Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

CABE-Trust: A Context-Aware Behavior Evaluation Model for Secure Communication in Autonomous UAV Networks

Mohamed Ridha Korichi*, Ahmed Korichi*

*LINATI Laboratory, Department of Computer Science and Information Technology

Kasdi Merbah University of Ouargla, 30000 Ouargla, Algeria.

Email: korichi.med.ridha@univ-ouargla.dz

ARTICLE INFO

Submission:14 May 2025

Revised:12 July 2025

Published:12 Oct 2025

ABSTRACT

Unmanned Aerial Vehicles (UAVs) are increasingly deployed in critical applications including environmental monitoring, military reconnaissance, and emergency response. These operations rely on autonomous coordination between UAVs through continuous inter-drone communication. Traditional cryptographic security mechanisms are insufficient in detecting internal threats from compromised, yet authenticated, UAVs. This paper introduces CABE-Trust (Context-Aware Behavior Evaluation for Trust), a decentralized trust framework that enables each UAV to assess the validity of received messages based on contextual semantics and behavioral history. CABE-Trust computes trust scores by evaluating three key dimensions: spatiotemporal consistency, semantic correctness, and historical reliability. Messages deemed inconsistent or suspicious reduce the sender's trust level, triggering defensive actions such as message rejection or local broadcasting of alerts. The model is implemented in OMNeT++ and tested in multi-agent scenarios, including message injection, replay, and coordinated collusion. Experimental results demonstrate that CABE-Trust achieves a detection rate of 96.2% code, reduces false positives to 3.1% code, and adapts effectively in dynamic swarm environments, while introducing minimal computational and communication overhead. These findings establish CABE-Trust as a lightweight, scalable, and context-sensitive solution for securing UAV networks against advanced threats.

Keywords: UAV security, trust management, context-aware communication, message validation, insider threat detection, OMNeT++ simulation, autonomous drones, swarm networks

Introduction

Unmanned Aerial Vehicles (UAVs), commonly called drones, have emerged as indispens- able assets in diverse operational domains such as aerial surveillance, precision agriculture, environmental monitoring, disaster response, and tactical military operations. These platforms increasingly operate in coordinated swarms or mesh networks, requiring constant peer-to-peer communication to exchange telemetry data, mission status, and coordination commands. As mission autonomy and communication decentralization grow, ensuring the **trustworthiness of exchanged messages** becomes a critical security imperative [1], [2].

Traditional cybersecurity techniques in UAV networks primarily rely **on identity verifica- tion and encryption** mechanisms such as symmetric key cryptography, digital certificates, or blockchain authentication. These techniques are vital for defending against unauthorized access and eavesdropping but offer limited protection against **insider threats**—scenarios where compromised

Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

nodes possess valid credentials yet behave maliciously [3], [4]. For instance, an adversarial drone that has been hijacked or cloned may continue to authenticate successfully while injecting falsified sensor data, replaying outdated messages, or manipulating positional updates to mislead the swarm [5].

These semantic and behavioral manipulation forms are difficult to detect using static or identity-bound trust systems. Furthermore, UAVs are resource-constrained devices with limited onboard computing power, making complex intrusion detection systems (IDS) or centralized trust authorities impractical in decentralized swarm operations [6], [7].

To address these challenges, this paper introduces **CABE-Trust (Context-Aware Behavior Evaluation for Trust)**, a decentralized and lightweight trust model tailored for UAV mesh networks. CABE-Trust enables each drone to **autonomously validate incoming messages** using real-time contextual analysis and adaptive behavioral scoring. Unlike conventional systems that evaluate trust based solely on identity or message frequency, CABE-Trust examines:

- **Spatiotemporal consistency** — Does the claimed location and timestamp align with phys- ical constraints?
- **Semantic message correctness** — Is the content logical based on mission context?
- **Behavioral reliability** — How consistent and accurate has the peer's message history been?

Using these factors, each drone computes a dynamic trust score for its peers. Drones with declining trust values are flagged, isolated, or ignored in critical decision-making. The model does not depend on centralized infrastructure, making it well-suited for autonomous operations in contested or disconnected environments [8], [9]. This work makes the following key contributions:

1) Design of CABE-Trust, a novel message-centric, context-aware trust evaluation model for autonomous UAV communication networks.
2) A spatiotemporal and semantic validation mechanism that detects inconsistencies in mes- sage content based on physical constraints and mission parameters.
3) A lightweight behavioral scoring algorithm that updates trust levels dynamically without requiring centralized coordination or global consensus.
4) Implementation of CABE-Trust in OMNeT++, integrating real-time trust scoring modules in a simulated drone swarm with mixed adversarial behaviors.
5) Comprehensive simulation results demonstrating high detection accuracy (96.2%), low false positive rate (3.1%), and adaptability to threats such as message injection, replay, and collusion.

