Cyber Security and Applications 1 (2023) 100012

Contents lists available at ScienceDirect

Cyber Security and Applications

journal homepage: http://www.keaipublishing.com/en/journals/cyber-security-and-applications/

Secure session key pairing and a lightweight key authentication scheme for liable drone services

Rajkumar .S.C[a,*], Jegatha Deborah .L[b], Vijayakumar .P[b], Karthick .KR[a]

[a] Department of Computer Science and Engineering, Anna University Regional Campus Madurai, keelakuilkudi Rd, Madurai, Tamil Nadu, India-625019
[b] Department of Computer Science and Engineering, University College of Engineering Tindivanam, Melpakkam, Tindivanam, Tamil Nadu, India-604001

ARTICLE INFO

Keywords:
Authentication
Session key
Drone
IoT
Communication
Secret key

ABSTRACT

Recent advancements in drone technology have created new application opportunities, particularly for small drones. However, these advancements raise concerns about security, adaptability, and consistency. Data security is jeopardized by flying intelligent devices. The distributed nature of drones, their accessibility, mobility, adaptability, and autonomy will all have an effect on how security vulnerabilities and threats are identified and controlled. However, attackers and cybercriminals have begun to employ drones for malevolent reasons in recent years. These attacks are frequent and can be fatal. There is also the matter of prevention to consider. The communication entities of the drone network can communicate securely via authentication procedures. Such solutions, however, must strike a balance between security and portability. However, the proposed technique is implemented to improve security to avoid attacks and provides a secure, lightweight, and proven solution to a key agreement for drone communication. A novel certificate-less Drone integration approach that depends on trusted authorities centres to help communication entities establish their key pairs while keeping those same trusted authorities centers from knowing about them has been devised. The proposed scheme results achieved higher security of 94 percent than existing schemes.

1. Introduction

Drones, also known as Autonomous Unmanned Vehicles (AUVs) or Aerial Surveillance Systems (ASS), which serve as sensing technologies, can now be connected to floor sensor nodes via the IoT technology to create a new cluster known as the internet of drones, which is a subset of the Internet of Drones (IoD). Disaster response actions, transportation surveillance, workplace inspection, predictive maintenance, guidance systems, farming, distribution network modeling, and contingency planning are all examples of where drones are used [1]. In the next generation of advanced smart cities, the Internet of Things is projected to play a critical role [4]. Today's advanced public services can handle both natural and manmade complicated processes by employing the Drone paradigm [5]. However, the drones share sensitive information through a channel that can't be trusted (primarily wireless networks and Wi-Fi), and it is possible that a lot of hostile attacks will be target them.

As a result of these developments, privacy and security may be jeopardized. Malicious hackers can gain remote access to the systems that control the drones by exploiting open-source drone hijacking software. Because commercial drones were constructed without such features, there have been no security or authentication difficulties. Drones with limited resources, which are essential components of a drone network, have limited capacity, computing capabilities, and standby time. A Drone network sends confidential, vital and moment data between participating organizations over an unsecured channel of communication. It is crucial to ensure the validity and reciprocal credibility of all involved parties when maintaining the confidentiality material. Due to the limited capabilities of drones, it is not possible to use sophisticated multifactor authentication such as fingerprints, bilinear map pairings, and digital certificates within the Drone network itself. This is because of the complexity of the computations.

Drone entities must be able to interact securely with each other using a form of authentication protocol that combines secure and compact attributes due to the inherent resource limits of drones. According to research on Drone deployment, there are a variety of authentication techniques that prioritize security above low-weight requirements or the other way around. If this tradeoff is not properly addressed, the security of the drone entity communication may be imperiled. It is also worth noting that, depending on the situation, drones in the Drone network can connect with other drones in flying zones, either within the same zone or elsewhere. A way for dynamically adding drones after the initial deployment should be included in Drone authentication procedures.

* Corresponding author.
E-mail address: rjkumar0814@gmail.com (Rajkumar .S.C.).

https://doi.org/10.1016/j.csa.2022.100012
Received 26 July 2022; Received in revised form 20 November 2022; Accepted 30 November 2022
Available online 15 December 2022

1.1. Inspiration

Innumerable IoT-based networks, such as the internet of drones, can benefit from a variety of Authentication and key agreement mechanisms (Drone). A proven authenticated key agreement is proposed to be capable of addressing the current situation has not yet been found to meet the protection and portable elements specified. Internet of drones (Drone) networks face issues to secure communications.

1.2. Our contribution

In place of certificate-based cryptography, the proposed technique employs elliptic curve cryptography for increased security. A novel certificate-less Drone integration approach that depends on trusted authorities centres to help communication entities establish their key pairs while keeping those same trusted authorities centers from knowing about them has been devised.

Objectives

1. To provide an effective authentication scheme for user registration
2. To establish a secure session key between user and drone for communication

2. Literature review

Effective and scalable Drone approaches are those that can be applied in many zones. Most proposed authentication solutions failed to take into account a crucial aspect of the Drone ecosystem. As the Internet of Things and the Internet of Devices grow in popularity, so does the need for secure, efficient authentication mechanisms for these new networks. Current efforts are underway to meet the security and weight requirements for IoT-based networks' authentication methods. Researchers have devised many AKA-based methods for keeping IoT networks safe from eavesdroppers. Simple hash functions and XOR operations were employed instead of complicated algorithms in the AKA systems explained in [7–10].

However, this cryptanalysis is ineffective because of the employment of Hash and XOR algorithms for their construction, which will be explained further in Section II. Another sort of AKA approach is based on bilinear map pairing (BMP). Elliptic curve cryptography (ECC) is used in this collection of algorithms, which increases security greatly. Even still, the BMP mechanism's high computational and communication costs result in undesirable lightweight features. BMP procedures are not recommended by the Drone network. Public key infrastructure (PKI) protocols are being used to construct certificate-based systems to address BMP method concerns. This helps to alleviate the issue of key management in public key (asymmetric) cryptography [2,11].

An alternative technique that does not involve the maintenance of public file directories and large certificate administration overheads is PKI-based. Because PKI-based approaches have some limitations, certificate less AKA solutions are being explored. With the help of an established authority center, key pairs of communicating entities are formed. Key-escrow attacks are conceivable in certificate-less schemes as long as the trusted authority is privy to their secret key. They can then pretend to be authorised drone communicators. This means that certificate fewer systems are vulnerable to key-escrow attacks. Methods [12–14] are among the most advanced certificate less-based, otherwise known as "state of the art," approaches when it comes to IoT-based networks and secure communication. According to [13], a replay attack was possible, and the computational and transmission overheads of [12] were significantly higher than those of comparable systems. Because of the BMP approach, [13,15] has high processing and transmission expenses. Partial key escrow, known CK adversary attack, and replay attack are all issues with the system in [14,29–35] because a first-message consistency is inadequate.

The method, on the other hand, requires a lot of processing.

To secure an IoT-based network like the Internet of Drones (Drone), a number of academics have developed novel cryptographic authentication mechanisms. Using a single secret session key in a vulnerable wireless network, such as the Internet of Things (IoT), communicative nodes can securely exchange data. Turkishovic et al. created the first AKA-based algorithm that guarantees key agreement between users and nodes without a gateway node [10]. For this method, only the XOR and hash functions were used. Node impersonation attacks can compromise the Turkanovic et al. approach, and nodes in the network will no longer be anonymous or traceable, according to Farash et al. [8]. Thus, Farash et al. proposed an updated solution to overcome Turkanovic et al. original scheme's security problems. A known-specific session temporary information attack, password offline guessing assault, and impersonation attack were identified by Amin et al. [9] in Farash et al. technique. Due to security weaknesses uncovered, a smart card-based solution was developed. Amin et al. systems were subject to both a lost smart card assault and an offline guessing attack, according to another study.

As a response to the stated security concerns, an authenticated technique was proposed based on Rabin cryptosystem computational capabilities. The Rabin cryptosystem, on the other hand, has a large computational cost, making it less practical [17]. Researchers in the field of the Internet of Things (IoT) have worked tirelessly to ensure the safety of IoT networks [38–46]. In the IoT-based smart grid network, Wu D. and Zhou [18] suggested an ECC-based fault-tolerance and scaling AKA approach. This approach makes use of public key infrastructure (PKI). Wu D. and Zhou C.'s technique is vulnerable to a man-in-the-middle attack, according to writers in [19].

