electronics

MDPI

Article

An Efficient and Provably Secure Certificateless Blind Signature Scheme for Flying Ad-Hoc Network Based on Multi-Access Edge Computing

Muhammad Asghar Khan [1], Ijaz Mansoor Qureshi [2], Insaf Ullah [3], Suleman Khan [2], Fahimullah Khanzada [4] and Fazal Noor [5,*]

1 Department of Electronic Engineering, ISRA University, Islamabad 44000, Pakistan; khayyam2302@gmail.com
2 Department of Electrical Engineering, AIR University, Islamabad 44000, Pakistan; imqureshi@mail.au.edu.pk (I.M.Q.); 171518@students.au.edu.pk (S.K.)
3 Department of Computer Sciences, Hamdard University, Islamabad 44000, Pakistan; insafktk@gmail.com
4 Descon Engineering Limited, Lahore 54000, Pakistan; fahimullahk@gmail.com
5 Department of Computer and Information Systems, Islamic University of Madinah, Madinah 400411, Saudi Arabia
* Correspondence: mfnoor@gmail.com; Tel.: +966-551497218

Received: 31 October 2019; Accepted: 22 December 2019; Published: 26 December 2019

Abstract: Unmanned aerial vehicles (UAVs), when interconnected in a multi-hop ad-hoc fashion, or as a flying ad-hoc network (FANET), can efficiently accomplish mission-critical tasks. However, UAVs usually suffer from the issues of shorter lifespan and limited computational resources. Therefore, the existing security approaches, being fragile, are not capable of countering the attacks, whether known or unknown. Such a security lapse can result in a debilitated FANET system. In order to cope up with such attacks, various efficient signature schemes have been proposed. Unfortunately, none of the solutions work effectively because of incurred computational and communication costs. We aimed to resolve such issues by proposing a blind signature scheme in a certificateless setting. The scheme does not require public-key certificates, nor does it suffer from the key escrow problem. Moreover, the data that are aggregated from the platform that monitors the UAVs might be too huge to be processed by the same UAVs engaged in the monitoring task. Due to being latency-sensitive, it demands high computational capability. Luckily, the envisioned fifth generation (5G) mobile communication introduces multi-access edge computing (MEC) in its architecture. MEC, when incorporated in a UAV environment, in our proposed model, divides the workload between UAVs and the on-board microcomputer. Thus, our proposed model extends FANET to the 5G mobile network and enables a secure communication between UAVs and the base station (BS).

Keywords: blind signature; security; MEC; UAVs; FANET; 5G; IoT

1. Introduction

During the last couple of years, the exponential advancement in the manufacturing of small unmanned aerial vehicles (UAVs) has led to a new clan of networks, referred to as flying ad-hoc network (FANET). The prominent features of agility, low-cost, and easy deployment, among others, are paving ways for FANET to offer successful solutions for diverse military and civilian application. In case of a disastrous situation, FANET can offer a cost-effective solution for real-time data communication as compared to its predecessors, these being, mobile ad-hoc networks (MANETs) and vehicular ad-hoc networks (VANETs) [1]. Not only does FANET have the capability of collecting and sharing the aggregated data amongst the UAVs, it can also send it to the base station (BS). Additionally,

if some of the UAVs are detached during the mission, irrespective of any reason, they still have the facility to remain associated to the network with the support of other UAVs due to an ad-hoc network between the UAVs. Furthermore, the inherent multi-hop networking schema counters the obstacles of short-range communication and limited guidance that normally arise in a stand-alone UAV system [2]. Nevertheless, such exclusive attributes make FANET a suitable solution for various applications. The small UAVs have restricted capabilities in terms of power, sensing, communication, and computation. This renders the small UAVs as luring targets to different kinds of known and unknown cyber-attacks. Generally, in a FANET environment, multiple UAVs are integrated into a team that cooperates with each other to accomplish critical tasks [3]. Hence, when a self-governing UAV desires to perform a certain task, it receives the command containing relevant task-specific information such as time, target location, and actions, among others. Then, it either flies autonomously to the target position in the assigned time, or it may cruise in the air while waiting for commands, thus reducing the response time and accomplishing the results proficiently.

The ground station interconnects with UAVs over an unauthenticated and unencrypted channel. Therefore, anyone with a suitable transmitter can link with the UAV and insert commands into an ongoing session, and thus can easily interpret any UAV. Thus, it is important for a UAV to ascertain the origination of a command. Normally, digital signatures are used to ascertain the source of command. He et al. [4] described the overall process as follows:

(1) A command center initiates command and computes the corresponding digital signature.
(2) The corresponding command and signature are then forwarded to the UAV by the command center.
(3) The UAV, upon receiving the command and signature, attempts to verify the signature.

- If the signature is valid, the UAV deems it to be issued by the command center and proceeds with executing the command.
- Otherwise, the command is considered counterfeit and, thus, the UAV does not execute it.

However, due to its intrinsic complexities and security requirements, the mutual digital signature scheme is not appropriate for an UAV-based network. Additionally, the average speed of a typical UAV can lie in the range of 30–460 km/h in a three-dimensional (3D) setting [5]. Moreover, the topology of the particular network varies rapidly, which necessitates the need of ascertaining the validity of a command in the shortest time. Therefore, it is essential for the UAV to validate the signature in a timely manner, especially for location-based services. For example, the user or ground station (GS) pledges a command and the corresponding signature to the UAV; however, the concerned UAV can only verify the signature. Even in the worst case, if an intruder eavesdropped on the command and corresponding signature, they cannot authenticate the signature and authorize the task to be accomplished next. In addition, frequent changes in topology also increase the latency and communication cost. In order to accommodate the key escrow problem, a certificateless signature scheme is required. In a certificateless cryptosystem, a participant private key is composed of two parts: the partial private key and a secret value. The trusted third-party key generation center (KGC) generates the partial private key, whereas the secret value is affirmed by the participant. Similarly, a participant's public key also consists of two parts, these being the participant's identity information and the public key conforming to the secret value. Therefore, the cost of public key management is significantly reduced due to the fact that the public key does not require any certificate. Furthermore, it does not suffer from the key escrow problem because the KGC has no information about the participant secret value.

Typically, small UAVs have batteries that last for merely 20 to 30 min [6]. Therefore, it is of utmost importance to manage the battery resources efficiently. This prolongs the network lifetime especially for large-scale deployments of UAVs. Thus, it is harder for the UAVs to complete these resource-hungry applications in a timely fashion. Furthermore, FANET can be deployed in remote

locations to assist the Internet of Things (IoT) devices for collecting large volumes of data. Fortunately, these impediments can be mitigated by employing multi-access edge computing (MEC) technology. The MEC shifts the job performed by the commanding UAV to the edge of the network, which is closer to UAV, thus reducing the propagation delay. The MEC thus paves way for a diverse set of applications that, explicitly, demand a real-time response. The heterogeneous radio access network of a ground-based network is composed of macro cells and small cells. The network assists the mobile phones, driver-less cars, and IoT gadgets, among others, in performing the required operations. Therefore, as a direct consequence, a multitude of emerging technologies can synergize with the 5G (fifth generation) wireless networks. A symbiotic relation can be visualized between the UAVs, engaged in scheduling the computing tasks, and the onboard microprocessor, dedicated to executing the particular operations. Furthermore, the usable data can be stored temporarily for retrieval by either the UAVs or the ground devices, while, concurrently, the drone-cells transmit the data.

Normally, the security and efficiency of the aforementioned signature scheme is based on some computationally hard problems, for example, Rivest–Shamir–Adleman (RSA), bilinear pairing, and elliptic curve cryptosystems (ECC). RSA offers a solution based on large factorization [7,8], which utilizes a 1024 bit large key [9]. However, due to the restricted on-board processing capabilities on UAVs, the solution is not appropriate for the resource-constrained FANET system. In addition, bilinear pairing, which suffers from high pairing and map-to-point function computations, is 14.90 times worse than RSA [10]. Therefore, in order to counter the shortcomings of RSA and bilinear pairing, a new category of cryptography, elliptic-curve cryptography (ECC) was introduced [11]. ECC is characterized by a smaller parameter size and involves miniaturized versions of public key, private key, identity, and certificate size, among other factors. Moreover, unlike bilinear pairing and RSA, the security hardiness and efficiency of the scheme is based on 160 bit small key, which is still not suitable for resource-hungry devices [12]. Thus, a new type called hyperelliptic-curve cryptography (HECC) was proposed [13]. The hyperelliptic curve uses an 80 bit key, identity, and certificate and offers security to the degree comparable to that of elliptic curve, bilinear pairing, and RSA [14,15]. It is, hence, a far better choice for energy-constrained devices.

1.1. Authors' Motivations and Contributions

A comprehensive literature review of the existing blind signature schemes was carried out. It was found that these schemes are based on hard problems, that is, elliptic curve, bilinear pairing, and modular exponential, and thus suffer from high computational and communication costs. Hence, the existing schemes are not compatible with small devices, that is, UAVs that have limited computational power. Moreover, these schemes are not validated using formal security validation tools such as automated validation of internet security protocols and applications (AVISPA) or Scyther, among others, which can, somehow, guarantee security. There is a critical need to harness the state-of-the-art certificateless blind signature scheme so as to engineer a viable cryptographic solution for FANET that poses less danger to the battery lifetimes of resource-constrained UAVs.

The authors, motivated by the aforementioned objectives, to name a few, propose a new scheme, called provably verified certificateless blind signature (CL-BS) scheme for FANET. The proposed scheme is based on hyperelliptic curve, which is an advanced version of the elliptic curve. It provides the same level of security as elliptic curves, bilinear pairing, and modular exponential with smaller key size. Some of the salient features signifying contributions of our research work, in this paper, are as follows:

- We introduce a novel architecture for flying ad-hoc network (FANET) constituted by UAVs with a multi-access edge computing (MEC) facility that leverages the 5G wireless technology.
- We propose an efficient and provably secure certificateless signature (CL-BS) scheme for the same architecture using the concept of hyperelliptic curve for operating in resource-constrained environments.

- The proposed scheme is shown to be resistant against various attacks through formal as well as informal security analysis using the widely-accepted automated validation for internet security validation and application (AVISPA) tool.
- The proposed scheme is also compared with existing counterparts and it is shown that our approach provides better efficiency in terms of computational and communication costs.

1.2. Structure of the Paper

The remainder of the paper is structured as follows: Section 2 contains a brief about the related work; Section 3 presents the foundational concepts; Section 4 presents the proposed architecture and construction of proposed scheme (i.e., CL-BS); Section 5 holds implementation of the proposed scheme in FANET; Section 6 outlines the AVISPA tool component of our proposed scheme for formal security verification as well as informal security analysis; Section 7 compares the proposed scheme with the existing schemes; and in the end, Section 8 succinctly culminates the manuscript by concluding the work.

