IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received July 4, 2021, accepted August 29, 2021, date of publication September 7, 2021, date of current version September 28, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3110804

Identity and Aggregate Signature-Based Authentication Protocol for IoD Deployment Military Drone

SAEED ULLAH JAN[1] AND HABIB ULLAH KHAN[2], (Member, IEEE)
[1]Department of Computer Science and Information Technology, University of Malakand, Chakdara, Khyber Pakhtunkhwa 18800, Pakistan
[2]Department of Accounting and Information Systems, College of Business and Economics, Qatar University, Doha, Qatar

Corresponding author: Habib Ullah Khan (habib.khan@qu.edu.qa)

This work was supported in part by Qatar National Library, Doha, Qatar, and in part by Qatar Univeristy (QU) Internal Grant, QU, under Grant IRCC-2021-010.

ABSTRACT With the rapid miniaturization in sensor technology, ruddervator, arduino, and multi-rotor system, drone technology has fascinated researchers in the field of network security. It is of critical significance given the advancement in modern strategic narratives. This has special relevance to drone-related operations. This technology can be controlled remotely by an invisible yet credible operator sitting to a powerful intelligence computer system (PICS) or an airborne control and command platform (AC2P). The two types of drones (reconnaissance and attacking) can communicate with each other and with the PICS or AC2P through wireless network channels referred to as Flying Ad Hoc Network or Unmanned Aerial Vehicular Network (FANET or UAVN). This mode of communication is not without some inconvenience. For instance, when the line of sight is broken, communication is mainly carried out through satellite using GPS (Global Positioning System) signals. Both GPS and UAVN/FANET use open network channels for data broadcasting, which are exposed to several threats, thus making security risky and challenging. This risk is specifically eminent in monitoring data transmission traffic, espionage, troop movement, border surveillance, searching, and warfare battlefield phenomenon, etc. This issue of security risk can be minimized conspicuously by developing a robust authentication scheme for IoD deployment military drones. Therefore, this research illustrates the designing of two separate protocols based on the aggregate signature, identity, pairing cryptography, and Computational Diffie-Hellman Problem (CDHP) to guarantee data integrity, authorization, and confidentiality among drones and AC2P/PICS. More importantly, the outdated data transmission flaw has also been tackled, which is of obvious concern to the past designed protocols. The security of the proposed designs is formally verified using a random oracle model (ROM), a real-or-random (ROR) model, and by informally using pragmatic illustration and mathematical lemmas. Nonetheless, the performance analysis section will be executed using the algorithmic big-O notation. The results show that these protocols are verifiably protected in the ROM and ROR model using the CDHP.

INDEX TERMS Aggregation, authentication, encryption, paring cryptography, unforgeability.

I. INTRODUCTION

The use of drones in the military field is more prominent than the civilian domain. This rapid advancement in military drone technology can be used for stealth, espionage, attacking, border monitoring, and surveillance of troops movement. Besides these, the military mission delivery is crucial because it carries sensitive data using an open network channel, which requires secure IoD architecture and needs physical logistic security to the intersecting route. This mission delivery of miliatry drone face many issues and challenges, especially the protection of intelligent command delivery, privacy, message authentication, and identification authentication [1]. It is mandatory that, before operationalizing a drone for military mission delivery, its control infrastructure is required for securing its open network channel. As wireless networking and computing technologies are contemporary fields of computing technologies, like Unmanned Aerial Vehicular

The associate editor coordinating the review of this manuscript and approving it for publication was Aneel Rahim.

Network (UAVNs) and Flying Ad Hoc Network (FANET) have been contributed a lot in providing numerous applications in the military domain. Miliatary drone technologies monitors suspicious spots, collect information, control flowing of data, intelligence exchange of command and control in the warfare battlefield. This bilateral exchange of data needs to be controlled by the system (AC2P/PICS). The synergy among UAVN/FANET and control system periodically transmits real-time information fusion. A small dubious command can mislead the attacking drone for a wrong decision. By deploying drones in warfare, efficient information authentication is needed [2]; identification authentication is beyond the scope of this paper. Nevertheless, the vulnerability of such data may threaten the security of the entire country.

Overall, drone technology has matured, and unmanned aviation and aircraft, alone or in combination with AC2P/PICS and maritime vehicles, possess a high significance in the military sector. Despite increasing interest in civilian applications, military use is currently the largest market for drones/UAVs and is expected to remain so in the near future. The creation of Sense and Avoid (S&A) technology [3] will enable the UAV to autonomously detect a manned aircraft and then make flight path corrections to avoid a midair collision. Integrating military UAVs into congested airspace for current technology (FANET/UAVNs) is one of the most critical research areas [4]. Other associated issues and challenges in the military domain must be addressed for UAVs to remain operational, such as GPS signal spoofing/jamming is a severe threat that stops a receiver from receiving a reliable GPS signal. The cameras inside the military drone catch photograph containing invisible information like resolution, shooting time, and coordinates. This hidden information, in turn, badly affects the security and privacy of the system. An adversary can break the communication session by generating a fake signal and forging sensitive information. For example, system failure occurs, an adversary controls the signal's frequency used by the drone for sensitive data transmission and uses it for malicious deeds [5], [6].

Furthermore, the military drone is potentially vulnerable to several attacks, such as spoofing, physical capture, collation, and forgery attacks. Before exchanging secrets and confidential information over an unreliable communication channel (FANET/UAVNs), there is a lack of coordination and collaboration for not allowing a registered and permitted entity to interact securely in IoD. Similarly, drones also have limited flight time and energy resources, due to which it is exposed to many security threats. However, without solving these issues successfully, it would cause immense harm at any time [7]–[10] to IoD. So, these challenges can be addressed only by designing a flawless authentication protocol to effectively operationalize drones for military mission delivery and qualify for complex operation in IoD environment.

A. MILITARY DRONE SYSTEM ARCHITECTURE

Drone technology has become a precious weapon to militarized forces worldwide which is evident from its widespread use in many recent conflicts. This technology has minimized radar subscriptions, improved longevity, and emancipated humans from immediate danger. Even though none of these UAVs has an operator on board, human supervision remotely is an integral part of the technology. Similarly, though less developed, civilian uses of UAVs still necessitate supervisory authority for complex operations such as border patrol, agriculture monitoring, and disaster response. In order to develop an IoD environment that can effectively support single operator and multiple UAV control, efforts should be put together by a team of human operators, software agents, and UAVs to optimize mission effectiveness while keeping costs down. To do so, the system architecture presented here in this paper consists of reconnaissance drones, attacking drones, airborne control and command platform (AC2P), and a powerful intelligence computer system (PICS). All the participants are equipped with UAVNs/FANETs and can also be enabled for other wireless communication interfaces and integrated with GPS signals. The reconnaissance drones communicate with each other and with AC2P but not with a powerful intelligence computer system (PICS). In contrast, AC2P and PICS can speak directly and coordinate reconnaissance drones at any time. Similarly, attacking drones can communicate with AC2P, PICS, and with each other but not with reconnaissance drones. Collaboration and coordination (synergy) among all the participants are mandatory; otherwise, it cannot perform a complex tactical task, as shown in figure 1.

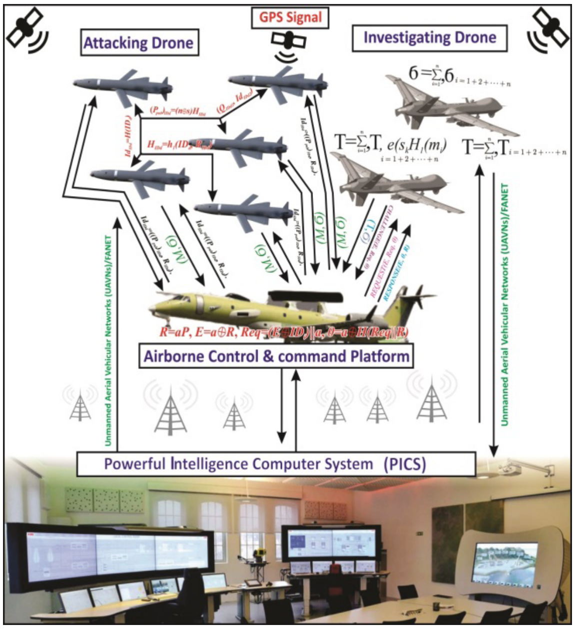
GPS Signal
Attacking Drone
Investigating Drone
$6=\sum_{i=1}^{n} 6_{i=1+2+\cdots+n}$
$(P_{pub})_{IDd}=(n\oplus s)H_{IDd}$
(Q_{IDd}, Id_{IDd})
$Id_{IDd}=H(ID)$
$H_{IDd}=h_1(ID_d, R_{IDd})$
$T=\sum_{i=1}^{n} T_i\ e(s_k H_1(m_i)$
$i=1+2+\cdots+n$
$T=\sum_{i=1}^{n} T_{i=1+2+\cdots+n}$
$(M, 6)$
$(T, 6)$
CHALLENGE(E, Req, θ)
REQUEST(E, Req, θ)
RESPONSE(E, θ, R)
$R=aP, E=a\oplus R, Req=(E\oplus ID)\|a, \theta=a\oplus H(Req\|R)$
Airborne Control & command Platform
Unmanned Aerial Vehicular Networks (UAVNs)/FANET
Powerful Intelligence Computer System (PICS)

FIGURE 1. Military drone system architecture.

B. FLYING ZONE DESCRIPTION

Drones must be deployed in a specific flying zone, and their clusters are also be operationalized in pre-determined flight zones. PICS or AC2P can access a designated drone from some location and can detect unauthorized/compromised drones of any type. When a drone is in a specified zone, PICS/AC2P regulates its flight and authenticates its legitimacy. Confirming a legitimate drone's authenticity, integrity, and confidentiality or identifying an illegal drone in the flying zone can also easily be detected due to the intermediary agent (AC2P/PICS). Garibi *et al.* [11] explained the flying zone strategy for a vast terrestrial space in detail. We recognize their zone strategy for delivering neutrality, modularity, and uniformity so that a drone can broadcast information with AC2P/PICS and another drone securely. Also, to cover a larger area, such as a long border, the AC2P/PICS must be logically interacting. This strategy will supervise multiple UAVs in a cluster at different flying zones, traffic, shifting a UAV from one flying zone to another and providing mandatory statistics. Gharibi *et al.* [11] also explained the handover tactics when a drone turns its location from one to another flying zone.

C. NOMENCLATURE

The different notations used in this paper are described here in this subsection, as shown in Table 1.

TABLE 1. Notations and its descriptions.

