TELKOMNIKA Telecommunication, Computing, Electronics and Control
Vol. 24, No. 3, June 2026, pp. 991∼1002
ISSN: 1693-6930, DOI: 10.12928/TELKOMNIKA.v24i3.27677

A robust blind signcryption scheme for secure internet of drones communication

Tahri Rachid[1], Abdellah Ouammou[1], Abdellatif Lasbahani[2], Hibat Eallah Mohtadi[1]
[1]Faculty of Sciences and Technologies, Hassan First University, Settat, Morocco
[2]Faculty of Sciences and Technologies, Sultan Moulay Slimane University, Beni Mellal, Morocco

Article Info

Article history:

Received Nov 18, 2025
Revised Mar 3, 2026
Accepted Mar 29, 2026

Keywords:

Formal verification
Hyper-elliptic curve cryptography
Identity-based cryptography
Internet of drones
Lightweight cryptography
Privacy preservation
Secure communication

ABSTRACT

The rapid deployment of the internet of drones (IoD) exposes aerial networks to authentication failures, eavesdropping, data theft, and impersonation attacks due to open wireless communication. This paper presents a lightweight identity-based blind signcryption scheme for secure IoD communication. The scheme leverages hyper-elliptic curve cryptography to provide strong security with reduced computational overhead, making it suitable for resource-constrained drones. The blind signcryption mechanism enhances privacy by preventing the signer from accessing message content. Informal analysis shows that the scheme achieves confidentiality, authentication, anonymity, forward secrecy, and resistance to common protocol-level attacks. Formal verification using the Scyther tool confirms secrecy, agreement, and authentication properties under a standard symbolic adversary model. Analytical and simulation-based evaluations demonstrate average reductions of 59.60% in computational cost, 48.86% in communication overhead, and 55.75% in energy consumption compared with existing schemes. While the results confirm protocol-level efficiency, real-world implementation and testbed validation remain future work.

Corresponding Author:

Tahri Rachid
Faculty of Sciences and Technologies, Hassan First University
Km 3, B.P. 577 Route de Casablanca, Settat, Morocco
Email: rachid.tahritr@gmail.com

1. INTRODUCTION

The internet of drones (IoD) interconnects unmanned aerial vehicles (UAVs) to support coordinated operations and real-time data exchange across diverse application domains [1], [2]. In IoD environments, drones communicate with neighboring UAVs, ground stations, and external IoT infrastructures through heterogeneous wireless technologies such as wireless fidelity (Wi-Fi), cellular networks (e.g., fourth/fifth generation (4G/5G)), and UAV-to-UAV links. As illustrated in Figure 1, a typical IoD architecture comprises drone, communication, and application layers, enabling scalable and interoperable system operation [3]. This architecture supports latency-sensitive services, including disaster response and surveillance, as well as data-intensive applications such as real-time video transmission for logistics and environmental monitoring [4].

Despite these advantages, the open and dynamic nature of IoD communications introduces significant security risks. Wireless broadcast channels expose systems to eavesdropping, impersonation, replay attacks, and unauthorized command injection [5]. Weak authentication may enable session hijacking and malicious UAV control, while insufficient confidentiality can compromise sensitive mission data [6], [7]. Conventional

approaches rely on separate signature and encryption mechanisms, which increase computational and communication overhead and are often unsuitable for resource-constrained UAV platforms.

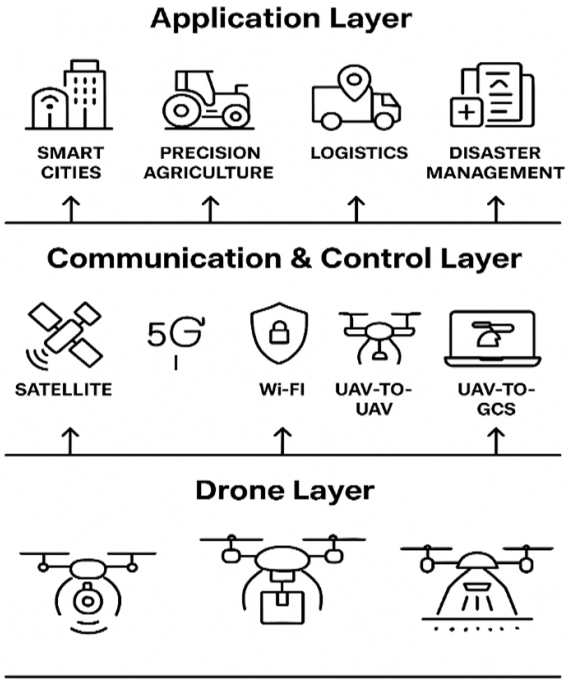


Figure 1. Typical architecture of the IoD

Signcryption integrates encryption and digital signature into a single operation, reducing overhead while preserving essential security properties [8]-[10]. Identity-based cryptography (IBC) further simplifies key management by deriving public keys from unique identifiers, eliminating certificate infrastructure [11]. Blind signcryption enhances privacy by preventing the signer from accessing message content during the signing process [12], [13]. To meet IoD resource constraints, hyper-elliptic curve cryptography (HECC) offers reduced key sizes and lower computational complexity compared with conventional elliptic curve schemes under equivalent security assumptions [14]-[16].