2. Related Work

2.1. Flying Ad-Hoc Network

In flying ad-hoc network, the security and privacy are important because UAVs are always unattended. The primary security mechanisms for FANET emphasize authenticity, confidentiality and integrity of data via cryptography. A well-designed data protection mechanism can significantly reduce the probability of the data becoming compromised, irrespective of the malicious technique involved. There are a few studies dedicated to investigating the data protection issues for UAV networks. Won et al. [16], proposed a suite of cryptographic protocols for drones and smart objects. The protocols deal with three communication scenarios: one to-one, one-to-many, and many-to-one. In the first scenario, that is, one-to-one, the efficient encapsulation mechanism, a certificateless signcryption tag key, backs the authenticated key agreement in addition to offering non-repudiation and user revocation. The one-to-many scenario involves a certificateless multi-recipient encryption scheme, which allows a UAV to transmit privacy-intensive data to multiple smart objects. Lastly, UAVs are able to collect data from multiple smart objects in the "many-to-one" communication scenario. The protocol, however, finds it difficult to transmit a multitude of encrypted messages and at the same time assure privacy of the end devices. 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. A novel approach to mitigate the broadcast storm problem during the interest's dissemination is proposed by Barka et al. [17]. The approach is based on a trust-aware monitoring communication architecture for flying named data networking. It makes use of the inter-UAV communication for checking the data authenticity on a particular UAV without disturbing the desired level of security. However, data privacy and caching policies are not taken into consideration in the proposed scheme.

In order to resist the physical capturing of drones with minimum exposure of confidential data, Bae et al. [18] proposed a saveless-based key management and delegation system for a multi-drone environment. Nevertheless, the proposed scheme is not compatible with devices such as UAVs equipped with limited on-board energy that hinder the potency of finding a proper key renewal period with low computation cost and more security guarantee. Seo et al. [19] proposed a pairing-free approach for drone-based surveillance applications. However, this approach faces the user revocation problem in the case of a physical attack. In such a case, the intruders can access not only current but future information of the drones. In order to cater the forward secrecy problem in drones, Liu et al. [20] proposed two construction schemes that achieve better performance in terms of the computational cost required by the recipient. However, the approach uses the elliptic curves and, thus, it suffers from high computational cost. Moreover, the proposed scheme is not validated through

formal security analysis. In 2018, Reddy et al. [21] presented a pairing-free key insulated signature scheme in the identity-based setting for improving the computational and communication efficiency. Later, in 2019, Xiong et al. [22] also proposed a pairing-free and provably secure certificateless parallel key-insulated signature (CL-PKIS) scheme in order to secure the communication in the IIoT setting. However, because the scheme involves the concept of elliptic curve, it is not free from the issue of high computational cost. Moreover, the proposed schemes are not validated through formal security analysis.

2.2. Multi-Access Edge Computing

It is mandatory for a FANET system to diminish latency to the maximum possible extent. MEC can solve the problem of latency resulting from long communication distance. So far, studies have been conducted to examine the usage of edge computing for UAVs [23–25]. However, the studies do not discuss the topic of communication link quality. ETSI proposed a reference architecture of MEC [26]. Primarily, the MEC reference architecture is composed of user equipment, mobile edge applications, and networks. The network is classified into either of the following three levels: system level, host level, and network level. The reference points and functional elements of the reference architecture are depicted by the reference architecture. Garg et al. aimed to answer the surveillance-related concerns by proposing a data-driven transportation optimization model [27]. The model comprises UAV, dispatcher, aggregator, and edge devices. Each of the constituents undertake the designated tasks as follows: the UAV captures and validates the date; the dispatcher, in addition to validating the tasks, schedules the processing tasks in the edge computing devices; the aggregator assures a secure transmission of data; and the edge devices analyze the data. A hierarchical MEC architecture has been proposed by Lee et al. [28]. It involves utilizing the resources of the MEC server for providing services customized on the basis of content type and the computing demand. After exploring the major causes of communication and computational latencies, Intharawijitr et al. proposed a mathematical model. The model is used to estimate the computing latency in an edge node selected on the basis of either of the three policies [29]. A game theoretic model is proposed by Messous et al. in which the UAVs, as game players, strategize to achieve the optimal tradeoff between energy overhead and the execution delay. As a result, the UAVs do not stay overburdened anymore [30]. Ansari et al. addressed the issue of end-to-end delay between the proxy virtual machine and the device. They claim to resolve the problem by suggesting two dynamic proxy virtual machine migration methods, which is corroborated by simulation results [31]. Zhang et al. attempted to resolve the issue of increased energy consumption and longer execution time by proposing a mobility-aware hierarchical MEC framework [32]. The proposed solution involves the MEC servers and, for sharing the computing tasks, a backup computing server. An incentive-based optimal computational offloading scheme was developed. The objective of quick-response and energy conservation was achieved to a significant extent.

The methodology proposed by Christian et al. [33] 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. The UAVs are accoutered with MEC facilities while carrying out the processing tasks and they follow a policy for mutual help for improved performance. However, the work fails to address the issue of limited battery duration of MEC UAVs.

2.3. Related Certificateless Blind Signature Schemes

As early as 1983, Chaum presented a blind signature scheme that significantly reduces the probability of detectability [34]. The scheme, for the case of transmitting a message, revolves around two major players: signer, the entity that computes the signature, and provider, the part tasked to blind the message. The signer transmits the computed signature to the provider, who deciphers and retrieves the original signature. Owing to its versatility, the scheme can, in e-commerce settings, help establish a forgery-resistant payment system. In 1996, Mambo et al. proposed a proxy signature

scheme in which the original signer can delegate the task of issuing signature to a proxy security and communication network 5 [35]. Tan et al. applied the concepts of discrete logarithm and elliptic curve discrete logarithm to suggest two proxy blind signature schemes [36]. Each of the schemes offers the security threshold promised by the proxy and blind signature schemes. Tan proposed another proxy blind signature scheme as well [37]. The comparatively efficient scheme is based on identity and is pairing-free. It proves to be secure in random oracle model. A proxy partially blind signature scheme has been proposed by Yang et al. The scheme can revoke the proxy privileges and is characterized by security features [38]. Verma et al. proposed a proxy blind signature scheme [39]. The scheme exhibits message recovery and caters to the requirements of low-bandwidth because it abbreviates the size of message signature. The efficient identity-based proxy blind signature scheme proposed by Zhu et al. can even overcome a quantum computer attack [40]. A designated verifier signature scheme is proposed by Jakobsson et al. [41]. Dai et al. further advanced the concept of designated receiver proxy signature scheme by presenting a combo of a designated verifier signature scheme and a proxy signature scheme [42]. In the schema, a proxy signer is delegated the authority to sign, and then authenticate, in lieu of the original signer.

A short-designated verifier proxy signature (DVPS) scheme is proposed by Huang et al. [43]. The scheme is characterized by signatures of comparatively shorter length and, thus, caters to the applications requiring low bandwidth. Shim furthered the idea by presenting a short DVPS scheme based on BLS signature. The scheme proves to be superior when tested using the random oracle model [44]. Islam et al. considered the concept of bilinear pairing to propose an efficient identity-based DVPS scheme [45]. The scheme assigns private keys to the involved entities generated from a private key generator (PKG). Hu et al. proposed two DVPS schemes: weak DVPS and strong DVPS [46]. Although the weak DVPS scheme is not able to compute a DVPS, the strong DVPS scheme can do so. The random oracle model is used to prove the effectiveness of the proposed scheme. It has been demonstrated on multiple occasions that the blind signature scheme offers forgery-proof operations when applied in sensitive applications such as e-voting and e-cash, among other applications [47,48]. However, anonymity and intractability of the voter and the unforgeability of the electronic vote are the main security concerns. In addition, the proposed schemes are based on bilinear pairing and elliptic curves, both of whom are costly operations in cryptography. Chin et al. [49] presented a certificateless blind signature scheme based on bilinear pairing. Likewise, the proposed scheme is based on bilinear pairing. Furthermore, the security analysis is done through random oracle model and has not been authenticated using any tool.

3. Preliminaries

A brief overview of some of the foundational concepts, along with their formal definitions, is presented in this section.

3.1. Hyperelliptic Curve Cryptosystems (HECC)

Hyperelliptic curves can be viewed as generalizations of ECC (elliptic curve cryptosystems), introduced by Koblitz [50]. A hyperelliptic curve [51] is denoted over curves, whose genus is greater than 1, as shown in Figure 1. Similarly, the curves with genus 1 are generally known as elliptic curves. The group order of the field F_q for genus 1, 160 bit long operands are required, that is, we need at least $g.\log_2(q) \approx 2^{160}$, where g is the genus of curve over F_q that is a set of finite fields of order q. Likewise, for curves with genus 2, 80 bit long operands, and, for curves with genus 3, 54 bit long operands are needed [52].

A hyper elliptic curve C of genus greater than 1 over F is a set of solutions $(x, y) \in F \times F$ to the following equation:

$$C: \ y^2 + h(x)y = f(x). \tag{1}$$

A divisor D is a finite formal sum of points on hyper elliptic curve and represented as

$$D = \sum_{P_i \in C} m_i p_i \ , \ m_i \in Z. \tag{2}$$

The two divisors can be added as follows:

$$\sum_{P_i \in C} m_i p_i + \sum_{P_i \in C} n_i p_i = \sum_{P_i \in C} (m_i + n_i) p_i. \tag{3}$$

Each element of the Jacobian can be represented in the semi-reduced divisor form [53]:

$$D = \sum_i m_i p_i - \left(\sum_i m_i \right), \ \forall mi \ \geq \ 0. \tag{4}$$

If the divisor is subjected to the additional constraint, that is, $r \leq g$, such a divisor is defined as a reduced divisor. Additionally, in [50], the author shows that the divisors of the Jacobian can be denoted as a pair of polynomials $a(x)$ and $b(x)$ with following degrees: $b(x) \ \leq \deg a(x) \leq \ g$, where the coefficients of $a(x)$ and $b(x)$ are elements of F and $a(x)$ divided by $y^2 \ + \ h(x)y \ - \ f(x)$.

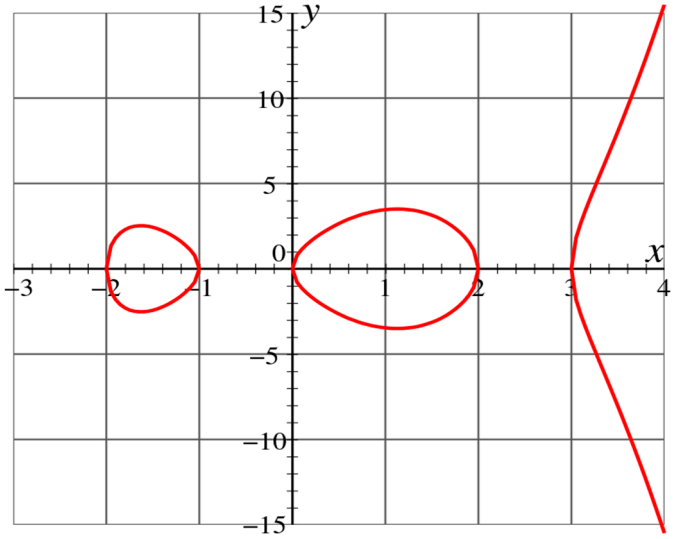

Figure 1. Hyper elliptic curve of genus 2, that is, g = 2.