Notation	Description
$R_e^{(ob)}$	Observed Resource
$R_e^{(al)}$	Available Resource
N, dN	No. of resource, rate of change of resource
L, dL, L_o,	Link, rate of change of link, Link at the origin,
L_P	present link
t, t_x, $t^/$	Future, current time slot, last recorded duration
λ	Resource survivability
μ	network's periodicity
dt_x	Change in current time
s	Private key of the system
P_{pub}	Public key of the system
P	Public key
ID_d	Drone's Identity generated initially
Id_{IDd}	Drone's Private Identity
t	Timestamp
χ_{IDi}	Drone's secrete values
Q_{IDd}	Drone's secret key
$Q_{IDd}^/$	Drone's public key
$TempK_{IDd}$	Temporary key for the signer
σ	Signature
RD_d	Reconnaissance Drone
h	Collision free one-way hash function

D. TRAJECTORY DESCRIPTION

Using Dubin's route theory to establish a trajectory to materialize multiple UAVs and optimize the contact relay between UAVs and PICS/AC2P that can centrally administer the entire mission. Various strategic constraints should be considered, like planning, AC2P/PICS position, flying zone, and UAVs. But synergy is mandatory amongst all the participants for efficient and effective channel accessibility and minimum communication overheads. It is worth mentioning that the said communication is synchronous; AC2P/PICS must check every connection (drone → to → drone or drone → to → AC2P or drone → to → PICS) to qualify for a complex military operation. According to [12], [13] and [14], the path is allocated only to authorized participants. By doing so, the network too dynamically change its topology depends upon " *who access whom*" that can be obtained using semi-elasticity as given:

$$\mathcal{F}_{\mathrm{s}}^{(\mathrm{R})} = \frac{\mathrm{d}\ln \int (\mathrm{R}_{\mathrm{e}}^{(0\mathrm{b})})}{\mathrm{dN}} \tag{1}$$

where $f\mathrm{R}_{\mathrm{e}}^{(\mathrm{ob})}$ means change in topology without adding any additional resource, while $f\mathrm{R}_{\mathrm{e}}^{(\mathrm{ob})}$ means change is made with the addition of allowed resource. According to [14], (1) is deduces as;

$$\mathcal{F}_{\mathrm{s,i}}^{(\mathrm{R})} = \frac{d\ln \int i\mathrm{R}_{\mathrm{e}}^{(0\mathrm{b})}}{\mathrm{dL}} \tag{2}$$

where L = no. of links on ith drone

$$\mathrm{fi}(\mathrm{R}_{\mathrm{e}}^{(\mathrm{ob})}) = \int_0^t \mathrm{t_x} \frac{\mathrm{R}_{\mathrm{e,P}}^{(\mathrm{ob})}}{\mathrm{R}_{\mathrm{e,E}}^{(\mathrm{ob})}} \mathrm{dt_x} \tag{3}$$

$\mathrm{t_x} \leq \mathrm{t}$, whereas $\mathrm{t_x}$ current time-slot, $\mathrm{R}_{\mathrm{e,P}}^{(\mathrm{ob})}$ means present values for ith drone and $\mathrm{R}_{\mathrm{e,E}}^{(\mathrm{ob})}$ is expected values for the available resources and is given as:

$$\mathrm{R}_{\mathrm{e,E}}^{(\mathrm{ob})} = \frac{\text{Resources} \times \text{No.of drones}}{\mathrm{N}^/} \tag{4}$$

Resource survivability is given as

$$\mathrm{R}_{\mathrm{e,P}}^{(\mathrm{ob})} = \mathrm{R}_{\mathrm{e,ob}}^{(\mathrm{ob})} \mathrm{e}^{-\lambda \mathrm{t_x}} \tag{5}$$

Macaulay's equation [14] is a guarantee for the current value of the additional resource in the topology, as given:

$$\mathrm{R}_{\mathrm{e,P}}^{(\mathrm{ob})} = \int_0^t \frac{\mathrm{t_x}}{\mathrm{L_p}} . \frac{\mathrm{L_0}}{(1+\frac{\lambda}{\mu})^{\mu \mathrm{t_x}}} \mathrm{dt_x} \tag{6}$$

Next, network management over a specified channel can enhance connectivity, is given as:

$$\Delta \mathrm{M}_{\mathrm{f}}^{(\mathrm{D})} = \mathcal{F}_{\mathrm{s,i}}^{(\mathrm{R})}(\mathrm{t}) - \mathcal{F}_{\mathrm{s,i}}^{(\mathrm{R})}(\mathrm{t}^/) \tag{7}$$

According to (6), channel connectivity as:

$$\begin{aligned} &\min(\Delta M_f^{(D)}, \quad \forall \cup,\ \forall E,\ N^/ \neq 0, \\ &\min\left(\frac{\mathrm{R}_{\mathrm{e,P}}^{(\mathrm{ob})}}{\mathrm{R}_{\mathrm{e,E}}^{(\mathrm{ob})}}\right), \quad \forall \mathrm{L}, \\ &\mathrm{t} \leq \mathrm{t_x} \leq \mathrm{t}, \quad \mathrm{R}_{\mathrm{e,P}}^{(\mathrm{ob})} \geq 0, \text{ and } \mu \neq 0,\ \lambda \geq (\mathrm{t_x} - \mathrm{t_o}). \end{aligned} \tag{8}$$

E. THREAT MODEL

In the context of network security, a threat means any potential danger to the IoD architecture using any wireless network (FANET/UAVN) that can exploit a vulnerability to breach system security. As the communications between all the participants are performed via a public network (wireless communication) channel, all known attacks are possible because the adversary is much strong nowadays. The possibilities [15], [16] of different kinds of attacks are listed as i) can de-authenticate one or all drones, ii) might inject false information on the exchanged information, iii) alter it at any stage, iv) disturbs the privacy of a drone, v) find the location of a drone and launch a physical attack on it, vi) can desynchronize the shared secrets, vii) spoof AC2P/PICS for a wrong decision, and viii) might mislead AC2P/PICS for a wrong decision by changing the coordinates' intelligence command regarding the suspicious target. The adversary cannot compromise the fully trusted entity PICS/AC2P at any stage, while all others are partially trusted entities. The different domains that identified for the possible threat are as under:

1) SIGNAL JAMMING THREAT

By jamming the signal, the adversary could disable the drone's link with the PICS/AC2P. An adversary obtains and monitors the critical GPS signals required by drones for data transmission; it then creates and regulates a fake GPS signal using Ettus-USRP, which has the same frequency and bandwidth as the real one. It aligns fake and reliable signals, increases the frequency of the fake signal to block the reliable signal, and then uses it to launch a GPS spoofing/jamming assault on both PICS/AC2P and drones.

2) FLIGHT-CONTROLLER THREAT

This threat is associated with falsifying factual data, disclosing data, and damaging the IoD infrastructure. This threat launched by an adversary by controlling all the services provided by ground-control-station for air traffic controllers; instead of GCS, the adversary directs the drone and fully manages it in the airspace; and offers advisory services to drone in the air non-controlled airspace.

3) SIGNAL SPOOFING THREAT

The adversary can mislead the drone for a wrong decision. The intelligence data has a command sent by PICS/AC2P towards a drone; the attacker can catch it, after possible injection; mislead the attacking drone for a wrong decision.

4) FALSE DATA INJECTION THREAT

The attacker can manipulate the data sensed by the embedded sensor for a different physical phenomenon like troop movement, border surveillance, suspicious spot monitoring etc. This is a dangerous and undetected threat launched by an adversary to calculate the state variables and values.

5) ROUTING CONTROL THREAT

The adversary also can launch grey-hole, wormhole and black-hole attacks and constantly monitor the data flood by launching a rushing attack on it.

6) UNAUTHORIZED ACCESS THREAT

The attacker can also have a chance to modify the different parameters of the legal entity in the IoD environment. The adversary gains access to legitimate communication among drone and AC2P by bypassing a system's security protections in this threat.

7) PRIVACY THREAT

An adversary may use aircrack-ng software to extract the drone's coordinates and other helpful information from stolen data packets, airodump-ng to detect signal power, store and filter it for future attacks, and airplay-ng to disrupt the synergy. By sending disassociation packets regularly, the attacker might disrupt the entire network's regular operation.

8) PHYSICAL CAPTURE THREAT

An adversary can physically capture a drone. If a drone is lost or if an adversary can transcribe or kill it, the adversary can target it to gain access to the information contained in the drone's memory. After that, he or she may reveal the encrypted data and begin authentication with AC2P, PICS, or any other drone in the cluster or any other.

9) TRAFFIC ANALYSIS THREAT

The adversary will analyze drone traffic in order to derive useful information from IoD devices and networks. The traffic is made up of packets sent and received by the drone and AC2P/PICS. The forensic examination of traffic packets reveals sensitive information. The drone is fitted with sensors that capture data from the real-world environment on the battlefield, stored in packets containing helpful information. The adversary studied it to see if it could be used as a weapon.

10) ACCESS CONTROL THREAT

An attacker can be aware of all the rules, procedures, and communication channels available to a legitimate participant. He/she then has access to change rights, approvals, authorization, and authentication, resulting in significant losses.

11) IDENTITY SPOOFING THREAT

An adversary can effectively impersonate a legitimate entity by spoofing the identity of a real drone. After that, he or she has power over the public communication channel.

F. MOTIVATION AND CONTRIBUTIONS

As FANET/UAVN is an infrastructure-less, resource-less and self-organizing network, FANET$\subseteq$MANET but the security features being operationalized for MANET cannot apply to FANET/UAVN. Similarly, the available threats caused to the IoD environment don't include all security features. By mitigating all the associated threats to such a low-latency network, there is a dire need for a robust security mechanism to guarantee security against the known loopholes attached to IoD deployment military drone and data transmission over a public channel. Although numerous authentication protocols were proposed for IoD by different researchers using different techniques, no one claims with full confidence about a foolproof security mechanism. These schemes are either handicapped from a privileged insider, stolen-verifier attacks, or having outdated data transmission and designed flaws. The poor design can emerge that these cryptographic techniques don't work against many vulnerabilities because they can easily be targeted and malfunctioned by attackers. Therefore, we attempt to propose an identity and aggregate signature-based authentication protocol based on [17]–[20] that ensures IoD deployment military drone information broadcasting security, efficient access by a legitimate user, and high availability. The key contributions of this research paper are as under:

i. We have used pairing cryptography for generating public-private key pairs in protecting data from a strong adversary. While the computational Diffie-Hellman key exchanged method is used for communicating keys among all the participants of IoD.

ii. These protocols/frameworks are free of forgery, privileged insider, collation, and stolen-verifier attacks. It doesn't have an outdated data transmission flaw.

iii. A malicious node/drone cannot misguide a legitimate drone or AC2P/PICS for a wrong decision.

iv. If an adversary physically captures a drone, it cannot figure out the internal credentials for a possible replay, side-channel, and DoS attacks.

v. Each drone can individually check the validity of the aggregate signature to guarantee a GPS spoofing attack.

vi. Due to the usage of pairing cryptography and the Computational Diffie-Hellman Problem (CDHP), the identities generated and used for different IoD participants in the proposed authentication protocol are verifiably unforgeable.

vii. The aggregate signature length is equivalent to the independently generated signature, which offers better performance and minimum time complexity or computation cost.

II. PRELIMINARIES

The purpose of this section in the research paper is to attempt a concise definition of some indispensable cryptographic approaches which are needed for securing drone communication in the military environment. We discuss some mathematical background and associated preliminaries necessary for designing security frameworks, scrutinizing the security, and evaluating its performance. The other aspect of this section is to offer some scoop regarding pedagogic cryptography, public-key cryptosystem, certificateless cryptography, and associated computational complex problems. Finally, we have presented a concise description of the provable security. This foundation is, by no means, exhaustive so that it is just used to speed up drone application in both military and civilian domains.

A. DIGITAL SIGNATURE

An algorithm [21] used for information security having the following three sub-algorithms:

Gen: By giving some security parameters (λ), this algorithm outputs public-private key pairs (P_{pk}, P_{sk}) i.e. $Gen(\lambda) \leftarrow \mathrm{P_{pk}}, \mathrm{P_{sk}}$

Sign: By giving P_{sk} and message m, this algorithm output a signature σ i.e. $Sign(m, P_{sk}) \leftarrow (\sigma)$

Verify: By inputting $\mathrm{P_{pk}}$, message m, and σ, the output is either 1 accept or 0 reject, i.e.

verify $(m, \sigma, P_{pk}) \leftarrow 1(\,valid)\;\; or\; 0\;\;(invalid)$

Example: Let $\mathrm{M} = \{\mathrm{m_1, m_2, m_3}\}$ and $\mathrm{S} = \{\mathrm{s_1. s_2, s_3}\}$, The signature algorithm produces $\mathrm{S_A} = \{(\mathrm{m_1, s_1}), (\mathrm{m_2, s_2}), (\mathrm{m_3, s_3})\}$ while the verification algorithm produces $\mathrm{V_A} = \{(\mathrm{m_1, s_1}), (\mathrm{m_1, s_2}), (\mathrm{m_1, s_3})\}, \{(\mathrm{m_2, s_1}), (\mathrm{m_2, s_2}), (\mathrm{m_2, s_3})\}$ and $\{(\mathrm{m_3, s_1}), (\mathrm{m_3, s_2}), (\mathrm{m_3, s_3})\}$ as shown in Fig. 2. Only valid signature will be accepted, the other entire signature pairs which are not valid shall deemed to be rejected.

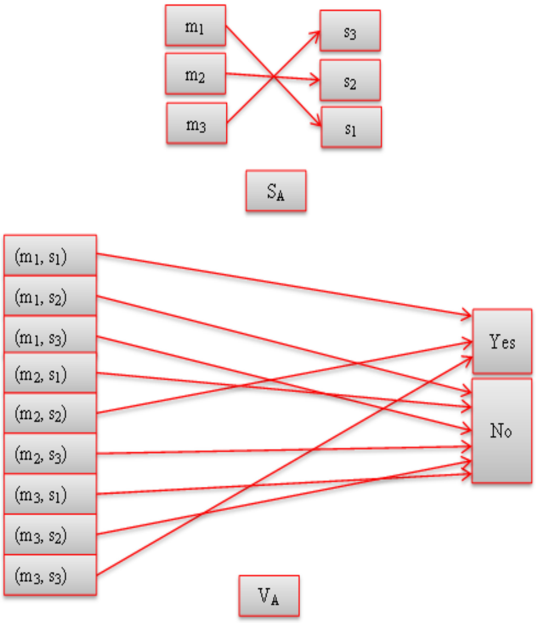

FIGURE 2. Digital signature scenarios.

