IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received August 14, 2021, accepted August 19, 2021, date of publication August 26, 2021, date of current version September 8, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3108130

An Improved Identity-Based Generalized Signcryption Scheme for Secure Multi-Access Edge Computing Empowered Flying Ad Hoc Networks

NIZAMUD DIN[1], ABDUL WAHEED[2,3], MAHDI ZAREEI[4], (Senior Member, IEEE), AND FAISAL ALANAZI[5]

[1]Department of Computer Science, University of Chitral, Chitral 17200, Pakistan
[2]Department of Information Technology, Hazara University Mansehra, Mansehra 21120, Pakistan
[3]School of Electrical and Computer Engineering, Seoul National University, Seoul 08826, South Korea
[4]School of Engineering and Sciences, Tecnológico de Monterrey, Zapopan 45201, Mexico
[5]Department of Electrical Engineering, College of Engineering, Prince Sattam Bin Abdulaziz University, Al-Kharj 16278, Saudi Arabia

Corresponding authors: Abdul Waheed (abdul@netlab.snu.ac.kr) and Faisal Alanazi (faisal.alanazi@psau.edu.sa)

ABSTRACT Emerging Unmanned Aerial Vehicles (UAVs) have applications for traffic monitoring, public safety, surveillance, agriculture, health services. Collaborative UAVs can form flying ad hoc networks, although such networks are especially vulnerable to security vulnerabilities due to open access media and limited power. Very recently, Khan *et al.* presented an Identity-Based Generalized Signcryption having Multi-access Edge computing to secure Flying Ad hoc Networks (FANETs). First, this paper presents the cryptanalysis of the Khan *et al.* scheme and shows that their scheme does not provide message confidentiality, Authenticity, and integrity. Second, it presents an improved scheme as well. The comparison of the improved scheme with the state of the art schemes based on security and cost shows, it is efficient, provably secure against security attacks, and suitable for multi-access edge computing empowered FANETs.

INDEX TERMS Unmanned aerial vehicles, FANETs, edge computing, multi-access, signcryption.

I. INTRODUCTION

Unmanned aerial vehicles (UAVs) are emerging and have extensive and diverse technologically based applications. Some of the applications domains are national security [1], disaster relief operations [2], surveillance [3], border control [4], traffic monitoring [5], farming and goods transportation [1], managing wildfires [6] and wind estimation [7]. Recently, Amazon introduced Amazon Prime Air [8] for quick and safe customer parcel delivery. FANETs consist of multiple small UAVs collecting and exchanging data with each other and ground stations. Due to their unique structure, FANETs have numerous challenges such as dynamic Topology, Mobility management, Latency, Frequent Link Disconnection, Flight Formation, Collision Avoidance, Combat with External Disturbances, and Scalability [9]. FANETs have limited resources and face security challenges such as GPS spoofing, black hole attacks, Denial of Service attacks, Spam, traffic, Sybil, and Man-in-the-Middle attacks [10]. Therefore, for efficient and secure information communication, smart and secure solutions are in demand.

Formally designed data and network security solutions can significantly reduce the threat to data and nodes compromised in FANETs. He *et al.* [11], proposed a hierarchal broadcast identity-based encryption to offload the need for certificate verification burden. Won *et al.* [12] proposed a certificateless multi-receiver encryption scheme for one-to-one, one to many, and many-to-one secure communication. Asghar *et al.* [13] proposed a certificateless blind signature scheme for sender anonymous authenticated communication in FANETs.

Signcryption combines the functionality of public-key signature and encryption with a significantly reduce cost. Lal *et al.* [14] first introduced the notions of ID-based generalized signcryption schemes(ID-GSCS). Wei *et al.* [15] proposed an ID-GSCS formally secure in the random

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

oracle model. However, Waheed *et al.* [16] showed that the scheme of Wei *et al.* is insecure in their defined model. Shen *et al.* [17] first proposed an ID-GSCS in the standard model. Zhou *et al.* [18] proposed an ID based combined public key signcryption scheme for signature encryption and signature to provide sufficient security functionality. To cope with the efficient security requirements of FANETs, Khan *et al.* [19] proposed an ID based generalized signcryption for secure multi-access edge computing empowered FANETs. This paper analyzes the Khan *et al.* solution and proves that this scheme does not provide message confidentiality. This paper also presents an improved scheme that provides necessary security features for secure multi-access edge computing-empowered FANETs.

A. PAPER ORGANIZATION

The rest of this paper is organized as follows: The literature review presented in section II, and preliminaries is defined in section III. Section IV represents the review of khan's scheme and section V presents the cryptanalysis of the said scheme. Section VI, presents the improved scheme and its correctness and analysis with its deployment. Section VII of the paper presents the analysis of the improved scheme having the security and cost analysis. The conclusion of the paper is described in section VIII.

II. RELATED WORK

This section reviews some relevant literature. Zhang *et al.* [20] proposed a Chinese remainder theorem-based privacy-preserving authentication scheme using fingerprints for securing communications in VANETs. The scheme has performance effectiveness and security under the random oracle model. Future work extends the enhanced user privacy in emerging dynamic environments comprising 5G network base stations, driver handheld devices, etc. Due to enhancement in communication technologies, the concept of the Internet of Battle Things (IoBT) emerges, which empowers armed forces in the battle to face challenges in command and control (C2) scenarios. Leal *et al.* [21] proposed an architecture for the software-defined and information-centric network nodes that meet the high-level operational requirements for "C2 agility" provides a more efficient data distribution.

Reddy *et al.* [22] proposed a pairing-free key insulated signature scheme in an identity-based setting having computational and communication efficiency. Xiong *et al.* [23] also proposed a provable secure pairing-free Certificateless Parallel Key-Insulated Signature (CL-PKIS) scheme for Industrial Internet of Things (IIoT). Both the mentioned approaches are based on an elliptic curve and suffer from high computational costs. Khan *et al.* [24] proposed a CL Key-Encapsulated Signcryption scheme based on Hyper Elliptic Curve Cryptosystem (HECC) for FANETs. HECC having a shorter key size and is efficient compare to elliptic curves. Khan *et al.* [25] proposed an access control and key agreement HECC based scheme and the security and cost analysis is presented.

Next, we introduce FANETs's common security attack known as Sybil Attack. Where an attacker pretends that many people communicate within the same time and hide his/her identity to users of the network, that causes connectivity issues mainly in the Peer-to-Peer communications as it is creating multiple identities which look like regular users of a network and thus behind the scene a single attacker manipulates and controls the whole network. In contrast, in the eclipse attack, the attacker targets the few nodes within the network and eclipse/restrict them to communicate with the other nodes. Fig 1 shows the Sybil attack where the blue Sybil nodes prevent the honest nodes from connecting to other network nodes by creating multiple fake identities and preventing the information transmission lines among the nodes in a network. The Sybil attack can be prevented when the cost of identities is so high that the attacker cannot compute the high number of fack identities, however, at the same time, the cost of identification should not be too high that it's burdensome for legitimate users, and possible for them to communicate without facing any difficulties. This would be possible via using the digital signature based on HECC having a minimal cost with the same level of security.

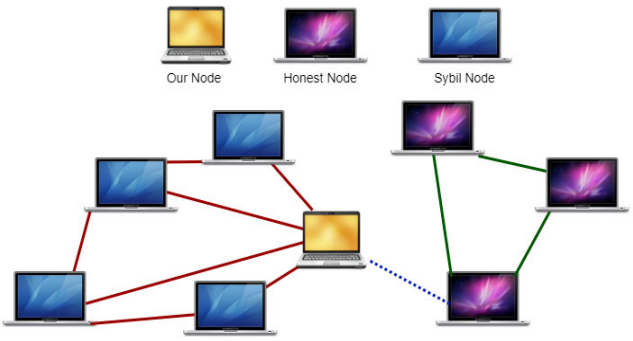

FIGURE 1. Sybil attack.