3.2. Threat Model

The widely used Dolev–Yao (DY) threat model [54] is used in the proposed scheme. According to the DY model, an insecure public channel (open channel) is used for communication between any two parties and the end-point entities have an untrustworthy nature. Therefore, the system is prone to eavesdropping of exchanged messages and deletion/modification attempts by the attacker. Moreover, as the UAVs may roam around in unattended hostile areas, there exists the probability of them getting physically captured. This may lead to leakage of precious data from a UAV's memory. The KGC, on the other hand, is a fully trusted entity.

4. Proposed Architecture

The proposed architecture of flying ad-hoc network based on multi-access edge computing is illustrated in Figure 2. The application scenario considered is the surveillance of a specific area, which may collect data, that is, video streaming and images. We consider two representative classes of UAVs: monitoring UAV (M-UAV) and raspberry pi-based multi-access edge computing UAV (RMEC-UAV). M-UAV perform data acquisition and monitoring only from the assigned zone. In our proposed architecture, the set of M-UAVs are assigned to one RMEC-UAV that is used to reduce the

power consumption while executing the security mechanism (i.e., sign, verify). The set of M-UAVs allocated to RMEC-UAV is essentially subjected to the load produced by M-UAV. RMEC-UAV collects data from M-UAVs and forwards this to the base station. RMEC-UAV can also connect with the IoT devices and collect data from them. Prior to transmitting, the RMEC-UAV validates the authenticity of the M-UAVs. Upon successful validation, the RMEC-UAV forwards the data to the BS. The RMEC-UAV transmits not only the IoT data but also the flight information and the information about the role of each M-UAV.

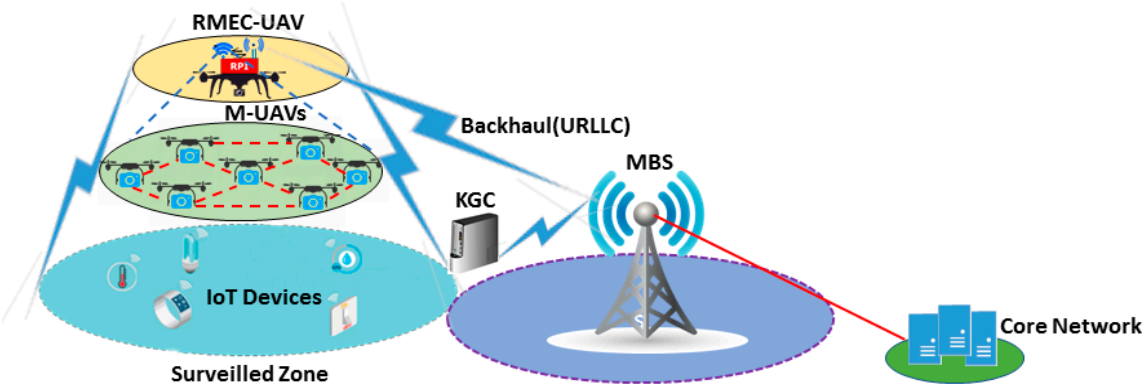

Figure 2. Proposed architecture of flying ad-hoc network with 5G and multi-access edge computing (MEC) facilities. RMEC-UAV: raspberry pi-based multi-access edge computing unmanned aerial vehicle, M-UAV: monitoring UAV, IoT: Internet of Things, URLLC: ultra-reliable low latency communications, KGC: key generation center.

Raspberry PI (RPI) board was considered for RMEC-UAV. Even though there are other substitutions for RPI, with sophisticated hardware configurations, such as LattePanda 4G/64 GB, Qualcomm Dragon board, ODROID-XU4, and ASUS Tinker Board, among others, RPI is nonetheless considered to be the most cost-effective and energy-efficient option. Other alluring features of RPI 4 that further defend its selection are the built-in wireless networking support, that is, Wi-Fi (dual-band 802.11 b/g/n/ac) and Bluetooth 5.0 BLE. RPI 4 is equipped with a 1.5 GHz 64-bit quad core ARM Cortex-A72 processor. The 5G and 802.11 ac wireless modules are enabled on RMEC-UAV in order to link it with the BS/IoT devices and hence provide a hotspot service over the M-UAVs. Fifth generation (5G) is further classified into enhanced mobile broadband (eMBB), massive machine-type communications (mMTC), and ultra-reliable low latency communications (URLLC) by the International Telecommunication Union (ITU) in order to fulfill the requirements of diverse industrial and market demands. However, we have considered URLLC in the proposed architecture, as of it offers very high mobility, which further defends its selection for UAV-based operations [55].

The images transmitted by the monitoring UAVs, ground cameras, and the sensors, among other sources, are all received by the RMEC-UAV on-board microcontroller. The microcontroller, then, generates the tasks that will be processed by the local microcomputer, or the decision support engine (DSE). The human operator receives a decreased share of the data flow so as to decide quickly. In case the human decisions are not timely, the predictive and interpolative/extrapolative modules mounted on the RMEC-UAV DSE step in. The probability of response-delays resulting from the queues of to-be-processed jobs can never be ignored. To compensate for such time lapse and to enhance reliability, the RMEC-UAVs synergize with each other. Further, each of the M-UAVs, after being equipped with the essential gadgets, these being cameras, IMU, sensors, and a GPS unit, among others, can be accustomed to different application scenarios.

The proposed architecture can be divided into the following three main layers:

- **Layer 1** consists of the ground-level IoT devices that are devoted to different tasks as per application scenario. The ground-level IoT devices are connected with the RMEC-UAV and BS via URLLC, a 5G wireless link. Furthermore, the macro base station (MBS) are typically linked with the core network via wires that have huge bandwidth.
- **Layer 2** comprises a team of M-UAVs equipped with the essential gadgets, these being cameras, IMU, sensors, and a GPS unit, among others, for monitoring the assigned zone. Moreover, M-UAVs are connected with each other using Bluetooth 5 (2.4 GHz) link and with the RMEC-UAV with 802.11 ac (5 GHz) Wi-Fi link.
- **Layer 3** is composed of RMEC-UAV that is used to collect data from M-UAVs and forwards it to the base station. RMEC-UAV can also connect with the ground-level IoT devices and collect data from them.

Construction of the Proposed Scheme

The proposed scheme includes the following four entities: KGC, blind signer, requester, and verifier. Further, it involves the following six sub-algorithms for producing the certificateless blind signature: setup, partial private key setting (PPKS), secret value setting (SVS), private key setting (PKS), public key setting (PBKS), blind signature, and verification.In Table 1, we provide an explanation about the notations used in the proposed algorithm. Therefore, for representing the whole process of certificateless blind signature, we aimed to provide the simplest explanation by using the following steps:

1. Setup: In this sub-algorithm, the KGC selects the following parameters:

   - A hyper elliptic curve (C);
   - A divisor ($\mathscr{D}$), where D is the divisor in C;
   - The hash function (h);
   - Select ∂ from $\{1, 2, \ldots, n-1\}$ and the size of $n = 2^{80}$.

   After the above process, the KGC determines the master public key using $\Upsilon = \partial.\mathscr{D}$. Then, it publishes the set of selected parameters, $\{C, \mathscr{D}, \Upsilon, n = 2^{80}\}$.

2. Partial private key setting (PPKS): In order to set the partial private key for the participating users (verifier and signer) with identity $\mathscr{ID}_u$, the KGC performs the following sub-steps:

   - It selects X_u from $\{1, 2, ..., n-1\}$;
   - It computes $\alpha_u = X_u.\ \mathscr{D}$ and $\beta_u = X_u + \partial.\ \alpha_u$;
   - It computes $\delta_u = \beta_u.\ \mathscr{D}$;
   - It sends (β_u, δ_u) to the users (verifier and signer) with identity $\mathscr{ID}_u$.

   The users can verify the pair (β_u, δ_u) such as: $\beta_u.\ \mathscr{D} = \alpha_u + \alpha_u.\Upsilon = \alpha_u + \alpha_u.\Upsilon = X.\mathscr{D} + \alpha_u\ (\partial.\mathscr{D}) = \mathscr{D}\ (X + \alpha_u.\ \partial) = \mathscr{D}\ (\beta_u) = \beta_u.\mathscr{D}$.

3. Secret value setting (SVS): The user (verifier and signer) with identity $\mathscr{ID}_u$ selects $\mathscr{Q}_u$ from $\{1, 2, ..., n-1\}$ and keeps it as his secret value.
4. Private key setting (PKS): The user (verifier and signer) set the private key as $\sigma_u = <\mathscr{Q}_u, \beta_u>$.
5. Public key setting (PBKS): The user (verifier and signer), with identity $\mathscr{ID}_u$, compute $\chi_u = \sigma_u.\mathscr{D}$.

   The user sets his/her public key as $\mathscr{B}_u = <\chi_u, \delta_u>$.

   - Blind signature: In this part, the blind signer first selects ω from $\{1, 2, \ldots, n-1\}$, computes $\Delta_1 = \omega/\mathscr{Q}_s$, $\Delta_2 = \beta_s/\omega$, and then sends it (Δ_1, Δ_2) to the requester. Further, the requester proceeds as follows:

- It selects (τ, φ) from $\{1, 2, \ldots, n-1\}$;
- It computes $\mathscr{E} = \hbar(m, \Delta_1, \Delta_2, \sigma_r)$ and $\mathscr{Z} = \mathscr{E} + \varphi$;
- It sends $\mathscr{Z}$ to the blind signer. The blind signer generates the partial blind signature $\mathscr{S}^* = \mathscr{Q}_s - \mathscr{Z}.\beta_s$ and sends it to the requester;
- The requester, then, generates the hash value as $r = (m, \text{Ns})$ and full blind signature, using $\mathscr{S}^{**} = \mathscr{S}^* - \tau$, and transfers it $(\mathscr{S}^{**}, r)$ to the verifier.

6. Verification: The verifier can verify the blind signature if either of the following equalities are satisfied: $r^* = (m, \text{Ns}) = r = (m, \text{Ns})$ or $r^* = r$.

Table 1. Notations used in proposed algorithm.

S.NO	Symbol	Definition
1	C	Means hyperelliptic curve with genus 2, which is the generalized form elliptic curve requiring 80 bit key
3	$\mathscr{D}$	A divisor, which is a finite formal sum of points on hyperelliptic curve
4	∂	Master secret key which is generated by KGC for producing partial private key
5	Υ	The master public key of KGC
6	N	Randomly generated number and the size of N as $n = 2^{80}$
7	$\hbar$	One-way hash function, which means that it has the property of irreversibility
8	$\sigma_r = <\mathscr{Q}_r, \beta_r>$	Private key of requester
9	$\sigma_s = <\mathscr{Q}_s, \beta_s>$	Private key of signer
10	Ns	A fresh nonce that is used for anti-replay attack
11	$\mathscr{ID}_u$	Identities for sender and receiver
12	m	Plain-text (message)

5. Implementation of Proposed Scheme in FANET

We divided this process in two sub-phases that are (1) initialization and registration, and (2) signing and verifying Phase, which are illustrated in Figures 3 and 4, respectively.