B. BILINEAR MAPPING

Suppose two groups, namely $\mathrm{G_1}$ and $\mathrm{G_2}$, of order prime q, then $\widehat{\mathrm{e}} = \mathrm{G_1}$ x $\mathrm{G_1} \rightarrow \mathrm{G_2}$ called bilinear pair/map [22] having the following features:

i. *Non-degeneracy*: If $\mathrm{G_1}$ is a multiplicative group of generator $\mathrm{g_1}$ and $\mathrm{g_2}$ of order prime q, then $\mathrm{g_1, g_2} \in \mathrm{G_2}$ s.t. $\widehat{\mathrm{e}}(\mathrm{g_1, g_2}) \neq 1$

ii. *Computability*: The existence of $\mathrm{g_1, g_2} \in \mathrm{G_2}$ means there must be an algorithm available for computing the pair $\widehat{\mathrm{e}}(\mathrm{g_1, g_2})$.

iii. *Bilinearity*: For all $\mathrm{g_1, g_2} \in \mathrm{G_2}$ and $\mathrm{a, b} \in \mathrm{Zq}^*$, these are valid tuples $\widehat{\mathrm{e}}(\mathrm{g_1^a, g_2^b})$, $\widehat{\mathrm{e}}(\mathrm{g_1, g_2})^{\mathrm{ab}}$, $\widehat{\mathrm{e}}(\mathrm{g_2, g_1})$, and $\widehat{\mathrm{e}}(\mathrm{g_1}, \mathrm{g_1} + \mathrm{g_2})$.

Inventive protocols for tasks like one-round three-party key agreement, identity-based encryption, and aggregate signatures can be constructed using the bilinear map process.

Three parties share the secret M = xyzP; the bilinear method provides a secure way to the condition that if the key pairs xP, yP, zP, xyP, xzP and yzP are computationally hard for an adversary to calculate. While the following properties of pairing cryptography can easily be proved:

i. $\widehat{e}(P, \infty) = 1$, and $\widehat{e}(\infty, P) = 1$

ii. $\widehat{e}(P, -Q) = \widehat{e}(-P, Q) = \widehat{e}(P, Q)^{-1}$

iii. $\widehat{e}(xP, yQ) = \frown e(P, Q)^{xy}$ for all $x, y \in Z$

iv. $\widehat{e}(P, Q) = \widehat{e}(Q, P)$

v. $\widehat{e}(Q, g_1) = 1$ for all $g_1 \in G_1$ and $P = \infty$.

If $\widehat{e}$ is represented as a bilinear map/pair, then the Bilinear Diffie-Hellman Problem (BDHP) on xP, yP, zP can be computed $\widehat{e}(P, P)^{xyz}$.

C. PUBLIC KEY INFRASTRUCTURE (PKI)

There is no need to exchange key privately in conventional public-key cryptography but must be adequately managed each time. During the whole process, securely and efficiently, management of public/private keys pair is challenging. For such purpose, cryptographers [23] developed scenarios in which key pair is created, efficiently utilized it (public access for encryption and private for decryption), and finally, the key pairs invalidated. The invalidation phase has happened when the life cycle of the key pair becomes wind-off or compromised. This methodology is called public key infrastructure (PKI). In PKI, the key pair must be available to peers to verify its authenticity, validity and confirm other security features. If the session of one key becomes expire and declared invalid, PKI can manage the null key.

D. CERTIFICATELESS CRYPTOGRAPHY [24]

A novel idea aims to realize the benefits of identity-based cryptography without the need for key escrow problems. This technique bridges the gap between identity-based and PKI-based cryptography and eliminates identity-based cryptosystems (ID-PKC). Its encryption process does not necessitate any pairing computation, substantially lighter and quicker. It outperforms other cryptographic techniques in terms of computational performance, supports public keys that humans can remember, provides randomness in key construction, and re-use for the sake of understanding. It has a high level of unforgeability, solves issues with encryption methods, no need to use a certificate to connect the identity to the public key since any string, including identity, can be used as a public key, and keys can be revoked for a fixed time [24].

E. COMPUTATIONAL DIFFIE-HELLMAN PROBLEM (CDHP) [25]

In 1976, Diffie and Hellman [25] demonstrated an elegant, efficient and reliable technique for establishing a secure key exchanging among two legitimate peers. Their idea is as under:

Let a cyclic group G of random numbers of order prime, and g be a generator of G, then: Peer A chooses x, and peer B chooses y. A publishes $P = g^x$, B published $Q = g^y$; A computes $L = Q^x$ and B computes $R = P^y$. Finally, L, Q are public, and $L = Q^x = P^x = g^{xy}$ remains secret and is termed as Diffie-Hellman, shared private key. This is hard for an adversary to find or compute at any stage, called Computational Diffie-Hellman Problem (CDHP).

F. BIG O NOTATION

It's the most widely used metric for determining time complexity. It expresses a task's execution time regarding the number of steps taken to complete the protocol or standard symbols such as big-O to indicate execution time complexity and computation cost [26]. There are numerous forms of big-O notations; some of these are described as under:

- $O(n)$ = Linear task's run time
- $O(n^2)$ = Quadratic task's run time
- $O(2^n)$ = Exponential execution time complexity
- $O(\log n)$ = Logarithmic Time complexity

The other big-O types are beyond the scope of this research.

III. RELATED WORK

Kettering Bug was a person in the US Navy who first flew a drone in 1918 but was not deployed for war. Elmer Sperry led a project and invented a drone, which is said to be the founder of a drone. Initially, a drone was deployed for three main tasks: dangerous, dirty and dull, and was called the three-D operations.

The first identity-based cryptographic protocol was presented by Shamir [27] in 1984. He was the founder of identity and digital signature for message authentication. He said that a public key could easily be generated from a user's unique identity without any extra certificate. In contrast, the first aggregate signature-based protocol was presented by Boneh *et al.* [28] in 2003 by aligning n signatures on n messages for n signers. The signature of [28] was worked for two parties, but it couldn't resist forgery attack when users' number increased.

Srinivas *et al.* [29] demonstrated a mechanism consisting of five entities, i.e., Ground-Station-Server (GSS), flying zones (FZ), drones (D), external users (MU), and a control room (CR). They said that FANET is a low latency network, and limited bandwidth needs more attention for its security in performing any sensitive task. FANET/UAVN is suitable for drone technology in the IoD environment to track suspicious spots and location identification. FANET/UAVN is open network communication, and an adversary can track a drone, maliciously act to interrupt its services, and physically capture it. To make it protected from such a powerful adversary, [29] said that drones are exposed to potential threats because external users can operate drones from anywhere. However, the mechanism proposed by [29] is suffering from stolen-verifier, tractability attacks, and doesn't facilitate anyone for dynamic addition of a drone.

Chaudhry *et al.* [30] tackled forgery attacks for a complex system by designing three-factor biometrics-based authentication schemes. They mitigated the privacy, location disclosure, and traceability concerns for the end-user in distributed cloud computing. Besides this, several other attempts have also been made to achieve the system's protection and privacy. But without strong authentication and privacy-preserving, no one can guarantee secure communication. The researchers of [30] have demonstrated that some identity-based authentication protocols are now vulnerable in distributed mobile cloud computing environments, especially suffered from forgery attacks. Since any adversary with access to only public parameters may forge the secret parameters of a legitimate service provider.

Chen *et al.* [31] proposed an ECC-based security framework for small UAVs to work collaboratively because FANET in IoD lacks fixed topology, challenging to make it secure. Their framework consists of manufacturers (UAVs), a trusted authority centre (TAC), a player (mobile device), and a ground-control station (GSC). UAVs, mobile-user, and GSC first registered with TAC, player, and manufacturer mutually authenticate each other and then deployed in IoD. They used the computational Diffie-Hellman key exchanged technique to advance the security of random keys among participants. But forgot to mentioned drone addition, revocation, and reissue phases. Also, their scheme is suffering from a privileged insider, stolen-verifier, and outdated data transmission flaw. Cho *et al.* [32] demonstrated that information security is crucial for drone technology before operationalizing it for a complex operation. They suggested that the drone, operator, and station must first register with the certificate authority, and then giving permission in the IoD environment for complex task, but protocol is lacking dynamic drone addition, revocation, and reissue phases.

Seo *et al.* [33] confessed the secure transmission of information between drones and GCS, a white-box encryption method efficiently delivered food, goods, and medicine and used in agricultural land monitoring. Farash *et al.* [34] proposed a secure and confidential data transmission for heterogeneous WSN enabled IoT can also be feasible in the IoD environment. Farash *et al.* used a simple symmetric encryption/decryption method to design a highly efficient scheme. Al-Turjman *et al.* [35] presented protocol for public cloud data security in IoT enabled equipment using MANET. They used bilinear pairing cryptography in combination with the ECC technique. Also feasible in IoD deployment drone technology. Jiang *et al.* [36] presented a three-factor key-agreement protocol for network-enabled devices using WSN. They claim that the Rabin cryptosystem is fast and secure than RSA and ECC; therefore, they named it 3FARC (Three-Factor Rabib Cryptosystem) technique. Ever *et al.* [37] demonstrated an authentication scheme for an e-health-care system using WMSN. An improved elliptic curve cryptographic system was used and claimed that their protocol is feasible against password guessing and stolen verifier attacks. Cheon *et al.* [38] urged that when an IoD environment's published homomorphic encryption-based authentication scheme has been presented; their method is innovative for drone deployment in different environments.

Zhang *et al.* [39] designed a privacy protection protocol for grid computing has been presented to guarantee secure communication between service providers and smart objects. Their scheme is also feasible for 5G enabled drones. Teng *et al.* [40] demonstrated an identity-based ECC certification method was used to design a three-factor authentication scheme for working in Unmanned Aerial Vehicular Networks (UAVNs) enabled vehicles (drones). They said that RSA couldn't be feasible for such a resourceless environment, as it provides a log certification facility. Feng *et al.* [41] proposed identity-based lightweight authentication for the distributed computing environment. Ali *et al.* [42] cryptanalyzed the TCALAS of Srinivas *et al.* and proposed an improved mechanism for drone monitoring smart city that works for the different physical phenomenon and named it iTCALAS. Ko *et al.* [43] proposed a hybrid cryptographic based protocol for IoD deployment military drone. Encryption/Decryption, Elliptic Curve Digital Signature Algorithm and Hash Message Authentication Code were used for designing the security framework and claimed that their protocol is guaranteed for the security of communication security amongst drone-to-drone instead of drone-to-GCS. Besides, they verified the security of their proposed using BAN authentication logic and Scyther software toolkit. To monitor a large geographic region Utsav *et al.* [44] proposed a UAV network-based technique in the military domain that utilized radar and antenna for beam steering to detect the unwanted signal. Their proposed scenario is a significant contribution to the knowledge field, but it couldn't perform well for UAVs working for a complex tactical operation.

Furthermore, Shen *et al.* [45] presented an identity-based aggregate signature authentication scheme grounded on pairing cryptography. Their scheme consisted of setup phase, key-generation, signing, aggregation and verification phase. The cryptanalysis result of Shen *et al.* [45] scheme shows that it is suffered from a ***forgery attack***. Because, if a challenger says C picks a security parameter W and runs a setup algorithm, C not only calculates the valid $param$ of the user but also retrieve a valid $tuple$.