PKI-based strategies, on the other hand, are expensive to maintain. Because of this, the authors came up with an upgraded version of AKA that includes a trusted anchor (TA) and a lightweight directory-access protocol (LDAP). After [19] 's approach had been decrypted, Park and colleagues [20] discovered that it is subject to impersonation attacks and does not guard against a transitory information assault that is specific to a given session. Smart grid communication authentication can now be accomplished with the AKA protocol, thanks to work by Mahmood et al. [21]. The strategy is less time-consuming than the other benchmarking strategies reviewed. Both authors, Abbasinezhad-Mood and Nikooghadam [12], have done research on cryptanalysis. This method is vulnerable to the session-specific temporary information attack, as well as the privacy leakage attack, and does not guarantee perfect forward secrecy for the entities. This led them to develop new Elliptic curve cryptography skills to solve the privacy concerns they uncovered [21].

It offers a framework that is less risky while also requiring less computing and communication. This vulnerability to replay attacks was pointed up by Chen et al. [13] in their study on Abbasinezhad-Mood and Nikooghadam protocols during the authentication phase. After that, they complain about how difficult it is to register for the planned scheme. Chen Y. et al. developed a bilinear pairing-based authentication method to overcome the concerns stated. Despite a formal and theoretical study, the proposed method is not as light as Mahmood et al. and Abbasinezhad-Mood et al. systems because of the high computing cost involved with bilinear pairing. Using Jo et al. signature, schnorr's IoT-based smart grid network was recently built with certificate less authentication [22]. Once installed, smart meters can be added dynamically using elliptical curve cryptography. This technique is not protected by a trusted agent.

The cost of calculation and communication must also be reduced. In order to construct a lightweight authentication mechanism for the deployment of the Internet of Drones, researchers in [10,23] developed an authenticated key agreement (AKA) approach using just hash functions and XOR operations (Drone). No comprehensive safety verification of the proposed AKA protocols has been carried out using the known computer-based encryption methods evaluation testing tools. However, the schemes are light and incur minimal high processing costs. An asymmetric wavelet transforms pairing-based key agreement mechanism has been proposed for Drone deployments [24,25]. As a result of its low-cost

mutual authentication, the Drone network has shown to be an effective and convenient lightweight solution [48–50].

In [24], there are no formal proofs that the schemes are secure. Last but not least, Wizid et al. [26] developed a lightweight AKA technique for authenticating users and piloting drones in Drone applications. In this approach, only fuzzy extractor and hash functions are used, resulting in remarkable lightweight properties with little memory overhead and computational and communication expenses. As long as a powerful Canetti-Krawczyk (CK) adversary has access to all the exchanged messages in the proposed authentication protocol, a session-specific temporary information attack is achievable. The authors proposed a method for maintaining privacy while enabling authentication [6].

MEC devices, which significantly reduce authentication costs, were included in the study to account for the great mobility of flying drones. On the other side, formal proof does not support the proposed method for ensuring privacy while simultaneously authenticating users. Drones' use could benefit from the use of an elliptic curve cryptography architecture proposed by Ever [27]. An advanced technique known as bilinear pairing is also being researched. The approach given in [6] does not, according to the authors of [14], take into mutual account authentication while providing secure communication between the organizations.

Drone communication in the Internet of Things can be protected by a certificates-AKA privacy-preserving authentication method proposed by Chen et al. [14]. The scheme assures the confidentiality, availability and privacy of the data. As a result, [14] is vulnerable to a partial key-escrow attack by the trusted authority center, a known session-specific temporary information (CK) adversary and a replay attack due to a loss of integrity in the first message exchange during the authentication phase. As a result, the Drone ecosystem faces potentially catastrophic risks due to the vulnerability of the information it transmits. A single drone's flying area is likewise restricted to the Drone network. In addition, no automated cryptographic protocol verification methods are used to examine the proposed scheme's security. Additionally, the system's lightweight components are inefficient and should be enhanced.

3. Proposed system

The proposed system secure drone communication is established using the shared session key. Users should register with authority control for getting access from drones. The unregistered user will not gain access from the drones due to secure registration. Drones details are registered with authority control, the location and coverage are always updated to the authority control. The proposed system architecture is illustrated in Fig. 1.

3.1. The elliptic curve cryptography foundations

It is possible to acquire compact attributes in encryption by using elliptic curve cryptography (ECC). Because of the reduced keystrokes, it consumes less memory and is faster in field arithmetic [28]. ECC is a good choice for developing public-key cryptography algorithms for devices with limited resources, such as drones. The finite field F_i of the elliptic curve E can be written as $y^2 = x^3 + ax + b, \in F_i$, $4a^3 + 27\, b(mod\ i) \neq \Delta$ where a and Δ is referred to as the basis point and generator point that serves to cyclic groups. These procedures are merely a few of the many ECC algorithms that can be performed. Even with the most powerful computers in the world, it is impossible to find x utilizing elliptic curve cryptography given two random points in a and b is equal to $x.a$, where $x \in Z_i^*$ of a random integer and point of the elliptic curve, both of which are located on the elliptic curve. The elliptic curve discrete logarithmic problem (ECDLP) shares this feature. Here seem to be a few more things to look forward to. The proposed system secure, shared session key communication is depicted in Fig. 2. The proposed system scheme involved four phases: Initialization phase, Registration phase, authentication and key agreement phase, and the Communication phase.

3.1.1. Initialization phase

The elliptic curve E(x,y) of a finite field d is selected by an Authority Control (AC). Choose a collision-free and irreversible hash function h_i where $i = 1$ and 2. The random integer as RI_{AC} from the elliptic curve is selected as a private key to compute the public key as $PUK_{AC} = RI_{AC} * G$. The private key is kept securely by an Authority Control (AC), and other remaining parameters are distributed through the original communication entities.

3.1.2. Registration phase

The participant X wants to communicate the drone system that is symbolized as T_x. Likewise, all communicating entities should be registered with a trusted authority. The following registration steps ensure the registration to gain access to the drone system.

- Step1: T_x selects a random integer as its ephemeral secret element on an elliptic curve as αT_x. The second ephemeral secret element on the elliptic curve is selected as a random integer and is defined as βT_x. Computes a message digest $M_{T_x} = h_1(\alpha T_x \parallel \beta T_x)$, followed by the point computation as $P_{T_x} = h_1(\alpha T_x \parallel \beta T_x) * G$. The identity selection represents ID_{T_x} which is further used send a message (ID_{T_x}, P_{T_x}) toAC.
- Step 2: AC receives the message, then selects ephemeral secret as a random integer, μ_{AC}, from the elliptic curve, then computes equivalent public parameter, $\gamma_{AC} = \mu_{AC} * G$, which computes $T_x = P_{T_x} + \gamma_{AC}$. The schnorr's signature [1] is employed to compute $UT_x = h_1(ID_{T_x} \parallel ET_x)$, and signature $ST_x = UT_x\, SG_{AC} + \mu_{AC}$. AC Sends (ST_x, γ_{AC}) to T_x.
- Step 3: T_x then computes static private key $SG_{T_x} = M_{T_x} + ST_x$, and public key $PuB_{T_x} = SG_{T_x} * G$.
- The following equation confirms the trusted authority of the public key

$$SG_{T_x} * G = ET_x + h_1\left(ID_{T_x} \parallel ET_x\right) * PuB_{AC}$$

Proof:

$$\begin{aligned} SG_{T_x} * G &= \left(M_{T_x} + ST_x\right) * G \\ &= \left(h_1\left(\alpha T_x \parallel \beta T_x\right) + UT_x\, SG_{AC} + \mu_{AC}\right) * G \\ &= \left(h_1\left(\alpha T_x \parallel \beta T_x\right) * G + UT_x\, SG_{AC}\right) * G + \mu_{AC} * G \\ &= \gamma_{AC} + P_{T_x} + UT_x * PuB_{AC} \\ &= \gamma_{AC} + P_{T_x} + UT_x * PuB_{AC} \\ &= ET_x + h_1\left(ID_{T_x} \parallel ET_x\right) * PuB_{AC} \end{aligned}$$

3.1.3. Authentication and key agreement phase

The two communicating entities T_x and T_y establish communication to generate and agree on a common shared secret session key that is used to perform encryption and decryption of the message exchanged during communication between entities.

Steps for Authentication

Step1: By selecting a random integer I_{T_x} of an element from the elliptic curve as a secret ephemeral to compute public parameter $J_{T_x} = I_{T_x} * G$ of the computational timestamp t sends a message $(ID_{T_x}, J_{T_x}, P_{T_x}, t)$ to T_y.