5.1. Initialization and Registration

In this sub algorithm, the KGC selects a hyper elliptic curve (C), a divisor ($\mathscr{D}$), the hash function ($\hbar$), and then computes ∂ from $\{1, 2, \ldots, n-1\}$ and the size of $n = 2^{80}$.

After the above process, the KGC determines the master public key using $\Upsilon = \partial.\mathscr{D}$. Then, it publishes the set of selected parameters, $\{C, \mathscr{D}, \Upsilon, n = 2^{80}\}$.

- ***Partial Private Key Generation for RMEC-UAV:*** In order to set the partial private key for *RMEC-UAV* with identity $\mathscr{ID}_{rv}$, the KGC performs the following sub steps:

  i. It selects X_{rv} from $\{1, 2, \ldots, n-1\}$;
  ii. It computes $\alpha_{rv} = X_{rv}.\mathscr{D}$ and $\beta_{rv} = X_{rv} + \partial.\alpha_{rv}$;
  iii. It computes $\delta_{rv} = \beta_{rv}.\mathscr{D}$;
  iv. It sends $(\beta_{rv}, \delta_{rv})$ to the *RMEC-UAV*.

The *RMEC-UAV* can verify the pair $(\beta_{rv}, \delta_{rv})$, such as $\beta_{rv}.\mathscr{D} = \alpha_{rv} + \alpha_{rv}.\Upsilon = \alpha_{rv} + \alpha_{rv}.\Upsilon = X.\mathscr{D} + \alpha_{rv}.(\partial.\mathscr{D}) = \mathscr{D}(X + \alpha_{rv}.\partial) = \mathscr{D}(\beta_{rv}) = \beta_{rv}.\mathscr{D}$.

- ***Secret Value Setting for RMEC-UAV:*** The *RMEC-UAV* selects $\mathscr{Q}_{rv}$ from $\{1, 2, \ldots, n-1\}$ and keeps it as their secret value.
- ***Private Key Setting for RMEC-UAV:*** The *RMEC-UAV* sets the private key as $\sigma_{rv} = <\mathscr{Q}_{rv}, \beta_{rv}>$.

- ***Public Key Generation for RMEC-UAV*:** The RMEC-UAV computes $\chi_{rv} = \sigma_{rv}.\mathcal{D}$ and sets their public key as $\mathcal{B}_{rv} = <\chi_{rv}, \delta_{rv}>$.
- ***Partial Private Key Setting for BS/IoT:*** In order to set the partial private key for *BS/IoT* with identity $\mathcal{JD}_{BI}$, the KGC performs the following sub steps:

  i. It selects X_{BI} from $\{1, 2, \ldots, n-1\}$;
  ii. It computes $\alpha_{BI} = X_{BI}.\ \mathcal{D}$ and $\beta_{BI} = X_{BI} + \partial.\ \alpha_{BI}$;
  iii. It computes $\delta_{BI} = \beta_{BI}.\ \mathcal{D}$;
  iv. It sends $(\beta_{BI}, \delta_{BI})$ to *BS/IoT*.

The *RMEC-UAV* can verify the pair $(\beta_{BI}, \delta_{BI})$, such as $\beta_{BI}.\mathcal{D} = \alpha_{BI} + \alpha_{BI}.\mathcal{Y} = \alpha_{BI} + \alpha_{BI}.\mathcal{Y} = X.\mathcal{D} + \alpha_{BI}.(\partial.\mathcal{D}) = \mathcal{D}\ (X_{BI} + \alpha_{BI}.\ \partial) = \mathcal{D}\ (\beta_{BI}) = \beta_{BI}.\mathcal{D}$.

- ***Secret Value Setting for BS/IoT:*** The *BS/IoT* selects $\mathcal{Q}_{BI}$ from $\{1, 2, \ldots, n-1\}$ and keeps it as their secret value.
- ***Private Key Setting for BS/IoT:*** The BS/IoT sets the private key as $\sigma_{BI} = <\mathcal{Q}_{BI}, \beta_{BI}>$.
- ***Public Key Setting for BS/IoT:*** The BS/IoT computes $\chi_{BI} = \sigma_{BI}.\mathcal{D}$ and sets their public key as $\mathcal{B}_{B} = <\chi_{BI}, \delta_{BI}>$.

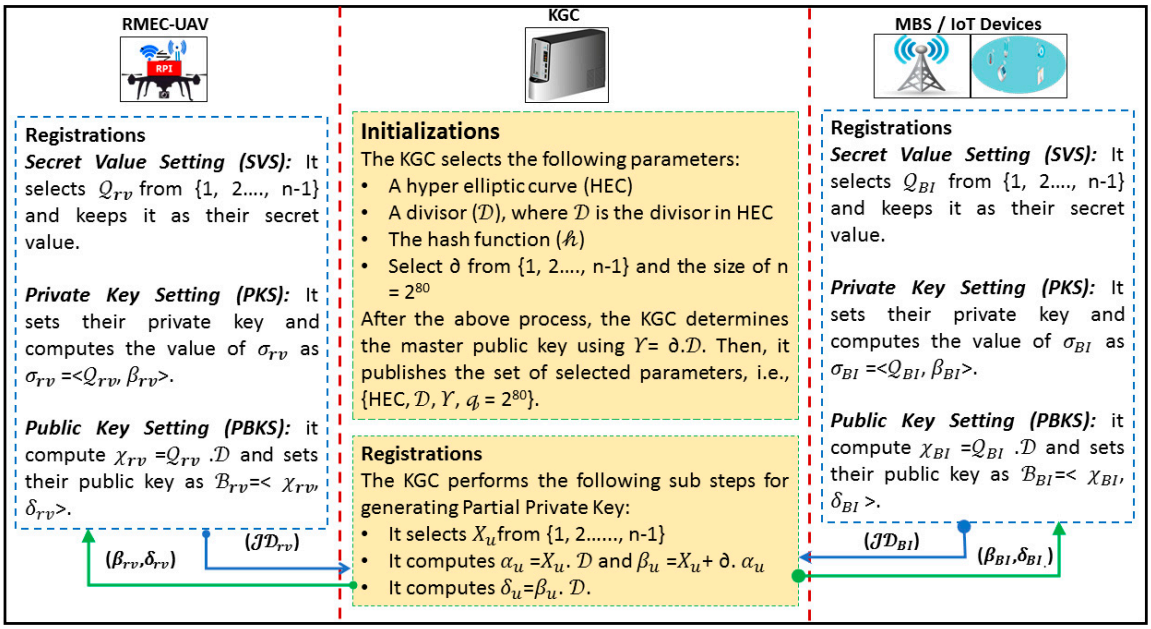

Figure 3. Initialization and registration phase.

5.2. Signing and Verifying Phase

In this part, the *RMEC-UAV* first selects ω from $\{1, 2, \ldots, n-1\}$ and then computes $\Delta_1 = \omega/\mathcal{Q}_{rv}$, $\Delta_2 = \beta_{rv}/\omega$, and then sends it (Δ_1, Δ_2) to the M-UAV. Further, the M-UAV proceeds as follows:

- It selects (τ, φ) from $\{1, 2, \ldots, n-1\}$;
- It computes $\mathcal{E} = \mathcal{h}(m, \Delta_1, \Delta_2, \sigma_{muv})$ and $\mathcal{Z} = \mathcal{E} + \varphi$;
- It sends $\mathcal{Z}$ to the *RMEC-UAV*. The *RMEC-UAV* generates the partial blind signature $\mathcal{S}^* = \mathcal{Q}_{rv} - \mathcal{Z}.\beta_{rv}$ and sends it to the M-UAV;
- The M-UAV, then, generates the hash value as $r = (m, Ns)$ and full blind signature, using $\mathcal{S}^{**} = \mathcal{S}^* - \tau$, and transfers it $(\mathcal{S}^{**}, r)$ to the BS/IoT.

Then BS/IoT can verify the blind signature if either of the following equalities are satisfied: $r^* = (m, Ns) = r = (m, Ns)$ or $r^* = r$.

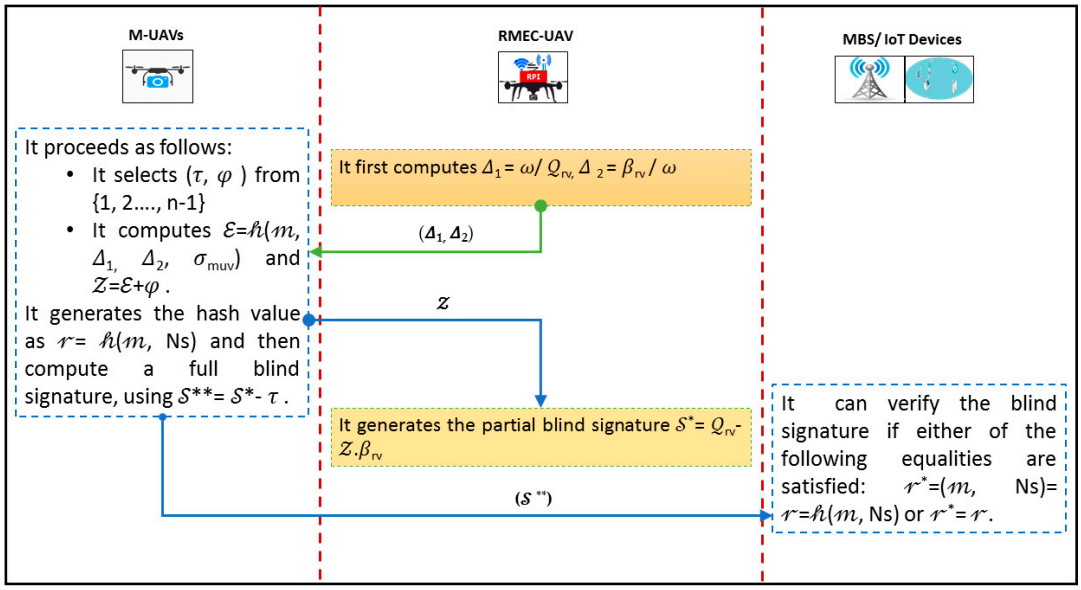

Figure 4. Signing and verifying phase.

6. Security Analysis

This section aims to justify the effectiveness of the proposed scheme in resisting well-known attacks.

6.1. Informal Security Analysis

6.1.1. Theorem 1 ←Unforgeability

A certificateless blind signature is obviously assumed to provide security from a forgeability attack if there is no malicious attacker, $\mathcal{MA}$, which produces the forge blind signature.