III. PRELIMINARY OF HYPERELLIPTIC CURVE CRYPTOSYSTEM

Definition 1: Let F_q be a finite field of order q and F'_q are the algebraic closure of F_q. Hyper-elliptic curves hEc of genus $g \geq$ over F_q is a set of solutions $(x,\ y) \in F_q \times F_q$ of the equations $hEc : \ y^2 + h(x)y \ = f(x)(1)$: Where $h(x)) \in F_q$ is a polynomial of degree g and $f(x)) \in F_q$ is a monic polynomial of degree $2g + 1$ and there should be no solutions $(x,\ y) \in F_{q'} \times F'_q$ simultaneously satisfy the Eq. (l) and partial derivatives of Eq. (1) [26]

A Divisor D is a finite formal sum of points $D = \sum_{P_i \in hEc} m_i P_i$, $m_i \in Z_q$ a reduced divisor is of the form $D = \sum_{P_i \in hEc} m_i P_i - (\sum_{P_i \in hEc} m_i) \infty$. Divisors can be represented as pairs of polynomials in the form of Mumford. $D = (a(x),\ b(x))$ Where

1) $a(x) = \prod (x - x_i)^{m_i}$ *is monic polynomial*
2) $b(x_i) = y_i$ *and* $degb(x) < \deg(a(x)) \leq g$
3) $a(x) | (b(x)^2 - h(x)b(x) - f(x))$

The Jacobian $J(F_q)$ is finite abelian group under addition and each element in $J(F_q)$ is an equivalence class of reduced divisor. The following inequality calculates the order of the Jacobian $J(F_q)$

$|(\sqrt{q}-1)^{2g}| \leq \#J/F_q \leq |(\sqrt{q}+1)^{2g}|$

Definition 2: Hyper-elliptic Curve Discrete Logarithm Problem (HECDP): $D_1$and D_2 are two divisor in $J(F_q)$ find an integer k, $0 \leq k \leq n-1$ such that $D_2 = kD_1$. Where $kD_1 = (D_1+D_1+D_1+\ldots)_{k\ times}$ Koblitz [27] first introduced a hyper-elliptic curve cryptosystem over $J(F_q)$ the jacobians of hyper-elliptic curves on the presumed intractability of the discrete logarithm problem. HECDP is prioritized over other cryptosystems due to high efficiency and shorter key size. The notation used in this paper are shown in Table 1:

TABLE 1. Notations guide.

Symbols	Definition
I_q	Finite field of the order q
hEc	Hyperelliptic curve
D	Divisor
$PKGC$	Private key generation center
$(\delta,\ \Lambda)$	Master key pair of PKG
E	Public parameter
$h_a,\ h_b$	Hash functions
ID_{cs}	Sender Identity
ID_{cr}	Receiver Identity
A_{cs}	Sender private key
A_{cr}	Receiver private key
B_{cs}	Sender public key
B_{cr}	Receiver public key
e_β	Encryption using
d_β	Encryption using
$\psi = (\partial, \sigma, \eta, \Delta)$	Generalized signcrypted text
$\perp$	Error
$[\cdot]_j$	Mapping from to
$a\|b$	a Divide b

IV. REVIEW OF KHAN *et al.* SCHEME

A. SYSTEM MODEL

As depicted in Fig 2, Khan *et al.* system model consists of UAVs with multi-access edge computing (MEC) capability and connected with Macro Base Station (SBS) using 5G wireless communication technology.

B. KHAN et al. IDENTITY-BASED GENERALIZED SIGNCRYPTION SCHEME

Khan *et al.* scheme consists of four phases: Setup, Key extraction, Generalized signcryption, and Generalized unsigncryption. The detail of each phase is as under:

1) **Setup:** PKGC performs the following steps:
   a) Selects a hyper-elliptic curve (HEC) over a finite field I_q, of order is q
   b) Selects a divisor D in the Jacobian $J(F_q)$ of HEC
   c) Selects a number uniformly $\delta \in [1, 2, \cdots, (q-1)]$ as PKGC private key
   d) PKGC Computes its public key as $\Lambda = \delta D$
   e) Selects two one-way hash functions: $h_a,\ h_b$
   f) Publish public parameters $E = [I_q$, HEC, D,Λ, $h_a,\ h_b]$
2) **Key extraction:**
   a) Each node sends their identity (ID_{pc}) to the PKGC
   b) PKGC Computes private key for the sender (ID_{cs}) as $A_{cs} = \delta \cdot h_a(ID_{cs}) \bmod q$ and public key as $B_{cs} = A_{cs} \cdot D$
   c) PKGC Computes private key for the receiver (ID_{cr}) as $A_{cr} = \delta \cdot h_a(ID_{cr}) mod\ q$ and public key as $B_{cr} = A_{cr} \cdot D$
   d) Transmit securely the private-public key pair to the node having identity ID_{cr}
3) **Generalized signcryption:**
   a) Having a message (m), the sender identity & private key (ID_{cs}, A_{cs}), the receiver identity and public key (ID_{cr}, B_{cr}), the sender generate generalized signcrypted text:
   b) Select $\varphi \in [1, 2, \cdots, (q-1)]$
   c) Computes $\Delta = \varphi \cdot D$
   d) Computes $\beta = \varphi \cdot B_{cr} \cdot ID_{cr}$
   e) Computes $\eta = e_\beta(m||ID_{cs}||ID_{cr}||n_{cs})$
   f) Compute $\sigma = h_b(m||ID_{cs}ID_{cr}||n_{cs})$
   g) Computes $\partial = (IDcr \cdot \varphi - \sigma \cdot \Delta \cdot A_{cs} \cdot ID_{cs}) \bmod q$ Generalized signcryption text $\psi = (\partial, \sigma, \eta, \Delta)$
4) **Generalized Unsigncryption**:
   a) Receiver generalized signcryption text $\psi = (\partial, \sigma, \eta, \Delta)$ and $(A_{cr}, B_{cs},\ B_{cr},\ ID_{cr})$
   b) Computes $\beta = \partial \cdot B_{cr} + ID_{cs} \cdot \Delta \cdot \sigma \cdot B_{cs} \cdot A_{cr}$
   c) Computes $(m||ID_{cs}||ID_{cr}||n_{cs}) = d_\beta(\eta)$
   d) Computes $\sigma^{\wedge} = h_b(m||ID_{cs}||ID_{cr}||n_{cs})$ if $\sigma^{\wedge} = \sigma$, accept ψ otherwise $\perp$

V. CRYPTANALYSIS OF KHAN *et al.* SCHEME

Without knowing the key, breaking a cryptographic scheme known as cryptanalysis as shown in Fig 3.

Khan *et al.* work in three different modes: Encryption only, signature only, and Signcryption. The scheme has been analyzed in these three modes as below:

A. ATTACK ON ENCRYPTION ONLY MODE

If $ID_{cs} = null$ and $ID_{cr} \neq null$ null, then GSC proceeds in an encryption only mode. The Generalized signcryption algorithm with $ID_{cs} = null$ in last step, Computes encrypted text as:

$$\begin{aligned}\partial &= (IDcr \cdot \varphi - \sigma \cdot \Delta \cdot A_{cs} \cdot ID_{cs}) \bmod q \\ &= (IDcr \cdot \varphi - \sigma \cdot \Delta \cdot A_{cs} \cdot 0) \bmod q = (IDcr \cdot \varphi) \bmod q \\ &= (ID_{cr} \cdot \varphi) \bmod q\end{aligned}$$