Similarly, Hong *et al.* [46] presented an identity-based aggregate signature authentication scheme for UAVs working in the cluster and are possibly to be deployed in warfare battle filed or for border surveillance. Their strategy consisted of setup, request, response, aggregate, and verification phases. However, after the extensive analysis, their scheme is suffered from the following security vulnerabilities:

1) COLLATION ATTACK

Suppose adversary A identifies the frequency and bandwidth of a legitimate signal, A generates spoof signals of greater strength and higher intensity and sends $REQ = Area||T_A$ message over it. It overlays the system's request signals used for suspicious target monitoring. And let challenger C chooses a random number r, calculate public key $R^* = rP$, obtained private key s and given back it to the A. A recycled it for calculating $\theta^* = sH(REQ||R^*)$ and sends a fake request towards a valid user U_n. Upon receiving θ^* for m_i^*, U_n is forced to verify $e(\theta^*, P) = e(H(REQ||R^*), P_{pub})$, which in turn gained for a potential replay attack. Because the user at this stage led to the wrong estimation of the current position and predicts wrong coordinates, promptly locks the target or suspicious spot and informs the base system for performing an action called ***collation attack***. Due to this alignment of a forged signal on an original signal, the adversary successfully accesses the internal credentials of the system. Therefore, the scheme [46] is suffering from a ***collation attack***.

2) FORGERY ATTACK

Suppose a challenger C obtained system public key P_{pub} and *param and* returns it to A. A chooses a random number r, calculates $R = rP_{pub}$, after polynomial times attempts by A and gets system secret key s. He/she can quickly produce user's identity ID_i and computes user's public key Q_{Idi} and sends a request message $REQ||R$ towards user. Upon receiving $REQ||R$ message from the adversary, the user calculates P_{pub} from $REQ||R$ and generates a fake signature $\sigma = sH(REQ||R)$, sends towards the base station for verification, the system at the moment is forced to validate it. It means that adversary A successfully launched a forgery attack or forges the signature and obtained a valid signature. Therefore, scheme [46] is suffering from a ***forgery attack***.

3) PRIVILEGED INSIDER ATTACK

Actually, the identity in the user is $P_{pub} = sP$, and in the server, it is $P = rP$. Here, P_{pub} matches P. A newly key, say $T_i = t_iP$ is built temporarily for the cluster head and is exposed to the server; the privileged insider can easily identify this public parameter (key) of the system. And then masquerade the user in the request message from the server and impersonate the other users to the defrauded cluster head.

IV. PROPOSED SOLUTION

The Powerful Intelligence Computer System (PICS) registers Airborne Control and Command Platform (AC2P) and each drone (reconnaissance and attacking) before deploying to the area for the tactical task. It is worth mentioning that the bilinear mapping technique is used for calculating the keys (both public and private keys). Suppose G_1 and G_2 are two groups of order q (prime number). Let P be a generator of G_1 and $|G_1| = |G_2|$, then $e : G_1 xG_1 \rightarrow G_2$ called bilinear pairing/map that satisfies: $e(\tau P_1, pP_2) = (P_1, P_2)\tau p$, $e(P, P) \neq 1$. If P_1 and $P_2 \in G_1$, a successful algorithm exists to calculate $e(P_1, P_2)$. And the Computational Diffie-Hellman Problem (CDHP) can be applied for calculating the secret key to make it hard for the adversary when forging some information: The unforgeability can be confirmed subject to the use of Pairing Cryptography, Discrete Logarithmic Problem (DLP) and Computational Diffie-Hellman Problem (CDHP) for key generation and exchanging among each participant by AC2P/PICS, correspondingly.

A. GLOBAL SETUP PHASE

The availability of security parameters λ and secret key s, the algorithm in AC2P/PICS randomly picks a large number P from G_2, and computes $P_{pub} = sP$, selects collision free four hash functions i.e. h_1: $\{0, 1\}^*xG_2 \rightarrow Zq^*$, h_2: $\{0, 1\}^*xG_2xG_2xG_2 \rightarrow Z_q^*$, $h_3 = \{0, 1\}^*xG_2xZ \rightarrow Z_q^*$ and h_4: $\{0, 1\}^*x\ \{0, 1\}^*xG_2xG_2xG_2xG_2 \rightarrow Z_q^*$ and finally the algorithm output $pram = \{h_1, h_2, h_3, h_4, P, G_2, P_{pub})$.

Remark: By inputting P, xP, yP, zP, whereas $x, y, z \in Zq^*$, the Bilinear Diffie-Hellman (BDH) can calculate $\hat{e}(P, P)^{xyz}$.

Remark: By giving public key (P), private key pair xP, yP, zP whereas $x, y, z \in Zq^*$, the Computational Diffie-Hellman problem (CDHP) can calculate xyP, xzP, yzP or $xyzP$.

Remark: By giving $P, uP,$ *or* vP, uvP, whereas $u, v \in Zq^*$, the Inverse Computational Diffie-Hellman problem (ICDHP) can calculate $u^{-1}P, v^{-1}P$ or $(uv)^{-1}P$.

Remark: By giving P, rP, sP, rsP whereas $r, s \in Zq^*$, the modified Inverse Computational Diffie-Hellman problem (mICDHP) can calculate $(r + s)P$, and $(r + s)^{-1}P$.

B. FRAMEWORK FOR ATTACKING DRONE

AC2P and PICS are strong intelligence commuting power, much storage capacity, and no one can compromise their trust. It can investigate, coordinate and process the attacking drones for maritime services. Secondly, without a cluster head in the attacking drones, such a sensitive task cannot perform well, so we must declare one drone as a cluster head with some communication and coordination abilities (synergy) with AC2P/PICS. It signs different individual signatures received from other drones, includes its own signature and sends toward AC2P/PICS for decision. And the last thing is all the remaining drones, which have limited processing capability and less storage capacity and limited battery power, are commanded directly by AC2P/PICS or cluster head to fulfill a tactical task. Generally, we propose the following scenarios for attacking drones.

i. **Partial Private Key Generating Phase**: In this phase AC2P's *param*, public-key P_{pub}, and dron's identity ID_d computes partial private key $Id_{IDd} = H(ID_d)$ i.e. the AC2P randomly selects a number $n \in Z_q{}^*$ and computes $R_{IDd} = nP$ and $H_{IDd} = h1(ID_d, R_{IDd})$, $(P_{pub})_{IDd} = (n \oplus s)H_{IDd}$ and rebound $Id_{IDd} = ((P_{pub})_{IDd}, R_{IDd})$.

ii. **Actual Key Generating Phase:** Next, *param*, ID_d and timestamp t can create drone's values χ_{IDd}, drone's secret key $Q_{IDd} = H(Id_{IDd})$ and drone's public key $Q^{/}_{IDd}$, which in turn generates the corresponding private and public key pairs $(Q_{IDd1}, Q^{/}_{IDd1})$, $(Q_{IDd2}, Q^{/}_{IDd2})$, ………………., $(Q_{IDdn}, Q^{/}_{IDdn})$ for different drones.

iii. **Actual Key Updating Phas*e:*** In this phase, the public parameters *param*, identity ID_d, time t, and Q_{IDd} can update the real drone's key Q_{IDd}.

iv. **Signer Temporary Key Generating Phas*e:*** The security parameters *param*, ID_d, t, and Q_{IDd} create the temporary key for signer (cluster head drone) $TempK_{IDd}$.

v. **Signature Generating Phase**: Security parameters *param*, identity ID_d, timestamp t, and $TempK_{IDd}$ along with message M, generate aggregate signature σ.

vi. **Signature Verification Phas*e:*** AC2P upon receiving *(M, σ)* tuple verify the internal credentials in it, i.e. *param*, ID_d, Q_{IDd}, (Q_{IDd1}, Id_{IDd2}) and confirms its validity *(M, σ)*, if found true secure communication initiate, else, discard and consider a potential replay attack.

C. FRAMEWORK FOR RECONNAISSANCE DRONE

We propose the following security mechanism for reconnaissance (investigating) drones in our system model.

1) REQUEST PHASE

Initially, AC2P chooses a random number a, whereas $a \in_R Zq^*$, computes $R = aP$, $E = a \oplus R$, $Req = (E \oplus ID_i)||a$, $\theta = a \oplus H(Req||R)$ and submits *REQUEST(E, Req, θ)* towards reconnaissance drone RD_i where i = 1, 2 . . . . n).

2) CHALLENGE PHASE

Upon receiving the *REQUEST(E, Req, θ)* message, the drone (RD_i) first retrieves the identity from the message and checks whether it is valid as per the identity table in its memory? If not hold, it denies the message; otherwise, the drone (RD_i whereas i = 1, 2 . . . . n) extracts a random number b and relays a challenge message towards AC2P to confirm the legitimacy of a peer who sent the *REQUEST(E, Req, θ)* to whom, by sending a message *(CHALLENGE(E, Req, θ))* whereas $Req = (E \oplus ID_i)||b$ and $E = b \oplus R$, $R = bP$.

3) RESPONSE PHASE

Upon receiving the *CHALLENGE(E, Req, θ)* message from RD_i, AC2P verify the message integrity by computing $e(\theta, P) = e(bH(Req||R), P)$, $e(\theta, P) = e(H(Req||R), bP)$, $e(\theta, P) = e(H(Req||R), P)$ and confirms $e(\theta, P)? = e(H(Req||R), P)$. Finally resubmits a *RESPONSE(E, θ, R)* message towards RD_i. Where each drone (*RD*) once again checks identity in the *RESPONSE(E, θ, R)* message and hash code $H_1(m_i)$ for message m_i. RD_i randomly selects another large integer value $c_i \in_R Z_q^*$, creates signature $\sigma_i = H_1(m_i).d_{Idi} + c_iR$, $T_i = c_iP$ and submits it to the cluster head $RD\ sig_i = \sigma_i ||T_i ||m_i$. Here each drone can individually check the validity of the aggregate signature which is a guarantee for GPS spoofing attack.

4) AGGREGATOR PHASE

Upon receiving the n-1 signatures $\{sig_1, sig_2, sig_3 \ldots sig_{n-1}\}$ of $\{RD_1, RD_2, RD_3, \ldots\ldots\ldots\ldots, RD_{n-1}\}$, the cluster head aggregates all the received signatures and makes an aggregate of it along with its own signature and form aggregate signature $\mathrm{sig_n}$. The final aggregate signature is built as $\sigma = \sum_{i=1}^{n} \sigma_i$, $T = \sum_{i=1}^{n} T_i$, $\mathrm{e(s_kH_1(m_i)}$ for message m_1, m_2, m_3, *up to* m_n, and sends (σ, T) towards AC2P/PICS, as show in module 1.

5) VERIFICATION PHASE

Upon receiving the aggregate signature (σ, *T)*, AC2P/PICS validate $\mathrm{e(s_kH_1(m_i)}$ tuple in σ for each message ranges from m_1, m_2, m_3, to m_n by calculating:

$$\begin{aligned}
\mathrm{e}(\sigma, \mathrm{P}) &= \mathrm{e(T, R).e}\left(\sum\nolimits_{i=1}^{n} T_i\,(m_i)\,Q_{ID_i}, P\right),\\
\mathrm{e}(\sigma, \mathrm{P}) &= \prod\nolimits_{i=1}^{n} e(s_kH_1\,(m_i)\,Q_{ID_i} + t_ibP, P),\\
\mathrm{e}(\sigma, \mathrm{P}) &= \prod\nolimits_{i=1}^{n} [e(s_kH_1\,(m_i)\,Q_{ID_i}, s_kP + e(t_iP, bP)],\\
\mathrm{e}(\sigma, \mathrm{P}) &= \prod\nolimits_{i=1}^{n} [e(s_kH_1\,(m_i)\,Q_{ID_i}, s_kP + e(T_i, R)],\\
\mathrm{e}(\sigma, \mathrm{P}) &= \prod\nolimits_{i=1}^{n} e(T_i, R). \prod\nolimits_{i=1}^{n} e(s_kH_1\,(m_i)\,Q_{ID_i}, s_kP),\\
\mathrm{e}(\sigma, \mathrm{P}) &= e\,(T, R)\,.\prod\nolimits_{i=1}^{n} e(H_1\,(m_i)\,Q_{ID_i}, P).
\end{aligned} \tag{9}$$

V. SECURITY DISCUSSION

In this section of the research, a pragmatic illustration about the security of the proposed scenarios has given in the form of theorems which are described as under:

A. SECURITY ANALYSIS BASED ON THEOREMS

We present the following theorems to prove the security of the proposed suite of protocols.