Motivated by these challenges, this paper proposes an identity-based blind signcryption scheme for secure IoD communication. The main contributions are summarized as:

- A lightweight identity-based blind signcryption scheme based on hyper-elliptic curve cryptography for secure and privacy-aware IoD communication.
- Integrated authentication and confidentiality with privacy preservation, forward secrecy, and resistance to impersonation, replay, Sybil, denial-of-service (DoS), and man-in-the-middle (MiTM) attacks under standard adversary assumptions.
- Comprehensive security evaluation through informal analysis and formal symbolic verification.
- Performance assessment demonstrating reduced computational cost, communication overhead, and energy consumption compared with representative state-of-the-art schemes under unified analytical assumptions.

2. RELATED WORK

Signcryption has been extensively studied as an efficient mechanism for securing communications in UAV networks and IoD environments. By integrating digital signature and encryption into a single operation, signcryption reduces computational and communication overhead while preserving confidentiality, integrity, and authentication.

Certificateless and elliptic curve cryptography (ECC)-based signcryption schemes have been widely explored. Yu and Wang [17] proposed a certificateless blind signcryption scheme with reduced computational complexity; however, replay and Sybil attack mitigation are not explicitly addressed. Da *et al.* [18] introduced a

certificateless scheme for UAV cluster networks that ensures authentication and replay resistance, though with relatively high overhead and without automated formal verification. Similarly, Yang *et al.* [19] presented a heterogeneous signcryption scheme supporting multi-ciphertext equality testing, while Ullah *et al.* [20] proposed a generalized ring signcryption scheme providing anonymity and traceability. Despite enhanced functionality, these ECC-based approaches often incur increased computational cost or lack comprehensive protection against replay and Sybil attacks.

Pairing-based constructions have also been investigated to strengthen security guarantees. Qu and Zeng [21] developed a certificateless proxy signcryption scheme in the standard model with resistance to replay and man-in-the-middle attacks; however, bilinear pairings significantly increase computational and energy consumption. Hundera *et al.* [22] proposed an online/offline heterogeneous proxy signcryption scheme to reduce online overhead, though forward secrecy is not fully ensured.

To improve efficiency, lightweight designs have been proposed. Khan *et al.* [23] introduced a certificate-based ring signcryption scheme using HECC, achieving improved efficiency and replay resistance. Verma *et al.* [24] proposed a signcryption-based data aggregation scheme with batch verification, though it remains vulnerable to denial-of-service attacks. Other aggregate and heterogeneous approaches [25]-[27] focus on efficiency and authentication but often lack anonymity guarantees or comprehensive formal validation.

More recently, identity-based and online/offline signcryption schemes have aimed to simplify key management and reduce overhead. Ali *et al.* [28] presented an identity-based online/offline scheme for UAV-to-ground communication with formal security analysis under the random oracle model. Zou *et al.* [29] proposed a certificateless aggregated signcryption scheme for edge-assisted aerial and vehicular networks, achieving authentication and efficiency but still relying on elliptic curve operations with non-negligible resource consumption.

Recent surveys emphasize that most existing IoD signcryption schemes focus primarily on protocol-level security and analytical evaluation [30]. Implementation-level threats including side-channel leakage, physical capture, weak randomness, and hardware-induced vulnerabilities are typically outside the scope of symbolic verification tools [31], [32]. These limitations motivate the proposed identity-based blind signcryption scheme, which combines lightweight HECC-based design, formal symbolic verification, and consideration of implementation-oriented security aspects for resource-constrained IoD environments.

3. NETWORK MODEL

The proposed architecture consists of three entities: drones, a key generation center (KGC), and a ground station (GS), as illustrated in Figure 2. These entities enable secure and privacy-aware communication in IoD environments under resource and mobility constraints.

Drones operate across different regions to perform sensing and monitoring tasks. They communicate with neighboring UAVs via short-range drone-to-drone (D2D) links (e.g., mesh or Wi-Fi) and with the GS through medium- or long-range wireless technologies such as 4G/5G. This hybrid connectivity supports local coordination and reliable data delivery.

The GS serves as a gateway between drones and the control infrastructure. It receives signcrypted messages, verifies their authenticity, decrypts valid ciphertexts, and forwards verified data to upper-layer applications. To enhance privacy, drones interact with the GS using pseudo-identities rather than real identities.

The KGC is a trusted-but-curious authority responsible for identity-based key generation. During initialization, drones and the GS submit pseudo-identities to the KGC, which generates and securely distributes corresponding private keys. Although trusted to execute key generation correctly, the KGC does not access plaintext messages. In the blind signcryption process, it operates only on blinded values and cannot link signatures to specific communications.

When transmitting sensitive data, a drone performs blind signcryption by generating a signature with its identity-based private key and encrypting the message using a session key derived from the GS's public parameters. Upon reception, the GS executes unsigncryption, verifying authenticity before decrypting the ciphertext. This design ensures authenticated and privacy-preserving communication under the assumed adversarial model.