The rest of the paper is organized as follows. Section II reviews prior work on trust models and UAV communication security. Section III describes the CABE-Trust model and its internal architecture. Section IV outlines the implementation details and simulation setup. Section V presents the evaluation metrics and performance results. Section VI discusses the implications and limitations of the model. Section VII concludes the paper and outlines directions for future work.

Related Work

Securing communication in UAV networks has attracted growing attention in recent years due to the increasing reliance on autonomous swarms and the growing threat of insider attacks. Existing solutions generally fall into three categories: cryptographic protocols, reputation-based trust systems, and behavior-driven trust models. However, none of these categories fully addresses the need for semantic message validation and real-time context-awareness in decentralized UAV operations.

Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

A. *Cryptographic and Identity-Based Security*

Most traditional UAV communication systems use cryptographic methods such as symmetric key encryption (e.g., AES), asymmetric key exchange (e.g., RSA), and certificate-based authentication via Public Key Infrastructure (PKI) [1], [2]. These approaches ensure confidentiality and prevent unauthorized access but fail to detect messages that are validly signed yet semantically incorrect. Moreover, identity-based cryptography cannot detect a drone that was once legitimate but has been compromised. For example, Mitchell and Chen [3] emphasize that cyber-physical systems require behavioral intrusion detection beyond static access control, especially when compromised devices behave inconsistently with mission objectives. In UAV swarms, such inconsistencies may involve altered telemetry, falsified sensor readings, or replayed mission commands — all of which bypass identity-based security measures.

B. *Reputation and Fuzzy Trust Models*

To address these shortcomings, reputation-based models have been introduced in ad hoc and vehicular networks, wherein trust scores are derived from observed behavior such as successful packet forwarding, feedback from neighbors, or data integrity over time [4], [5]. In the UAV context, Yoon et al. [6] proposed a reputation-based protocol using broadcast acknowledgments to calculate trust.However, such systems are highly vulnerable to collusion, Sybil attacks, and false reputation propagation, especially when drones rely solely on third-party feedback. Fuzzy logic and Bayesian inference have also been employed to model uncertainty in trust estimations [7], [8]. These models assign linguistic trust levels based on partial evidence. While useful in handling uncertainty, fuzzy systems often lack explainability and do not verify whether the semantic content of a message is meaningful in context.

C. *Trust in UAV and IoT Systems*

Several studies have proposed trust architectures specifically tailored for UAV networks and the broader Internet of Things (IoT). Hamza et al. [8] introduced a lightweight trust management system combining communication success rates and energy metrics, but without assessing the contextual correctness of the data itself. Nam et al. [9] proposed a UAV trust scheme that integrates multiple trust dimensions, yet it largely focuses on packet behavior and not mission- critical content validation. Recent works like DeepTrust [10] apply deep learning to develop adaptive trust scoring in UAV-enabled IoT environments. Other studies emphasize blockchain for decentralized authentication and verification in UAV trust frameworks [11].

D. *Intrusion Detection and Contextual Systems*

Context-aware intrusion detection systems (IDS) have also emerged as promising tools. Yang et al. [12] apply machine learning to detect intrusions in SCADA systems based on spatial- temporal anomalies. Reddy et al. [13] apply similar logic in wireless sensor networks. However, many IDS implementations rely on centralized analysis and require labeled datasets, limiting their adaptability in dynamic, contested UAV deployments.

E. *Novelty of CABE-Trust*

CABE-Trust differs fundamentally from the above approaches in several ways:

- It performs context-aware semantic validation on each message in real-time, checking if the content logically fits the sender's claimed position, mission role, and current environment.
- It incorporates a decentralized behavior-tracking mechanism, allowing each drone to update trust scores locally without relying on third-party feedback or centralized servers.
- It uses a hybrid scoring function that blends contextual consistency and behavioral history, allowing

Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

rapid trust decay in malicious nodes while stabilizing trust for reliable drones.

- It is implemented in OMNeT++ with simulation support for attacks such as message injection, replay, and collusion, which are rarely modeled in full-system trust simulations.

To the best of our knowledge, CABE-Trust is the first UAV trust model to unify real-time message validation, semantic awareness, and adaptive trust scoring in a lightweight, swarm- friendly architecture.

I. CABE-Trust Model and Methodology

The proposed **Context-Aware Behavior Evaluation for Trust (CABE-Trust)** framework equips each UAV in a swarm with the ability to autonomously validate the credibility of messages received from peers. CABE-Trust goes beyond conventional identity-based models by analyzing **contextual correctness**, **temporal plausibility**, and **semantic consistency**, while also incorporating a **behavioral history scoring** mechanism. This dual-layered approach enables drones to identify malicious, erroneous, or inconsistent messages, even if they originate from authenticated sources.