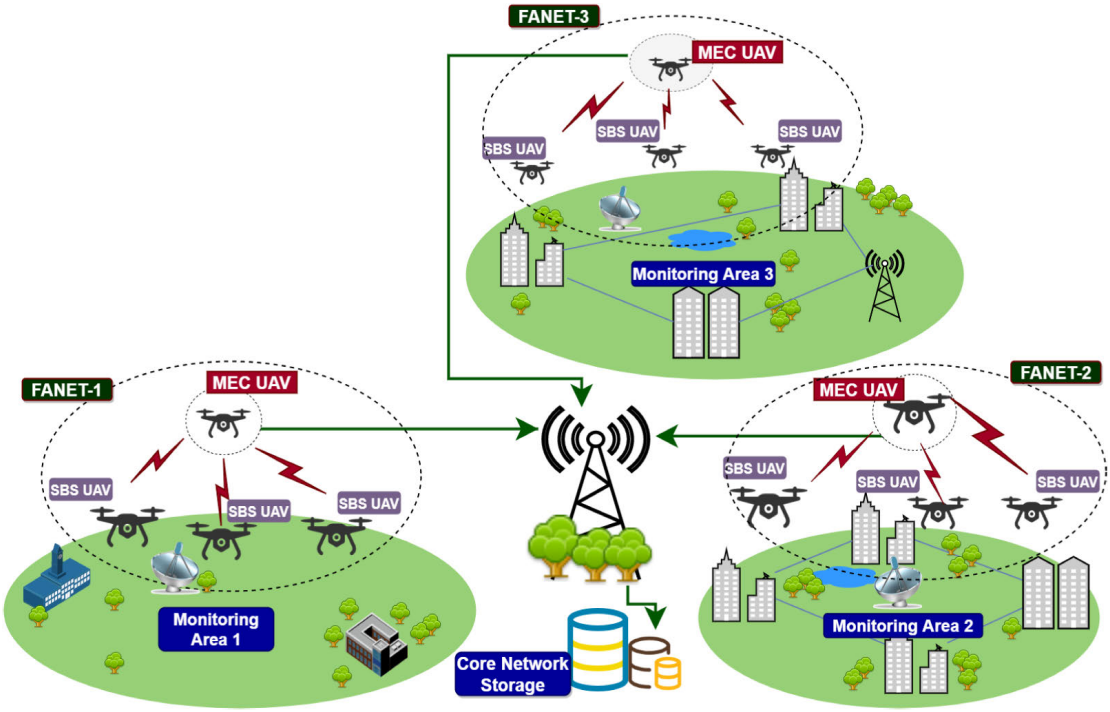

FIGURE 2. Multi-access edge computing architecture.

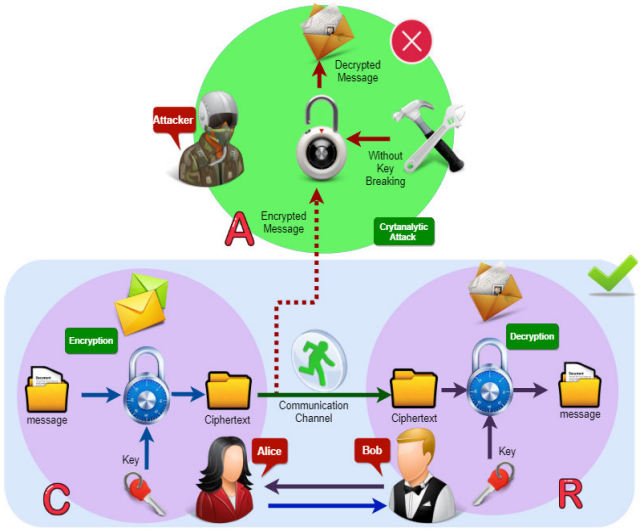

FIGURE 3. Cryptanalysis model.

For an attacker

- ∂ & ID_{cr} are known parameters
- Equation $\partial = (ID_{cr} \cdot \varphi) \bmod q$ has only one unknown φ, that can be easily computed in polynomial time
- and attacker can compute session key as $\beta = \varphi \cdot B_{cr} \cdot ID_{cr}$.

Therefore, this scheme does not provide message confidentiality in encryption-only mode.

B. ATTACK ON SIGNATURE ONLY MODE

If $ID_{cr} = null$ and $ID_{cs} \neq null$ null, then generalized signcryption proceeds in an signature only mode.

Sender set session key to zero as $\beta = \varphi \cdot B_{cr} \cdot (0) = 0$, compute $\eta = e_0(m||ID_{cs}||ID_{cr}||n_{cs}) = (m||ID_{cs}||ID_{cr}||n_{cs})$. The attacker obtain Generalized signcryption text $\psi = (\partial, \sigma, \eta, \Delta)$ and will change the message $\eta = (m||ID_{cs}||ID_{cr}||n_{cs})$ to $\eta' = (m'||ID_{cs}||ID_{cr}||n_{cs})$ and $\sigma' = h_b(m'||ID_{cs}||ID_{cr}||n_{cs})$ and forward the Generalized signcryption text $\psi = (\partial, \sigma', \eta', \Delta)$ to the receiver.

Receiver computes session key as:

$$\begin{aligned}
\beta &= \partial \cdot B_{cr} + ID_{cs} \cdot \Delta \cdot \sigma \cdot B_{cs} \cdot A_{cr} \\
&= (IDcr \cdot \varphi - \sigma \cdot \Delta \cdot A_{cs} \cdot ID_{cs}) B_{cr} + ID_{cs} \cdot \Delta \cdot \sigma \cdot B_{cs} \cdot A_{cr} \\
&= ((0) \cdot \varphi - \sigma \cdot \Delta \cdot A_{cs} \cdot ID_{cs}) B_{cr} + ID_{cs} \cdot \Delta \cdot \sigma \cdot B_{cs} \cdot A_{cr} \\
&= -\sigma \cdot \Delta \cdot A_{cs} \cdot ID_{cs} B_{cr} + ID_{cs} \cdot \Delta \cdot \sigma \cdot B_{cs} \cdot A_{cr} \\
&= ID_{cs} \cdot \Delta \cdot \sigma \cdot B_{cs} \cdot A_{cr} - \sigma \cdot \Delta \cdot ID_{cs} \cdot A_{cs} \cdot B_{cr} \\
&= ID_{cs} \cdot \Delta \cdot \sigma \cdot A_{cs} A_{cr} \cdot D - \sigma \cdot \Delta \cdot ID_{cs} \cdot A_{cs} \cdot A_{cr} \cdot D \\
&= 0.
\end{aligned}$$

Receiver then computes $\sigma^* = h_b(m'||ID_{cs}||ID_{cr}||n_{cs})$ compares $\sigma^* = \sigma'$ that hold, and the fraudulent message is authenticated. Therefore, the scheme does not provide message authentication and integrity.

C. ATTACK ON SIGNCRYPTION MODE

In signcryption only mode sender computes $\partial = (ID_{cr} \cdot \varphi - \sigma \cdot \Delta \cdot A_{cs} \cdot ID_{cs}) = (ID_{cr} \cdot \varphi - \sigma \cdot A_{cs} \cdot ID_{cs} \cdot \Delta)$

Let $A = ID_{cr} \cdot \varphi$ (Is arithmetic multiplication that result an integer as both ID_{cr} *and* φ are integer like number.

Let $B = \sigma \cdot A_{cs} \cdot ID_{cs} \cdot (\Delta)$ (Is repetitive addition of divisor that result a divisor in the $J(F_q)$ Abelian groups under addition)

The sender can only simplify $\partial = A - B$ and further simplification is not possible as an integer $A = ID_{cr} \cdot \varphi$ could not be subtracted from divisor $B = \sigma \cdot A_{cs} \cdot ID_{cs} \cdot (\Delta)$ in the $J(F_q)$ both are of different nature. Now the attacker can easy compute φ from $ID_{cr} \cdot \varphi$ as in encryption mode and break message confidentiality.