Proof. In our case, if an $\mathcal{MA}$ desires the generation of the forge blind signature, then he/she must compute Equation (5). Here, it is the need of $\mathcal{S}^*$, and can be calculated from Equation (6); however, processing this equation, is the need for the calculation of $\mathcal{Q}_s$ from Equation (7) is further needed, which is equal to the processing of the hyper elliptic curve discrete logarithm problem. Also, it is a need for β_s from Equation (8), which further requires an equivalent process for the hyper elliptic curve discrete logarithm problem. Thus, the aforementioned assumption proves that an $\mathcal{MA}$ cannot generate the forge blind signature.

$$\mathcal{S}^{**} = \mathcal{S}^* - \tau, \tag{5}$$

$$\mathcal{S}^* = \mathcal{Q}_s - \mathcal{Z}.\ \beta_s, \tag{6}$$

$$\sigma_s = \mathcal{Q}_s.\mathcal{D}, \tag{7}$$

$$\delta_s = \beta_s.\mathcal{D}. \tag{8}$$

□

6.1.2. Theorem 1 ←Integrity

A certificateless blind signature is supposed to secure from integrity attack if there is no malicious attacker, $\mathcal{MA}$, which becomes modified in the plain text.

Proof. In our proposed work, the requester produces the hash value of a plain text m as $\mathcal{X} = \hbar_2$ (m, Ns) and sent it to the verifier, along with signature $\mathcal{S}^{**}$and m as ($\mathcal{S}^{**}$, m). However, if the $\mathcal{MA}$ wishes to

change the plain text m into $\vec{m}$, then the $\mathscr{MA}$ also needs to amend $\mathscr{X} = \hbar_2$ (m, Ns) into $\vec{\mathscr{X}} = \hbar_2$ ($\vec{m}$, Ns). Therefore, the $\mathscr{MA}$ cannot perform this process because of the one-way nature of the hash function. Thus, keeping in view the aforesaid discussion, our scheme is far more secure against breaking the integrity of plain text. □

6.1.3. Theorem 1 ←Unlinkability

A certificateless blind signature is presumed to offer security from the linkability attack if the blind signer has no access to the plain text.

Proof. In our designed scheme, first of all, the requester selects two blind factors (τ, φ), then performs calculations to find out the value of hash, using $r = \hbar_1(m, \Delta_1, \Delta_2, \sigma_r)$, and $\mathscr{Z}$, using $\mathscr{Z} = r + \varphi$. Further, the requester sends $\mathscr{Z}$ to the blind signer. In case the signer wants to see the plain text, it is mandatory for him/her to recover m from r, where $r = \hbar_1(m, \Delta_1, \Delta_2, \sigma_r)$. This, however, is not feasible because of the one-way nature of the hash function. After this, the signer also needs the blind factor φ, which is only known to the requester. Thus, the aforementioned discussion clearly justifies that the scheme, decently, fulfills the security property of unlinkability. □

6.1.4. Theorem 1 ←Replay Attack

In the proposed scheme, the adversary may not give responses to old messages.

Proof. The scheme is resilient against replay attack by offering renewal of nonce Ns. In case an attacker intrudes the message of one session, he/she may not intrude the messages of other sessions with the same Ns because the Ns is renewed at every instance. The receiver is required to perform an up-to-date check with every message and, in the case of an outdatedness being detected in the message, that particular message is trashed into the black box. □

6.2. Formal Security Analysis Using Analysis

In this subsection, results produced from the simulation work using AVISPA tool are presented [56]. This is done, primarily, to ascertain the potency of the proposed scheme against replay and man-in-the-middle attacks. AVISPA is a push-button tool for providing an expressive and modular formal language to simulate protocols and their security properties. SPAN (specific protocol animator for AVISPA) [57], the protocol of security animator for AVISPA, is designed to assist protocol developers write high level protocol specification language (HLPSL) specifications [58]. The HLPSL specifications are interpreted into an intermediate format (IF) by the HLPSLIF translator. Then, it is transformed to the output format (OF) with either on-the-fly model-checker (OFMC) [59], CL-based attack searcher (AtSe) [60], SAT-based model-checker (SATMC), or tree automata-based protocol analyzer (TA4SP). These embedded tools examine the security claims of the aforementioned IF code of an algorithm for two types of attack—replay and man-in-the-middle attacks. The IF code works under two validation states: SAFE, if the cryptographic scheme can safeguard the man-in-the-middle attack, and UNSAFE, in cases where the IF code does not provide protection against man-in-the-middle attack. Formal security verification using the AVISPA tool can be found in several studies to determine the security of many authentication protocols against replay along with man-in-the-middle attacks [61–66]. The basic structure of the AVISPA tool is revealed in Figure 5.

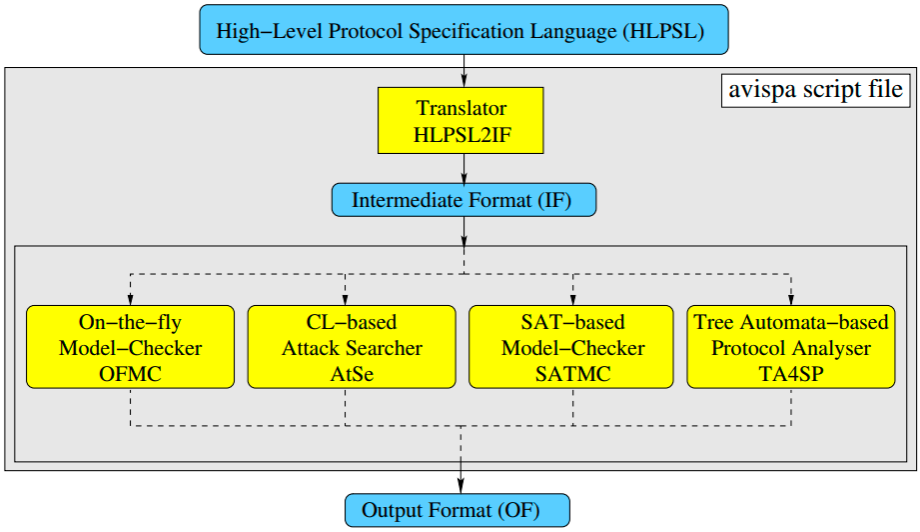

Figure 5. Architecture of the automated validation of internet security protocols and applications (AVISPA) tool v.1.1 [67].

7. Performance Comparison

This section compares the performance of the proposed scheme with the existing counterparts suggested by Lei et al. [4], Islam et al. [47], Nayak et al. [48], and Chen et al. [49].

7.1. Computational Cost

In Table 2, the proposed scheme is compared, in terms of computational cost, with the existing ones, that is, Lei et al.'s scheme [4], Islam et al.'s scheme [47], Nayak et al.'s scheme [48], and Chen et al.'s scheme [49], hereinafter also referred to as the "four chosen schemes", on the basis of major operations. We considered hyperelliptic divisor multiplication as elliptic curve scalar multiplication, and bilinear pairings are the most expensive operations used in the relevant existing schemes. The variables $\hbar m$, em, bp, and mxp denote the hyperelliptic curve divisor multiplication, elliptic curve scalar multiplication, bilinear pairing, and modular exponential, respectively. It has been observed that a single scalar multiplication takes 0.97 ms for elliptic curve point multiplication (ECPM), 14.90 ms for bilinear pairing, and 1.25 ms for modular exponential [15]. The Multi-Precision Integer and Rational Arithmetic C Library (MIRACL) [68] was used to test the runtime of the basic cryptographic operations up to 1000 times to measure the performance of the proposed approach. The phenomenon was observed on a workstation having following specifications: Intel Core i7- 4510U CPU @ 2.0 GHz, 8 GB RAM and Windows 7 Home Basic 64-bit Operating System [19]. Similarly, the hyperelliptic curve divisor multiplication (HCDM) was assumed to be 0.48 ms due to the smaller key size—80 bit key size [69].

Table 2. Computational cost.

Schemes	Signing	Verifying	Total
Lei et al.'s scheme [4]	16 em	5 em	21 em
Islam et al.'s scheme [47]	7 em	1 bp + 4 em	11 em + 1 bp
Nayak et al.'s scheme [48]	5 em	2 em	7 em
Chen et al.'s scheme [49]	2 em + 3 mxp	1 em + 1 bp + 1 mxp	3 em + 1 bp + 4 mxp
Proposed	1 $\hbar m$	0 $\hbar m$	1 $\hbar m$

The computational costs provided in Table 3 and illustrated in Figure 6 clearly show that our proposed scheme, when compared with the "four chosen schemes" outperforms in terms of computational cost. The presented scheme is quicker than the existing ones by the following degrees:

Lei et al. [4] by 97.64% (20.37 − 0.48/20.37 × 100 = 97.64%); Islam et al.'s scheme [47] by 98.12% (25.57 − 0.48/25.57 × 100 = 98.12%); Nayak et al.'s scheme [48] by 92.93% (6.79 − 0.48/6.79 × 100 = 92.93%); and Chen et al.'s scheme [49] by 97.89% (22.81 − 0.48/22.81 × 100 = 97.89%).

Table 3. Computational cost in milliseconds.

Schemes	Signing	Verifying	Total
Lei et al.'s scheme [4]	15.52 ms	4.85 ms	20.37 ms
Islam et al.'s scheme [47]	6.79 ms	18.78 ms	25.57 ms
Nayak et al.'s scheme [48]	4.85 ms	1.94 ms	6.79 ms
Chen et al.'s scheme [49]	5.69 ms	17.12 ms	22.81 ms
Proposed	0.48 ms	0 ms	0.48 ms

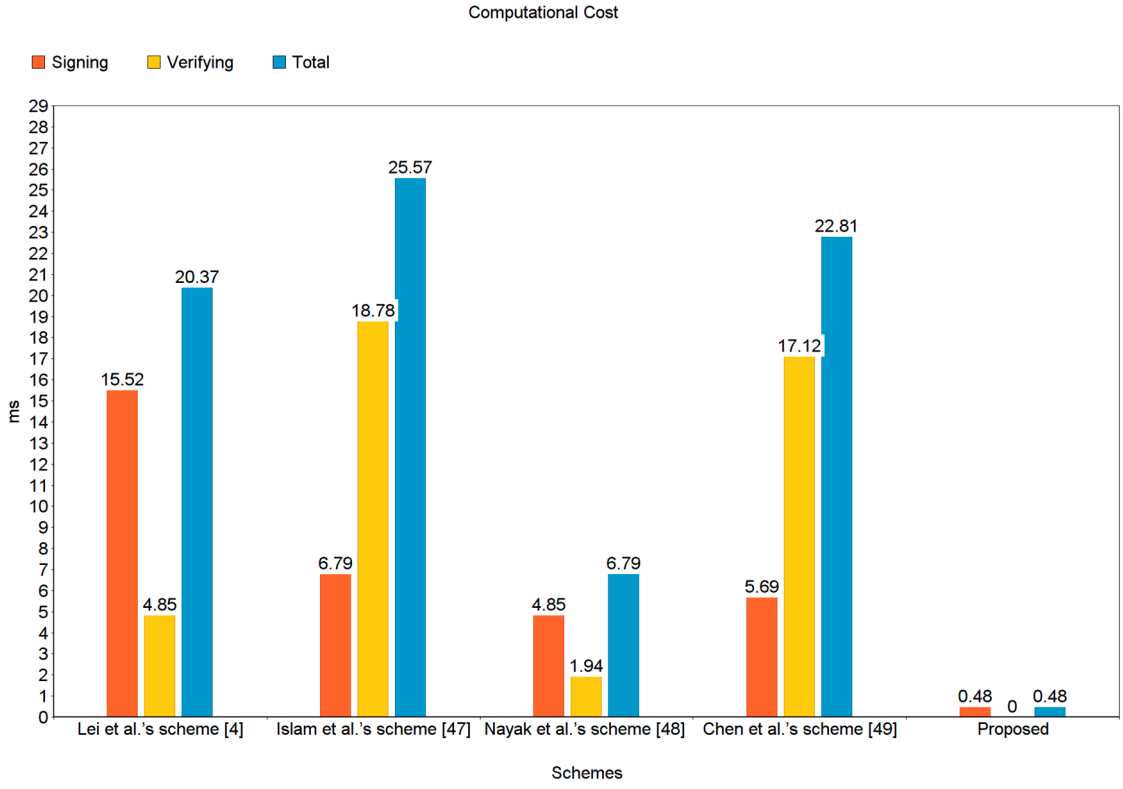

Figure 6. Computational cost (in ms).