Theorem1: Let suppose an adversary has taken (t/, ε/) for generating a valid signature from n signatures. An adversary has a chance to calculate the secret key in it by using Group Diffie-Hellman Problem (GDHP), Co-Gape Diffie-Hellman Problem (CGDHP), Co-Gape Computational Diffie-Hellman Problem, (CCGDHP) [49] using the equation given as:

$$t \leq 2t' + 2C_G(2n + 2q_H + nq_s) \tag{10}$$

$$\varepsilon \geq \left(\left(\frac{\varepsilon'}{e}\right)(1 + q_s)\right)^2 \tag{11}$$

whereas $\mathrm{q_s}$ is the signature queries and $\mathrm{q_H}$ is a hash query in the signature

If the output query for a secret key is zero, it means the adversary is forging the valid signature. But the value for the query is ranged from 1 to n. Besides this, if the adversary received some output $\mathrm{tuple_1}$, $\mathrm{tuple_2}$ . . . . $\mathrm{tuple_n}$ and chooses any tuple from it, suppose $\mathrm{tuple_2} \in Zq^*$ and imagine $\mathrm{tuple_1}$ =1 with the system public key P, message $\mathrm{m_1}$, $\mathrm{q_H}$. Before sending the given message to the system, the adversary needs to get some output from the PICS/AC2P. He/She must flip a coin for a probable win. In this regard, he/she either get nothing (coin-value = 0) or real identities (ID_d, $\mathrm{ID_i}$) and get a valid output signature [*(M, σ)* or (σ, T)]. For doing so, an adversary needs n exponentiation for oracle to calculates hash queries $\mathrm{q_s}$, $\mathrm{q_1}$, $\mathrm{q_H}$ and n exponentiation for calculating n signatures (σ_1, σ_2, σ_3 . . . . .σ_n). But doing such a huge calculation adversary spent much time, later on when sending it towards a drone or AC2P or PICS, should be considered a potential reply or DoS attack because of a timestamp in the aggregate signature. Therefore, both the schemes show resistance to such an attempt of an adversary.

Theorem 2: Let H_1 and H_2 denote hash queries taken for random oracle model (ROM), and there exists an attacker A with the possibility ε for calculating a valid signature in time interval t. He has to develop a method for generating at most sign key Ks and chooses l_i for the H_1 hash query. Then there exists an algorithm B for the Computational Diffie-Hellman Problem (CDHP) of precedence $\varepsilon/ \geq (1/l_i) \geq \varepsilon$ in $t/ \leq t + (l_1 + l_2 + l_{key} + 4l_s)$. $\mathcal{T}_{SM}$ [whereas $\mathcal{T}_{SM}$ represents scalar multiplication]. The attacker can break the signing signature using this method. But as we have designed both the schemes using CDHP by calculating public key $P_{pub} = sP$ and set system parameters $pram = \{h_1, h_2, h_3, h_4, P, G_2, P_{pub})$ for attacking drone; and R= aP and set system parameters $pram = \{H, R, a, \theta, E, R_{eq}, aP)$ for reconnaissance drone. If B chooses $n \in [1, l_1]$ specifically for identity and gets $n \neq 1, Z_q^*$, sP query not rP, aP, and bP. He couldn't succeed for practical computation of either hash-query or key-query, identity, or any other tuple. Therefore, the proposed suite of protocols is unconditionally secure against such an attempt.

Theorem 3: Let a is a key for a drone RD_i and $a \in Zq^*$, an attacker A has the probability of inputting some values to an algorithm and get r is at most $1/[RD_i]$ is given as Prob[Algorithm($\sigma) = r]$. In contrast, σ is an aggregate signature for RD_n of Identity ID_n and ID_d, let the values input by an attacker are denoted by l *and* $l \in G$ and r, whereas $1 \leq r \leq l$. The attacker couldn't identify a legitimate drone's identity due to different sessions like public, private, partial private, actual, and so on are defined in a valid oracle $R_{IDd} = nP$, $P_{pub} = sP$, $R = aP$, and $c_i \in RZq^*$. In contrast, P is a 160-bits considerable number randomly picked from G_2 from the bilinear pair $G_1 x G_1 \rightarrow G_2$, which is impossible for an adversary to calculate. Therefore, the keys in the proposed suite of protocols are highly protected.

Theorem 4: Let their available two types of adversaries, Type-I adversary knows the public key of a drone; Type-II adversary knows the private key of the same drone. We claim with conviction that our suite of protocols will resist if anyone among these or both available. The reason, we have proposed seven (07) phases in our first protocol (setup, partial-private-key-extractor, actual-key-extractor, actual-key-updating, signer-temporary-key-generating, signature-generating, and signature-verification algorithms) and six(06) steps in the second protocol (configuration, request, challenge, response, aggregation, and verification). The adversary cannot pass to any successive phase of any of our protocols.

Suppose an adversary A chooses a security parameter λ and inputs it to an algorithm B. In that case, A's output is let suppose the public key P_{pub} or R (Type-I adversary). Might he/she can break the protocol subject to the condition that he/she must have maximum access power [50], which is impossible for the proposed protocols. For doing such a massive calculation, an adversary needs at least two to three years. After it, the system is promptly discarded and considered his/her request as a potential reply or by viewing an outdated data transmission attempt. Therefore, such an attempt is a wastage of time. Our scenario is secure for the probabilistic polynomial-time calculation by an adversary of either type – I, type – II, or both.

Theorem 5: Suppose a challenger C uses the setup algorithm and sends the public parameters to an adversary A. And A produces a random number and launches an attack to verify the drone's signature. In this case, the adversary's first attempt consists of concatenating a message M with various identities for different drones and sending it to the PICS/AC2P. He/she does not obtain the correct private keys and identity. Also, if an adversary issues a new set of criteria in his/her second attempt, subject to the condition that he/she is allowed to compute some signatures for different drones, if the signature delivering authority is deterministic, the adversary will never obtain a legitimate signature.

Theorem 6: If there exists no algorithm for an adversary to attempts polynomial times in solving the Computational Diffie-Hellman Problem (CDHP) either the additive group $(G_1, +)$ or the multiplicative group $(G_2, .)$, then the proposed mechanism is considered to be secure against Type-I attacks in the random oracle model [49].

Theorem 7: If there exists no algorithm for an adversary to attempts polynomial times for solving the Computational Diffie-Hellman Problem (CDHP) in either additive group $(G_1, +)$ or multiplicative group $(G_2, .)$, each participating party sign only one message during synchronous link establishment, then the proposed framework is secure against type-I attack in the random oracle model [49].

Theorem 8: If an aggregate signature is valid in hash values, a unique signature inside the aggregate signature is also valid [49].

B. RANDOM ORACLE MODEL (ROM) ANALYSIS

In ROM [49], if available an attacker A_I against protocol ρ with the advantage of δ, then there exists an algorithm $\mathtt{C}$ to solve the CDHP with the benefit is given as:

$$\geq \delta . \left(1 - \frac{q_{ppk}}{q\mathtt{C}.qH_0}\right) . \left(1 - \frac{q_{sk}}{q\mathtt{C}.qH_0}\right) . \left(\frac{1}{q\mathtt{C}.qH_0 - q_{ppk-p_{sk}}}\right) . \left(\frac{1}{qH_1}\right) \tag{12}$$

whereas qH_0, qH_1, q_{ppk}, q_{sk} are all queries inclusive for an adversary to check the identity, secret key and partial private key values. The attacker A_I might attempt polynomial times to get helpful information to the ROM $H1(0 \leq i \leq \varepsilon)$. For such polynomial bounded, $\mathtt{C}$ respond as If A_I puts Create(Identity) query to $\mathtt{C}$, for such input $\mathtt{C}$ must select some random integers/numbers of order prime, but couldn't aP, xP, yP, zP, xyP, xzP, yzP etc. private-public key pair due to CDHP. And if the adversary gives some random values to $\mathtt{C}$ for getting Identity, he/she must picks s and l from two different groups and computes $P_A = sl$ whereas P_A adversary public key. For such key, he/she cannot match P_A to P_{pub} when the adversary

AC2P		Drone(s)
Chooses a random number a Computes: $a \in_R Zq^*$ $R=aP$ $E=a \oplus R$ $Req=(E \oplus ID_i)\|\|a\|\|t$ $\theta=a \oplus H(Req\|\|R)$		
	$\xrightarrow{REQUEST(E,\ Req,\ \theta,\ t)}$	
		$t^{/}$ - $t \leq \Delta t$ and Extracts random number b Computes: $Req=(E \oplus ID_i)\|\|b\|\|t$ $E=b \oplus R$ $R=bP$
	$\xleftarrow{CHALLENGE(E,\ Req,\ \theta,\ t)}$	
$t^{/}$ - $t \leq \Delta t$ and Verifies $e(\theta, P)=e(bH(Req\|\|R), P)$ Computes: $e(\theta, P)=e(H(Req\|\|R), bP)$ $e(\theta, P)=e(H(Req\|\|R), P)$ Confirms: $e(\theta, P)?=e(H(Req\|\|R), P)$		
	$\xrightarrow{RESPONSE(E,\ \theta,\ R,\ t)}$	
		$t^{/}$ - $t \leq \Delta t$ and Choose random number c Computes: $\sigma_i=H_1(m_i).d_{Idi}+c_iR$ $T_i=c_iP$ $sig_i=\sigma_i\|\|T_i\|\|m_i$ $\sigma=\sum_{i=1}^{n} 6_i$ $T=\sum_{i=1}^{n} T_i$, $e(s_kH_1(m_i)$
	$\xleftarrow{(\sigma,\ T,\ t)}$	
$t^{/}$ - $t \leq \Delta t$ and validate $e(s_kH_1(m_i)$ tuple in σ Computes: $e(\sigma, P)=e(T, R).\ e(\sum_{i=1}^{n} T_i\ (m_i)Q_{ID_i}, P)$, $e(\sigma, P)=\prod_{i=1}^{n} e(s_kH_1\ (m_i)Q_{ID_i} + t_ibP, P)$, $e(\sigma, P)=\prod_{i=1}^{n}[e(s_kH_1\ (m_i)Q_{ID_i}, s_kP + e(t_iP, bP)]$, $e(\sigma, P)=\prod_{i=1}^{n}[e(s_kH_1\ (m_i)Q_{ID_i}, s_kP + e(T_i, R)]$, $e(\sigma, P)=\prod_{i=1}^{n} e(T_i\ , R).\prod_{i=1}^{n} e(s_kH_1\ (m_i)Q_{ID_i}, s_kP)$, $e(\sigma, P)=e(T, R).\prod_{i=1}^{n} e(H_1\ (m_i)Q_{ID_i}, P)$.		

Module. 1. Steps representing authentication of AC2P with reconnaissance drones.

submits H_0, H_1, H_2 choirs and Identity into C if some useful information obtained by the adversary C must abort or retry values and return irregular values that cannot satisfy $s\ P = R + H_0(\text{identity}, P, R)P_{pub}$. Therefore, the adversary failed to do it for the proposed protocol suite due to not maximum access power [50] and CDHP.

Theorem 9: Let ê denoted as bilinear paring on G_1, G_2, then CDHP is P, xP, yP, zP can calculate $\hat{e}(P, P)^{xyz}$. This is because xP, xyP, xyP, zP and xP, yzP, then $\hat{e}(xP, yzP) = \hat{e}(P, P)^{xyz}$. Similarly, if CDHP can solve these types of pairs, it can also efficiently compute $g = \hat{e}(P, P)$, $g^{xy} = \hat{e}(xP, yP)$, $g^{z} = \hat{e}(P, zP)$ and then g^{xyz}. But it is hard for an adversary to di such calculations. Because CDHP implies hardness to the measures of key pairs tuples in both groups G_1 and G_2.

Theorem 10: If the cryptographically calculated keys aP, bP, cP, abP, bcP, acP, abcP from groups (G_1, +), and (G_2, .) are secure against potential attacker A, who attempts polynomial times [50] over it, then the probability of breaking is negligible for any number k:

$$\left| pr \begin{bmatrix} (pk, sk, s_0) \leftarrow & G\left(1^k\right) & +, \times \\ (s, x_0, x_1) \leftarrow & A\left(1^k, pk.s_0\right) & : \forall = b \\ b \leftarrow \{0, 1\} & s^* \leftarrow T\ (pk, s, x_b) & b^{/} \leftarrow A(s^*) \end{bmatrix} \right| \tag{13}$$

This means that the cryptographic counter shall be verifiable for each session.

From these theorems, it has been clear that the proposed suite of protocols is efficient and effective for military drone communication using either FANET/UAVN or GPS for information transmission with PICS/AC2P. It ensures the integrity, identity, and compression of several signatures to a single one, reducing the communication cost and computation time complexity.

