEEE Access*, vol. 7, pp. 81057–81105, 2019.

[5] V. Sharma and R. Kumar, "G-FANET: an ambient network formation between ground and flying ad hoc networks," *Telecommunication Systems*, vol. 65, no. 1, pp. 31–54, 2017.

[6] M. A. Khan, I. M. Qureshi, and F. Khanzada, "A hybrid communication scheme for efficient and low-cost deployment of future flying ad-hoc network (FANET)," *Drones*, vol. 3, no. 1, p. 16, 2019.

[7] M. Marchese, A. Moheddine, and F. Patrone, "IoT and UAV integration in 5G hybrid terrestrial-satellite networks," *Sensors*, vol. 19, no. 17, p. 3704, 2019.

[8] C. Lin, D. He, N. Kumar, K.-K. R. Choo, A. Vinel, and X. Huang, "Security and privacy for the Internet of drones: challenges and solutions," *IEEE Communications Magazine*, vol. 56, no. 1, pp. 64–69, 2018.

[9] Y. Zhi, Z. Fu, X. Sun, and J. Yu, "Security and privacy issues of UAV: a survey," *Mobile Networks and Applications*, vol. 25, pp. 95–101, 2019.

[10] Y. Zheng, "Digital signcryption or how to achieve cost(signature & encryption) ≪ cost(signature) + cost(encryption)," in *Proceedings of the Advances in Cryptology - CRYPTO '97*, pp. 165–179, Springer, Santa Barbara, CA, USA, August 1997.

[11] Y. Han, X. Yang, P. Wei, Y. Wang, and Y. Hu, "ECGSC: elliptic curve based generalized signcryption," in *Proceedings of the Third International Conference Ubiquitous Intelligence and Computing, Vol. 4159 of Lecture Notes in Computer Science*, Springer, Wuhan, China, pp. 956–965, September 2006.

[12] Shamus Sofware Ltd, "Miracl Library," GitHub, Inc., San Francisco, CA, USA, http://github.com/miracl/MIRACL.

[13] G. Yu, X. Ma, Y. Shen, and W. Han, "Provable secure identity based generalized signcryption scheme," *Theoretical Computer Science*, vol. 411, no. 40-42, pp. 3614–3624, 2010.

[14] M. Suárez-Albela, P. Fraga-Lamas, and T. Fernández-Caramés, "A practical evaluation on RSA and ECC-based cipher suites for IoT high-security energy-efficient fog and mist computing devices," *Sensors*, vol. 18, no. 11, p. 3868, 2018.

[15] M. Yu1, J. Zhang, J. Wang et al., "Internet of Things security and privacy-preserving method through nodes differentiation, concrete cluster centers, multi-signature, and blockchain," *International Journal of Distributed Sensor Network*, vol. 14, p. 12, 2018.

[16] A. Braeken, "PUF based authentication protocol for IoT," *Symmetry*, vol. 10, p. 8, 2018.

[17] C. Zhou, Z. Zhao, W. Zhou, and Y. Mei, "Certificateless key-insulated generalized signcryption scheme without bilinear pairings," *Security and Communication Network*, vol. 2017, Article ID 8405879, 17 pages, 2017.

[18] S. Kumari, M. Karuppiah, A. K. Das, X. Li, F. Wu, and N. Kumar, "A secure authentication scheme based on elliptic curve cryptography for IoT and cloud servers," *The Journal of Supercomputing*, vol. 74, p. 12, 2017.

[19] A. Omala, A. Mbandu, K. Mutiria, C. Jin, and F. Li, "Provably secure heterogeneous access control scheme for wireless body area network," *Journal of Medical Systems*, vol. 42, p. 6, 2018.

[20] C. Tamizhselvan and V. Vijayalakshmi, "An energy efficient secure distributed naming service for IoT," *International Journal of Advanced Studies of Scientific Research*, vol. 3, p. 8, 2019.

[21] V. S. Naresh, R. Sivaranjani, and N. V. E. S. Murthy, "Provable secure lightweight hyper elliptic curve-based communication system for wireless sensor Network," *International Journal of Communication Systems*, vol. 31, p. 15, 2018.

[22] A. Rahman, I. Ullah, M. Naeem, R. Anwar, H. Khattak, and S. Ullah, "A lightweight multi-message and multi-receiver heterogeneous hybrid signcryption scheme based on hyper elliptic curve," *International Journal of Advanced Computer Science and Applications*, vol. 9, p. 5, 2018.

[23] S. Ouahouah, T. Taleb, J. Song, and C. Benzaid, "Efficient offloading mechanism for UAVs-based value-added services," in *Proceedings of the 2017 IEEE International Conference on Communications (ICC)*, pp. 1–6, Paris, France, May 2017.

[24] N. H. Motlagh, M. Bagaa, and T. Taleb, "UAV-based iot platform: a crowd surveillance use case," *IEEE Communications Magazine*, vol. 55, no. 2, pp. 128–134, 2017.