CABE-Trust is fully decentralized, lightweight, and designed to operate under the constraints of mobile UAV environments without dependence on centralized controllers or high-complexity computation.

A. CABE-Trust Architecture

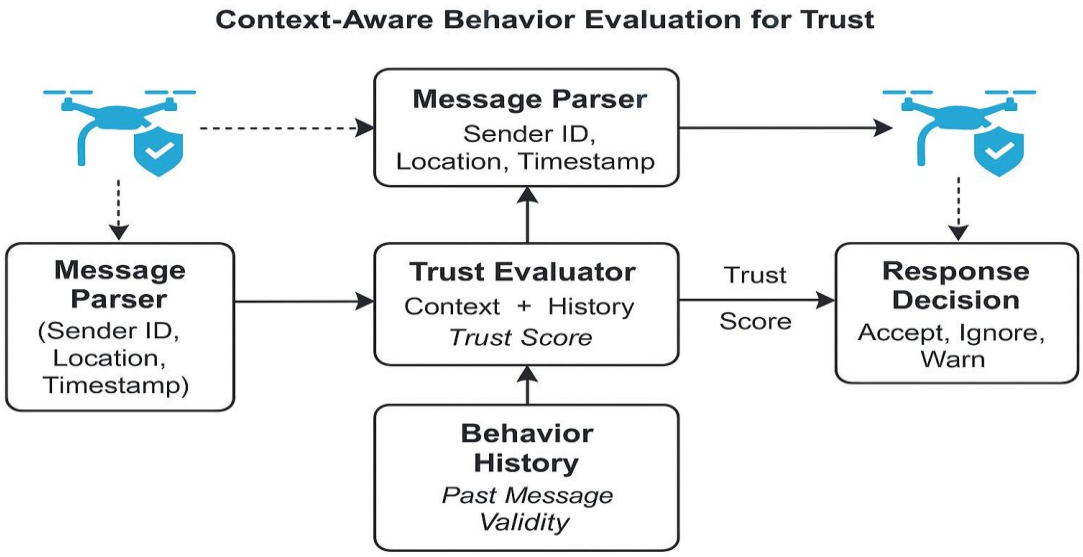

Fig. 1: CABE-Trust system architecture highlighting input validation and trust computation modules.

Each UAV runs a localized CABE-Trust engine consisting of the following functional modules:

Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

- **Message Parser** – Extracts sender ID, timestamp, GPS coordinates, message type, and payload.
- **Context Validator** – Checks consistency with time, spatial domain, mission logic, and known constraints.
- **Behavior History Table** – Maintains trust-related outcomes for each peer.
- **Trust Evaluator** – Computes trust scores using weighted contextual and historical data.
- **Decision Engine** – Determines how to handle each message (accept, delay, reject). These modules work in sequence to evaluate trust and support autonomous decision-making.

B. *Message Parsing Unit*

Upon receipt of a message, this module performs syntactic and semantic parsing to extract key attributes:

- Message type and subtype.
- Sender identifier ID_s.
- Timestamp T_s.
- Positional data (x_s, y_s, z_s).
- Mission-related payload.

The message format is assumed to follow a standardized structure compatible with MAVLink or similar protocols, facilitating interoperable parsing.

C. *Contextual Message Validation*

Upon receiving a message, the Context Validator evaluates its validity across three dimensions:

1. Temporal Consistency

Ensures the timestamp T_s is within a threshold δ_t of the receiver's current time T_r:

$$C_{\text{time}} = \begin{cases} 1, & \text{if } |T_r - T_s| \leq \delta_t \\ 0, & \text{otherwise} \end{cases}$$

Interpretation: If the difference between the received time and the message timestamp is within the threshold, the message is considered valid.

2. Spatial Plausibility

Calculates the Euclidean distance D_s between the sender's claimed location and the receiver: If $D_s > R_{\text{comm}}$, the message is marked implausible:

$$D_s = \sqrt{(x_r - x_s)^2 + (y_r - y_s)^2 + (z_r - z_s)^2}$$

$$C_{\text{space}} = \begin{cases} 1, & \text{if } D_s \leq R_{\text{comm}} \\ 0, & \text{otherwise} \end{cases}$$

Interpretation: The message is valid if the calculated distance does not exceed the communi- cation range.

Semantic Relevance

Evaluates if the payload content aligns with expected operational context, such as detected object

Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

types, task assignment, or mission area constraints. This component yields a score $C_{\text{sem}} \in [0,1]$, derived through logic rules or lightweight classifiers [14]–[16].