Step 2: Entity T_y checks the threshold of the message timestamp, if the time is within a limit, the message is not discarded; otherwise, the integer I_{T_y} is selected as a random element from the elliptic curve, and that is used for ephemeral secrets, and then the public parameter is represented as $J_{T_y} = I_{T_y} * G$.

The shared secret key computation parameter is represented as $CK_{T_yT_x} = (I_{T_y} + M_{T_y} + ST_y) * J_{T_x} + P_{T_x} + \gamma_{AC} + (h_1(ID_{T_x} \parallel ET_x)PuB_{AC})$ and the verifier computation follows $V_{T_yT_x} = h_1\,(CK_{T_yT_x} \parallel ID_{T_y})$. Finally, the transmission is as follows $(ID_{T_y}, J_{T_y}, P_{T_y}, V_{T_yT_x})$ to the entity T_x.

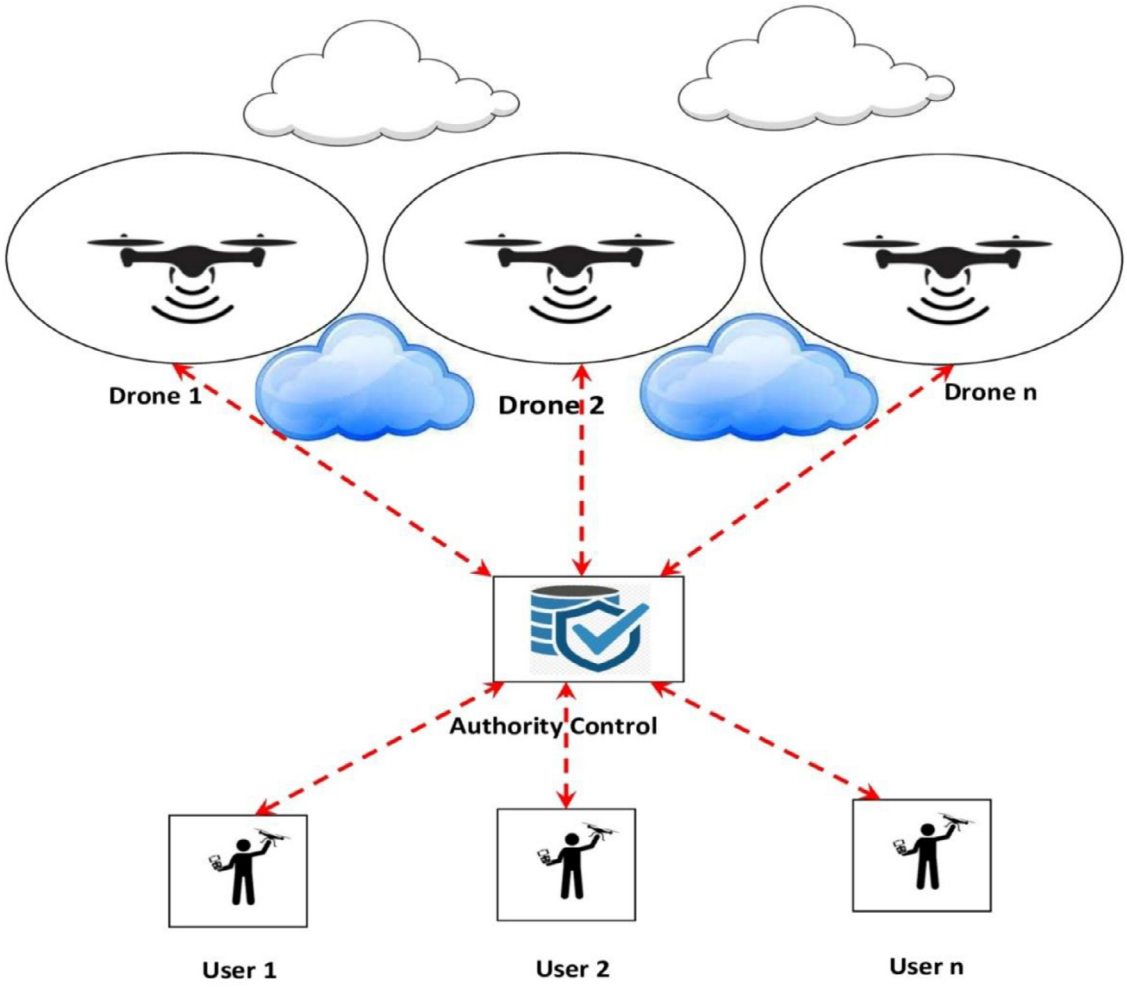

Fig. 1. System Architecture.

Step 3: The T_x computes shared key parameter: $CK_{T_xT_y,} = (I_{T_x} + M_{T_x} + ST_x) * J_y + P_y + \gamma_{AC} + (h_1(ID_{T_x} \parallel ET_y)PuB_{AC})$ verifier computation, $V_{T_xT_y} = h_1(CK_{T_xT_y,} \parallel ID_{T_x})$. Finally, the transmission follows $(ID_{T_x}, J_{T_x}, P_{T_x}, V_{T_xT_y})$ to T_y.

Step 4: T_y checks the verifiers whether they are equal $V_{T_yT_x} = V_{T_xT_y}$ then shared the session key as $SSK_{T_xT_y} = (h_2(ID_{T_y} \parallel ID_{T_x} \parallel V_{T_yT_x})$ if not, discard the message

Proof for the shared secret key is equal:

Proof: $V_{T_xT_y} = V_{T_yT_x}\ V_{T_xT_y}$

$$= (M_{T_x} + ST_x + I_{T_x}) * \left(J_{T_x} + P_{T_x} + \gamma_{AC} + h_1\left(ID_{T_x} \parallel ET_x\right)PuB_{AC}\right))$$

$$= (M_{T_x} + ST_x + I_{T_x}) * I_{T_y} + M_{T_y} + \mu_{AC} + h_1(ID_{T_y} \mid ET_y) * G$$

Substitute, $UT_x = h_1(ID_{T_x} \parallel ET_x)$,

$$V_{T_xT_y} = (M_{T_x} + ST_x + I_{T_x}) * I_{T_y} + M_{T_y} + \mu_{AC} + UT_x\ SG_{AC}) * G$$

Substitute, $ST_x = UT_xSG_{AC} + \mu_{AC}$

So, that $V_{T_xT_y} = (M_{T_x} + ST_x + I_{T_x}) * (M_{T_y} + ST_y + I_y) * G = V_{T_yT_x}$

3.1.4. Communication phase

The proposed system communicating entities establish and share a communication using session key through the following steps:

Step 1: The entity, T_x establish a communication to the T_y which encrypts the message M by the shared session key.

$$CT_x = S_{SSK_{T_xT_y}}(M)$$

Checksum computes,

$CKS_{T_xT_y} = h_2[SSK_{T_xT_y}, J_{T_y}]$, then it sends $(ID_{T_x}, CT_x, CKS_{T_xT_y})$ to T_y

Step 2

T_y then verifies the trust of T_x checking the following equation to be valid

As $CKS_{T_xT_y} = h_2[SSK_{T_yT_x}, J_{T_y}]$

If it is not valid, the message is discarded. Otherwise, the message can be decrypted by the shared session key to obtain the message M,

$$M = DSSK_{T_yT_x}(CT_x)$$

Step 3:

CT_y encrypted message is received by sending acknowledgement from T_y which contains both the original and acknowledged message as M_{Ack} toT_x.

$$CT_y = ESSK_{T_yT_x}(M, M_{Ack})$$

4. Performance analysis

The proposed system approach can be proven to be reliable by comparing it to recent security and lightweight methods. The proposed system scheme's most important contributions are as follows: Partial key escrow (PKE), known session-specific temporary information attack under the Canetti-Krawczyk (CK) opponent and repeat the attack as a result of a lack of authenticity in the original message in Chen et al. [14] 's most recent and effective technique for genuine communication in Drone networks. Furthermore, the scheme's significant linguistic and technical