7.2. Communication Cost

In this subsection, the proposed scheme is compared, in terms of communication cost, with the existing ones, these being Lei et al.'s scheme [4], Islam et al.'s scheme [47], Nayak et al.'s scheme [48], and Chen et al.'s scheme [49]. For the comparison, we supposed that, $|\mathbb{G}| = 1024$ bits, $|\mathcal{Z}_q| = 160$ bits, $|\mathcal{Z}_n| = 80$ bits, $|\mathrm{H}| = 512$ bits, $|m| = 1024$ bits, and $|\mathcal{W}| = 1024$ bits [70]. According to our suppositions, the communication cost for Lei et al.'s scheme [4] is $4|\mathcal{Z}_q| + 2|\mathcal{W}| + |\mathrm{H}| + |m|$, for Islam et al.'s scheme [47] is $2|\mathbb{G}| + |m|$, for Nayak et al.'s scheme [48] is $2|\mathcal{Z}_q| + |m|$, for Chen et al.'s scheme [49] is $|\mathbb{G}| + |\mathrm{H}| + |m|$, and for our proposed scheme is $|\mathcal{Z}_n| + |\mathrm{H}| + |m|$.

The reduction in communication cost of our proposed CL-BS scheme compared with the existing ones as provided in Figure 7 is shown by following degrees: from Lei et al.'s scheme [4] at $(4|\mathcal{Z}_q| + 2|\mathcal{W}| + |\mathrm{H}| + |m|) - (|\mathcal{Z}_n| + |\mathrm{H}| + |m|)/(4|\mathcal{Z}_q| + 2|\mathcal{W}| + |\mathrm{H}| + |m|) = (4224 - 1616/4224 \times 100 = 61.74\%)$; from Islam et al.'s scheme [47] at $(2|\mathbb{G}| + |m|) - (|\mathcal{Z}_n| + |\mathrm{H}| + |m|)/(2|\mathbb{G}| + |m|) = (3072 - 1616/3072 \times 100 = 47.39\%)$; from Nayak et al.'s scheme [48] at $(2|\mathcal{Z}_q| + |\mathrm{H}| + |m|) - (|\mathcal{Z}_n| + |\mathrm{H}| +$

$|m|)/(2|\mathcal{Z}_q| + |\mathrm{H}| + |m|) = (1856 - 1616/1856 \times 100 = 14.8\%)$; and from Chen et al.'s scheme [49] at $(|\mathcal{S}| + |\mathrm{H}| + |m|) - (|\mathcal{Z}_n| + |\mathrm{H}| + |m|)/(|\mathcal{S}| + |\mathrm{H}| + |m|) = (2560 - 1616/2560 \times 100 = 36.78\%)$.

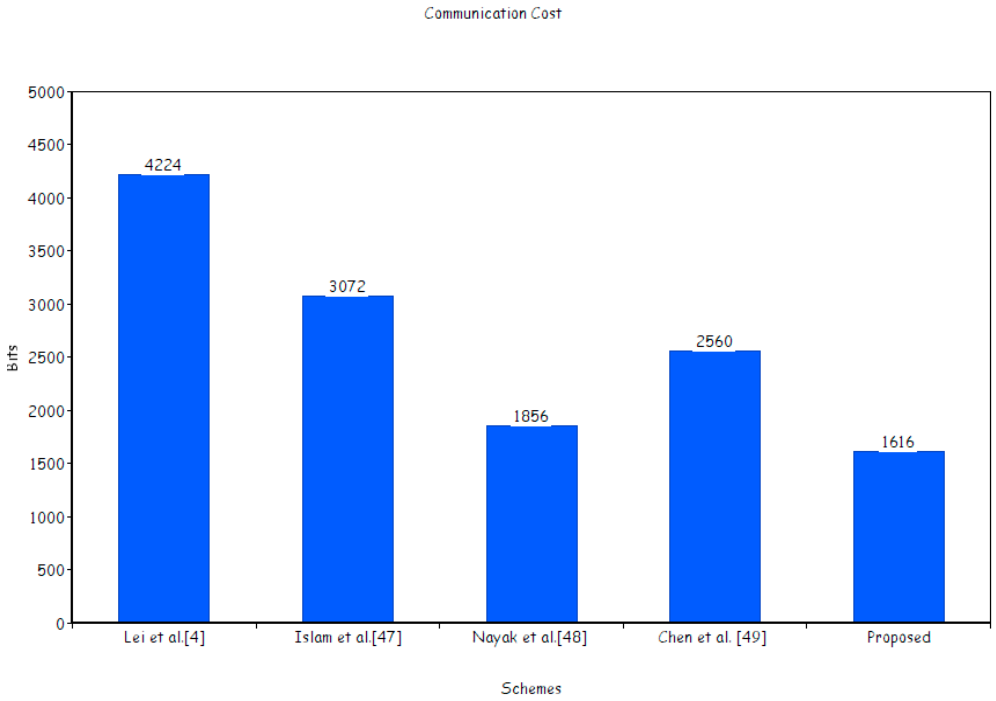

Figure 7. Communication cost (in bits).

7.3. Security Funtionalities

Table 4 presents a brief comparison between the proposed scheme and relevant existing schemes in terms of security functionality. It is worth noting, from Table 4, that the related schemes are not validated through formal security validation tools, such as AVISPA, and none of them guarantee replay attack (RA) and integrity (I). Our proposed scheme is shown to be resistant against various attacks through formal analysis using the widely-accepted automated validation for internet security validation and application (AVISPA) tool as shown in Appendix A.

Table 4. Comparison with relevant existing schemes. Legend: U: unforgeability, I: integrity, UL: unlinkability, RA: replay attack, FA: formal analysis; symbols: ✓: satisfies the security functionality, X: does not satisfy the security functionality.

Schemes	Security Functionalities				
	Informal				Formal
	U	I	UL	RA	FA
Lei et al.'s scheme [4]	✓	X	X	X	X
Islam et al.'s scheme [47]	✓	X	✓	X	X
Nayak et al.'s scheme [48]	✓	X	X	X	X
Chen et al.'s scheme [49]	✓	X	X	X	X
Proposed	✓	✓	✓	✓	✓

8. Conclusions

In this article, we proposed an efficient and provably secure certificateless signature scheme, CL-BS, based on multi-access edge computing (MEC) for a FANET environment using the concept of hyperelliptic curve. The proposed scheme was shown to be resistant against various attacks through informal security analysis, as well as through the formal security verification using

the widely-accepted AVISPA tool. The scheme was also efficient in terms of computational and communication costs. On doing a comparative analysis with existing counterparts, it was noticed that the proposed scheme was characterized by least computational and communication costs, these being 0.48 ms and 1616 bits, respectively, which authenticates the superiority of our scheme.

In future, we intend to integrate a computational offloading and scheduling mechanism, where M-UAVs will offload and schedule the computing tasks in the RMEC-UAV for fast processing and execution.

Author Contributions: Conceptualization, M.A.K. and I.M.Q.; methodology and implementation, M.A.K., I.M.Q., I.U., and F.N.; simulation, M.A.K. and I.U.; validation, M.A.K., I.M.Q., I.U., and S.K.; data curation, M.A.K., S.K., and F.K.; writing—original draft preparation, M.A.K., F.K., and F.N.; writing—review and editing, M.A.K., F.N., and F.K.; supervision, I.M.Q. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A. Implementation of Our Proposed CL-BS Scheme in AVISPA

The proposed scheme has been implemented for blind signer and verifier in HLPSL, as illustrated in Algorithms A1 and A2. The experiment was performed on a computer workstation having the specifications as follows: Haier Win8.1 PC; Intel Core i3-4010U CPU @ 1.70 GHz; 64-bit operating system and ×64-based processor. The software platforms consulted were Oracle VM Virtual Box (version: 5.2.0.118431) and SPAN (version: SPAN-Ubuntu-10.10-light_1). As with any security protocol, to be analyzed in AVISPA, the roles for session, goal, and environment were executed as shown in Algorithms A3 and A4. In order to gauge the probability of attacks on the proposed scheme, the widely-used OFMC and CL-AtSe backends were selected for the execution test. Because other backends such as SATMC and TA4SP are not compatible with bitwise XOR operations, the simulation results of SATMC and TA4SP were not included in the research work. Here, it is imperative to ascertain the execution of specified protocol in terms of whether the authentic agents can execute the specified protocol or not. To do so, the back-ends perform check operations. Then, the information is provided to the intruder about a few normal sessions between authentic agents. Secondly, the susceptibility of the system to man-in-the-middle attack is also estimated by the back-ends. This is done to verify the Dolev–Yao (DY) model [54]. The scheme is also simulated under SPAN (specific protocol animator for AVISPA) web-tool. The results for OFMC and AtSe are shown in Figures A1 and A2, respectively. It is evident that the scheme is safe against replay and man-in-the-middle attack.