VI. IMPROVED IDENTITY BASED GENERALIZED SIGNCRYPTION SCHEME

It consists of the following four phases:

1) **Setup:** PKGC performs the following steps:
   a) Selects a hyper-elliptic curve (HEC) over a finite field I_q, of order is q
   b) Selects a divisor D in the Jacobian $J(F_q)$ of HEC
   c) Selects a number uniformly $\delta \in [1, 2, \cdots, (q-1)]$ as PKGC private key
   d) PKGC Computes its public key as $\Lambda = \delta D$
   e) Selects two one-way hash functions: h_a, h_b
   f) Publish public parameters $E = [I_q, \text{HEC}, \text{D}, \Lambda, h_a, h_b]$
2) **Key extraction:**
   a) Each node sends their identity (ID_{pc}) to the PKGC
   b) PKGC Computes private key for identity (ID_{pc}) as $A_{pc} = \delta \cdot h_a(ID_{pc})$ mod q and public key as $B_{pc} = A_{pc} \cdot D$
   c) Transmit securely the private-public key pair to the node having identity ID_{pc}
3) **Generalized signcryption:**
   a) Having a message (m), the sender identity & private key (ID_{cs}, A_{cs}), the receiver identity and public key (ID_{cr}, B_{cr}), the sender generate generalized signcrypted text:
   b) Select $\varphi \in [1, 2, \cdots, (q-1)]$
   c) Computes $\Delta = \varphi \cdot D$
   d) Computes $\beta = \varphi \cdot ID_{cr} \cdot B_{cr}$
   e) Computes $\eta = e_\beta(m||ID_{cs}||ID_{cr}||n_{cs})$
   f) Compute $\sigma = h_b(m||ID_{cs}ID_{cr}||n_{cs})$
   g) Computes $\partial = (\frac{\varphi}{\sigma + A_{cs}} ID_{cs}) \text{mod} q$
   h) Generalized signcryption text $\psi = (\partial, \sigma, \eta, \Delta)$
4) **Generalized Unsigncryption:**
   a) Receiver generalized signcryption text $\psi = (\partial, \sigma, \eta, \Delta)$ and $(A_{cr}, B_{cs}, B_{cr}, ID_{cr})$
   b) Computes $\beta = ID_{cr} \cdot A_{cr} \cdot \Delta$
   c) Computes $(m||ID_{cs}||ID_{cr}||n_{cs}) = d_\beta(\eta)$
   d) Computes $\sigma = h_b(m||ID_{cs}||ID_{cr}||n_{cs}$
   e) If $ID_{cs} \cdot A_{cr} \cdot \Delta = \partial(B_{cs} + \sigma \cdot D)$ accept ψ else $\perp$.

A. CORRECTNESS ANALYSIS

This section presents the proposed scheme's consistency proofs in signature-only mode, encryption-only mode, signcryption mode, and judge verification.

Theorem 1: Improved ID-based Generalized Signcryption (Encryption only mode), Encryption/Decryption is correct if the sender and receiver confirm the equation. $ID_{cr} \cdot A_{cr} \cdot \Delta = ID_{cr} \cdot \varphi \cdot B_{cr}$

Proof: Let

$$\begin{aligned} & ID_{cr} \cdot A_{cr} \cdot \Delta \\ &= ID_{cr} \cdot A_{cr} \cdot \varphi \cdot D \\ &= ID_{cr} \cdot \varphi \cdot A_{cr} D \\ &= ID_{cr} \cdot \varphi \cdot B_{cr} \end{aligned}$$

Clearly, the equation $ID_{cr} \cdot A_{cr} \cdot \Delta = ID_{cr} \cdot \varphi \cdot B_{cr}$ is established. □

Theorem 2: Improved ID based Generalized Signcryption (signature only mode) Signature/Verification is valid if sender and each receiver confirm to the Equation. $\partial(B_{cs} + \sigma \cdot D) = ID_{cs} \cdot \Delta$

Proof: Let

$$\begin{aligned} & \partial(B_{cs} + \sigma \cdot D) \\ &= (\frac{\varphi}{\sigma + A_{cs}} ID_{cs})(B_{cs} + \sigma \cdot D)) \\ &= (\frac{\varphi}{\sigma + A_{cs}} ID_{cs})(A_{cs} \cdot D + \sigma \cdot D)) \\ &= (\frac{\varphi}{\sigma + A_{cs}} ID_{cs})(A_{cs} + \sigma) D)) \\ &= (\frac{\varphi}{\sigma + A_{cs}} ID_{cs})(A_{cs} + \sigma) D)) \\ &= \phi \cdot ID_{cs} \cdot D \\ &= ID_{cs} \cdot \varphi \cdot D \\ &= ID_{cs} \cdot \Delta \end{aligned}$$

Clearly, the equation $\partial(B_{cs} + \sigma \cdot D) = ID_{cs} \cdot \Delta$ is established. □

Theorem 3: Improved ID based Generalized Signcryption (signcryption only mode) Signcryption/ Unsigncryption is valid if sender and receiver confirm to the Equation $ID_{cr} \cdot A_{cr} \cdot \Delta = ID_{cr} \cdot \varphi \cdot B_{cr}$ *and* $\partial(B_{cs} + \sigma \cdot D) = ID_{cs} \cdot \Delta$

Proof: Both the equation holds as proved in Theorem 1 and 2. □

B. PROPOSED SCHEME DEPLOYMENT

This section of the paper presents the proposed scheme deployment in the UAV networks within different filed for monitoring purposes. This scheme comprises three distinct phases: System initialization, registration, transmission, and verification.

1) SYSTEM INITIALIZATION

It starts the setup algorithm after calling PKG to initiate the process. Its chooses the security parameters such k, HEC with a genus number, a divisor D, q a parameter with a length of 80 bits, two one way hash functions (h_a and h_b) a keyspace for randomly choosing a private key $\delta \in \{1, 2, \cdots, (q-1)\}$ and associated public key computed as $\Lambda = \delta \cdot D$. The key tuple $E = \{k, h_a, h_b, q, D, HEC, \Lambda\}$ share publicly for the various communication processes. This phase of the proposed technique also introduces the identities of the various nodes participating in the secure communication process: ID_{mec} identity for MEC-UAV, ID_{mbs}, the identity used for

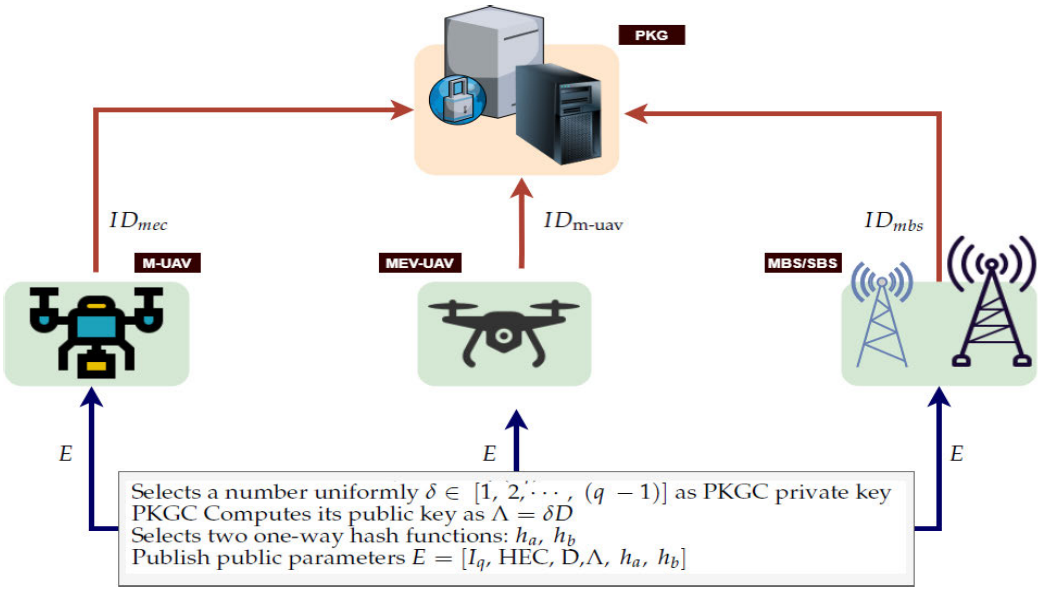

FIGURE 4. System initialization.