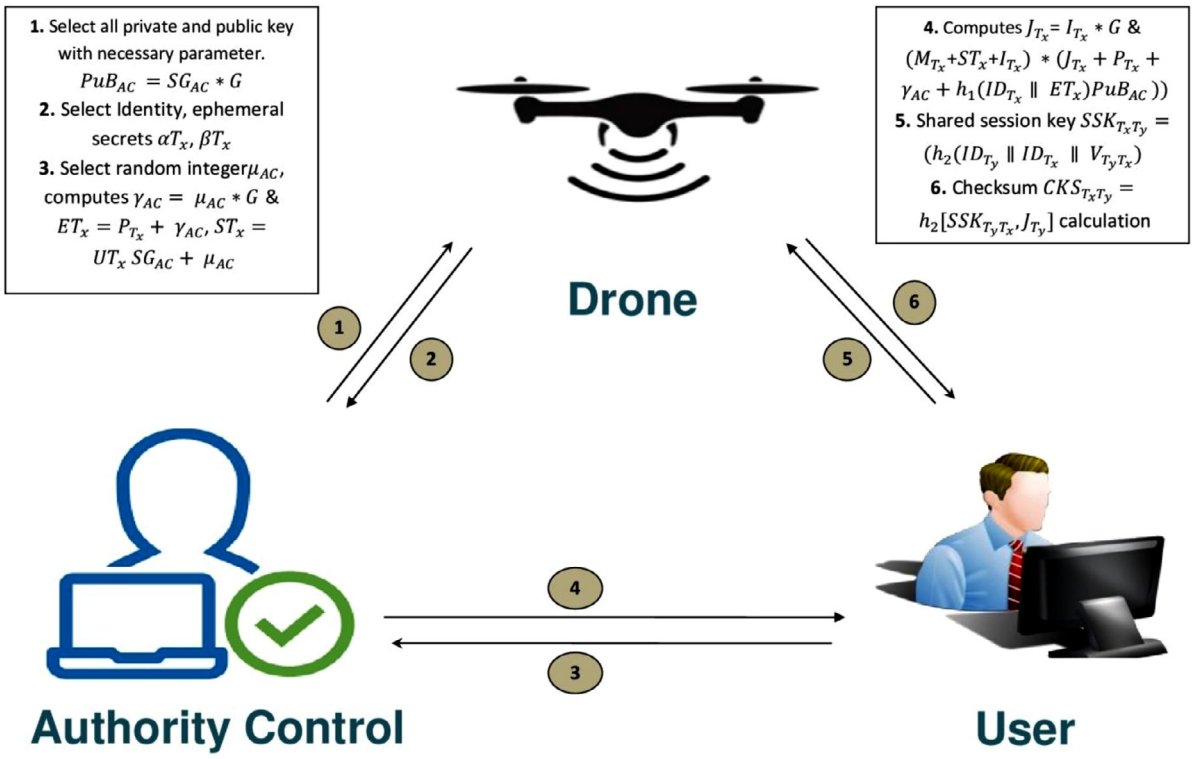

Fig. 2. Drones Secure Communication.

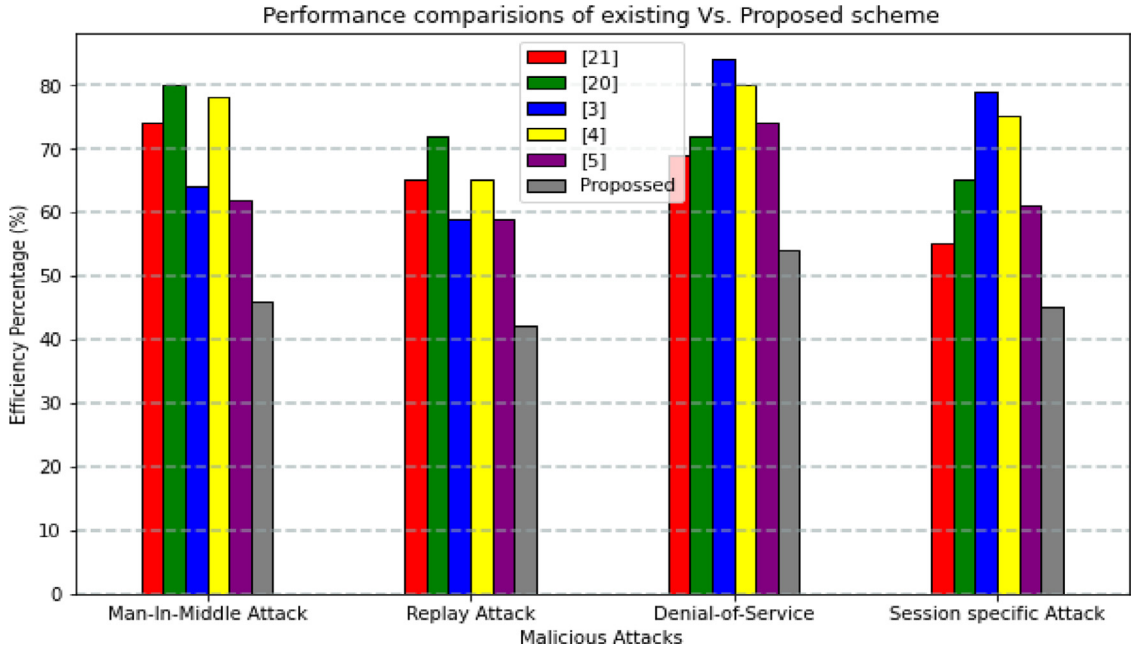

Fig. 3. Comparative attack resilience of Proposed Scheme with Existing system.

costs are investigated in comparison to the proposed system method. The strategy outlined in [14] has a number of limitations that the method does not. It is possible to expand the number of drones that can be utilized in the proposed system approach as the Drone network expands, and this is why AC is included in the proposed strategy. The validity and secrecy of the proposed approach can be verified using the widely acknowledged automatic cryptographic protocol verification tool, ProVerify. To verify its reliability, the proposed system performance is compared to benchmarking methods. Python programming may also be used to compare the proposed energy consumption and computing time to that of the method described in [14].

4.1. Real-time implementation for system evaluation

Using real drones, we showed that the proposed system performed effectively in dense drone networks with up to 11 nodes when tested.

The proposed system discusses the overall effort and time required to complete the protocol. In order to show the efficiency of the proposed system, this is compared with the Zigbee 3.0 protocol and the standard CL-PKC procedures, respectively.

Using the OpenMote-b hardware platform, the proposed protocol was developed and implemented. Here is a cutting-edge Internet of Things (Drone) board for speedy prototyping of new algorithms and applications. An ARM Cortex M3 CPU running at 32 MHz, 512 kB of flash memory, and 32 MB of RAM are all built into the system on chip (SoC) CC2538. The average time length for the communication is about 48 ns.

Drone devices should be protected using the OpenWSN operating system, which has an inbuilt slotted channel access mechanism and the IEEE 802.15.4 standard running in TSCH mode, which serves as the Zigbee 3.0 protocol's PHY and MAC layer. As of IEEE 802.15.4, the MAC layer has added the Proposed protocol (i.e. layer-2).

IEEE 802.15.4 has a maximum packet size of 127 bytes. Message fragmentation is essential in systems where huge volumes of data must be exchanged between nodes. When it comes to difficult cryptographic processes like large atomic number modular and Elliptic Curve Cryptography, OpenMote-most b is quite outstanding (ECC). Our software routines efficiently integrate and handle these atomic activities for complex cryptographic procedures, such as those required by Proposed and competing approaches. During our testing of cryptographic curves, we used elliptic curves secp160r1, secp192r1, and secp256r1. Alternatively, these curves are known to be safe, and each one has a security level that is higher than the 80-bit criterion for an ECC curve. According to many, the use of Montgomery Ladder in the CC2538 crypto processor prevents timing-based attacks by preventing side-channel attacks on ECC operations.

A well-known P1363 KDF was utilized to convert the input strings into a key of the required length [47] using the CC2538 hardware HMAC-SHA function. SoC-integrated 32 MHz clock was utilized in order to precisely measure the time required to perform various hardware and software functions. It was determined that the CC2538 chipset used one probe resistor and a Key sight Infinite-Vision DSOX2012A oscilloscope with two input channels and a resolution of 100 MHz. There is a 1 m/s horizontal range, an 8-bit vertical range, and a 50 mV/div vertical resolution on the oscilloscope.

The OpenMote-b hardware platform needs both time and energy to accomplish each atomic hardware operation. If you are doing point multiplication, there is no such thing as an ideal elliptic curve size. The secp160r1 curve can take 58.0 milliseconds, while the secp256r1 can take up to 109.3 milliseconds. It takes between 1:44 and 2:75 ms to perform an elliptic curve addition, as opposed to 2:53 for an HMAC-SHA. They are also running quicker than ever before, with a completion time of fewer than 0.05 milliseconds each time.

A job's completion time is not necessarily connected with its energy use, according to our research. Multiplication of elliptic curves (using secp161–1, secp162–1, and secp256–1) always consumes the most energy (11.045 mJ), even though increasing the elliptic curve size for the other operations usually results incomparable energy consumption levels of around 244 millijoules. Even though the proposed protocol takes up 2:65 percent of the ROM and 960 bytes of RAM, it can be fully implemented with only 13:594 kB ROM and those meager resources [13]. The open-source nature of our protocol allows us to give researchers and academics a ready-made foundation for future software development.