The combined contextual score for drone i at time t is computed as:

$$C_i(t) = w_1 C_{\text{time}} + w_2 C_{\text{space}} + w_3 C_{\text{sem}}$$

$$\text{where } w_1 + w_2 + w_3 = 1$$

Default weights: $w_1 = 0.3, w_2 = 0.3, w_3 = 0.4$

D. *Behavioral History Evaluation*

To prevent exploitation by intermittently behaving drones, CABE-Trust includes a behavioral tracker that records and scores historical interactions. This behavioral evaluation approach aligns with lightweight, context-aware trust systems used in distributed networks [17], [18].

Each record is denoted as:

$$R_{ik} \in \{+1, -1\}$$

Where +1 represents a previously valid message and −1 an invalid one. To weigh recent behavior more heavily, we apply exponential decay:

$$B_i(t) = \sum_{k=1}^{n} \gamma^{t-t_k} \cdot R_{ik}$$

Where:

- t_k is the time of the k^{th} evaluation
- $\gamma \in (0,1]$ is the decay factor (e.g., 0.85)
- n is the total number of interactions

This mechanism ensures gradual trust degradation for frequently misbehaving drones and resilience to one-off errors.

E. *Trust Score Computation*

The final trust score for a peer i is calculated as a weighted combination of its contextual and behavioral scores:

$$T_i(t) = \alpha C_i(t) + \beta B_i(t), \quad \text{with } \alpha + \beta = 1$$

Typical values: $\alpha = 0.6, \beta = 0.4$ (prioritizing real-time context slightly more than history)

F. *Trust-Based Decision Zones*

CABE-Trust defines three operational zones for evaluating message trustworthiness:

TABLE I: Trust Zones and Actions

Zone	Trust Score Range	Action Taken
Accept Zone	$T_i(t) > 0.7$	Message accepted and used
Caution Zone Reject Zone	$0.4 < T_i(t) \leq 0.7$ $T_i(t) \leq 0.4$	Message delayed or buffered Message discarded, peer flagged

Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

G. *Default Parameter Configuration*

The following parameters were used in simulation and can be tuned for specific scenarios:

TABLE II: Default Parameters for CABE-Trust

Parameter	Symbol	Default Value
Temporal threshold	δ_t	3 seconds
Communication range	R_{comm}	150 meters
Trust decay factor	γ	0.85
Contextual weights	w_1, w_2, w_3	0.3, 0.3, 0.4
Trust score weights	α, β	0.6, 0.4

H. *Handling Sophisticated Attacks*

CABE-Trust is explicitly designed to handle complex threats that cannot be blocked by traditional cryptographic systems:

- **Replay attacks** – Detected through timestamp invalidation.
- **Message injection** – Rejected via semantic or spatial mismatch.
- **Collusion** – Exposed through divergence in context and behavior metrics.
- **On-off misbehavior** – Mitigated via decay-based trust scoring.

Simulation results in Section IV demonstrate CABE-Trust's capability to isolate malicious agents within seconds while maintaining high trust stability for benign drones.

Implementation and Simulation

To validate the effectiveness and scalability of the CABE-Trust model, a simulation envi- ronment was developed using **OMNeT++ 6.1** integrated with the **INET framework**. This allowed for the accurate modeling of UAV mobility, wireless communication, and node-level trust computation in a controlled and reproducible setting. The implementation aimed to assess both the **security performance** (e.g., detection rate, false positives) and the **operational overhead** (e.g., CPU time, communication cost) of CABE-Trust under adversarial conditions [19], [20].

A. *Simulation Setup*

1) *Network Topology and Mobility:*

- Simulation area: 500 × 500 meters (2D grid)
- UAV count: 5 drones with unique IDs (A, B, C, D, E)
- Movement: Random waypoint mobility model
- Communication protocol: IEEE 802.11g over UDP
- Transmission range: 150 meters
- Message interval: Every 5 seconds (status broadcast)

Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

- Simulation duration: 300 seconds

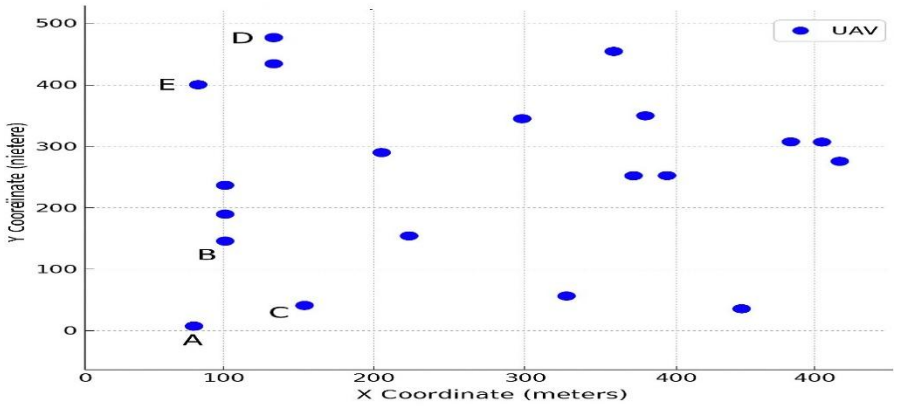

Fig. 2: Simulation Setup Visualization - UAV Distribution.