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

```
role
  role_Blindsigner(Blindsigner:agent,Verifier:agent,Xs:public_key,Xv:public_key,SND,RCV:channel(dy))
played_by Blindsigner
def=
        local
              State:nat,Ns:text,Sub:hash_func,Z:text,T:text
       init
              State: = 0
        transition
              1. State=0 /\ RCV (start) =|> State': =1 /\
SND (Blindsigner.Verifier)
              2. State=1 /\ RCV (Verifier. {Ns'} _Xv) =|> State': =2 /\ T':=new() /\ Z':=new() /\
SND(Blindsigner.{Sub(Z'.T')}_inv(Xs))
end role
```

Algorithm A2 High-level protocol specification language (HLPSL) code for Verifier role

```
role
role_Verifier(Blindsigner:agent,Verifier:agent,Xs:public_key,Xv:public_key,SND,RCV:channel(dy))
played_by Verifier
def=
        local
                State:nat,Ns:text,Sub:hash_func,Z:text,T:text
         init
                State: = 0
        transition
                1. State=0 /\ RCV(Blindsigner.Verifier) =|> State':=1 /\ Ns':=new() /\ SND(Verifier.{Ns'}_Xv)
                2. State=1 /\ RCV (Blindsigner. {Sub (Z'. T')} _inv (Xs)) =|> State': =2
end role
```

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

```
role
   session1(Blindsigner:agent,Verifier:agent,Xs:public_key,Xv:public_key)
def=
        local
                SND2,RCV2,SND1,RCV1:channel(dy)
        composition
                role_Verifier(Blindsigner,Verifier,Xs,Xv,SND2,RCV2) /\
role_Blindsigner(Blindsigner,Verifier,Xs,Xv,SND1,RCV1)
end role

role
session2(Blindsigner:agent,Verifier:agent,Xs:public_key,Xv:public_key)
def=
        local
                SND1,RCV1:channel(dy)
        composition
                role_Blindsigner(Blindsigner,Verifier,Xs,Xv,SND1,RCV1)
end role
```

Algorithm A4 High-level protocol specification language (HLPSL) code for Environment role

```
role
   environment()
def=
         const

        hash_0:hash_func,xs:public_key,alice:agent,bob:agent,xv:public_key,const_1:agent,const_2:public_key,
const_3:public_key,auth_1:protocol_id,sec_2:protocol_id
         intruder_knowledge = {alice,bob}
        composition
                session2(i, const_1, const_2, const_3) /\ session1(alice,bob,xs,xv)
end role

goal
                 authentication_on auth_1
                secrecy_of sec_2
end goal
```

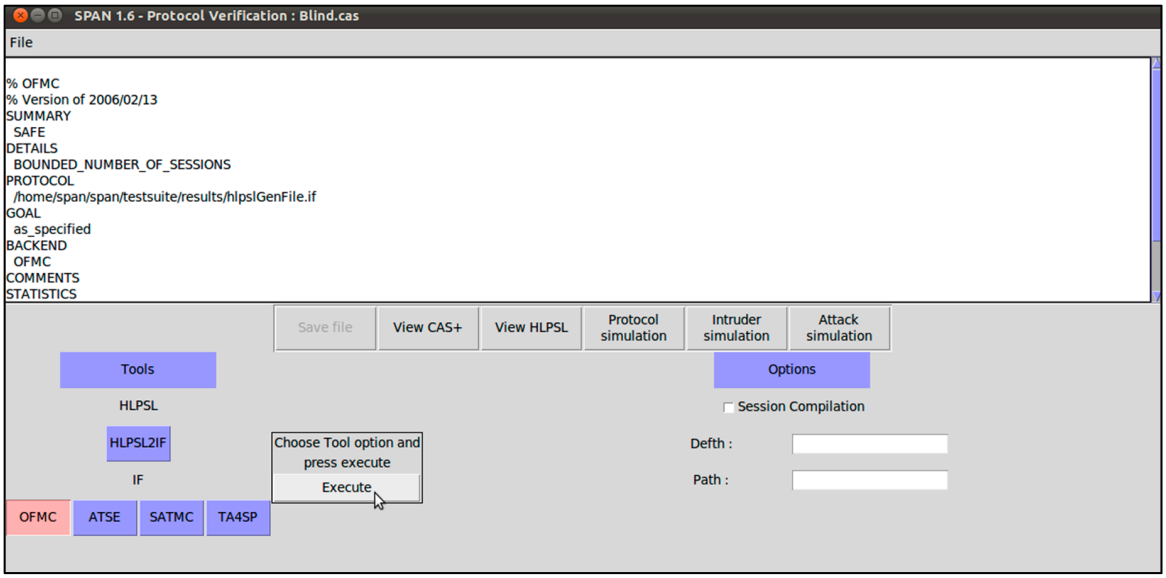

Figure A1. Simulation results for on-the-fly model-checker (OFMC).

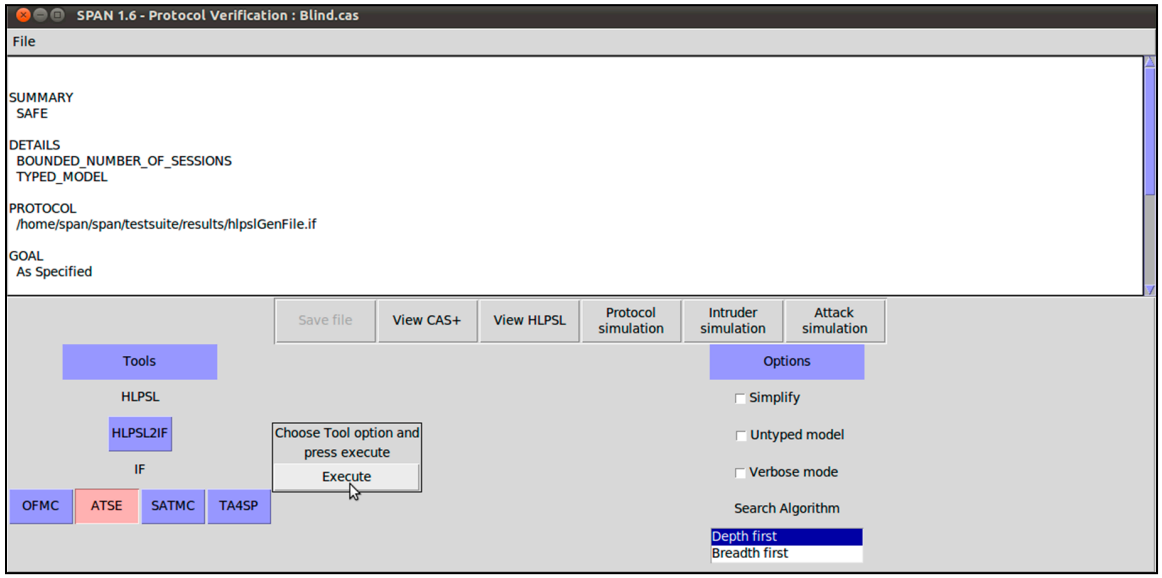

Figure A2. Simulation results for AtSe.

References

1. Khan, M.A.; Qureshi, I.M.; Khanzada, F.A. Hybrid Communication Scheme for Efficient and Low-Cost Deployment of Future Flying Ad-Hoc Network (FANET). *Drones* **2019**, *3*, 16. [CrossRef]
2. Bekmezci, I.; Sahingoz, O.K.; Temel, Ş. Flying ad-hoc Network (FANET): A survey. *Ad Hoc Netw.* **2013**, *11*, 1254–1270. [CrossRef]
3. Khan, M.A.; Safi, A.; Qureshi, I.M.; Khan, I.U. Flying ad-hoc Network (FANET): A review of communication architectures, and routing protocols. In Proceedings of the 2017 First International Conference on Latest trends in Electrical Engineering and Computing Technologies (INTELLECT), Karachi, Pakistan, 15–16 November 2017; pp. 1–9.
4. He, L.; Ma, J.; Mo, R.; Wei, D. Designated Verifier Proxy Blind Signature Scheme for Unmanned Aerial Vehicle Network Based on Multi-access Edge Computing (MEC). *Secur. Commun. Netw.* **2019**, *2019*, 8583130. [CrossRef]

5. Khan, M.A.; Qureshi, I.M.; Khan, I.U.; Nasim, M.A.; Javed, U.; Khan, M.W. On the performance of flying ad-hoc Network (FANET) with directional antennas. In Proceedings of the 2018 5th International Multi-Topic ICT conference (IMTIC), Jamshoro, Pakistan, 25–27 April 2018; pp. 1–8.
6. Khan, M.A.; Khan, I.U.; Safi, A.; Quershi, I.M. Dynamic Routing in Flying Ad-Hoc Networks Using Topology-Based Routing Protocols. *Drones* **2018**, *2*, 27. [CrossRef]
7. Suárez-Albela, M.; Fraga-Lamas, P.; Fernández-Caramés, T.M. A Practical Evaluation on RSA and ECC-Based Cipher Suites for IoT High-Security Energy-Efficient Fog and Mist Computing Devices. *Sensors* **2018**, *18*, 3868. [CrossRef]
8. Yu, M.; Zhang, J.; Wang, J.; Gao, J.; Xu, T.; Deng, R.; Zhang, Y.; Yu, R. Internet of Things security and privacy-preserving method through nodes differentiation, concrete cluster centers, multi-signature, and blockchain. *Int. J. Distrib. Sens. Netw.* **2018**, *14*, 12. [CrossRef]
9. Braeken, A. PUF Based Authentication Protocol for IoT. *Symmetry* **2018**, *10*, 8. [CrossRef]
10. Zhou, C.; Zhao, Z.; Zhou, W.; Mei, Y. Certificateless Key-Insulated Generalized Signcryption Scheme without Bilinear Pairings. *Secur. Commun. Netw.* **2017**, *2017*, 8405879. [CrossRef]
11. Kumari, S.; Karuppiah, M.; Das, A.K.; Li, X.; Wu, F.; Kumar, N. A secure authentication scheme based on elliptic curve cryptography for IoT and cloud servers. *J. Supercomput.* **2017**, *74*, 12. [CrossRef]
12. Omala, A.; Mbandu, A.; Mutiria, K.; Jin, C.; Li, F. Provably Secure Heterogeneous Access Control Scheme for Wireless Body Area Network. *J. Med. Syst.* **2018**, *42*, 6. [CrossRef]
13. Tamizhselvan, C.; Vijayalakshmi, V. An Energy Efficient Secure Distributed Naming Service for IoT. *Int. J. Adv. Stud. Sci. Res.* **2019**, *3*, 8.
14. Naresh, V.S.; Sivaranjani, R.; Murthy, N.V.E.S. Provable secure lightweight hyper elliptic curve-based communication system for wireless sensor Network. *Int. J. Commun. Syst.* **2018**, *31*, 15. [CrossRef]
15. Rahman, A.; Ullah, I.; Naeem, M.; Anwar, R.; Khattak, H.S.; Ullah, A. Lightweight Multi-Message and Multi-Receiver Heterogeneous Hybrid Signcryption Scheme based on Hyper Elliptic Curve. *Int. J. Adv. Comput. Sci. Appl.* **2018**, *9*, 5. [CrossRef]
16. Won, J.; Seo, S.H.; Bertino, E. Certificateless Cryptographic Protocols for Efficient Drone-Based Smart City Applications. *IEEE Access* **2017**, *5*, 3721–3749. [CrossRef]
17. Barka, E.; Kerrache, C.; Hussain, R.; Lagraa, N.; Lakas, A.; Bouk, S. A Trusted Lightweight Communication Strategy for Flying Named Data Networking. *Sensors* **2018**, *18*, 2683. [CrossRef]
18. Bae, M.; Kim, H. Authentication and Delegation for Operating a Multi-Drone System. *Sensors* **2019**, *19*, 2066. [CrossRef]
19. Seo, S.-H.; Won, J.; Bertino, E. pCLSC-TKEM: A pairing-free certicateless signcryption-tag key encapsulation mechanism for a privacy-preserving IoT. *Trans. Data Priv.* **2016**, *9*, 101–130.
20. Liu, W.; Strangio, M.A.; Wang, S. Efficient Certificateless Signcryption Tag-KEMs for Resource constrained Devices. *arXiv* **2015**, *1510*, 01446.
21. Reddy, P.V.; Babu, A.R.; Gayathri, N.B. Efficient and Secure Identity-based Strong Key Insulated Signature Scheme without Pairings. *J. King Saud Univ. Comput. Inf. Sci.* **2018**.
22. Xiong, H.; Mei, Q.; Zhao, Y. Efficient and provably secure certificateless parallel key-insulated signature without pairing for IIoT environments. *IEEE Syst. J.* **2019**, 1–11. [CrossRef]
23. Bekkouche, O.; Taleb, T.; Bagaa, M. UAVs Traffic Control based on Multi-Access Edge Computing. In Proceedings of the 2018 IEEE Global Communications Conference (GLOBECOM 2018), Abu Dhabi, UAE, 9–13 December 2018.
24. Ouahouah, S.; Taleb, T.; Song, J.; Benzaid, C. Efficient offloading mechanism for UAVs-based value-added services. In Proceedings of the 2017 IEEE International Conference on Communications (ICC), Paris, France, 21–25 May 2017; pp. 1–6.
25. Motlagh, N.H.; Bagaa, M.; Taleb, T. Uav-based iot platform: A crowd surveillance use case. *IEEE Commun. Mag.* **2017**, *55*, 128–134. [CrossRef]
26. ETSI. Multi-Access Edge Computing (MEC). In *Framework and Reference Architecture*; DGS MEC; ETSI: Sophia Antipolis, France, 2016; Volume 3.
27. Garg, S.; Singh, A.; Batra, S.; Kumar, N.; Yang, L.T. UAV empowered edge computing environment for cyber-threat detection in smart vehicles. *IEEE Netw.* **2018**, *32*, 42–51. [CrossRef]
28. Lee, J.; Lee, J. Hierarchical Multi-access Edge Computing (MEC) architecture based on context awareness. *Appl. Sci.* **2018**, *8*, 1160. [CrossRef]