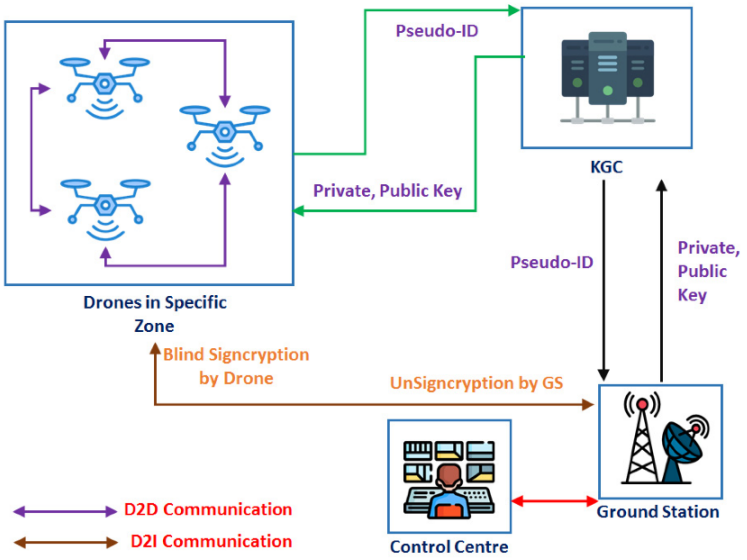


Figure 2. Flow of the proposed scheme

4. CONSTRUCTION OF THE PROPOSED SCHEME

This section presents the proposed identity-based blind signcryption scheme under standard cryptographic assumptions and a protocol-level adversary model. The adopted notation is summarized in Table 1.

Table 1. Symbols used in the proposed scheme

Symbol	Explanation	Symbol	Explanation
Mpv_{KGC}	Master private key of the KGC	Mpb_{KGC}	Master public key of the KGC
Pid_{entity}	Pseudo-identity	α_{entity}	Private key
β_{entity}	Public key	B_F	Blinding factor
δ	Blind signature	k	Ephemeral private key
n	Nonce	$\mathcal{C}$	Ciphertext
Sh	Shared secret	sk	Session key

5. INFORMAL SECURITY ANALYSIS

This section analyzes the security of the proposed identity-based blind signcryption scheme under a protocol-level adversary model. The analysis assumes standard cryptographic hardness (HECDLP) and secure key initialization. A comparison with representative schemes is summarized in Table 2.

- Authentication: is ensured by verifying the blind signature δ and response value R. Validity of δ confirms KGC authorization, while R requires knowledge of the drone's private key α_{drone}. Forgery is computationally infeasible under the HECDLP assumption.
- Confidentiality: messages are encrypted using a session key sk derived from the shared secret Sh. Without the corresponding ephemeral private keys, an adversary cannot recover sk.
- Integrity: is guaranteed through hash functions H_1, H_2, and H_3, as any modification alters verification values and leads to rejection.
- Anonymity and privacy preservation: pseudo-identities Pid_{entity} conceal real identities, while blind signcryption prevents the KGC from accessing message content or linking signatures to specific sessions.
- Forward secrecy: fresh ephemeral keys are generated for each session; compromise of long-term keys does not reveal previously established session keys.
- Replay and impersonation mitigation: the nonce n ensures freshness and prevents replay. Impersonation is infeasible without the KGC master key or the drone's private key.
- Sybil-attack mitigation: pseudo-identities are issued and controlled by the KGC, preventing arbitrary identity generation.

- DoS mitigation: the GS verifies δ and R prior to decryption, enabling early rejection of invalid messages and reducing resource exhaustion.
- Collision resistance: collision-resistant hash functions prevent adversaries from generating distinct inputs with identical hash outputs.
- Node-capture considerations: ephemeral key usage limits exposure of past sessions in case of device compromise; however, physical capture and side-channel threats remain outside the protocol-level model.
- MiTM mitigation: authenticated key establishment and signature verification prevent message alteration or injection without legitimate private keys.

Table 2. Comparative security analysis of existing schemes and the proposed approach

Scheme	F1	F2	F3	F4	F5	F6	F7	F8	F9	F10	F11	F12	F13	F14	F15
[17]	Y	Y	Y	Y	Y	N	Y	N	N	Y	Y	Y	Y	Y	N
[19]	Y	Y	Y	N	N	N	Y	N	N	Y	Y	Y	Y	Y	N
[21]	Y	Y	Y	N	N	Y	Y	N	N	Y	N	N	N	Y	N
[23]	Y	Y	Y	Y	N	Y	Y	N	Y	Y	Y	Y	N	Y	N
[26]	Y	Y	Y	N	N	Y	Y	Y	Y	Y	Y	N	Y	Y	N
Proposed	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

F1 : Authentication
F2 : Confidentiality
F3 : Integrity
F4 : Anonymity
F5 : Privacy preservation
F6 : Replay-attack mitigation
F7 : Eavesdropping resilience
F8 : DoS-attack mitigation
F9 : Sybil-attack mitigation
F10 : Impersonation-attack mitigation
F11 : Collision-attack resistance
F12 : Node-capture resilience
F13 : Forward secrecy
F14 : Man-in-the-middle (MiTM) mitigation
F15 : Formal security verification using automated tools
Y : Yes
N : No

5.1. Parameter rationale

The adopted parameters follow prior lightweight internet of things (IoT) and HECC-based security schemes to ensure fair comparison. Genus-2 hyper-elliptic curves balance efficiency and security, while SHA-3 with domain separation mitigates cross-protocol collisions. Message size and security-level mappings are selected for relative benchmarking under unified analytical assumptions rather than absolute deployment guarantees.

6. PERFORMANCE ANALYSIS

This section evaluates the proposed identity-based blind signcryption scheme through comparative analysis with representative approaches, focusing on computational and communication costs, which are critical in resource-constrained IoD environments. The evaluation follows standard analytical modeling and benchmark-based measurements under unified assumptions. The reported results reflect protocol-level efficiency. Hardware-specific latency, wireless channel variability, and battery discharge behavior are not directly measured and remain topics for future experimental validation.

6.1. Computational cost

Computational cost represents the total execution time of dominant cryptographic operations during signcryption and unsigncryption. Lightweight operations (e.g., hashing and concatenation) are neglected, consistent with prior comparative studies.