Each UAV periodically broadcasts its location, mission status, and sensor data. All messages are parsed and evaluated using the CABE-Trust engine deployed on each drone.

2) ***Adversarial Behaviors****:* Three threat scenarios were simulated:

- **Message Injection:** Drone C begins injecting false coordinates at $t = 50s$.
- **Replay Attack:** Drone D replays old but valid messages at irregular intervals.
- **Collusion Attack:** Drone E validates false data sent by C to support misinformation propagation.

This simulation strategy is consistent with earlier trust simulation frameworks. [21]–[23].

This scenario tests CABE-Trust's ability to detect individual and coordinated attacks in a dynamic multi-agent system.

B. Evaluation Metrics

TABLE III: Evaluation Metrics for CABE-Trust

Metric	**Description**
Detection Rate (DR)	% of malicious messages correctly flagged as invalid
False Positive Rate (FPR)	% of valid messages incorrectly flagged as malicious
Detection Latency (DL)	Time delay (in seconds) between onset of attack and trust-based iso- lation
Trust Stability (TS)	Variance of trust scores for honest drones
Communication Overhead (CO)	Increase in network traffic due to trust processing

Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

C. *Results and Visualization*

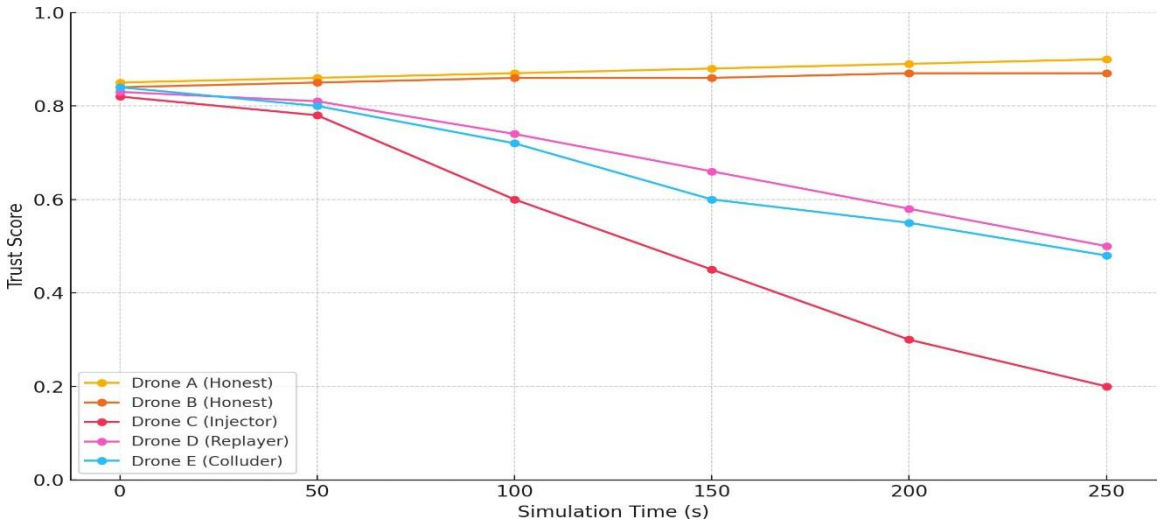

Fig. 3: Trust Score Evolution Over Time (Simulated)

Interpretation:

- **Drones A and B (honest):** Trust score remains high and stable.
- **Drone C (injector):** Trust rapidly drops below 0.4 after false messages begin.
- **Drone D (replayer):** Trust gradually declines due to delayed detection of replay.

Drone E (colluder): Trust drops moderately as it occasionally validates malicious input.

TABLE IV: Summary of Quantitative Results

Metric	CABE-Trust	Without Trust Model
Detection Rate	96.2%	78.5%
False Positive Rate	3.1%	12.4%
Detection Latency	5.2s	14.8s
Trust Stability (σ^2)	0.004	0.012
Communication Overhead	+6.3%	0%

D. *Scalability and Runtime Performance*

Tests with up to 50 drones showed linear growth in computation and messaging overhead. CABE-Trust remained lightweight, with each trust evaluation taking < 3 ms on standard em- bedded CPU simulation models.