MBS/SBS, and $ID_{\text{m-uav}}$ for the identity of M-UAV as shown in Fig 4.

2) REGISTRATION PHASE

This phase of the proposed scheme initializes the extraction algorithm first, and the nodes/participants share IDs with PKG shown in Fig 5. The PKG generates and transmits private keys to each node on behalf of the ID concern. Though, the KPG generates a private key for the ID_pc as $A_{pc} = \delta \cdot h_a(ID_{pc}) \bmod q$, and the associated public key for the said ID would be computed as $B_{pc} = A_{pc} \cdot D$. Similarly, the above public and private keys generation process for other nodes generated which would be (A_{mec}, B_{mec}), (A_{mbs}, B_{mbs}), and (A_{m-uav}, B_{m-uav}). PKG shares the respective key pair to each node using a private communication channel.

3) DATA TRANSMISSION AND VERIFICATION PHASE

This phase of the proposed scheme performs generalized signcryption operation on the sending data and forwards the message to the receiver of the message to receive and verify the message's contents after the Unsigncrypting received a signcrypted message as shown in Fig 6. The MEC-UAV plays the role as a sender and executes the following process as; first chooses a random number $\varphi \in \{1, 2, \cdots, (q-1)\}$ and computes $\Delta = \varphi \cdot D$, $\Delta = \varphi \cdot D$. Next computes $\beta = \varphi \cdot ID_{cr} \cdot B_{cr}$ and $\eta = e_\beta(m||ID_{cs}||ID_{cr}||n_{cs})$ and Compute $\sigma = h_b(m||ID_{cs}ID_{cr}||n_{cs})$. At the end computes $\partial = (\frac{\varphi}{\sigma + A_{cs}} ID_{cs}) \bmod q$ and sends the generalized signcrypted text $\psi = (\partial, \sigma, \eta, \Delta)$. In case the $ID_{mec} = null$ and $ID_mb \neq$ null,then MEC-UAV runs in the in the encryption only mode of generalized signcryption or if the $ID_{mec} \neq$ null, then sender MEC-UAV runs in the signature only mode or If $ID_{mbs} \neq$ null and $ID_mec \neq$ null, then MEC-UAV runs in the signcryption only mode. MBS/SBS unsigncryption process after receiving the text tuple $\psi = (\partial, \sigma, \eta, \Delta)$. The unsigncryption process areas; first computes $\beta = ID_{cr} \cdot A_{cr} \cdot \Delta$, than computes $(m||ID_{cs}||ID_{cr}||n_{cs}) = d_\beta(\eta)$, $\sigma = h_b(m||ID_{cs}||ID_{cr}||n_{cs}$, computes $ID_{cs} \cdot A_{cr} \cdot \Delta = \partial(B_{cs} + \sigma \cdot D)$ if holds, then accept ψ otherwise generates the error symbol $\perp$.

VII. IMPROVED SCHEME ANALYSIS

The improved scheme analyzed based on the security aspect and computational cost reflect in the following subsections.

A. SECURITY ANALYSIS

The Improved ID-based Generalized Signcryption provides basic security properties such as message confidentiality, message integrity, sender authenticity, unforgeability, as well as resistive against a replay attack and Sybil attack.

1) CONFIDENTIALITY

The improved ID based Generalized Signcryption ensures confidentiality. If an attacker wants to steal the contents of a message. The must have private key of the sender or receiver(A_{cs} *and* A_{cr}) or session key φ:

1) Computing A_{cs} from $B_{cs} = A_{cs} \cdot D$ and A_{cr} from $B_{cr} = A_{cr} \cdot D$ is equivalent to HECDLP solving, That is intractable.
2) Computing session key from φ from equation $\partial = (\frac{\varphi}{\sigma + A_{cs}} ID_{cs}) \bmod q$ is equivalent to solving one equation having two unknown, that is infeasible.

2) INTEGRITY

To generate generalized signcrypted text $\psi = (\partial, \sigma, \eta, \Delta)$, the Sender compute $\sigma = h_b(m||ID_{cs}||ID_{cr}||n_{cs}$ and $\partial = (\frac{\varphi}{\sigma + A_{cs}} ID_{cs}) \bmod q$ using hash function having strong

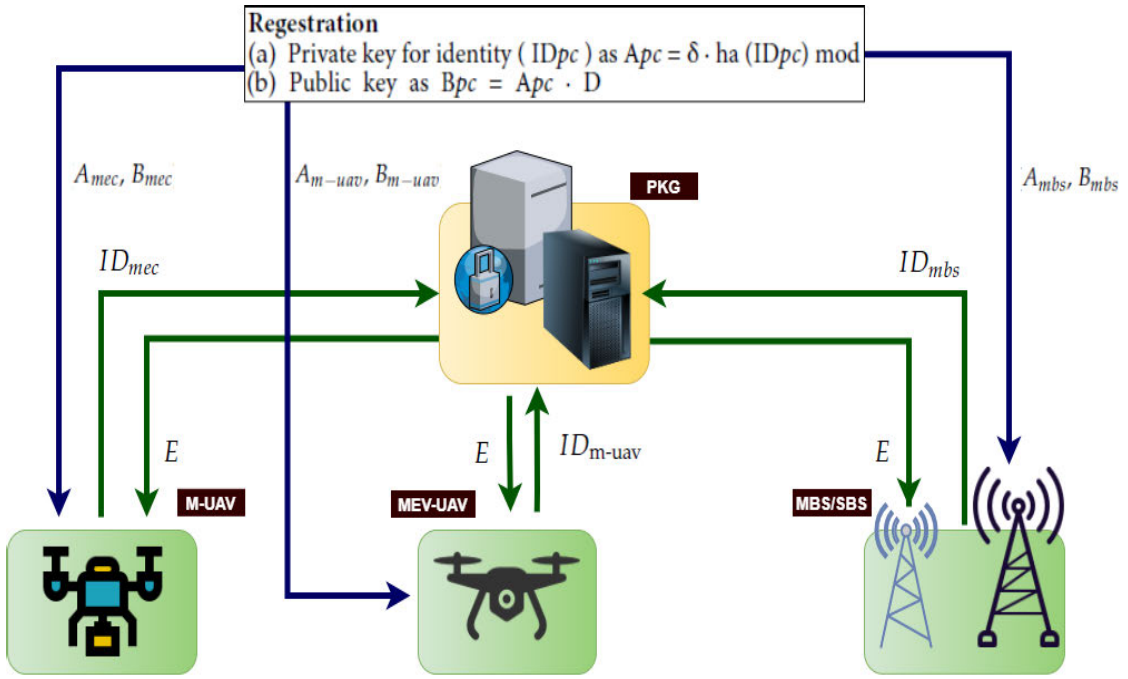

FIGURE 5. Registration phase.