The considered operations include bilinear pairing (β_P), pairing multiplication (p_m), elliptic-curve scalar multiplication (εC_m), and hyper-elliptic curve divisor multiplication ($h\varepsilon D_m$). Their average execution times are summarized in Table 3, based on benchmarks reported in [23], [27].

All simulations were conducted using an Intel Core i7-6700 @ 3.40 GHz with 8 GB RAM under Ubuntu 16.04 using the MIRACL cryptographic library. This configuration serves solely as a consistent baseline for comparison and does not represent a specific IoD deployment. Benchmarking scope: t he timing values adopted from [23], [27]. ensure consistency with prior studies. Results should therefore be interpreted as relative analytical comparisons rather than absolute performance guarantees for real-world drone hardware.

Table 3. Single operation time consumption (milliseconds)

Operation	β_P	p_m	εC_m	$h\varepsilon D_m$
Time (ms)	4.669	0.788	0.341	0.1705

Tables 4 and 5 present the number of cryptographic operations and the corresponding total execution time for each scheme. As illustrated in Figure 3, the proposed scheme achieves the lowest computational cost under the adopted benchmark assumptions.

Table 4. Computational cost in terms of operations used

Schemes	Signcryption	Unsigncryption	Total
[17]	$5\varepsilon C_m$	$2\varepsilon C_m$	$7\varepsilon C_m$
[19]	$3\varepsilon C_m$	$2\varepsilon C_m$	$5\varepsilon C_m$
[21]	$6p_m$	$3\beta_P + 5p_m$	$3\beta_P + 11p_m$
[23]	$3\varepsilon C_m$	$1\varepsilon C_m$	$4\varepsilon C_m$
[26]	$3\varepsilon C_m$	$2\varepsilon C_m$	$5\varepsilon C_m$
Proposed	$4h\varepsilon D_m$	$1h\varepsilon D_m$	$5h\varepsilon D_m$

Table 5. Computational cost comparison in milliseconds

Schemes	Signcryption	Unsigncryption	Total
[17]	1.705	0.682	2.387
[19]	1.023	0.682	1.705
[21]	4.728	17.947	22.675
[23]	1.023	0.341	1.364
[26]	1.023	0.682	1.705
Proposed	0.682	0.1705	0.8525

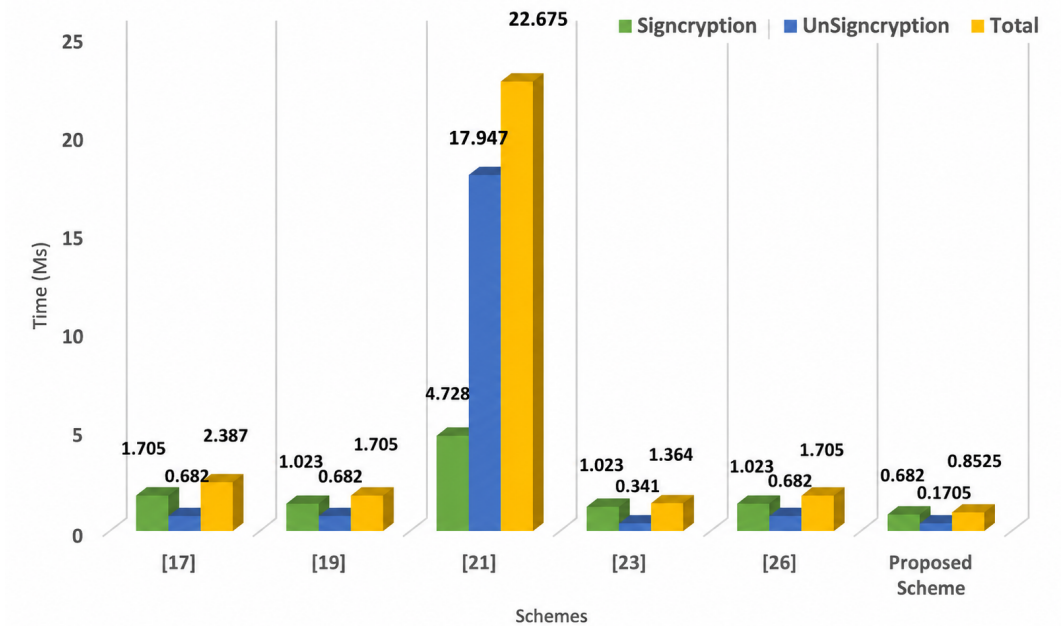


Figure 3. Computational cost comparison among existing and proposed schemes

Using the standard reduction metric Reduction (%) $= \frac{\text{Existing}-\text{Proposed}}{\text{Existing}} \times 100$, the proposed scheme achieves computational cost reductions of 64.28%, 49.99%, 96.24%, 37.51%, and 50% compared with [17], [19], [21], [23], [26], respectively, with an average improvement of 59.60%.

6.2. Communication cost

Communication cost is defined as the total number of transmitted bits. Consistent with prior studies, $|G| = 1024$ bits, $|E| = 160$ bits, $|n| = 80$ bits, and the message size $|m| = 1000$ bits. Table 6 and Figure 4 summarize the communication overhead. The pairing-based scheme in [21] incurs the highest cost due to large group elements, while ECC-based schemes [17], [19], [23], [26] exhibit moderate overhead. The proposed HECC-based design achieves the lowest communication cost owing to shorter divisor representations.

Compared with [17], [19], [21], [23], [26], the proposed approach reduces communication cost by 63.74%, 52.86%, 81.52%, 19.51%, and 26.67%, respectively, with an average reduction of 48.86%.