C. REAL-OR-RANDOM (ROR) MODEL ANALYSIS

We can also test the security of the identity-based aggregate signature-based authentication protocol by another widely used method [51] used by different researchers like [27], [48], [54], which consists of two entities, an adversary $\mathcal{A}$ and a responder ℜ. $\mathcal{A}$ established communication with AC2P, let E_i denotes AC2P, whereas i indicated the ith occurrence of AC2P. Whereas E_{DS} means adversary action to impersonate AC2P or PICS or Drone by forging *(M, σ)*, E_{SD} forges s or n, a, r, b, *pram* = {h_1, h_2, h_3, h_4, P, G_2, P_{pub}) for impersonating any participant and E_{SC} is considered to be an action of the adversary for semantic security of the proposed mechanism is given as under:

i. ***Setup Query*** in which challenger *C* return system parameters to $\mathcal{A}$.
ii. ***Hash Query*** in which *C* can store a list of parameters, apply one-way hash function h(M_s, M_p, M_n, M_a, M_b, etc.) and generates a random number *r* of order prime and stored with any of the given hash message (M_a, r) and return it to $\mathcal{A}$.
iii. ***MAC(M$_i$):*** Next, *C* authenticates the messag; if succeeded, return Mi to $\mathcal{A}$.
iv. ***Send (E^i, M$_i$):*** *C* sends it towards AC2P, acts as a legitimate drone, the response received also return to $\mathcal{A}$, but in our framework, we have added an extra step, *CHALLENGE*, AC2P, put a challenge message, which *C* cannot verify. Let *C* return the response to $\mathcal{A}$.
v. ***Execute(D_i^∞ , AC2P)***: Upon sending, the proposed protocol returns P_{pub} or R.
vi. ***Reveal(E^i)***: C given signature σ to A.
vii. ***Test(E^i)***: In this step, A can flip a coin 1– Valid σ (Win), 0 – Reject (Loss).

Also, we put the following reproduction algorithm (R) for polynomial-time attempt of an adversary with which the probability equals to 1.

D. DRONE TRAJECTORY SECURITY

This feature of the security frameworks can be tackled using lemmas, as under;

Lemma 1: According to [12]–[14], [52], the duration for transmission of a message through a dedicated path is given at the bottom of the page, for t > 0, and $\gamma = \lambda_0$, and

$$e^{-\ln(2)t\gamma}\left(e^{\ln(2)t\gamma} + ((1-\ln(2))\,t\gamma - 1)\,e^{t\gamma}\right)$$

for t > 0, and $\lambda = \mu_0 = \gamma$.

Reproduction Algorithm

```
Start
Test R (i) whereas R means
Ω ← Setup (1^i); (P, s) ← Reveal (Ω)
M ← {0, 1}*; r ← Z*_q
C ← Tuple (Ω, r, M, P)
(P, s) ← Execute (Ω); M/ ← {0, 1}*
If tuple (ID/, P/, r, M/, Ω)    =R(ID_d,
ID/_d, P, P/, s/, M/, Ω) then
Return 1,
else
return 0,
End if
Exit
```

Hints: λ = resource survivability, μ = network's periodicity, and t = upcoming time slot of the network

Proof: Suppose $t_x = x$, $\gamma = \lambda_0$, $\lambda = y$ then according to (6), $L_p = L_0 e^{-\gamma t_x}$, which is given as

$$R_{e,P}^{(ob)} = \int_0^t \frac{t_x}{e^{-yx}} \cdot \frac{L_0}{(1+\frac{y}{\mu})^{\mu t_x}} dt$$

Solving it, we get

$$= \frac{Xe^{yx}}{\left(\frac{y}{\mu}+1\right)^{\mu x} (\mu \ln\left(\frac{y+\mu}{\mu}\right) - y)} - \int \frac{e^{yx}}{\left(\frac{y}{\mu}+1\right)^{\mu x}\left(y - \mu \ln\left(\frac{y+\mu}{\mu}\right)\right)} dx$$

Now solve by parts, we get

$$= \int \frac{e^{yx}}{\left(\frac{y}{\mu}+1\right)^{\mu x}\left(y - \mu \ln\left(\frac{y+\mu}{\mu}\right)\right)} dx$$

$$= \int -\frac{1}{\left(\mu \ln\left(\frac{y+\mu}{\mu}\right) - y\right)\left(y - \mu \ln\left(\frac{y}{\mu}+1\right)\right)} du$$

$$= -\frac{1}{\left(y - \mu \ln\left(\frac{y+\mu}{\mu}\right)\right)\left(\mu \ln\left(\frac{y+\mu}{\mu}\right) - y\right)} \int 1\, du$$

$$= \frac{u}{\left(y - \mu \ln\left(\frac{y+\mu}{\mu}\right)\right)\left(\mu \ln\left(\frac{y+\mu}{\mu}\right) - y\right)}$$

$$= \frac{e^{yx}}{(\frac{y}{\mu}+1)^{\mu x}\left(y - \mu \ln\left(\frac{y+\mu}{\mu}\right)\right)\left(\mu \ln\left(\frac{y+\mu}{\mu}\right) - y\right)}$$

$$= \frac{Xe^{yx}}{(\frac{y}{\mu}+1)^{\mu x}\left(\mu \ln\left(\frac{y+\mu}{\mu}\right) - y\right)} - \int \frac{e^{yx}}{(\frac{y}{\mu}+1)^{\mu x}\left(y - \mu \ln\left(\frac{y+\mu}{\mu}\right)\right)} dx$$

$$\frac{e^{-\mu t ln(\gamma+\mu)}(e^{t(\gamma+\mu\ln(\mu))}\,(t\,(\mu\,(\ln(\gamma+\mu) - \ln(\mu)) - \gamma) + 1) - e^{\mu t ln(\gamma+\mu)})}{(\mu\,(\ln(\gamma+\mu) - \ln(\mu)) - \gamma)^2}$$

$$= -\frac{e^{yx}}{\left(\frac{y}{\mu}+1\right)^{\mu x}\left(y-\mu\ln\left(\frac{y+\mu}{\mu}\right)\right)\left(\mu\ln\left(\frac{y+\mu}{\mu}\right)-y\right)} - \frac{Xe^{yx}}{\left(\frac{y}{\mu}+1\right)^{\mu x}\left(\mu\ln\left(\frac{y+\mu}{\mu}\right)-y\right)}$$

For finit value t > 0, we get as shown at the bottom of the page.

And can also be written as shown at the bottom of the page.

That is the desired result, similarly, for $\lambda = \mu$, the procedure will go

$$= \int_0^t \frac{x}{e^{-yx}}.\frac{1}{2^{yx}}dx = -\frac{Xe^{yx}}{y\left(\ln(2)-1\right).2^{yx}} - \int \frac{e^{yx}}{y91-\ln(2)).2^{yx}}dx$$
$$= -\frac{e^{yx}}{y^2\left(1-(2)\right)\left(\ln(2)-1\right).2^{yx}} - \frac{Xe^{yx}}{y\left(\ln(2)-1\right).2^{yx}}$$

Let t is finite whoes value is greater than 0, then

$$= \frac{e^{-\ln(2)ty}(e^{\ln(2)ty} + ((1-\ln(2))\,ty-1)e^{ty})}{ln^2(2)-2\ln(2)+1)y^2}$$

Put λ = y, we will get:

$$= \frac{e^{-\ln(2)t\gamma}(e^{\ln(2)t\gamma} + ((1-\ln(2))\,t\gamma-1)e^{t\gamma})}{ln^2(2)-2\ln(2)+1)\gamma^2}$$

This is the required result

Lemma 2: Again, according to [12]–[14], [52]; let the relative speed of a drone is ϑ_s, and f_t (function of time) can be given to the trajectory being generated by drone, then the Macaulay duration as shown at the bottom of the page, and $\wp_C$ is shown to be the drone's coordinates. The specified points in the trajectory of a specific drone can be chosen based on decreasing line accessibility of function-timing control, which is safe to be overlapped/collided.

Proof: As per distance and channel equations, system main equation is:

$$\mathcal{T}_R^{(t)} = t^{/} \times \frac{\vartheta_{xvz} - \vartheta_{xvz}^{/}}{2\Delta R_{e,P}^{Avg}} \int\limits_0^{t^{/}} R_{e,P}^{(0)}dt$$

where $t^{/} \leq$ t and ϑ_{xvz} = velocity at current xy coordinates $\vartheta_{xvz}^{/}$ = velocity at expected coordinates, $R_{e,P}^{Avg}$ Macaulay duration at current $t^{/}$ can be solved as:

$$= \min\left(\sum_{i=1}^{N}\int_0^t R_{e,P}^{(0)}dt\right)$$

Now in lemma 1, the time complexity for the proposed model can be calculated using:

$$\mathcal{T}_C^{(t)} = \int_0^t \frac{tln\left(f\left(\tau_R\right)\right)}{dR}dt$$

where $f(\tau_R) = t_1e^{\lambda t}\cos(t) + t_2e^{\lambda t}\sin(t)$ and t_1 and t_2 are time calculated at a specific point in the trajectory, and time threshold in the above equation can be simplified, and we get:

$$T_C^{(t)} = \frac{2tTan(\frac{\cos 2t}{\sin 2t+1} - t\ln(2\sin(2t)+2)}{2} + \frac{2t\ln(t_1e^{\lambda t}\sin(t)+t_2e^{\lambda t}cost(t))}{2} + \frac{iL_{i_2}(e^{2\mathrm{it}}+(i-\lambda)\,t^2-iLi_2(i)}{2}$$

i = imaginary unit, and Li_2 = complex values polynomial function

E. KEY SECRECY AND IDENTITY SECURITY

The identity and random numbers extracted in different phases are unconditionally secure against any threat. We offer the following proof for key secrecy, random numbers and identity security.

Lemma 3: Let a, b are positive integers, and let P ∈ E(n), whereas E(n) is Miller's algorithm [53] for pairing cryptography and *q* is several order prime over aP, bP; *u* is another secret number of same order prime, then $f_{a+b} = f_af_b(c/u)$.

Proof: RHS = f_af_b(c/u), By taking divisor, we get div(f_af_b(c/u)) = div(f_a) + div(f_b) + div(c) − div(u) = {a(P) − (aP) − (a − 1)(∞)} + {b(P) − (bP) − (b − 1)(∞)} + {(aP) + (bP) + (− (a + b)P − 3(∞)} − {((a + b)P) + (− (a + b)P) − 2(∞)} = (a + b)(P) − ((a + b)P) − (a + b − 1)(∞) = div(f_{a+b}) = f_{a+b} = LHS

Lemma 4: Suppose P be extracted from a group G_1, then $\hat{e}(P, P)^{abc}$ and *s* removed from G_2 whereas s, P ∈ Z_q∗. Then

$$\frac{e^{-\mu tln(y+\mu)}(e^{t(y+\mu\ln(\mu))}\left(t\left(\mu\left(\ln(y+\mu)-\ln(\mu)\right)-y\right)+1\right)-e^{\mu tln(y+\mu)})}{\left(\mu\left(\ln(y+\mu)-\ln(\mu)\right)-y\right)^2}$$

$$= \frac{e^{-\mu tln(\gamma+\mu)}(e^{t(\gamma+\mu\ln(\mu))}\left(t\left(\mu\left(\ln(\gamma+\mu)-\ln(\mu)\right)-\gamma\right)+1\right)-e^{\mu tln(\gamma+\mu)})}{\left(\mu\left(\ln(\gamma+\mu)-\ln(\mu)\right)-\gamma\right)^2}$$

$$\mathcal{T}_R^{(t)} = t^{/} \times \frac{\vartheta_{xvz} - \vartheta_{xvz}^{/}}{2\Delta R_{e,P}^{Avg}} \times \frac{e^{-\ln(2)t\gamma}(e^{\ln(2)t\gamma} + ((1-\ln(2))\,t\gamma-1)e^{t\gamma})}{ln^2(2)-2\ln(2)+1)\gamma^2}$$

we can say that these are indistinguishable for any algorithm of polynomial-time attempts by adversary *A*.

Proof: Suppose a challenger has many instances like ((P, G_1, G_2, ê), P, P^a, P^b, P^c) and *s*. and given one by one to his/her algorithm for finding ê(P, P)^{abc}. An adversary has the following advantage to identify exact values; else, not possible for A.