4.2. Efficiency of the proposed system

OpenMote-b hardware platform, elliptic curve secp160r1, and ten independent Proposed protocol executions were used to calculate an average claimed time length for that protocol. When two devices are using the proposed protocol, it takes about 340:478 milliseconds for everything to be done. Once the key is generated, the exchange of authentication materials and computation of the final Session Key takes 243:392 ms. We found in OpenWSN that the number of RF slots available in a time unit can have a significant impact on the execution time of a given protocol. According to the IEEE 802.15.4 standard, a slot period of 10 milliseconds is provided by default. Within 30 milliseconds, data transmission from one device to another is deemed successful (or, in the worst-case scenario, 60 milliseconds). For the devices tested, Elliptic Curve Multiplication takes the longest time.

When working, bear this in mind: re-keying can save time. Because there are no cryptographic operations necessary at this level, a significant amount of time and effort can be saved" (in reality, cryptography components do not change). It takes just 157:818 ms for the proposed protocol to reduce its overhead when a new session key is used during re-keying.

Using a drone dense network with up to 11 nodes, the proposed protocol's completion time was also assessed. Execute one instance of the proposed protocol at a time if your Drone device has a limited amount of RAM (FCFS). A single sink Drone node and a number of leaf Drone nodes form the basic reference set-up. The number of leaf Drone nodes that need to create a session key with their preferred neighbor climbs dramatically as the number of nodes increases from one to ten. The mean and 95% confidence intervals are shown after conducting 100 tests.

It takes longer to set up session keys with Proposed if there are a lot of devices on the network. Because the sink Drone node can only participate in one proposed instance at a time, this is to be expected. It takes a total of 3:259 s for all the nodes in the network, as well as the sink Drone, to generate a secure session key. For us, this is a very real prospect. A chain topology, in which a single sink Drone node is connected to multiple leaf Drone nodes but only one leaf is connected to the sink. Leaf Drone devices should be configured to only accept requests to start an instance of the proposed protocol if they have established a session key with their preferred neighbor, which is the sink Drone node. If the source and sink nodes share a single unprotected link, an unsafe network would be created. Each node in the chain must have its own proposed protocol instance. As the number of nodes increases, so does the amount of time it takes to set up a safe and secure network.

4.3. Operational cost analysis of proposed system

When comparing the two algorithms, we take into account the addition and multiplication of ECC points as well as pairing and hashing operations. Modular addition and multiplication are omitted from the study. A total number of operations of the proposed system is compared to the existing system and that is represented in the graphical representation of the graph of Fig. 4. The size of a network is represented numerically by the letter n. Adding, multiplying, hashing, and exponentiation ECC points are easy with the proposed scalable and efficient approach. Drone devices with limited computing power can use proposed, which doesn't require a pairing process. This procedure was also compared against three other CL-PKC baseline methods, notably those described in [20,23], and [26].

A few fundamental methods were chosen based on their distinctions. Online interactions with the DA are included in this category; pairing and DA interactions are not included, as in [20] and [26]. It was necessary to consider the protocols of reference methods when making comparisons. On the target hardware board, time was recorded, and we predicted how long it would take to complete this procedure based on that time; multiplying a large number of ECC points often takes about 24 times longer than a simple pairing operation. Drone devices with low capabilities can considerably benefit from proposed capabilities. This method has a total key agreement time of less than a second, which sets it apart from the other methods studied. Regardless of the elliptic curve's size, this holds true. While [23], the most secure option (256-bit Elliptic Curve Group Size), takes 182 percentage points longer than proposed to do the same operation, [26] and [20] execute it in 182 percentage points less time.

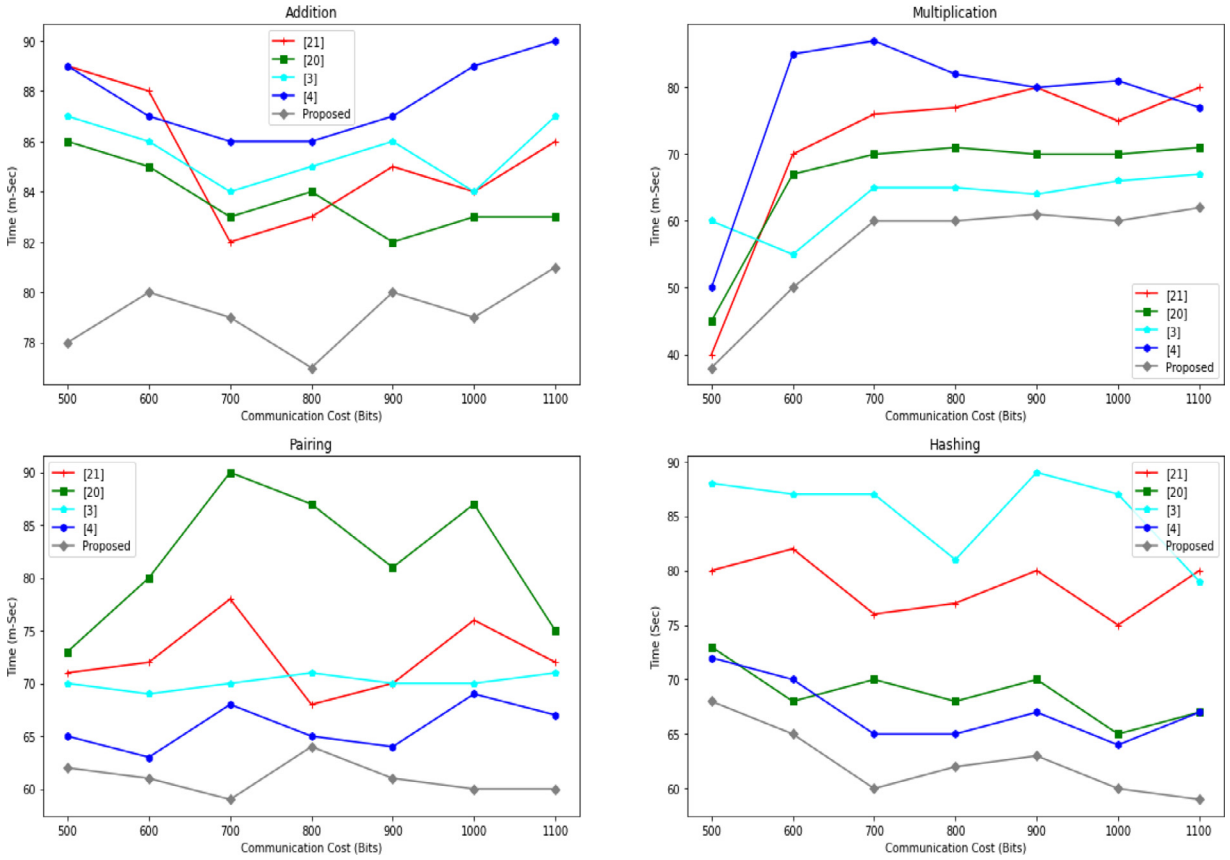

Fig. 4. Comparative operation cost of Proposed Scheme with Existing.

4.4. Energy comparative results of proposed scheme

Zigbee 3.0 standard specifications recommend testing proposed and two additional ways to provide a baseline and facilitate comparisons. ECDSA-signed X.509 certificates were our first assumption, and then we expected ECQV implicit certificates, which are also recommended by the Zigbee 3.0 protocol suite, to be utilized as well. Table 4 provides a summary of the bit-string widths used in the performance evaluation of the reference methodology. No point compression techniques for elliptic curves were used in order to guarantee the comparison was as objective as feasible.

We could compare the message overhead, and overall energy consumption of the Proposed protocol to those of competing techniques since these variables are transmitted in standard-compliant layer-2 frames (as per the proposed protocol). Measurements of ECDSA-signed X.509 certificates were carried out using Table VI and the commonly used OpenSSL application.

Using the three elliptic curves stated above, we first determined how many messages proposed and its competitors need per device. Fig. 10 depicts the findings of this study. X.509-ECDSA certificates must be transferred over a staggering 10 messages per participating device because of their large size, which is a severe drawback. As can be seen in [19], the number of messages required by both Proposed and the ECQV method is comparable. Secp160r1, secp192r1, and ECQV-based key agreement in [19] are all required for proposed to work. However, Secp256r1, in contrast to proposed, demands an additional overhead of six messages (three per device).