Table 6. Communication cost comparison

Schemes	Expression	Bits
[17]	$3\|m\| + 4\|E\|$	3640
[19]	$2\|m\| + 5\|E\|$	2800
[21]	$\|m\| + 6\|G\|$	7144
[23]	$\|m\| + 4\|E\|$	1640
[26]	$\|m\| + 5\|E\|$	1800
Proposed	$\|m\| + 4\|n\|$	1320

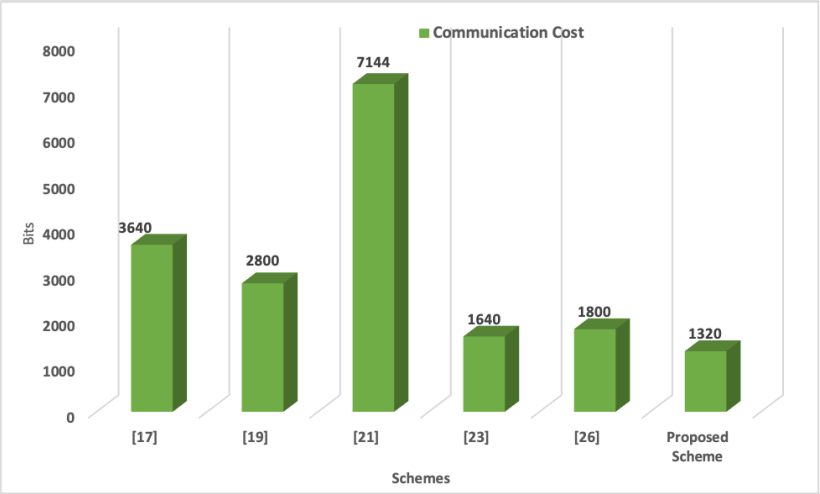


Figure 4. Communication cost comparison among existing and proposed schemes

7. FORMAL SECURITY VALIDATION

This section presents the formal validation of the proposed identity-based blind signcryption scheme using the Scyther verification tool [32]. The objective is to verify the logical correctness of the protocol under a standard symbolic adversary model rather than to claim implementation-level security.

Scyther operates under the Dolev–Yao assumption, where the adversary has full control over the communication channel but cannot break cryptographic primitives. Accordingly, the analysis focuses on secrecy, authentication, agreement, and freshness properties at the protocol level.

The protocol is specified in security protocol description language (SPDL), where roles, message flows, cryptographic operations, and security claims are explicitly modeled. The adversary is assumed capable of intercepting, modifying, replaying, and injecting messages, while cryptographic primitives are treated as ideal. This automated analysis complements the informal evaluation by verifying protocol correctness within the symbolic framework.

7.1. Verified security claims

The following standard Scyther claims were specified to assess secrecy and authentication guarantees:

- Secrecy: ensures that confidential protocol elements, including session keys and transmitted messages, are not disclosed to the adversary.
- Aliveness: confirms that a protocol participant completes a run with an active peer.
- Weak agreement (weak-agree): ensures that communicating entities agree on the occurrence of a protocol run and share at least one common value.
- Non-injective agreement (Ni-agree): strengthens authentication by ensuring mutual agreement on exchanged data values.
- Non-injective synchronization (Ni-synch): verifies correct message ordering and freshness, contributing to replay-attack resistance.

7.2. Verification results

The protocol roles, parameters, and verification settings used in the Scyther environment are illustrated in Figure 5, and the corresponding verification outcomes are shown in Figure 6. The analysis reports no attack traces for any of the specified security claims.

These results indicate that the proposed protocol satisfies secrecy, authentication, agreement, and freshness properties within the Scyther symbolic model. Accordingly, the scheme is formally validated against protocol-level attacks such as replay, impersonation, and man-in-the-middle attacks under the assumed verification scope.

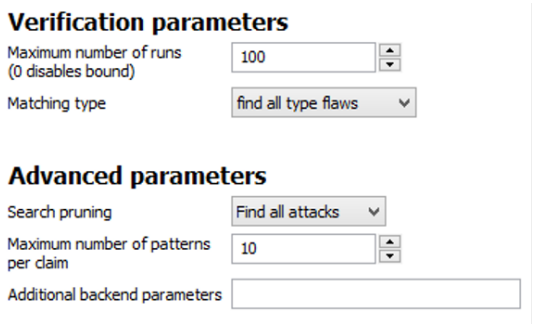


Figure 5. Simulation parameters used for Scyther verification

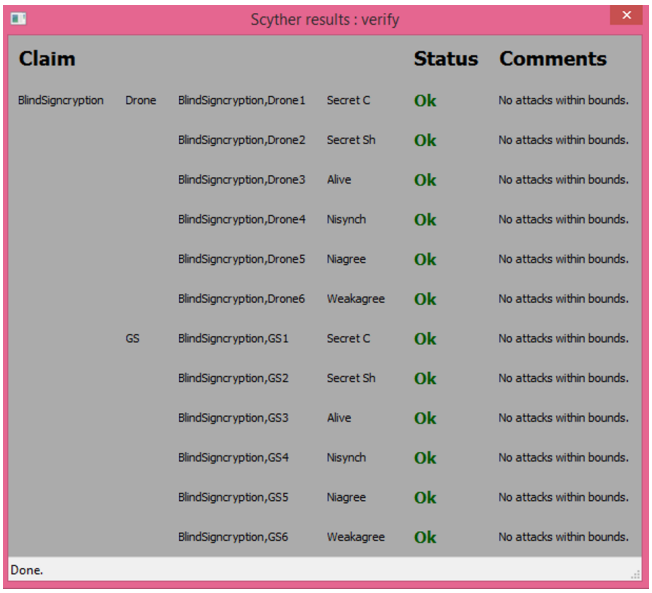


Figure 6. Verification results showing successful validation of all security claims

7.3. Discussion on implementation-level security

While the formal validation confirms protocol correctness, implementation-level threats such as side-channel leakage, fault injection, weak random number generation, and physical device capture remain outside the scope of symbolic verification tools.