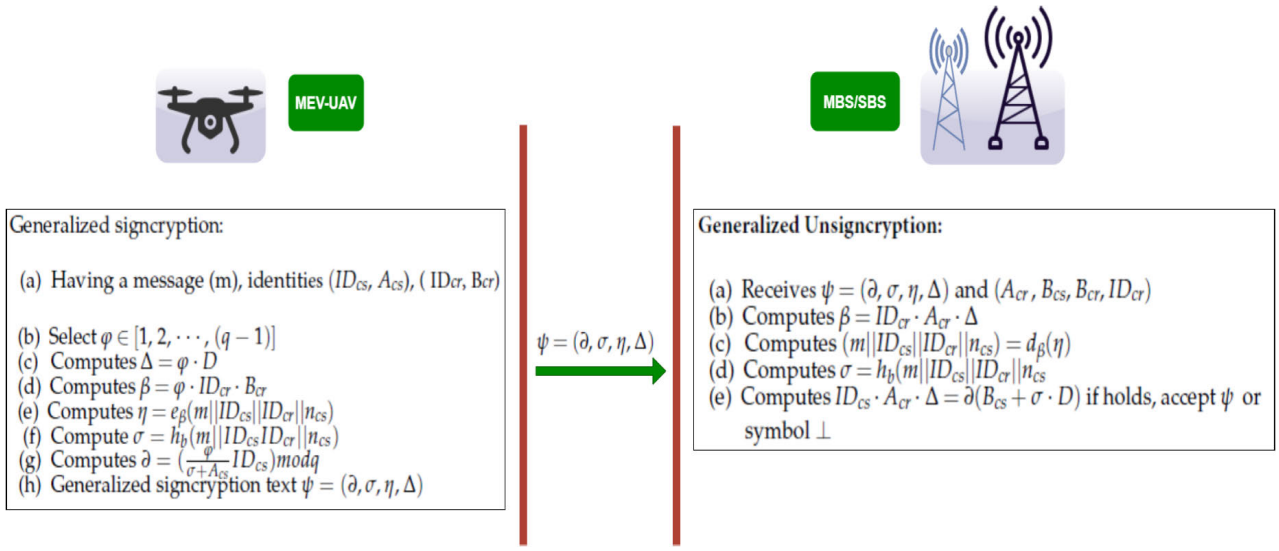

FIGURE 6. Data transmission and verification.

collision resistance and computes $\partial = (\frac{\varphi}{\sigma + A_{cs}} ID_{cs})$ mod q using sender priivate key. The receiver verify ψ using $\sigma = h_b(m||ID_{cs}||ID_{cr}||n_{cs}$ and $ID_{cs}.A_{cr}.\Delta = \partial(B_{cs} + \sigma.D)$. if the attacker change the message due to strong collision resistance the receiver can confirm either the message is original one or fabricated.

3) AUTHENTICITY

The improved scheme provides sender authenticity. The sender computes generalized signcrypted text $\psi = (\partial, \sigma, \eta, \Delta)$ using his private key A_{cs} as $\sigma = h_b(m||ID_{cs}||ID_{cr}||n_{cs}$ and $\partial = (\frac{\varphi}{\sigma + A_{cs}} ID_{cs})$ mod q. The receiver verify the message using sender public key $ID_{cs}.A_{cr}.\Delta = \partial(B_{cs} + \sigma.D)$, this confirm that the message is signcrypted by the legitimate sender.

4) UNFORGEABILITY

The proposed improved scheme provides sender unforgeability. The sender computes generalized signcrypted text $\psi = (\partial, \sigma, \eta, \Delta)$ using his private key A_{cs} as $\sigma = h_b(m||ID_{cs}||ID_{cr}||n_{cs}$ and $\partial = (\frac{\varphi}{\sigma + A_{cs}} ID_{cs})$ mod q. If an attacker wants to forge the message he/she must have sender

TABLE 2. Security analysis.

$\mathcal{S}$chemes	$\mathcal{C}$onfidentiality	$\mathcal{I}$ntegrity	$\mathcal{A}$uthenticity	$\mathcal{U}$nforgeability	$\mathcal{R}$eplay $\mathcal{A}$ttack
Yu *et al.* [28]	✓	✓	✓	✓	×
Kushwah *et al.* [29]	✓	✓	✓	✓	×
Wei *et al.* [15]	✓	✓	✓	✓	×
Shen *et al.* [17]	✓	✓	✓	✓	×
Zhou *et al.* [18]	✓	✓	✓	✓	×
Khan et al [19]	×	×	×	×	✓
Proposed	✓	✓	✓	✓	✓

TABLE 3. Cost analysis.

$\mathcal{S}$chemes	$\mathcal{G}$eneralized $\mathcal{S}$igncryption $\mathcal{C}$ost	$\mathcal{G}$eneralized $\mathcal{U}$nsigncryption $\mathcal{C}$ost	$\mathcal{C}$ommunication $\mathcal{O}$verhead
Yu *et al.* [28]	$4\mathbb{BPM} + 1\mathbb{BP} + 1\mathbb{M}$exp	$1\mathbb{BPM} + 3\mathbb{BP} + 3\mathbb{M}$exp	$\|\mathbb{S}\|$
Kushwah *et al.* [29]	$5\mathbb{BPM} + 2\mathbb{M}$exp	$4\mathbb{BPM} + 2\mathbb{BP} + 3\mathbb{M}$exp	$\|\mathbb{S}\|$
Wei *et al.* [15]	$9\mathbb{BPM} + 1\mathbb{BP} + 7\mathbb{M}$exp	$2\mathbb{BPM} + 4\mathbb{BP}$	$7\|\mathbb{S}\|$
Shen *et al.* [17]	$2\mathbb{BPM} + 6\mathbb{M}$exp	$5\mathbb{BPM} + 2\mathbb{M}$exp	$4\|\mathbb{S}\|$
Zhou *et al.* [18]	$3\mathbb{BPM} + 1\mathbb{BP}$	$1\mathbb{BPM} + 2\mathbb{BP}$	$\|\mathbb{S}\|$
Khan *et al.* [19]	$6\mathbb{HECDM}$	$5\mathbb{HECDM}$	$3\|\mathbb{Z}_n\|$
Improved	$2\mathbb{HECDM}$	$4\mathbb{HECDM}$	$3\|\mathbb{Z}_n\|$

$\mathbb{HECDM}$ = Hyperelliptic curve divisor scalar multiplication, $\mathbb{ECPM}$ = Elliptic curve point scalar multiplication, $\mathbb{BP}$ = Bilinear pairing, $\mathbb{BPM}$ = pairing-based point multiplications, $\mathbb{M}$exp= Modular exponentiation.

TABLE 4. Computational cost in milliseconds (ms).

$\mathcal{S}$chemes	$\mathcal{G}$eneralized $\mathcal{S}$igncryption (ms)	$\mathcal{G}$eneralized $\mathcal{U}$nsigncryption (ms)	$\mathcal{T}$otal $\mathcal{C}$ost (ms)
Yu *et al.* [28]	33.39	58.38	86.23
Kushwah *et al.* [29]	24.05	50.79	74.84
Wei *et al.* [15]	62.44	68.22	130.66
Shen *et al.* [17]	16.12	24.05	40.17
Zhou *et al.* [18]	27.83	34.11	61.94
Khan et al [19]	2.88	2.40	5.28
Improved	0.96	1.92	2.88

private key and computing sender private key is equivalent to solving intractable Hyperelliptic curve discrete log problem.

5) REPLAY ATTACK

The sender generate generalized signcrypted text using one time nonce n_{cs} and hash function $\sigma = h_b(m||ID_{cs}||ID_{cr}||n_{cs})$. for an intruder it is infeasible to launch a replay attack.

The improved scheme is compared with the state of the art schemes that are Yu *et al.* 's scheme [28], Wei *et al.* 's scheme [29], Kushwah *et al.* 's scheme [15], Zhou *et al.* 's scheme [17], Shen *et al.* 's scheme [18] and Khan *et al.* [19] as shown in Table 2.

6) SYBIL ATTACK

In this type of attack, a node in peer-to-peer networks operates with multiple identities actively at the same time and influences the authority/power in reputation systems. In the proposed system, the multi-access edge computing node verifies identity with each node's public key and prevents Sybil attack.

B. COST ANALYSIS

FANETs have low battery and computation power resources. Therefore, computational cost and communication overhead efficiency are of prime importance in FANETs.

1) COMPUTATION COST

Computation power is required for needed security operations. The proposed improved scheme consumed fewer computation resources and resources for the desired security requirement. The improved scheme compared with state of the art existing schemes proposed by Yu *et al.* [28], Kushwah *et al.* [29], Wei *et al.* [15], Shen *et al.* [17], Zhou *et al.* [18], and Khan *et al.* [19].

TABLE 5. Percent computation cost reduction.