Additionally, the amount of energy consumed by each of the three methods was compared and contrasted. The amount of energy required to send and receive a single data packet using the target hardware platform was first studied for a meaningful assessment that was not dependent on external factors such as the IEEE 802.15.4 MAC schedule and access to the transmission media. We totaled up how much energy is required to run an experiment, how many transmissions and receptions there were, and how much energy it took to do a cryptographic operation for each method that was studied

Sending a data packet and receiving an acknowledgement from the recipient is defined by IEEE 802.15.4 as a time window of one second. The same experimental set-up described in the previous part was used to assess how much power was consumed by a single IEEE 802.15.4 active slot's data transmitter and receiver (10 ms). When the offset is 3 ms or 6:5 ms, we see an increase in energy consumption. There are several ways in which the two functions of RF systems are interconnected. In terms of duration, the longest and most apparent spike is around 3 ms. The proposed protocol MAC layer payload and IEEE 802.15.4 MAC header are sent in the first data packet. As a result, data transmission and reception absorb around 112 and 96% of the energy consumed during this shortened time period (gray line). Raising the receiver in advance ensures that the complete packet of information is received. A second requirement stipulated by IEEE 802.15.4 is that all data packets be delivered with acknowledgement at the MAC layer. The energy consumption of these two devices differs because the data receiver broadcasts an acknowledgement while receiving RF signals. 35.28 millijoules of power are used by the two devices, while the RF radio chip is not in use (mJ). This is the fault of purely software-based processes. Using the area under the current consumption curve as an example, the total amount of energy used during that particular time period can be expressed in this way: Energy (in mJ), current (in mA), and time period are all elements that must be taken into consideration (in milliseconds). 3:3 V is needed to power the OpenMote-b board (in Volts). As a result, data transmission slots require 802:65 mJ of power, while data reception slots require 778:51 mJ.

To determine the energy consumption of CBKE with X.509-ECDSA or ECQV certificates, or the proposed protocol, a wide range of parame-

ters can be used, the experimental energy consumption for each atomic cryptographic operation, as well as the number of required messages and the elliptic curve size. X.509 certificates signed using a 160-bit elliptic curve use 21; 855 mJ of energy, but ECDSA certificates issued with a 256-bit elliptic curve use 38; 952:87 mJ of energy.

It appears that both ECQV and Proposed use a similar amount of energy. In RF activities, the Proposed uses less energy because there are fewer bytes required. The ECQV-based technique in [19] requires 98 percent more energy than Proposed since it uses 35.726 millijoules instead of 36.080 millijoules for a 256-bit elliptic curve.

In order to power the OpenMote-b board, you will need two AA batteries. Manganese/Alkaline batteries, on the other hand, use about 3:84 watt-hours of power, or 13; 824 Joules, each charge at a voltage of 1:5 V. A single usage of proposed system consumes less than 0.0134 percent of the battery capacity, making it virtually non-existent.

According to our article, ECQV-based techniques can be applied to massive Drone networks, and a minor increase is noticeable. To put it another way, Drone devices can gain up to 140:83 percent of their energy from X.509 ECDSA compared to Sec. VI-B-based solutions. Because of their ECQV foundation, proposed approach is impenetrable to the attackers. Impersonation attacks can't be prevented by using ECQV-based systems because the secret nodes' data on the DA is revealed. The proposed system is to be used instead of ECQV-based techniques in order to obtain the same (optimal) message overhead and energy consumption while yet being resistant against a formidable adversary using a 256-bit elliptic curve.

When it comes to preventing regular Man-In-The-Middle (MIM) attacks, only proposed is capable of withstanding leaks of secret node data, message overhead and energy usage are both reduced in Drone devices, according to our research. Even though proposed has the ability to detect an ongoing assault after exchanging just as many IEEE 802.15.4 messages as ECQV, 256-bit elliptic functions proposed secp256r1 are employed to build the curves. The Comparison of the proposed Key Agreement Time for different group size is compared with existing system and that is tabulated in Table 4.

5. Proposed scheme privacy achievements

Proposed system most critical security features are outlined in this chapter. Here we highlight the essential proposed confidentiality features in division- A, whereas division-B discusses the automated verification of the methods privacy accomplished using ProVerif.

5.1. Aspects of safety

Secret AC information is protected against breaches. The self-generated component of each device's public key is now associated with the identity of the party that produced it through the string ωi. When the AC's information gets disclosed to an opponent, this clever function comes in handy. There's no way for an enemy who knows only one device's private key to mimic any of the other devices since it doesn't know the other device's private key [36].

Consider, for the sake of illustration, a situation in which the attacker has access to the AC on which the Drone device's private keys are stored. In addition, let's suppose that the adversary only has temporary (e.g., reading or stealing the file) access to this data and that it is unable to get the AC's private key or complete control. The certificate-based systems of the past are obsolete (e.g. employing X.509-ECDSA and ECQV certificates) can no longer improve the protection of interactions among Drone systems in light of the challenging circumstances described above. Although these approaches are designed to keep private keys secure, it's quite possible for a device to deduce the session keys from a message exchange and use them to impersonate either one or both of the other devices on the network.

To put it another way, if proposed is employed, the opponent still lacks the entire private key of the device, which is constituted of a part that is unknown to AC, and so cannot rebuild the secret key that has already been formed or forecast future shared key that will be acquired. So any hostile object would cause the communication between two participants that computed separate interim session keys, which would cause unrecovered mistakes when the identification labels were transferred and validated. The proposed mechanisms have been independently validated by the ProVerif tool.

5.1.1. Cryptographic constraint

AC's cryptographic elements have been released, which means it may assign a brief validity term to each one. It will be possible for any offsite participant participating in the suggested based consensus mechanism to rapidly identify the validity of a public key even after the prescribed time period has expired. It is indeed possible to detect a localized fraudulent modification of the expiry period shortly, even as a distinctive connection between the identifier and the accompanying secret key might no longer be validated. The proposed system scheme feature is compared with existing system is tabulated in Table 3. The Table 3 features quickly configured to the proposed scheme based on the selection of the connection type, material and the performance. In that case the proposed scheme communication established faster than all other existing system is represented in Table 2.

5.1.2. Man-in-the-Middle attack

Using a trustworthy method, proposed binds its owner's partial public keys. A participant will require the public portion of the public key of a specific entity in order to fully impersonate that entity's identity using Proposed. The second component of Proposed also includes two authentication messages that include all of the data that was previously sent and received. To demonstrate the success of this technique in protecting against MITM and tampering attacks, the same proofs that were used for the TLS protocol [37] may be used for this strategy. The ProVerif tool has also been used to verify this property's formality (see Sec. V-B).

5.1.3. Replay attacks

Opcodes are created ex-negotiation at any moment, even though the initial session key is the same throughout all cases of Proposed. To put it another way, they ensure that each new protocol instance generates a unique set of session keys, preventing any replay attacks. The multiple nodes would be unable to construct the right identification codes if prior communications are replayed (see division B for the formal demonstration of this condition).

5.1.4. Pre-Known key attacks

The essential points of the first session and the new nonces are used to generate a new session key for each run of Proposed. To put it another way, the malicious entity can't re-compute formal organizations' confidential credentials since it is assumed that it cannot address the problem of the well-known ECCDHP and the Elliptic Curve Discrete Algorithm Problem (ECDLP). Because of this, the enemy will have to start from scratch when it comes to figuring out the new key.

5.1.5. Energy-Depletion attacks and their possible consequences

At stages 8 and 10, the proposed protocol can only identify the presence of an adversary during the key formation process by exchanging messages #3 and #4. It is easy for hackers to expose a real Drone system to power generation attacks if he or she is repeatedly involved in the scheme failures. Once 2k conceptual messages are exchanged, with a quadratic rise in the number of instances, the genuine Drone device will become aware of an attack. In order to minimize this problem, the count is set to 3 failed attempts before commencement, after that, the drone will refuse the requests from a given device. During this incident, the target device may produce an alert, requiring additional inquiry.