In practical deployments, these risks can be mitigated through constant-time cryptographic implementations, hardware-assisted key storage (e.g., secure elements or trusted execution environments), secure boot mechanisms, and side-channel evaluation tools such as ChipWhisperer or test vector leakage assessment (TVLA). Hardware-level protections against tampering and fault-based attacks remain important directions for future experimental studies.

8. DISCUSSION

Although the proposed scheme provides strong protocol-level security guarantees, several practical challenges must be considered before real-world deployment in IoD environments. These limitations stem from architectural assumptions and implementation constraints and motivate further research toward scalable integration.

- Centralized KGC architecture: dependence on a centralized KGC may create scalability bottlenecks and a potential single point of failure in large-scale or swarm-based IoD deployments.
- Interoperability constraints: compatibility with existing IoD protocols such as MAVLink and unmanned aerial vehicle controller area network (UAVCAN) has not been experimentally validated, and integration with platforms such as PX4 and ArduPilot remains an open challenge.
- Post-quantum readiness: the scheme relies on classical cryptographic assumptions and does not incorporate post-quantum primitives or explicitly model emerging 5G/B5G communication environments.
- Implementation-level vulnerabilities: as discussed in section 7. Side-channel leakage, fault injection, weak randomness, and physical device capture are beyond the scope of the current protocol-level analysis.
- Mobility-induced overhead: frequent drone mobility and zone transitions may require repeated authentication and key updates, potentially affecting communication continuity.
- Network-induced latency variability: wireless interference, congestion, and dynamic topology changes introduce latency variations that are not fully captured by analytical cryptographic evaluation.

To address these limitations, several research directions are identified:

- Developing distributed or hierarchical KGC architectures based on threshold cryptography to improve scalability and fault tolerance.
- Designing middleware adapters to integrate blind signcryption with MAVLink and UAVCAN message formats for seamless deployment on existing drone platforms.
- Investigating hybrid post-quantum extensions and evaluating performance on physical testbeds under realistic mobility, interference, and side-channel conditions.
- Incorporating hardware-assisted protection mechanisms (e.g., secure elements or trusted execution environments) within resource-aware security architectures aligned with emerging standards.
- Exploring quality-of-service–aware scheduling, edge-assisted pre-computation, and delegated zone-based authentication to reduce re-authentication latency.

Addressing these challenges will facilitate the transition of the proposed scheme from a protocol-level construct to a scalable and deployment-ready security framework for future large-scale autonomous aerial networks.

9. CONCLUSION

This paper addressed security and efficiency challenges in IoD communications by proposing a lightweight identity-based blind signcryption scheme for resource-constrained aerial environments. By integrating encryption and digital signature into a unified operation, the scheme reduces computational and communication overhead while preserving essential security properties. The incorporated blinding mechanism further enhances privacy by preventing the signing authority from accessing message contents or linking protocol executions.

Informal analysis confirmed support for authentication, confidentiality, integrity, anonymity, privacy preservation, and resistance to common protocol-level attacks. Formal validation using the Scyther tool verified secrecy, agreement, and freshness properties under a symbolic adversary model. Performance evaluation demonstrated significant reductions in computational cost, communication overhead, and energy consumption compared with representative state-of-the-art schemes.

Overall, the proposed design provides an efficient and privacy-aware security framework suitable for IoD environments with strict resource constraints. Future work will focus on hardware-level implementation and large-scale swarm validation to further assess deployment feasibility.

FUNDING INFORMATION

The authors declare that no funding was received to support this research.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Tahri Rachid	✓	✓	✓			✓		✓	✓	✓	✓	✓	✓	✓
Abdellah Ouammou	✓		✓		✓		✓		✓	✓		✓	✓	
Abdellatif Lasbahani		✓	✓		✓					✓	✓			
Hibat Eallah Mohtadi	✓			✓		✓				✓	✓			

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal Analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject Administration
Fu : **Fu**nding Acquisition

CONFLICT OF INTEREST STATEMENT

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

DATA AVAILABILITY

The data that support the findings of this study are available from the corresponding author, RT, upon reasonable request.

REFERENCES

[1] A. Derhab *et al.*, "Internet of drones security: Taxonomies, open issues, and future directions," *Vehicular Communications*, vol. 39, p. 100552, Feb. 2023, doi: 10.1016/j.vehcom.2022.100552.

[2] W. Yang, S. Wang, X. Yin, X. Wang, and J. Hu, "A Review on Security Issues and Solutions of the Internet of Drones," *IEEE Open Journal of the Computer Society*, vol. 3, pp. 96–110, 2022, doi: 10.1109/OJCS.2022.3183003.

[3] D. Mandloi, R. Arya, and A. K. Verma, "Internet of Drones," in *Recent Trends in Artificial Intelligence Towards a Smart World, Springer*, 2024, pp. 353–373. doi: 10.1007/978-981-97-6790-8_13.