$\mathcal{S}$chemes	$\mathcal{G}$eneralized $\mathcal{S}$igncryption	$\mathcal{G}$eneralized $\mathcal{U}$nsigncryption
Yu *et al.* [28]	97.12 %	96.71 %
Kushwah *et al.* [29]	96.008 %	96.21 %
Wei *et al.* [15]	98.46 %	97.18 %
Shen *et al.* [17]	94.044 %	92.01 %
Zhou *et al.* [18]	96.55 %	94.37 %
Khan et al [19]	66.66 %	20 %

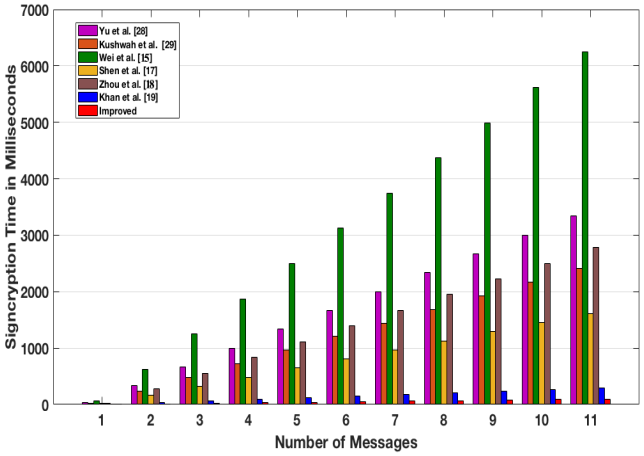

FIGURE 7. Signcryption performance comparison.

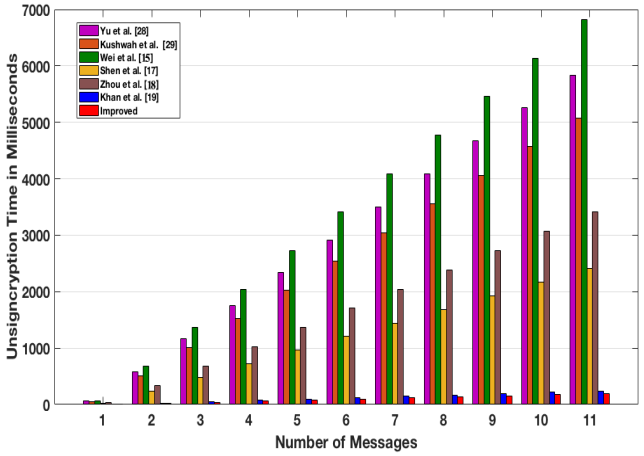

FIGURE 8. Unsigncryption performance comparison.

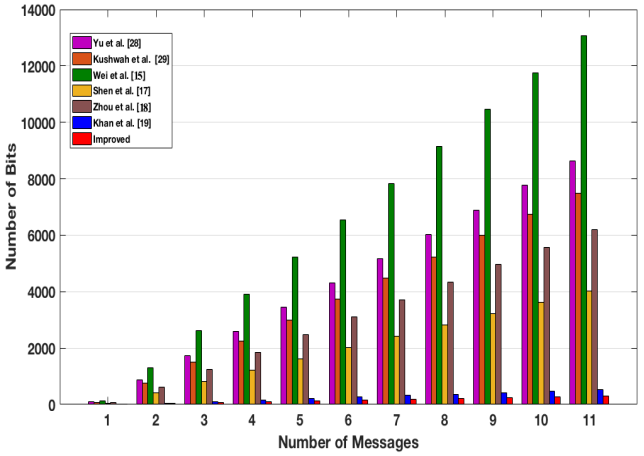

FIGURE 9. Communication overhead performance comparison.

TABLE 6. Communication overhead in bits.

$\mathcal{S}$chemes	$\mathcal{C}$omm-$\mathcal{O}$verhead (bits)
Yu *et al.* [28]	1024
Kushwah *et al.* [29]	1024
Wei *et al.* [15]	7168
Shen *et al.* [17]	4096
Zhou *et al.* [18]	1024
Khan et al [19]	240
Improved	240

TABLE 7. Percent communication overhead reduction.

$\mathcal{S}$chemes	$\mathcal{C}$omm-$\mathcal{O}$verhead $\mathcal{R}$eduction
Yu *et al.* [28]	76.56 %
Kushwah *et al.* [29]	76.56 %
Wei *et al.* [15]	96.65 %
Shen *et al.* [17]	94.14 %
Zhou *et al.* [18]	76.56 %

In all mentioned schemes, major and most expensive operations are $\mathbb{ECPM}$, $\mathbb{BP}$, $\mathbb{BPM}$, $\mathbb{M}$exp and $\mathbb{HECDM}$. Based on the result presented in [18], [19], [30], For testing the simulation results, a workstation having the specifications: Intel Core $i7-4510U$ CPU @ 2.0 GHz, 8 GB RAM, and Windows 7 Home Basic 64-bit Operating System is used. Based on the simulation results presented, $\mathbb{ECPM}$ takes 0.97 ms; $\mathbb{BP}$ takes 14.90 ms; $\mathbb{BPM}$ takes 4.31 ms; $\mathbb{M}$exp takes 1.25 ms, and $\mathbb{HECDM}$ takes 0.48 ms duration. Based on these results, the time comparison of the proposed and existing schemes is presented in Tables 3, 4, and the percent computation cost reduction is presented in Table 5.

2) COMMUNICATION OVERHEAD

Communication overhead is the extra bits appended with an encrypted message for security and is one of the vital performance indicators. The improved scheme compared with existing schemes Yu *et al.* [28], Kushwah *et al.* [29], Wei *et al.* [15], Shen *et al.* [17], Zhou *et al.* [18], Khan *et al* [19]. The comparison is based on the NIST standard parameters (value in bits): $|\mathbb{S}| = 1024$, $|\mathbb{Z}_q| = 160$, $|\mathbb{Z}_n| = 80$, $|\mathbb{H}| = 512$, $|\mathbb{W}| = 1024$. The results are presented in Tables 3,6 and the percent communication cost reduction is presented in Table 7.

Table 4 shows percent cost reduction of proposed then the existing schemes.

VIII. CONCLUSION

This paper presented cryptanalysis of Khan *et al.* scheme. The analysis of this paper showed that their scheme is insecure and did not provide message confidentiality, Authenticity, and integrity. This paper also presented an improved ID based generalized signcryption scheme. The proposed improved scheme is provably secure against the mentioned security attacks. The improved scheme is efficient and attractive for multi-access edge computing empowered FANETs proved after the comparison with other state-of-the-art schemes. In the future, it is possible to extend this concept for heterogeneous generalized signcryption for multi-access edge computing empowered FANETs.

REFERENCES

[1] P. Lottes, R. Khanna, J. Pfeifer, R. Siegwart, and C. Stachniss, "UAV-based crop and weed classification for smart farming," in *Proc. IEEE Int. Conf. Robot. Autom. (ICRA)*, May 2017, pp. 3024–3031.

[2] J. Sánchez-García, D. G. Reina, and S. L. Toral, "A distributed PSO-based exploration algorithm for a UAV network assisting a disaster scenario," *Future Gener. Comput. Syst.*, vol. 90, pp. 129–148, Jan. 2019.

[3] T. Kopfstedt, M. Mukai, M. Fujita, and C. Ament, "Control of formations of UAVs for surveillance and reconnaissance missions," *IFAC Proc. Volumes*, vol. 41, no. 2, pp. 5161–5166, 2008.

[4] D. Bein, W. Bein, A. Karki, and B. B. Madan, "Optimizing border patrol operations using unmanned aerial vehicles," in *Proc. 12th Int. Conf. Inf. Technol.-New Gener.*, Las Vegas, NV, USA, Apr. 2015, pp. 479–484.

[5] E. Semsch, M. Jakob, D. Pavlicek, and M. Pechoucek, "Autonomous UAV surveillance in complex urban environments," in *Proc. IEEE/WIC/ACM Int. Joint Conf. Intell. Intell. Agent Technol.*, vol. 2, Sep. 2009, pp. 82–85.