Let D = ((P, G_1, G_2, ê), P, P^a, P^b, P^c), s, a, b, c $\in Z_q^*$ $(Adv_A)^{CDHP}(\lambda) = |pr[A(D, e(g, g)^{abc}) = 1] - pr[A(D, s) = 1]|$. But such attempt of an adversary is not possible to identify the bilinear pairing over CDHP [47].

Lemma 5: Let H and H_1 are in the random oracle; there exists an adversary *A* for ID_s and ID_l to run in a time of advantage ε_0. And let *A* runs an algorithm at most $\varepsilon_0 \geq 10q_{H1}^2(qs + 1)(qs + qH)/q$, and they also exist a challenger *B* that can solve our scheme with some predefined time threshold $t_1 \leq 10qH_1\ t_0/\varepsilon_0$.

Proof: Challenger is given some possible tuple (P, sP, q_1, q_2, ..., q_n, $(1/q_1 + s)P$, ..., $(1/q_n + s)P$) of our protocol solution, whereas $n \geq qH$, qs. Challenger has a try to solve $(1/q_0 + s)P$ for some q_0. For accomplishing the said goal, *B* needs to set some public parameters from two groups of random numbers of order prime (G_1, G_2), (ê, G_1, G_2) and (ê, G_1, G_2, g, P_{pub}) and calculate $P_{pub} = sP$, and ê(P, P). Then *B* gives these parameters to A for launching attack(s) on our protocol(s). Initially, *A* input these public parameters to the ***Extract A*** **lgorithm**, which he/she cannot get matching a hash query, as these are collision-free hash values. This is because of forking lemma proof [49]–[51].

F. ProVerif2.02 SIMULATION

The issue of confidentiality, authorization, accessibility, reachability, credibility, integrity, and most importantly the issue of secrecy of all the credentials (secret keys, identity, random numbers, parameters, and time) have been programmed/simulated by using a world-widely used software toolkit ProVerif2.02 [57]. Specification of the same is very complex and elaborate as it is inappropriate to reveal it here in this analysis. The final result will, however, specifies that these are secure from any threats and untoward happenings as will be shown in the final result generated by the whole protocol simulation code.

G. INFORMAL SECURITY ANALYSIS

This subsection focuses on the analysis of trust; freshness, and robustness provided by the cryptographic protocols and designates a protocol's correctness or constructs attacks from the lack of security properties. Also, it tells the readers why widespread authentication protocol attacks occur, and then it addresses them based on trustworthiness and freshness. Therefore, keeping in view, our protocol suite covers these significant problems: (1) How to stop replay, parallel, and interleaving attacks? (2) What is the efficient way to distinguish whether a message is fresh or not? (3) How to prevent the dependencies of analysis on the idealization of a protocol? (4) How to avoid the concrete formalization of attackers' potential actions? (5) How to prevent the behavior of formalization of running a protocol? (6) What is the exact identification for guaranteeing authentication protocol security that proves the protocol's correctness, acceptably, and essentiality? (7) How to confirm integrity, confidentiality, authentication, and non-repudiation for a security protocol? And finally, (8) How to confirm that an adversary can break a protocol for known attack(s)? The given issues are the target of this analysis. However, these could not be stated or repeated given the space of this paper.

ProVerif2.02 Simulation Result

```
Completing equations ...
-- Query not attacker(kd[]) in process
Translating the process into Horn
clauses ...
Completing equations ...
Starting query not attacker(kd[])
Completing equations ...
RESULT not attacker(kd[]) is true.
---------------------------------
Verification summary:
Query not attacker(kd[]) is true.
Query inj-event(end_d(IDd[])) ==>
inj-event(start_d(IDd[])) is true.
Query inj-event(end_AC2P(IDac2p[]))
==> inj-event(start_AC2P(IDac2p[]))
is true.
---------------------------------
```

VI. PERFORMANCE AND COMPARISON ANALYSIS

It is worth mentioning that Flying Ad hoc Network (FANET) or Unmanned Aerial Vehicular Network (UAVN) is a decentralized, self-organized, and infrastructureless network; the storage capacity of the aggregate signature is equal to each drone signature; and the computation cost/time complexity of aggregate signature verification is independent of the number of each individual signature. Suppose, T_α is the time required for the execution of multiplication, T_β is the time for generating bilinear paring from a map, T_γ represents exponentiation execution time in bilinearity, and T_Ψ, the execution of addition in random number group. So, the performance comparison analysis for the proposed scheme with [41], [45], [46], [55] and [56] as show in table 2. Where I denote the data broadcasting between AC2P/PICS → Reconnaissance Drone, II: AC2P/PICS → Attacking Drone, III: Reconnaissance Drone → AC2P/PICS, and IV: Attacking Drone → AC2P/PICS. Similarly, let suppose for a given number of signatures (n = 1, 2, 3 . . . . n) to the verification function of AC2P. How much time does the verification function take on running these signatures, and how much time will it take to complete? To answer these questions, big-O notation is used subject to the input values. If the value is constant, then running time is O(1), linear task, O(n), while for quadratic values, the time complexity is O(n^2). For the

TABLE 2. Time complexity analysis and comparison.

Peer	[41]	[45]	[46]	[55]	[56]	Our
I	n(n-1)T_α+3 T_β	2T_α+T_β	3T_α+2T_β+T_ψ	3T_β+n T_ψ+2n T_χ	1T_α+3T_β+2T_γ	2(n-1)T_α
II	T_ψ+T_x+ T_β	(n-1)T_α+T_β	2(n-1)T_ψ	3T_x	(2n+1)T_x+(3n-1)T_ψ	nT_β+3T_γ
III	(n-1)T_β+2T_ψ	(n-1)T_α-(n-1)T_β+(2n-1)T_χ	nT_α+3T_β+T_χ	3T_β+ T_ψ+2GT_x	----	(n-1)T_α+T_β+T_χ
IV	(n-1)T_α+(n-1)T_x	(n-1)T_α-(n-1)T_β+(2n-1)T_χ	nT_α+3T_β+T_χ	2 T_β	1T_α+n T_β	(n-1)T_α+T_β+T_χ

TABLE 3. Performance comparison analysis with related schemes.

Feature	[41]	[45]	[46]	[47]	[55]	[56]	Our
I	4NW+ (L-1)	2NW+L+W	2NL	2log(N-1)+L	O(n^2)+L+W	W+nL	N+L
II	3O(n)	2O(n)	2(n^2)t^2	NO(n)	6O(n^2)	(n+1)W+nL	O(n)
III	8(L-1), *k*	L, *param*	nL, param	(logN+1)L	2n, param	n(n+1)W+L	nL, param

TABLE 4. Performance analysis in Milliseconds.

Operations	AC2P/PICS	Attacking Drone	Reconnaissance Drone
Multiplication Function	72ms	121ms	103ms
Signature Function	136ms	226ms	195ms
Verification Function	214ms	357ms	306ms
Paring Function	35ms	57ms	49ms
Key Generation	24 μs	40 μs	35 μs
Hash Function	57 μs	94 μs	81 μs
Addition Function	300 μs	502 μs	429 μs
Point Multiplication	1053ms	1754ms	1503ms
Point Addition	4355 μs	7258 μs	6263 μs
Encryption/Decryption	117 μs	194 μs	167 μs

proposed scheme, the aggregate signature has a fixed length; therefore, its time complexity is much less than that of other schemes.

Furthermore, suppose there are N numbers of drones; $N^{/}$ is an active drone involving for some current task. AC2P or PICS is denoted by E, and all other components are said to be C. And let the topology is true mesh Z(Z − 1)/2 where Z = $\mathrm{N}^{/}$ + M + |C, L denotes key length, W is the message size, s, t, and x are system *param* of size smaller than N. Suppose the mesh includes two drones except cluster head, then the evaluation results given are: the data sending rate is $2NW + L + W$, the computation overhead is 2O(n), and the storage overhead is L, *param*. So, by comparing the proposed scenarios with [41], [45], [46], [55] and [56], it is clear that our method is better, whereas I represent data rate, II represents computational overheads, and III for storage overheads; as shown in Table 3.

Likewise, our work refines and further improves upon [58]'s work. As for the execution of time for different cryptographic operations is concerned, the research takes the path of [58] in determining performance in milliseconds. It is significant to indicate that [58], [59] applied three types of STMicroelectronics devices. Of these, one has a 32 bit CPU 96KB SRAM. The second one has the same 32-bit CPU and 20KB of SRAM. The third one is similar to the second one except for the speed, which is 72HMz clock instead of 84. We will consider the first STMicroelectronics for AC2P/PICS, the second STMicroelectronics for attacking drones, and the third is for investigating (reconnaissance) drones. Therefore, the different cryptographic processes take varying amounts of time, as shown in Table 4. By considering these cryptographic values/execution time complexities, the difference indicates that computation cost for attacking drone is slightly greater than reconnaissance drone.

VII. CONCLUSION

The different attacks like collation, forgery, privileged insiders, etc., and privacy, authorization, and information authentication issues and challenges for IoD deployment military drone's open network channel (FANET/UAVNs) are crucial tasks for the researchers to tackle. Also, it's very difficult to trust drone usage in matters of war, espionage, troops movement, etc., and the leading drone manufacturer could not escape third-party allegations about data theft. Besides, when used in war times, all the required apparatuses like attacking drone(s), investigating (reconnaissance) drone(s), certification (peers legality), flying zone and trajectories, etc., shall be in the system of command and control (AC2P/PICS). Therefore, in this research, we have attempted to address these issues and challenges up to a maximum extent by designing two security frameworks; one is based on identity, and the other one is an aggregate signature-based authentication scheme. The robustness of its security has been verifiably protected in the random oracle model/real-or-random model using Computational Diffie-Hellman Problem (CDHP). And the synergy and effectiveness of the attacking and reconnaissance (investigating) drones in IoD have been discussed informally using lemmas and pragmatic illustrations. The performance analysis and comparison result show that the proposed frameworks are fast and secure in terms of computation time complexity or communication and computation costs/overheads. All the efforts show that these schemes are fast and secure and can easily be implemented in warfare battlefield deployment drones for a real-world environment.

REFERENCES

[1] A. Srivastava and J. Prakash, "Future FANET with application and enabling techniques: Anatomization and sustainability issues," *Comput. Sci. Rev.*, vol. 39, Feb. 2021, Art. no. 100359.

[2] I. Sumra, P. Sellappan, A. Abdullah, and A. Ali, "Security issues and challenges in MANET-VANET-FANET: A survey," *EAI Endorsed Trans. Energy Web*, vol. 5, no. 17, Apr. 2018, Art. no. 155884.

[3] K. Kumari, B. Sah, and S. Maakar, "A survey: Different mobility model for FANET," *Int. J. Adv. Res. Comput. Sci. Softw. Eng.*, vol. 5, no. 6, pp. 1170–1173, 2015.

[4] X. Yuan, Z.-Y. Feng, W.-J. Xu, Z.-Q. Wei, and R.-P. Liu, "Secure connectivity analysis in unmanned aerial vehicle networks," *Frontiers Inf. Technol. Electron. Eng.*, vol. 19, no. 3, pp. 409–422, Mar. 2018.

[5] C. Ge, L. Zhou, G. P. Hancke, and C. Su, "A provenance-aware distributed trust model for resilient unmanned aerial vehicle networks," *IEEE Internet Things J.*, vol. 8, no. 16, pp. 12481–12489, Aug. 2021.

[6] I. Bekmezci, E. Senturk, and T. Turker, "Security issues in flying adhoc networks (FANETS)," *J. Aeronaut. Space Technol.*, vol. 9, no. 2, pp. 13–21, 2016.

[7] E. G. Hundley, *Future Technology-Driven Revolutions in Military Operations*. document DB-110-ARPA, RAND Corporation, Santa Monica, CA, USA, 1994.

[8] S. Panasenko and S. Smagin, "Lightweight cryptography: Underlying principles and approaches," *Int. J. Comput. Theory Eng.*, vol. 3, no. 4, p. 516, 2011.

[9] Y. Ganesh, R. Ramya, and H. Rajeshwari, "Surveillance drone for landmine detection," in *Proc. Int. Conf. Adv. Comput. Commun. (ADCOM)*, Sep. 2015, pp. 33–38.

[10] F. Flammini, R. Naddei, C. Pragliola, and G. Smarra, "Towards automated drone surveillance in railways: State-of-the-art and future directions," in *Proc. Int. Conf. Adv. Concepts Intell. Vis. Syst.* Cham, Switzerland: Springer, 2016, pp. 48–336.