29. Intharawijitr, K.; Iida, K.; Koga, H. Simulation study of low latency network architecture using Multi-access Edge Computing (MEC). *IEICE Trans. Inf. Syst.* **2017**, *E100D*, 963–972. [CrossRef]
30. Messous, M.-A.; Sedjelmaci, H.; Houari, N.; Senouci, S.-M. Computation offloading game for an UAV network in Multi-access Edge Computing (MEC). In Proceedings of the 2017 IEEE International Conference on Communications, ICC 2017, Paris, France, 21–25 May 2017; pp. 1–6.
31. Ansari, N.; Sun, X. Multi-access Edge Computing (MEC) empowers internet of things. *IEICE Trans. Commun.* **2018**, *E101B*, 604–619. [CrossRef]
32. Zhang, K.; Leng, S.; He, Y.; Maharjan, S.; Zhang, Y. Multi-access Edge Computing (MEC) and networking for green and low-latency internet of things. *IEEE Commun. Mag.* **2018**, *56*, 39–45. [CrossRef]
33. Grasso, C.; Schembra, G. A Fleet of MEC UAVs to Extend a 5G Network Slice for Video Monitoring with Low-Latency Constraints. *J. Sens. Actuator Netw.* **2019**, *8*, 3. [CrossRef]
34. Chaum, D. Blind signatures for untraceable payments. *Adv. Cryptol.* **1983**, 199–203.
35. Mambo, M.; Usuda, K.; Okamoto, E. Proxy signatures for delegating signing operation. In Proceedings of the 3rd ACM Conference on Computer and Communications Security, New Delhi, India, 14–15 March 1996; pp. 48–56.
36. Tan, Z.; Liu, Z.; Tang, C. Digital proxy blind signature schemes based on DLP and ECDLP. *MM Res. Prepr.* **2002**, *21*, 212–217.
37. Tan, Z. Efficient pairing-free provably secure identity-based proxy blind signature scheme. *Secur. Commun. Netw.* **2013**, *6*, 593–601. [CrossRef]
38. Yang, F.-Y.; Liang, L.-R. A proxy partially blind signature scheme with proxy revocation. *J. Ambient Intell. Humaniz. Comput.* **2013**, *4*, 255–263. [CrossRef]
39. Verma, G.K.; Singh, B.B. Efficient message recovery proxy blind signature scheme from pairings. *Trans. Emerg. Telecommun. Technol.* **2017**, *28*, e3167. [CrossRef]
40. Zhu, H.; Tan, Y.-A.; Zhu, L.; Zhang, Q.; Li, Y. An efficient identity-based proxy blind signature for semi offline services. *Wirel. Commun. Mob. Comput.* **2018**, *2018*, 5401890. [CrossRef]
41. Jakobsson, M.; Sako, K.; Impagliazzo, R. Designated verifier proofs and their applications. In Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques, Berlin, Heidelberg, 13 July 2001; pp. 143–154.
42. Dai, J.Z.; Yang, X.H.; Dong, J.X. Designated-receiver proxy signature scheme for electronic commerce. In Proceedings of the IEEE International Conference on Systems, Man and Cybernetics, Washington, DC, USA, 10 November 2003; pp. 384–389.
43. Huang, X.; Mu, Y.; Susilo, W.; Zhang, F. Short designated verifier proxy signature from pairings. In Proceedings of the International Conference on Embedded and Ubiquitous Computing, Nagasaki, Japan, 6–9 December 2005; pp. 835–844.
44. Shim, K.-A. Short designated verifier proxy signatures. *Comput. Electr. Eng.* **2011**, *37*, 180–186. [CrossRef]
45. Islam, S.H.; Biswas, G. A provably secure identity-based strong designated verifier proxy signature scheme from bilinear pairings. *J. King Saud Univ. Comput. Inf. Sci.* **2014**, *26*, 55–67. [CrossRef]
46. Hu, X.; Tan, W.; Xu, H.; Wang, J. Short and provably secure designated verifier proxy signature scheme. *IET Inf. Secur.* **2016**, *10*, 69–79. [CrossRef]
47. Islam, S.; Obaidat, M.S. Design of provably secure and efficient certificateless blind signature scheme using bilinear pairing. *Secur. Commun. Netw.* **2015**, *8*, 4319–4332. [CrossRef]
48. Nayak, S.K.; Mohanty, S.; Majhi, B. CLB-ECC: Certificateless Blind Signature Using ECC. *JIPS* **2017**, *13*, 970–986.
49. Chen, H.; Zhang, L.; Xie, J.; Wang, C. New Efficient Certificateless Blind Signature Scheme. In Proceedings of the 2016 IEEE Trustcom/BigDataSE/ISPA, Tianjin, China, 23–26 August 2016; pp. 349–353.
50. Koblitz, N. Elliptic curve cryptosystems. *Math. Comput.* **1987**, *48*, 203–209. [CrossRef]
51. Hyperelliptic Curve. 2019. Available online: https://en.wikipedia.org/wiki/Hyperelliptic_curve (accessed on 25 October 2019).
52. Pelzl, J.; Wollinger, T.; Guajardo, J.; Paar, C. Hyperelliptic curve cryptosystems: Closing the performance gap to elliptic curves. In *International Workshop on Cryptographic Hardware and Embedded Systems*; Springer: Berlin, Heidelberg, 2003; pp. 351–365.
53. Cantor, D.G. Computing in Jacobian of a Hyperelliptic Curve. *Math. Comput.* **1987**, *48*, 95–101. [CrossRef]

54. Dolev, D.; Yao, A. On the security of public key protocols. *IEEE Trans. Inf. Theory* **1983**, *29*, 198–208. [CrossRef]
55. Siddiqi, M.A.; Yu, H.; Joung, J. 5G Ultra-Reliable Low-Latency Communication Implementation Challenges and Operational Issues with IoT Devices. *Electronics* **2019**, *8*, 981. [CrossRef]
56. AVISPA. Automated Validation of Internet Security Protocols and Applications. 2019. Available online: http://www.avispa-project.org/ (accessed on 25 October 2019).
57. AVISPA. SPAN: A Security Protocol Animator for AVISPA. 2019. Available online: http://www.avispa-project.org/ (accessed on 25 October 2019).
58. Oheimb, D.V. The high-level protocol specification language HLPSL developed in the EU project avispa. In Proceedings of the APPSEM 2005 Workshop, Tallinn, Finland, 13–15 September 2005; pp. 1–2.
59. Basin, D.; Modersheim, S.; Vigano, L. OFMC: A symbolic model checker for security protocols. *Int. J. Inf. Secur.* **2005**, *4*, 181–208. [CrossRef]
60. Turuani, M. The CL-Atse porotocol analyser. In Proceedings of the International Coneference on Rewriting Techniques and Applications (RTA), Seattle, WA, USA, 12–14 August 2006; pp. 227–286.
61. Yu, S.; Lee, J.; Lee, K.; Park, K.; Park, Y. Secure Authentication Protocol for Wireless Sensor Network in Vehicular Communications. *Sensors* **2018**, *18*, 3191. [CrossRef]
62. Park, K.; Park, Y.; Park, Y.; Reddy, A.G.; Das, A.K. Provably secure and efficient authentication protocol for roaming service in global mobility Network. *IEEE Access* **2017**, *5*, 25110–25125. [CrossRef]
63. Odelu, V.; Das, A.K.; Choo, K.R.; Kumar, N.; Park, Y.H. Efficient and secure time-key based single sign-on authentication for mobile devices. *IEEE Access* **2017**, *5*, 27707–27721. [CrossRef]
64. Odelu, V.; Das, A.K.; Kumari, S.; Huang, X.; Wazid, M. Provably secure authenticated key agreement scheme for distributed mobile cloud computing services. *Futuer Generat. Comput. Syst.* **2017**, *68*, 74–88. [CrossRef]
65. Park, K.; Park, Y.; Park, Y.; Das, A.K. 2PAKEP: Provably Secure and Efficient Two-Party Authenticated Key Exchange Protocol for Mobile Environment. *IEEE Access* **2018**, *6*, 30225–30241. [CrossRef]
66. Banerjee, S.; Odelu, V.; Das, A.K.; Chattopadhyay, S.; Kumar, N.; Park, Y.H.; Tanwar, S. Design of an Anonymity-Preserving Group Formation Based Authentication Protocol in Global Mobility Network. *IEEE Access* **2018**, *6*, 20673–20693. [CrossRef]
67. AVISPA v1.1 User Manual. 2019. Available online: http://www.avispa-project.org/package/user-manual.pdf (accessed on 25 October 2019).
68. Shamus Sofware Ltd. Miracl library. Available online: http://github.com/miracl/MIRACL (accessed on 25 October 2019).
69. Ullah, I.; Amin, N.U.; Naeem, M.; Khattak, S.; Khattak, S.J.; Ali, H. A Novel Provable Secured Signcryption Scheme PSSS: A Hyper-Elliptic Curve-Based Approach. *Mathematics* **2019**, *7*, 686. [CrossRef]
70. Ullah, I.; Alomari, A.; Ul Amin, N.; Khan, M.A.; Khattak, H. An Energy Efficient and Formally Secured Certificate-Based Signcryption for Wireless Body Area Network with the Internet of Things. *Electronics* **2019**, *8*, 1171. [CrossRef]

© 2019 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (http://creativecommons.org/licenses/by/4.0/).