According to the Section, it is not more difficult to identify an attack using the proposed protocol than existing PKC methods, such as X.509-EDSA certifications and ECQV explicit credentials. CBKE-ECQV

Table 1
Comparison of Security Attacks Efficiency.

security Attacks	Schemes										Proposed Scheme
	[20]	[12]	[4]	[5]	[14]	[16]	[7]	[3]	[19]	[24]	
Man- in the middle attack	×	√	√	×	×	×	√	NA	NA	√	×
Denial-of-Service Attack	×	√	×	×	×	×	NA	√	NA	NA	×
Forwarded Secrecy attack	√	×	√	×	√	√	√	√	√	√	×
Private key leakage attack	×	×	×	√	NA	√	NA	NA	√	√	×
Partial key-Escrow attack	×	×	√	NA	NA	√		√	√	×	×
Session specific Attack	√	×	√	√	√	NA	NA	√	√	×	×
Privileged Insider attack	×	√	×	N A	NA	√	NA	√	×	×	×
Replay Attack	√	×	×	NA	NA	NA	√	√	√	√	×

Table 2
Comparison of Operational Computation Cost.

Schemes	Phase	Operation(ms)					Total Computation (ms)
		Addition	Multiplication	Pairing	Hashing	Exponents	
[20]	Authentication	10	5	0	2	0	17
	Communication	5	9	0	3	2	19
[12]	Authentication	7	4 + 2n	1	2	4	18
	Communication	2	4 + 3n	0	4	4	14+3n
[4]	Authentication	7	5	2	2	4	20
[5]	Authentication	5	4	0	2	0	49
	Communication	5	2	0	3	2	12
[14]	Authentication	4	6	2	0	0	12
	Communication	5n	2	1	0	2	5 + 5n
[16]	Communication	4	3	1	0	2	14
[7]	Authentication	5	4 + 2n	2	0	2	16
	Communication	8	4	3	0	2	17
[24]	Authentication	7	4	8	1	2	22
	Communication	5	2	1	0	0	8
[3]	Authentication	7n	4	2	1	0	7 + 7n
	Communication	5	4	2	1	0	12
[19]	Authentication	6	4	3	2	0	9
	Communication	4	5	0	2	1	12
Proposed Scheme	Authentication	2	1	1	2	1	7
	Communication	1	2	2n	2	1	6 + 2n

CL-PKC schemes based on CBKE-ECDSA and CBKE-ECQV are expected to be implemented in Drone devices that use IEEE 802.15.4 and Zigbee 3.0 protocol stacks and this does not add any additional overhead.

Table 3
Comparison of Proposed scheme features with the existing system.

Proposed Scheme Features	Comparative Analysis of existing system with the proposed scheme										
	[20]	[12]	[4]	[5]	[14]	[16]	[7]	[3]	[19]	[24]	Proposed
Connection	×	√	√	×	×	×	√	NA	NA	√	√
Material of Ephemeral	×	√	×	×	×	×	NA	√	NA	NA	√
Integration of IoT	√	×	√	×	√	√	√	√	√	√	√
Real-Time Performance Evaluation	×	×	×	√	NA	√	NA	NA	√	√	√
Open Source Code access	×	×	√	NA	NA	√		√	√	×	√
Re-Keying	√	×	√	√	√	NA	NA	√	√	×	√
Energy Efficient	×	√	×	N A	NA	√	NA	√	×	×	√
Pairing	√	×	×	NA	NA	NA	√	√	√	√	√

Table 4
Comparison of Key Agreement Time for different group size.

Schemes	Key Agreement Time(ms)		
	Group Size 160 bit Elliptic Curve	Group Size 192 bit Elliptic Curve	Group Size 256 bit Elliptic Curve
[20]	856.562	1172.663	2488.426
[12]	957.562	1098.44	1928.772
[4]	555.38	896.25	1118.766
[5]	632.5	1263.2	2048.455
[14]	414.666	949.55	1543.3
[16]	881.367	1656.5	2588.22
[7]	354.88	854.36	1955.456
[24]	457.352	954.33	1468.88
[3]	645.36	1654.338	2317.227
[19]	568.33	1455.33	2544.36
Proposed	245.34	557.145	894.255

allows a Drone device to refuse an occurrence of the based consensus procedure (therefore identifying an attempt) just after the original message, but CBKE-ECDSA requires ninth messages to deny an attempt at the MAC-layer. To avoid delay, the devices deny the connections after getting two MAC-layer messages. Thus, there is no need to increase the number of messages exchanged at the MAC layer and that is designed to check an assault using the prototype. Thus, we may conclude that communication technology has no influence on how sensitive a based consensus technique is to resource starvation assaults.

6. Conclusion

In this paper, the tradeoff between security and lightweight features of the recent authenticated scheme for drones were fully implemented and investigated with the existing systems. From that, the proposed system achieved lower communication costs and energy consumption because of the ECC operations. Basically, all other systems require higher communication costs, but that elliptic curve used a digital signature algorithm for minimizing the communicated messages. The components of the exchanged messages are minimized as less as possible. Future work will consider the deployment of the secure, lightweight proven authenticated key agreement technique in a static IoT-based network such as healthcare and smart grid network.

Declaration of interests

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper

References

[1] A.K. Das, M. Wazid, N. Kumar, A.V. Vasilakos, J.J.P.C. Rodrigues, Biometrics-based privacy-preserving user authentication scheme for cloud-based industrial internet of things deployment, IEEE Internet Things J. 5 (6) (2018) 4900–4913 Dec.

[2] W. Khan, M. Rehman, H. Zangoti, M. Afzal, N. Armi, K. Salah, Industrial internet of things: recent advances, enabling technologies and open challenges, Comput. Electr. Eng. 81 (2020) 106522 [Online]. Available http://www.sciencedirect.com/science/article/pii/S0045790618329550.

[3] Z. Meng, Z. Wu, C. Muvianto, J. Gray, A data-oriented m2m messaging mechanism for industrial iot applications, IEEE Internet Things J. 4 (1) (Feb 2017) 236–246.

[4] C. Yin, J. Xi, R. Sun, J. Wang, Location privacy protection based on differential privacy strategy for big data in industrial internet of things, IEEE Trans. Ind. Inf. 14 (8) (Aug 2018) 3628–3636.

[5] W. Ali, I. Ud Din, A. Almogren, M. Guizani, M. Zuair, A lightweight privacy-aware iot-based metering scheme for smart industrial ecosystems, IEEE Trans. Ind. Inf. (2020) 1 1.

[6] I.Ud Din K.Haseeb, A. Almogren, N. Islam, A. Altameem, Rts: a robust and trusted scheme for IoT-based mobile wireless mesh networks, IEEE Access 8 (2020) 68 379–68 390.

[7] X. Li, J. Niu, M.Z.A. Bhuiyan, F. Wu, M. Karuppiah, S. Kumari, A robust ecc-based provable secure authentication protocol with privacy preserving for industrial internet of things, IEEE Trans. Ind. Inf. 14 (8) (Aug 2018) 3599–3609.

[8] I. Makhdoom, M. Abolhasan, J. Lipman, R.P. Liu, W. Ni, Anatomy of threats to the internet of things, IEEE Commun. Surv. Tutor. 21 (2) (2019) 1636–1675.

[9] J. Seto, Y. Wang, X. Lin, User-habit-oriented authentication model: toward secure, user-friendly authentication for mobile devices, IEEE Trans. Emerg. Top. Comput. 3 (1) (March 2015) 107–118.

[10] S. Roy, S. Chatterjee, A.K. Das, S. Chattopadhyay, N. Kumar, A.V. Vasilakos, On the design of provably secure lightweight remote user authentication scheme for mobile cloud computing services, IEEE Access 5 (2017) 25 808–25 825.

[11] C. Wang, L. Xiao, J. Shen, R. Huang, Neighborhood trustworthiness-based vehicle–to-vehicle authentication scheme for vehicular ad hoc networks, Concurr. Comput. 31 (2018) e4643 05.

[12] J. Shen, T. Zhou, X. Liu, Y. Chang, A novel latin-square-based secret sharing for m2m communications, IEEE Trans. Ind. Inf. 14 (8) (Aug 2018) 3659–3668.

[13] D. Liu, J. Shen, A. Wang, C. Wang, Lightweight and practical node clustering authentication protocol for hierarchical wireless sensor networks, Int. J. Sensor Netw. 27 (2) (2018).

[14] M. Wazid, A.K. Das, V. Odelu, N. Kumar, W. Susilo, Secure remote user authenticated key establishment protocol for smart home environment, IEEE Trans. Dependable Secure Comput. (2018) 1 1.

[15] J. Shen, S. Chang, J. Shen, Q. Liu, X. Sun, A lightweight multi-layer authentication protocol for wireless body area networks, Future Generat. Comput. Syst. 78 (2018) 956–963 [Online]. Available http://www.sciencedirect.com/science/article/pii/S0167739X16306963.

[16] B. Ying, A. Nayak, Anonymous and lightweight authentication for secure vehicular networks, IEEE Trans. Veh. Technol. 66 (12) (Dec 2017) 10 626–10 636.