[25] S. Garg, A. Singh, S. Batra, N. Kumar, and L. T. Yang, "UAV-empowered edge computing environment for cyber-threat detection in smart Vehicles," *IEEE Network*, vol. 32, no. 3, pp. 42–51, 2018.

[26] G. K. Xilouris, M. C. Batistatos, G. E. Athanasiadou, G. Tsoulos, H. B. Pervaiz, and C. C. Zarakovitis, "UAV-assisted 5G network architecture with slicing and virtualization," in *Proceedings of the 2018 IEEE Globecom Workshops (GC Wkshps)*, pp. 1–7, Abu Dhabi, UAE, December 2018.

[27] C. Grasso and G. Schembra, "A fleet of MEC UAVs to extend a 5G network slice for video monitoring with low-latency constraints," *Journal of Sensor and Actuator Networks*, vol. 8, no. 1, p. 3, 2019.

[28] W. Chen, B. Liu, H. Huang, S. Guo, and Z. Zheng, "When UAV swarm meets edge-cloud computing: the QoS perspective," *IEEE Network*, vol. 33, no. 2, pp. 36–43, 2019.

[29] J.-M. Fernandez, I. Vidal, and F. Valera, "Enabling the orchestration of IoT slices through edge and cloud microservice platforms," *Sensors*, vol. 19, no. 13, p. 2980, 2019.

[30] S. He, Q. Wu, J. Liu, W. Hu, B. Qin, and Y. N. Li, "Secure communications in unmanned aerial vehicle network," in *Proceedings of the International Conference on Information Security Practice and Experience*, Springer, Melbourne, Australia, pp. 601–620, December 2017.

[31] J. Won, S.-H. Seo, and E. Bertino, "Certificateless cryptographic protocols for efficient drone-based smart city applications," *IEEE Access*, vol. 5, pp. 3721–3749, 2017.

[32] J. Won, S. H. Seo, and E. Bertino, "A secure communication protocol for drones and smart objects," in *Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security, ser. ASIA CCS'15*, ACM, Singapore, pp. 249–260, April 2015.

[33] J. Srinivas, A. K. Das, N. Kumar, and J. P. C. Rodrigues, "CloudCentric authentication for wearable healthcare monitoring system," *IEEE Transactions on Dependable and Secure Computing*, 2018.

[34] S. Lal and P. Kushwah, "ID based generalized signcryption," Cryptology ePrint Archive, Report 2008/084, October 2019, http://eprint.iacr.org/2008/084.

[35] P. Kushwah and S. Lal, "An efficient identity based generalized signcryption scheme," *Theoretical Computer Science*, vol. 412, no. 45, pp. 6382–6389, 2011.

[36] G. Wei, J. Shao, Y. Xiang, P. Zhu, and R. Lu, "Obtain confidentiality or/and authenticity in Big Data by ID-based generalized signcryption," *Information Sciences*, vol. 318, pp. 111–122, 2015.

[37] X. Shen, Y. Ming, J. Feng, X. Shen, Y. Ming, and J. Feng, "Identity based generalized signcryption scheme in the standard model," *Entropy*, vol. 19, no. 3, p. 121, 2017.

[38] A. Waheed, A. I. Umar, N. Din, N. U. Amin, S. Abdullah, and P. Kumam, "Cryptanalysis of an authentication scheme using an identity based generalized signcryption," *Mathematics*, vol. 7, no. 9, p. 782, 2019.

[39] Y. Zhou, Z. Li, F. Hu, and F. Li, "Identity-based combined public key schemes for signature, encryption, and signcryption," in *Information Technology and Applied Mathematics*, pp. 3–22, Springer, Singapore, 2019.

[40] I. Ullah, A. Alomari, N. Ul Amin, M. A. Khan, and H. Khattak, "An energy efficient and formally secured certificate-based signcryption for wireless body area networks with the Internet of Things," *Electronics*, vol. 8, no. 10, p. 1171, 2019.

[41] Raspberry pi 4," 2019, https://www.raspberrypi.org/.

[42] 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.

[43] R. Canetti and H. Krawczyk, "Universally composable notions of key exchange and secure channels," in *Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques—Advances in Cryptology (EUROCRYPT'02)*, pp. 337–351, Amsterdam, The Netherlands, May 2002.

[44] C. Zhou, "An improved lightweight certificateless generalized signcryption scheme for mobile-health system," *International Journal of Distributed Sensor Networks*, vol. 15, no. 1, 2019.

[45] M. A. Khan, I. M. Qureshi, I. Ullah, S. Khan, F. Khanzada, and 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. 1, p. 30, 2019.

[46] M. A. Khan, I. Ullah, S. Nisa et al., "An efficient and provably secure certificateless key-encapsulated signcryption scheme for flying ad-hoc network," *IEEE Access*, vol. 8, pp. 36807–36828, 2020.