[6] C. Barrado, R. Messeguer, J. Lopez, E. Pastor, E. Santamaria, and P. Royo, "Wildfire monitoring using a mixed air-ground mobile network," *IEEE Pervasive Comput.*, vol. 9, no. 4, pp. 24–32, Oct./Dec. 2010.

[7] A. Cho, J. Kim, S. Lee, and C. Kee, "Wind estimation and airspeed calibration using a UAV with a single-antenna GPS receiver and Pitot tube," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 47, no. 1, pp. 109–117, Jan. 2011.

[8] *Amazon: Prime Air*. Accessed: Apr. 6, 2021. [Online]. Available: https://www.amazon.com/Amazon-Prime-Air/b?ie=UTF8&node=8037720011

[9] M. Y. Arafat and S. Moh, "Routing protocols for unmanned aerial vehicle networks: A survey," *IEEE Access*, vol. 7, pp. 99694–99720, 2019.

[10] I. García-Magariño, R. Lacuesta, M. Rajarajan, and J. Lloret, "Security in networks of unmanned aerial vehicles for surveillance with an agent-based approach inspired by the principles of blockchain," *Ad Hoc Netw.*, vol. 86, pp. 72–82, Apr. 2019.

[11] S. He, Q. Wu, J. Liu, W. Hu, B. Qin, and Y. Li, "Secure communications in unmanned aerial vehicle network," in *Proc. Int. Conf. Inf. Secur. Pract. Exper.*, 2017, pp. 601–620.

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

[13] J. Srinivas, A. K. Das, N. Kumar, and J. J. P. C. Rodrigues, "Cloud centric authentication for wearable healthcare monitoring system," *IEEE Trans. Dependable Secure Comput.*, vol. 17, no. 5, pp. 942–956, Sep. 2020.

[14] S. Lal and P. Kushwah, "ID based generalized signcryption," in *Proc. IACR*, 2008, p. 84.

[15] G. Wei, J. Shao, Y. Xiang, P. Zhu, and R. Lu, "Obtain confidentiality or/and authenticity in Big Data by ID-based generalized signcryption," *Inf. Sci.*, vol. 318, pp. 111–122, Oct. 2015, doi: 10.1016/j.ins.2014.05.034.

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

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

[18] Y. Zhou, Z. Li, F. Hu, and F. Li, "Identity-based combined public key schemes for signature, encryption, and signcryption," in *Information Technology and Applied Mathematics*. Singapore: Springer, 2019, pp. 3–22, doi: 10.1007/978-981-10-7590-2_1.

[19] M. A. Khan, I. Ullah, S. Nisar, F. Noor, I. M. Qureshi, F. Khanzada, H. Khattak, and M. A. Aziz, "Multiaccess edge computing empowered flying ad hoc networks with secure deployment using identity-based generalized signcryption," *Mobile Inf. Syst.*, vol. 2020, Jul. 2020, Art. no. 8861947.

[20] 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. 2021.

[21] G. M. Leal, I. Zacarias, J. M. Stocchero, and E. P. D. Freitas, "Empowering command and control through a combination of information-centric networking and software defined networking," *IEEE Commun. Mag.*, vol. 57, no. 8, pp. 48–55, Aug. 2019.

[22] P. V. Reddy, A. R. Babu, and N. B. Gayathri, "Efficient and secure identity-based strong key-insulated signature scheme without pairings," *J. King Saud Univ.-Comput. Inf. Sci.*, 2018, doi: 10.1016/j.jksuci.2018.08.011.

[23] H. Xiong, Q. Mei, and Y. Zhao, "Efficient and provably secure certificateless parallel key-insulated signature without pairing for IIoT environments," *IEEE Syst. J.*, vol. 14, no. 1, pp. 310–320, Mar. 2020.

[24] M. A. Khan, I. Ullah, S. Nisar, F. Noor, I. M. Qureshi, F. M. Khanzada, and N. U. Amin, "An efficient and provably secure certificateless key-encapsulated signcryption scheme for flying ad-hoc network," *IEEE Access*, vol. 8, pp. 36807–36828, 2020.

[25] M. A. Khan, I. Ullah, N. Kumar, O. Oubbati, I. Qureshi, F. Noor, and F. Ullah, "An efficient and secure certificate-based access control and key agreement scheme for flying ad hoc network," *IEEE Trans. Veh. Technol.*, vol. 70, no. 5, pp. 4839–4851, Feb. 2021.

[26] A. Menezes, R. Zuccherato, and Y. Wu, "An elementary introduction to hyperelliptic curves," Dept. C&O, Univ. Waterloo, Waterloo, ON, Canada, Tech. Rep. CORR 96-19, Nov. 1996.

[27] N. Koblitz, "Hyperelliptic cryptosystems," *J. Cryptol.*, vol. 1, no. 3, pp. 139–150, 1989.

[28] G. Yu, X. Ma, Y. Shen, and W. Han, "Provable secure identity based generalized signcryption scheme," *Theor. Comput. Sci.*, vol. 411, nos. 40–42, pp. 3614–3624, Sep. 2010.

[29] P. Kushwah and S. Lal, "An efficient identity based generalized signcryption scheme," *Theor. Comput. Sci.*, vol. 412, no. 45, pp. 6382–6389, Oct. 2011.

[30] M. A. Khan, I. M. Qureshi, I. Ullah, S. Khan, F. Khanzada, and F. Noor, "An efficient and provably secure certificateless blind signature scheme for flying ad-hoc network based on multi-access edge computing," *Electronics*, vol. 9, no. 1, p. 30, Dec. 2019.

NIZAMUD DIN received the M.Sc. degree from the University of Peshawar, in 2007, the M.S. degree from the International Islamic University Islamabad, in 2012, and the Ph.D. degree in computer science from Hazara University Mansehra, in 2016. He is currently working as an Assistant Professor with the Department of Computer Science, University of Chitral. He has published one book and more than 35 research papers in different conferences and journals of international repute. His current research interests include cryptography, *ad-hoc* and sensor network security, electronic voting security, and secure communications in the IoT.

ABDUL WAHEED received the master's and Ph.D. degrees in computer science from the Department of Information Technology, Hazara University Mansehra, in 2014 and 2021, respectively. He was a Ph.D. Researcher with the NetLab-INMC, School of Electrical and Computer Engineering (ECE), Seoul National University (SNU), South Korea, in 2019, under the HEC Research Program. He is currently a member of the Crypto-Net Research Group, Hazara University Mansehra. He also serves as a Lecturer for the Department of Computer Science, IQRA National University, Peshawar. He has numerous publications in journals and international conferences. His research interests include information security, secure and smart cryptography, heterogeneous communications within the IoT, mobile *ad-hoc* networks (MANETs), wireless sensor networks (WSNs) security, and fuzzy logic-based decision-making theory.

MAHDI ZAREEI (Senior Member, IEEE) received the M.Sc. degree in computer networks from the University of Science, Malaysia, in 2011, and the Ph.D. degree from the Communication Systems and Networks Research Group, Malaysia–Japan International Institute of Technology, University of Technology Malaysia, in 2016. In 2017, he joined the School of Engineering and Sciences, Tecnológico de Monterrey, as a Postdoctoral Fellow, where he has been working as a Research Professor, since 2019. His research interests include wireless sensor and *ad-hoc* networks, energy harvesting sensors, information security, and machine learning. He is a member of the Mexican National Researchers System (level I). He is serving as an Associate Editor for IEEE Access and *Ad Hoc & Sensor Wireless Networks*.

FAISAL ALANAZI received the B.Sc. degree in electrical engineering (electronics and communication) from KSU and the M.Sc. and Ph.D. degrees in electrical and computer engineering from The Ohio State University, in 2013 and 2018, respectively. He is currently working as an Assistant Professor at PSAU. His research interests include cryptography, vehicular *ad-hoc* networks, and delay-tolerant networks. He is a member of the IEEE Communication Society.