[4] J. B. R. Rose, T. Arulmozhinathan, V. T. Gopinathan, and J. V. B. Benifa, "Internet of Drones: Applications, Challenges, Opportunities," in *Internet of Drones, Boca Raton: CRC Press*, 2023, pp. 1–18. doi: 10.1201/9781003252085-1.

[5] L. Abualigah, A. Diabat, P. Sumari, and A. H. Gandomi, "Applications, Deployments, and Integration of Internet of Drones (IoD): A Review," *IEEE Sensors Journal*, vol. 21, no. 22, pp. 25532–25546, Nov. 2021, doi: 10.1109/JSEN.2021.3114266.

[6] A. F. Aldweesh and A. M. Almuhaideb, "Authentication Techniques in Internet of Drones (IoD): Taxonomy, Open Challenges and Future Directions," *Journal of Sensor and Actuator Networks*, vol. 14, no. 3, p. 57, May 2025, doi: 10.3390/jsan14030057.

[7] S. Sciancalepore, "Privacy and Confidentiality Issues in Drone Operations: Challenges and Road Ahead," *IEEE Network*, vol. 38, no. 6, pp. 227–233, Nov. 2024, doi: 10.1109/MNET.2024.3432730.

[8] Y. Zheng, "Digital signcryption or how to achieve cost(Signature &: Encryption) ¡¡ cost(signature) + cost(encryption)," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 1294, 1997, pp. 165–179. doi: 10.1007/BFb0052234.

[9] A. Shamir, "Identity-Based Cryptosystems and Signature Schemes," in *Advances in Cryptology, Berlin, Heidelberg: Springer Berlin Heidelberg*, pp. 47–53. doi: 10.1007/3-540-39568-7_5.

[10] S. Ullah and N. Din, "Blind signcryption scheme based on hyper elliptic curves cryptosystem," *Peer-to-Peer Networking and Applications*, vol. 14, no. 2, pp. 917–932, Mar. 2021, doi: 10.1007/s12083-020-01044-8.

[11] B. Hassan *et al.*, "A Cost Effective Identity-Based Authentication Scheme for Internet of Things-Enabled Agriculture," *Wireless Communications and Mobile Computing*, vol. 2022, no. 1, Jan. 2022, doi: 10.1155/2022/4275243.

[12] Z. Jamroz *et al.*, "An Optimal Authentication Scheme through Dual Signature for the Internet of Medical Things," *Future Internet*, vol. 15, no. 8, p. 258, Jul. 2023, doi: 10.3390/fi15080258.

[13] D. Chaum, "Blind Signatures for Untraceable Payments," in *Advances in Cryptology*, Boston, MA: Springer US, 1983, pp. 199–203. doi: 10.1007/978-1-4757-0602-4_18.

[14] N. Koblitz, "Hyperelliptic cryptosystems," *Journal of Cryptology*, vol. 1, no. 3, pp. 139–150, Oct. 1989, doi: 10.1007/BF02252872.

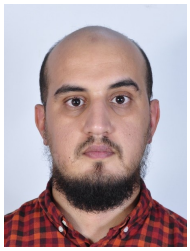
[15] M. A. Khan *et al.*, "An Improvised Certificate-Based Proxy Signature Using Hyperelliptic Curve Cryptography for Secure UAV Communications," *IEEE Transactions on Intelligent Transportation Systems*, vol. 26, no. 4, pp. 5264–5275, Apr. 2025, doi: 10.1109/TITS.2024.3524575.

[16] I. Ullah *et al.*, "A Multi-Message Multi-Receiver Signcryption Scheme with Edge Computing for Secure and Reliable Wireless Internet of Medical Things Communications," *Sustainability*, vol. 13, no. 23, p. 13184, Nov. 2021, doi: 10.3390/su132313184.