[11] M. Gharibi, R. Boutaba, and S. L. Waslander, "Internet of drones," *IEEE Access*, vol. 4, pp. 1148–1162, 2016.

[12] A. Khan and M. Hebert, "Learning safe recovery trajectories with deep neural networks for unmanned aerial vehicles," in *Proc. IEEE Aerosp. Conf.*, Mar. 2018, pp. 1–9.

[13] J. E. Marsden and T. J. Hughes, *Mathematical Foundations of Elasticity*. Chelmsford, MA, USA: Courier Corporation, 1994.

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

[15] Q. Do, B. Martini, and K.-K. R. Choo, "The role of the adversary model in applied security research," *Comput. Secur.*, vol. 81, pp. 156–181, Mar. 2019.

[16] R. Altawy and A. M. Youssef, "Security, privacy, and safety aspects of civilian drones: A survey," *ACM Trans. Cyber-Phys. Syst.*, vol. 2, no. 1, p. 7, 2016.

[17] J. Zhang, J. Cui, H. Zhong, Z. Chen, and L. Liu, "PA-CRT: Chinese remainder theorem based conditional privacy-preserving authentication scheme in vehicular ad-hoc networks," *IEEE Trans. Dependable Secure Comput.*, vol.18, no. 2, pp. 722–735, Mar./Apr. 2021.

[18] T. Alladi, V. Chamola, and N. Kumar, "PARTH: A two-stage lightweight mutual authentication protocol for UAV surveillance networks," *Comput. Commun.*, vol. 160, pp. 81–90, Jul. 2020.

[19] S. A. Chaudhry, K. Yahya, M. Karuppiah, R. Kharel, A. K. Bashir, and Y. B. Zikria, "GCACS-IoD: A certificate based generic access control scheme for internet of drones," *Comput. Netw.*, vol. 191, May 2021, Art. no. 107999.

[20] A. Ara, M. Al-Rodhaan, Y. Tian, and A. Al-Dhelaan, "A secure privacy-preserving data aggregation scheme based on bilinear ElGamal cryptosystem for remote health monitoring systems," *IEEE Access*, vol. 5, pp. 12601–12617, 2017.

[21] J. Katz, *Digital Signatures*. Berlin, Germany: Springer, 2010.

[22] J.-L. Beuchat, *An Introduction to Pairing-Based Cryptography*. Tsukuba, Japan: CiteSeerX, 2010.

[23] R. Housley and T. Polk, *Planning for PKI: Best Practices Guide for Deploying Public Key Infrastructure*. Hoboken, NJ, USA: Wiley, 2001.

[24] A. W. Dent, "A survey of certificateless encryption schemes and security models," *Int. J. Inf. Secur.*, vol. 7, no. 5, pp. 349–377, 2008.

[25] A. Joux and K. Nguyen, "Separating decision Diffie-Hellman from computational Diffie-Hellman in cryptographic groups," *J. Cryptol.*, vol. 16, no. 4, pp. 239–247, 2003.

[26] S. G. Devi, K. Selvam, and S. P. Rajagopalan, "An abstract to calculate big o factors of time and space complexity of machine code," in *Proc. Int. Conf. Sustain. Energy Intell. Syst. (SEISCON)*, Chennai, India, 2011, pp. 844–847.

[27] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Proc. CRYPTO* (Lecture Notes in Computer Science) vol. 196. Berlin, Germany: Springer-Verlag, Aug. 1984, pp. 47–53.

[28] G. L. Boneh and Shacham, "Aggregate and verifiably encrypted signatures from bilinear maps," in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn.* Berlin, Germany: Springer, 2003, pp. 416–432.

[29] J. Srinivas, A. K. Das, N. Kumar, and J. J. Rodrigues, "TCALAS: Temporal credential-based anonymous lightweight authentication scheme for internet of drones environment," *IEEE Trans. Veh. Technol.*, vol. 68, no. 7, pp. 6903–6916, Oct. 2019.

[30] S. A. Chaudhry, I. L. Kim, S. Rho, M. S. Farash, and T. Shon, "An improved anonymous authentication scheme for distributed mobile cloud computing services," *Cluster Comput.*, vol. 22, no. S1, pp. 1595–1609, Jan. 2019.

[31] C.-L. Chen, Y.-Y. Deng, W. Weng, C.-H. Chen, Y.-J. Chiu, and C.-M. Wu, "A traceable and privacy-preserving authentication for UAV communication control system," *Electronics*, vol. 9, no. 1, p. 62, 2020.

[32] G. Cho, J. Cho, S. Hyun, and H. Kim, "SENTINEL: A secure and efficient authentication framework for unmanned aerial vehicles," *Appl. Sci.*, vol. 10, no. 9, p. 3149, Apr. 2020.

[33] S. H. Seo, J. Won, E. Bertino, Y. Kang, and D. Choi, "A security framework for a drone delivery service," in *Proc. 2nd Workshop Micro Aerial Vehicle Netw., Syst., Appl. Civilian Use*, 2016, pp. 29–34.

[34] M. S. Farash, M. Turkanović, S. Kumari, and M. Hölbl, "An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment," *Ad Hoc Netw.*, vol. 36, pp. 152–176, Jan. 2016.

[35] F. Al-Turjman, Y. K. Ever, E. Ever, H. X. Nguyen, and D. B. David, "Seamless key agreement framework for mobile-sink in IoT based cloud-centric secured public safety sensor networks," *IEEE Access*, vol. 5, pp. 24617–24631, 2017.

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

[37] Y. K. Ever, "Secure-anonymous user authentication scheme for e-Healthcare application using wireless medical sensor networks," *IEEE Syst. J.*, vol. 13, no. 1, pp. 456–467, Mar. 2019.

[38] J. H. Cheon, K. Han, S. M. Hong, H. J. Kim, J. Kim, S. Kim, H. Seo, H. Shim, and Y. Song, "Toward a secure drone system: Flying with real-time homomorphic authenticated encryption," *IEEE Access*, vol. 6, pp. 24325–24339, 2018.

[39] L. Zhang, L. Zhao, S. Yin, C.-H. Chi, R. Liu, and Y. Zhang, "A lightweight authentication scheme with privacy protection for smart grid communications," *Future Gener. Comput. Syst.*, vol. 100, pp. 770–778, Nov. 2019.

[40] L. Teng, M. Jianfeng, F. Pengbin, M. Yue, M. Xindi, Z. Jiawei, C. Gao, and L. Di, "Lightweight security authentication mechanism towards UAV networks," in *Proc. Int. Conf. Netw. Netw. Appl. (NaNA)*, Oct. 2019, pp. 379–384.

[41] Q. Feng, D. He, Z. Liu, D. Wang, and K. K. R. Choo, "Distributed signing protocol for IEEE P1363-compliant identity-based signature scheme," *IET Inf. Secur.*, vol. 14, no. 4, pp. 443–451, 2020.

[42] Z. Ali, S. A. Chaudhry, M. S. Ramzan, and F. Al-Turjman, "Securing smart city surveillance: A lightweight authentication mechanism for unmanned vehicles," *IEEE Access*, vol. 8, pp. 43711–43724, 2020.

[43] Y. Ko, J. Kim, D. G. Duguma, P. V. Astillo, I. You, and G. Pau, "Drone secure communication protocol for future sensitive applications in military zone," *Sensors*, vol. 21, no. 6, p. 2057, Mar. 2021.

[44] A. Utsav, A. Abhishek, P. Suraj, and R. K. Badhai, "An IoT based UAV network for military applications," in *Proc. 6th Int. Conf. Wireless Commun., Signal Process. Netw. (WiSPNET)*, Chennai, India, Mar. 2021, pp. 122–125.

[45] L. Shen, J. Ma, X. Liu, F. Wei, and M. Miao, "A secure and efficient ID-based aggregate signature scheme for wireless sensor networks," *IEEE Internet Things J.*, vol. 4, no. 2, pp. 546–554, Apr. 2017.

[46] W. Hong, L. Jianhua, L. Chengzhe, and W. Zhe, "A provably secure aggregate authentication scheme for unmanned aerial vehicle cluster networks," *Peer–Peer Netw. Appl.*, vol. 13, no. 1, pp. 53–63, Jan. 2020.

[47] D. He, S. Zeadally, B. Xu, and X. Huang, "An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 12, pp. 2681–2691, Dec. 2015.

[48] S. Hussain, S. A. Chaudhry, O. A. Alomari, M. H. Alsharif, M. K. Khan, and N. Kumar, "Amassing the security: An ECC-based authentication scheme for internet of drones," *IEEE Syst. J.*, vol. 15, no. 3, pp. 4431–4438, Sep. 2021.

[49] R. Canetti, O. Goldreich, and S. Halevi, "The random Oracle methodology, revisited," *J. ACM*, vol. 51, no. 4, pp. 557–594, 2004.

[50] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Advances in Cryptology–(CRYPTO)*. Berlin, Germany: Springer, 1999, pp. 388–397.

[51] A. Irshad, M. Sher, H. F. Ahmad, B. A. Alzahrani, S. A. Chaudhry, and R. Kumar, "An improved multi-server authentication scheme for distributed mobile cloud computing services," *KSII Trans. Internet Inf. Syst.*, vol. 10, no. 12, pp. 5529–5552, 2016.

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

[53] V. S. Miller, "The Weil pairing, and its efficient calculation," *J. Cryptol.*, vol. 17, no. 4, pp. 235–261, 2004.

[54] S. A. Chaudhry, K. Yahya, F. Al-Turjman, and M.-H. Yang, "A secure and reliable device access control scheme for IoT based sensor cloud systems," *IEEE Access*, vol. 8, pp. 139244–139254, 2020.

[55] H. Zhong, S. Han, J. Cui, J. Zhang, and Y. Xu, "Privacy-preserving authentication scheme with full aggregation in VANET," *Inf. Sci.*, vol. 476, pp. 211–221, Feb. 2019.

[56] G. Thumbur, P. V. Reddy, G. S. Rao, N. B. Gayathri, D. V. R. K. Reddy, and M. Padmavathamma, "Efficient and secure certificateless aggregate signature-based authentication scheme for vehicular *ad hoc* networks," *IEEE Internet Things J.*, vol. 8, no. 3, pp. 1908–1920, Feb. 2021.

[57] B. Blanchet, B. Smyth, V. Cheval, and M. Sylvestre, "ProVerif 2.00: Automatic cryptographic protocol verifier, user manual and tutorial," *Version From*, pp. 5–16, May 2018.

[58] D. Abbasinezhad-Mood and M. Nikooghadam, "Efficient anonymous password-authenticated key exchange protocol to read isolated smart meters by utilization of extended Chebyshev chaotic maps," *IEEE Trans. Ind. Informat.*, vol. 14, no. 11, pp. 4815–4828, Nov. 2018.

[59] (2018). *ArduinoLibs: Cryptographic Library*. [Online]. Available: http://rweather.github.io/arduinolibs/crypto.html

SAEED ULLAH JAN received the Ph.D. degree in network security from the University of Malakand, in 2021. He is currently working as a Lecturer in computer science at the Higher Education Achieves and Libraries Department Government of Khyber Pakhtunkhwa, Pakistan. He is also working as a Coordinator for nine (09) B.S. disciplines at the Government Degree College Wari (Dir Upper)–a far-flung remote area of the province where most of the youngsters have no access to Universities/Institutions for Higher Education. He has published over 15 research articles in prestigious conferences and journals and written an introductory book in computer science for beginners. His research interests include green computing, distributed computing, privacy-preserving parallel computation, and drone security and authentication. The Government of Khyber Pakhtunkhwa awarded "Best Teacher Award" for the year 2019–2020 out of 11000 College Teachers in 309 public sector colleges in the Province.

HABIB ULLAH KHAN (Member, IEEE) received the Ph.D. degree in management information systems from Leeds Beckett University, U.K. He is currently working as a Professor of management information systems (MIS) with the Department of Accounting and Information Systems, College of Business and Economics, Qatar University, Qatar. He has more than 20 years of industry, teaching, and research experience. He is an Active Researcher. His research work has published in leading journals of the MIS field. His research interests include IT security, online behavior, IT adoption in supply chain management, internet addiction, mobile commerce, computer-mediated communication, IT outsourcing, big data, cloud computing, and e-learning.