[17] M. Wazid, A.K. Das, N. Kumar, A.V. Vasilakos, J.J.P.C. Rodrigues, Design and analysis of secure lightweight remote user authentication and key agreement scheme in internet of drones deployment, IEEE Internet Things J. 6 (2) (April 2019) 3572–3584.

[18] Vijayakumar. Pandi, Naresh. Ramu, Jegatha Deborah. Lazarus, S.K. Hafizul Islam, in: An Efficient Group Key Agreement Protocol For Secure P2P Communication, 9, Security and Communication Networks, 2016, pp. 3952–3965. volno.

[19] J. Srinivas, S. Mukhopadhyay, D. Mishra, Secure and efficient user authentication scheme for multi-gateway wireless sensor networks, Ad Hoc Netw. 54 (2017) 147–169.

[20] D. Wang, W. Li, P. Wang, Measuring two-factor authentication schemes for real-time data access in industrial wireless sensor networks, IEEE Trans. Ind. Inf. 14 (9) (Sep. 2018) 4081–4092.

[21] A. Esfahani, G. Mantas, R. Matischek, F.B. Saghezchi, J. Rodriguez, A. Bicaku, S. Maksuti, M.G. Tauber, C. Schmittner, J. Bastos, A lightweight authentication mechanism for m2m communications in industrial IoT environment, IEEE Internet Things J. 6 (1) (2019) 288–296.

[22] M. Wazid, A.K. Das, V. Odelu, N. Kumar, M. Conti, M. Jo, Design of secure user authenticated key management protocol for generic IoT networks, IEEE Internet Things J. 5 (1) (Feb 2018) 269–282.

[23] Azees. Maria, Vijayakumar. Pandi, Deboarh.Lazarus Jegatha, EAAP: efficient anonymous authentication with conditional privacy-preserving scheme for vehicular ad hoc networks, IEEE Trans. Intell. Transp. Syst. 18 (9) (2017) 2467–2476.

[24] A. Karati, S.H. Islam, M. Karuppiah, Provably secure and lightweight certificateless signature scheme for iiot environments, IEEE Trans. Ind. Inf. 14 (8) (Aug 2018) 3701–3711.

[25] Y. Zhang, R.H. Deng, D. Zheng, J. Li, P. Wu, J. Cao, Efficient and robust certificateless signature for data crowdsensing in cloud-assisted industrial iot, IEEE Trans. Ind. Inf. 15 (9) (Sep. 2019) 5099–5108.

[26] H.N. Almajed, A.S. Almogren, Se-enc: a secure and efficient encoding scheme using elliptic curve cryptography, IEEE Access 7 (2019) 175 865–175 878.

[27] M. Hassan, A. Gumaei, S. Huda, A. Almogren, Increasing the trustworthiness in the industrial iot networks through a reliable cyberattack detection model, IEEE Trans. Ind. Inf. (2020) 1 1.

[28] F. Rezaeibagha, Y. Mu, X. Huang, W. Yang, K. Huang, Fully secure lightweight certificateless signature scheme for iiot, IEEE Access 7 (2019) 144 433–144 443.

[29] X. Li, J. Peng, J. Niu, F. Wu, J. Liao, K.R. Choo, A robust and energy efficient authentication protocol for industrial internet of things, IEEE Internet Things J. 5 (3) (2018) 1606–1615.

[30] A.K. Das, M. Wazid, A.R. Yannam, J.J.P.C. Rodrigues, Y. Park, Provably secure ecc-based device access control and key agreement protocol for IoT environment, IEEE Access 7 (2019) 55 382–55 397.

[31] Y. Yu, L. Hu, J. Chu, A secure authentication and key agreement scheme for iot-based cloud computing environment, Symmetry (Basel) 12 (150) (2020) 1–16 01.

[32] A.S. Almogren, Intrusion detection in edge-of-things computing, J. Parallel Distribut. 137 (2020) 259–265 [Online]. Available http://www.sciencedirect.com/science/article/pii/S074373151930872X.

[33] A.Al-Mogren K.Haseeb, I. Ud Din, N. Islam, A. Altameem, Sasc: secure and authentication-based sensor cloud architecture for intelligent internet of things, Sensors 20 (2468) (April 2020).

[34] Y. Dodis, L. Reyzin, A. Smith, Fuzzy extractors: how to generate strong keys from biometrics and other noisy data, in: C. Cachin, J.L. Camenisch (Eds.), Advances in Cryptology - EUROCRYPT, Springer Berlin Heidelberg, Berlin, Heidelberg, 2004, pp. 523–540. 2004.

[35] Z. Liu, Z. Cao, D.S. Wong, White-box traceable ciphertext-policy attribute-based encryption supporting any monotone access structures, IEEE Trans. Inf. Forensics Secur. 8 (1) (Jan 2013) 76–88.

[36] Vijayakumar. Pandi, Bose. Sudan, Kannan. Arputharaj, Chinese remainder theorem based centralised group key management for secure multicast communication, IET Inf. Secur. 8 (3) (2014) 179–187 IETvolno.

[37] Vijayakumar. Pandi, Naresh. Ramu, Islam.SK Hafizul, Deborah.Lazarus Jegatha, in: "An Effective Key Distribution for Secure Internet payTV using Access key Hierarchies", Security and Communication Networks, 9, John Wiley & Sons Ltd Chichester, UK, 2016, pp. 5085–5097.

[38] Shen. Jian, Yang. Huijie, P. Vijayakumar, Kumar. Neeraj, A privacy-preserving and untraceable group data sharing scheme in cloud computing, IEEE Trans. Dependable Secure Comput., IEEE (2021).

[39] D. Wang, D. He, P. Wang, C. Chu, Anonymous two-factor authentication in distributed systems: certain goals are beyond attainment, IEEE Trans. Dependable Secure Comput. 12 (4) (2015) 428–442.

[40] D. Wang, P. Wang, Two birds with one stone: two-factor authentication with security beyond conventional bound, IEEE Trans. Dependable Secure Comput. 15 (4) (2018) 708–722.

[41] D. Wang, P. Wang, On the anonymity of two-factor authentication schemes for wireless sensor networks, Comput. Netw. 73 (C) (Nov. 2014) 41–57 [Online]. Available, doi:10.1016/j.comnet.2014.07.010.

[42] C.G. Ma, D. Wang, S.D. Zhao, Security flaws in two improved remote user authentication schemes using smart cards, Int. J. Commun. Syst. 27 (10) (2014) 2215–2227.

[43] M. Gupta, N.S. Chaudhari, Anonymous two factor authentication protocol for roaming service in global mobility network with security beyond traditional limit, Ad Hoc Netw. 84 (2019) 56–67 [Online]. Available http://www.sciencedirect.com/science/article/pii/S1570870518301859.

[44] Feifei Wang, Guoai Xu, Lize Gu, A secure and efficient eccbased anonymous authentication protocol, Secur. Commun. Netw. (2019) 1–13 08 2019.

[45] Q. Jiang, N. Zhang, J. Ni, J. Ma, X. Ma, K.R. Choo, Unified biometric privacy preserving three-factor authentication and key agreement for cloud-assisted autonomous vehicles, IEEE Trans. Veh. Technol. (2020) 1 1.

[46] D. Wang, H. Cheng, P. Wang, X. Huang, G. Jian, Zipf's law in passwords, IEEE Trans. Inf. Forensics Secur. 12 (11) (2017) 2776–2791.

[47] P. Gope, A.K. Das, N. Kumar, Y. Cheng, Lightweight and physically secure anonymous mutual authentication protocol for real-time data access in industrial wireless sensor networks, IEEE Trans. Ind. Inf. 15 (9) (2019) 4957–4968.

[48] Vijayakumar. Pandi, Bose. Sundan, Kannan. Arputharaj, P.H. Himesh, Key Distribution protocol for secure multicast with reduced communication delay, in: International Conference on Active Media Technology, Berlin Heidelberg, Springer, 2011, pp. 312–323.

[49] Wang. Chen, Shen. Jian, Vijayakumar. Pandi, B. Gupta. Brij, Attribute-based secure data aggregation for isolated IoT-enabled maritime transportation systems, IEEE Trans. Intell. Transp. Syst. (2021).

[50] F. Wei, P. Vijayakumar, Q. Jiang, R. Zhang, A mobile intelligent terminal based anonymous authenticated key exchange protocol for roaming service in global mobility networks, IEEE Trans. Sustain. Comput. (2018) 1 1.