[17] H. Yu and Z. Wang, "Certificateless Blind Signcryption With Low Complexity," *IEEE Access*, vol. 7, pp. 115181–115191, 2019, doi: 10.1109/ACCESS.2019.2935788.
[18] L. Da, Y. Wang, Y. Ding, W. Xiong, H. Wang, and H. Liang, "An Efficient Certificateless Signcryption Scheme for Secure Communication in UAV Cluster Network," *2021 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing Communications, Social Computing & Networking (ISPA/BDCloud/SocialCom/SustainCom)*, New York City, NY, USA, 2021, pp. 884-891, doi: 10.1109/ISPA-BDCloud-SocialCom-SustainCom52081.2021.00125.
[19] X. Yang, N. Ren, A. Chen, Z. Wang, and C. Wang, "HSC-MET: Heterogeneous signcryption scheme supporting multi-ciphertext equality test for Internet of Drones," *PLoS ONE*, vol. 17, no. 9 September, p. e0274695, Sep. 2022, doi: 10.1371/journal.pone.0274695.
[20] I. Ullah *et al.*, "A Conditional Privacy Preserving Generalized Ring Signcryption Scheme for Micro Aerial Vehicles," *Micromachines*, vol. 13, no. 11, p. 1926, Nov. 2022, doi: 10.3390/mi13111926.
[21] Y. Qu and J. Zeng, "Certificateless Proxy Signcryption in the Standard Model for a UAV Network," *IEEE Internet of Things Journal*, vol. 9, no. 16, pp. 15116–15127, Aug. 2022, doi: 10.1109/JIOT.2022.3148038.
[22] N. W. Hundera, W. Shumeng, D. Mesfin, H. Xu, and X. Zhu, "An efficient online/offline heterogeneous proxy signcryption for secure communication in UAV networks," *Journal of King Saud University - Computer and Information Sciences*, vol. 36, no. 5, p. 102044, Jun. 2024, doi: 10.1016/j.jksuci.2024.102044.
[23] M. A. Khan *et al.*, "A Certificate-Based Ring Signcryption Scheme for Securing UAV-Enabled Private Edge Computing Systems," *IEEE Access*, vol. 12, pp. 83466–83479, 2024, doi: 10.1109/ACCESS.2024.3409359.
[24] G. K. Verma, V. Chamola, N. Kumar, A. K. Das, and D. Mishra, "Efficient and secure signcryption-based data aggregation for Internet of Drone-based drone-to-ground station communication," *Ad Hoc Networks*, vol. 159, p. 103502, Jun. 2024, doi: 10.1016/j.adhoc.2024.103502.
[25] E. Abouelkheir, "Securing Unmanned Aerial Vehicles Networks Using Pairing Free Aggregate Signcryption Scheme," *IEEE Open Journal of the Communications Society*, vol. 5, pp. 7552–7566, 2024, doi: 10.1109/OJCOMS.2024.3504353.
[26] A. M. Ejiyeh, "Secure, Robust, and Energy-Efficient Authenticated Data Sharing in Drone to Vehicles Communications," in *2024 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), IEEE*, Jul. 2024, pp. 380–389. doi: 10.1109/EuroSPW61312.2024.00049.
[27] B. Cui, L. Wei, and W. He, "A New Certificateless Signcryption Scheme for Securing Internet of Vehicles," *Security and Communication Networks*, Jan. 28, 2022. doi: 10.21203/rs.3.rs-1272183/v1.
[28] I. Ali, J. Li, J. Chen, Y. Chen, S. Ullah, and S. Khan, "IOOSC-U2G: An Identity-Based Online/Offline Signcryption Scheme for Unmanned Aerial Vehicle to Ground Station Communication," *IEEE Internet of Things Journal*, vol. 11, no. 18, pp. 29941–29955, Sep. 2024, doi: 10.1109/JIOT.2024.3407767.
[29] W. Zou, Q. Guo, and X. Xie, "A Certificateless Aggregated Signcryption Scheme Based on Edge Computing in VANETs," *Electronics*, vol. 14, no. 10, p. 1993, May 2025, doi: 10.3390/electronics14101993.
[30] Y. Sun, J. Cao, M. Ma, Y. Zhang, H. Li, and B. Niu, "EAP-DDBA: Efficient Anonymity Proximity Device Discovery and Batch Authentication Mechanism for Massive D2D Communication Devices in 3GPP 5G HetNet," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 1, pp. 370–387, Jan. 2022, doi: 10.1109/TDSC.2020.2989784.
[31] A. Rahmati and L. Zhang, "Context-for-Wireless: context-sensitive energy-efficient wireless data transfer," *Proceedings of the 5th international conference on Mobile systems, applications and services. ACM*, pp. 165–178, Jun. 13, 2007, doi: 10.1145/1247660.1247681.
[32] C. J. F. Cremers, "The Scyther Tool: Verification, Falsification, and Analysis of Security Protocols," in *Lecture Notes in Computer Science. Springer Berlin Heidelberg*, pp. 414–418, doi: 10.1007/978-3-540-70545-1_38.

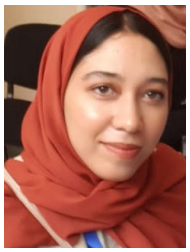
BIOGRAPHIES OF AUTHORS

Tahri Rachid was born in Zagora, Morocco, in 1990. He received the Master's degree in Networks and Informatics Systems from the Faculty of Sciences and Techniques, Settat, in 2014. He is currently pursuing a Ph.D. at the University of Hassan 1st, Morocco. His research interests include security integration in artificial intelligence and machine learning systems. He is the corresponding author of this article. He can be contacted at email: rachid.tahritr@gmail.com.



Abdellah Ouammou holds a Ph.D. in Applied Mathematics from the Computer, Networks, Mobility and Modeling Laboratory at the Faculty of Sciences and Techniques, Hassan First University of Settat, Morocco. He currently serves as a Professor at the Ministry of National Education, Preschool and Sports in Morocco, and is affiliated with the Faculty of Sciences and Techniques at Hassan First University. His research interests include probability theory, stochastic optimization, discrete stochastic processes, discrete optimization, and applications in cloud computing environments. He can be contacted at email: a.ouammou@uhp.ac.ma.

Abdellatif Lasbahani is a Professor at University Sultan Moulay Slimane and holds a Ph.D. from University Hassan First. His research focuses on formal methods and artificial intelligence, particularly modeling complex systems. He is committed to advancing knowledge in his field through publication and collaboration. He can be contacted at email: abbdellatif.lasbahani@gmail.com.



Hibat Eallah Mohtadi received her Bachelor's degree in Applied Mathematics at Hassan 1st University, Settat, Morocco the Faculty of Sciences and Techniques Settat, Morocco in 2018. In 2020, she obtained her Masters degree in Mathematics and Applications from Hassan 1st University, Settat, Morocco. She is currently a Ph.D. in Applied Mathematics and Computer Science at Computer, Networks, Mobility and Modeling laboratory, Faculty of Sciences and Techniques, Hassan 1st University, Settat, Morocco. Her research interests include Information theory, stochastic processes, Markov chains and their applications for modeling FC networks. She can be contacted at email: h.mohtadi@uhp.ac.ma.