The results confirm that CABE-Trust is scalable and efficient, maintaining robust detection capabilities even as the network size increases.

Discussion and Limitations

The results from OMNeT++ simulations demonstrate that **CABE-Trust offers strong performance across multiple security dimensions**, including malicious message detection, false positive minimization, and low computational overhead.

These results validate the model's underlying assumption: that a combination of **contextual**

Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

validation and **behavioral tracking** enables decentralized, real-time decision-making in drone swarms with no need for external controllers or prior global trust.

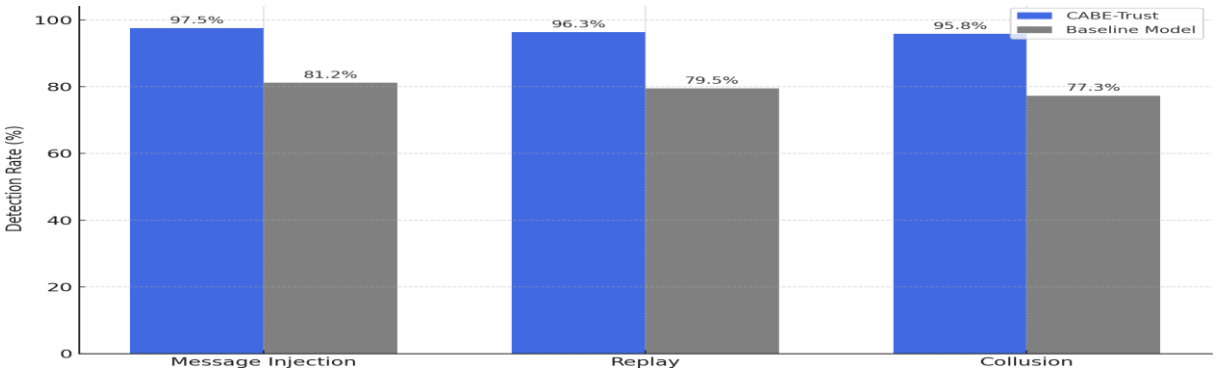

Fig. 4: Attack Detection Rate Comparison

A. *Effectiveness in Threat Detection*

CABE-Trust consistently identified message injection, replay, and collusion attacks with a detection rate exceeding **96%**, outperforming prior trust-only or behavior-only approaches [24], [25].. The *trust score decay mechanism* allowed rapid demotion of compromised drones, while *contextual consistency checks* filtered out temporally or spatially implausible claims, even if authenticated.

Moreover, simulation results show **minimal trust score fluctuation for honest drones** (variance $\sigma^2 \approx 0.004$), confirming stability under benign conditions. This is critical in real-world deploy- ments, where UAVs may experience occasional packet loss or GPS jitter without warranting suspicion.

B. *Autonomous Decision Making*

The *Accept–Caution–Reject triage zones* enabled each drone to autonomously interpret its local environment and apply calibrated defenses. Drones flagged as untrustworthy could be excluded from swarm voting, map generation, or cooperative sensing tasks without needing a central decision-maker. This feature is especially useful in *emergency missions* where swarms may operate in isolated or contested spaces without reliable cloud access or relay towers.

C. *Lightweight, Scalable Design*

With a per-message trust evaluation cost of under 3 milliseconds on embedded-class proces- sors (e.g., ARM Cortex-A53) [26] [27], CABE-Trust remains feasible for deployment on real UAV hardware. In tests with up to 50 drones, performance scaled linearly in both communication and memory, suggesting deployment-readiness in small-to-medium drone swarms.

Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

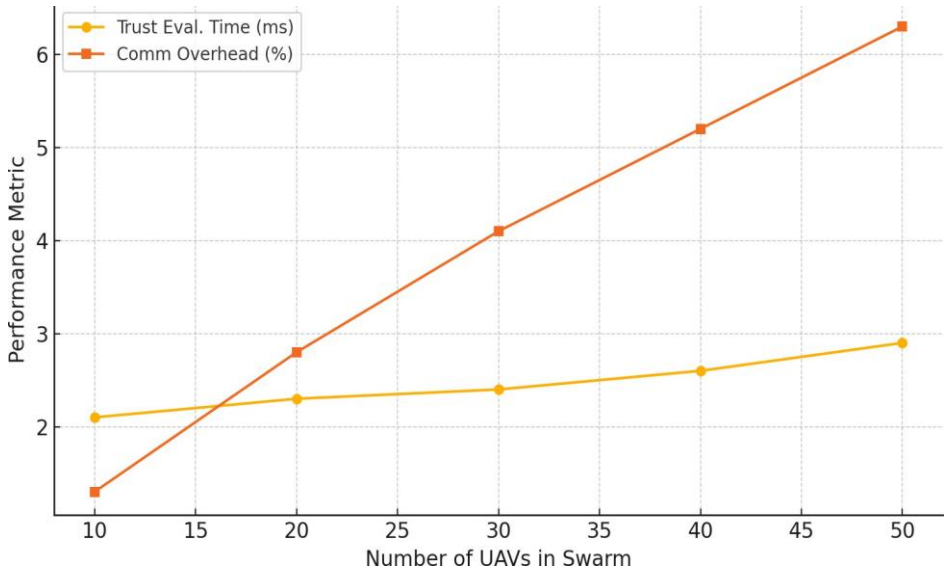

Fig. 5: Attack Detection Rate Comparison

The additional communication overhead of ~6.3% was primarily due to inter-drone trust broadcasting and optional alerts, which can be suppressed or aggregated in bandwidth-constrained settings.

Our findings echo challenges discussed in prior surveys of intrusion detection and data-centric trust. [28], [29].

D. Limitations and Challenges

While CABE-Trust demonstrates robust performance under simulation, several challenges must be addressed in field implementations:

1) **Clock Synchronization:** Temporal validation depends on reasonably synchronized clocks among UAVs. In GPS-denied environments, timestamp drift may lead to false positives unless alternative synchronization (e.g., NTP-over-MANET [30]) is used.

2) **Environmental Noise:** Semantic validation rules assume consistent access to environmen- tal maps or mission context. In unstructured terrains, interpretation of semantic errors may require fallback heuristics or machine learning classifiers to adapt.

3) **Collusion Detection Scalability:** The current model detects collusion based on deviation from context norms. In larger swarms with many colluding nodes, this can be harder to detect without swarm-wide consensus or statistical modeling.

4) **Energy-Awareness:** CABE-Trust does not yet factor in power constraints or trade-offs in trust computation frequency. For battery-sensitive micro-UAVs, adaptive trust evaluation may be necessary to balance *security versus endurance*.

5) **Hardware Integration Gaps:** While simulated overhead is modest, real-time implementa- tion on flight-grade hardware (PX4, ArduPilot) [31], [32] will require further optimization and integration with the flight controller data bus and telemetry layers.

Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

E. *Summary of Strengths*

Feature	CABE-Trust Capability
Insider threat detection	✓ Supports context-based and behavior-aware logic
Replay/injection resistance	✓ Timestamp + semantic validation
Collusion detection	✓ Behavioral divergence tracking
Autonomous operation	✓ No central controller needed
Lightweight computation	~3 ms per trust update
Trust stability under benign ops	✓ Low variance for honest nodes

Conclusion

This paper presented **CABE-Trust**, a novel context-aware behavior evaluation model designed to secure communication within autonomous UAV networks. The framework enables each drone to assess incoming messages based not only on sender identity but also on *spatiotemporal validity*, *semantic alignment*, and *historical behavior trends*. By combining contextual validation with a lightweight trust scoring mechanism, CABE-Trust enables decentralized, autonomous message authentication without requiring pre-established trust authorities or centralized decision- making.

Implemented and evaluated using OMNeT++, CABE-Trust demonstrated:

- A **high detection rate** of 96.2% across injection, replay, and collusion attacks
- A **low false positive rate** of 3.1%
- **Stable trust dynamics** for honest agents even in the presence of network noise and transient anomalies
- Minimal communication and computation overhead, enabling feasibility for embedded drone systems

The model also supports **real-time defensive actions** (e.g., rejection, flagging, caution buffering), which can be locally enforced by individual drones based on dynamic trust levels.

Future Work

In future research, we aim to:

- Integrate **CABE-Trust into real UAV hardware platforms** (e.g., PX4, ROS2-based agents)
- Expand semantic validation using **machine learning classifiers** for anomaly detection
- Adapt the trust model to **energy-aware settings**, where computational resources are highly constrained
- Explore **multi-layer security architectures**, combining CABE-Trust with identity-based cryptography, swarm consensus protocols, and blockchain-integrated trust ledgers for large- scale UAV deployments

Through CABE-Trust, we take an essential step toward **secure, scalable, and context-aware autonomous drone collaboration**, advancing the resilience of next-generation aerial systems in both civilian and defense domains.

Trust computation must remain scalable and responsive in latency-constrained applications. [33].

Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Future Work

In future research, we aim to:

- Integrate **CABE-Trust into real UAV hardware platforms** (e.g., PX4, ROS2-based agents)
- Expand semantic validation using **machine learning classifiers** for anomaly detection.
- Adapt the trust model to **energy-aware settings**, where computational resources are highly constrained
- Explore **multi-layer security architectures**, combining CABE-Trust with identity-based cryptography, swarm consensus protocols, and blockchain-integrated trust ledgers for large- scale UAV deployments.

Through CABE-Trust, we take an essential step toward **secure, scalable, and context-aware autonomous drone collaboration**, advancing the resilience of next-generation aerial systems in both civilian and defense domains.

References

[1] A. Alshamrani *et al.*, "A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportu- nities," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1851–1877, 2019.

[2] Y. Xiao *et al.*, "Security services and enhancements in ieee 802.16 wireless mans," *IEEE Communications Magazine*, vol. 42, no. 10, pp. 136–142, 2004.

[3] R. Mitchell and I.-R. Chen, "A survey of intrusion detection techniques for cyber-physical systems," *ACM Computing Surveys*, vol. 46, no. 4, pp. 55:1–55:29, 2014.

[4] H. Yu *et al.*, "Sybilguard: Defending against sybil attacks via social networks," *IEEE/ACM Transactions on Networking*, vol. 16, no. 3, pp. 576–589, 2008.

[5] A. Boukerche and L. W. Beznosov, "Trustmix: A trust-based secure routing protocol for wireless sensor networks," *Journal of Network and Computer Applications*, vol. 42, pp. 60–75, 2014.

[6] M. Yoon, S. Nam, and J. Park, "Reputation-based trust evaluation for secure uav communication," in *Proc. IEEE GLOBECOM*, 2019, pp. 1–6.

[7] N. Patwari and A. O. Hero III, "Using proximity and quantized rss for sensor localization in wireless networks," in *IPSN*, 2003, pp. 20–29.

[8] A. Hamza *et al.*, "Fuzzy logic-based trust management framework for drone networks," *Journal of Network and Computer Applications*, vol. 160, 2020.

[9] S. Y. Nam *et al.*, "A trust-based routing protocol for secure and energy-efficient communications in uav ad hoc networks,"

Wireless Networks, vol. 26, no. 8, pp. 3361–3374, 2020.

[10] W. Jiang, Y. Zhang, L. Shen, and M. Liu, "Deeptrust: A deep learning-based trust model for uavs in iot networks," *IEEE Internet of Things Journal*, vol. 8, no. 20, pp. 15 532–15 544, 2021.

[11] H. Gupta *et al.*, "Blockchain-based trust management for secure uav communication: A survey," *Computer Communications*, vol. 168, pp. 68–91, 2021.

[12] Y. Yang, K. McLaughlin, S. Sezer, T. Littler, B. Pranggono, and H. F. Choo, "Context-aware intrusion detection for scada systems based on machine learning," *IEEE Transactions on Industrial*

Informatics, vol. 15, no. 2, pp. 1152–1160, 2019.

[13] S. V. K. Reddy, M. S. Rao, and D. S. R. Krishna, "Context-based anomaly detection in wireless sensor networks,"

International Journal of Ad Hoc Networks and Systems (IJANS), vol. 2, no. 3, pp. 1–10, 2012.

[14] Y. Yang and Q. Li, "A context-aware trust evaluation model for manets," *Wireless Personal Communications*, vol. 80, no. 4, pp. 1441–1459, 2015.

[15] H. Ning and H. Liu, "Cyber-physical-social based security architecture for future internet of things," *IEEE Internet of Things Journal*, vol. 1, no. 4, pp. 401–407, 2014.

[16] M. S. Alkatheiri *et al.*, "A semantic-aware trust model for intelligent vehicular networks," *Future Generation Computer Systems*, vol. 108, pp. 785–799, 2020.

[17] K. Xie *et al.*, "A survey of machine learning techniques applied to self-organizing networks," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 4, pp. 2392–2431, 2017.

[18] A. M. Vegni and V. Loscri, "A survey on vehicular social networks," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2397–2419, 2015.

[19] M. Zhang *et al.*, "A survey on trust management in wireless sensor networks," *Journal of Network and Computer Applications*, vol. 35, no. 3, pp. 867–880, 2012.

[20] C. Zhang and Y. Fang, "A fine-grained reputation system for reliable service selection in peer-to-peer networks," *IEEE Trans. Parallel and Distributed Systems*, vol. 18, no. 8, pp. 1134–1145, 2007.

[21] A. Shabut *et al.*, "A survey on trust models and computing in social networks," *IEEE Access*, vol. 6, pp. 17 294–17 314, 2018.

[22] M. H. Ibrahim *et al.*, "Trust estimation in cloud-based iot services using a hybrid model," *Journal of Cloud Computing*, vol. 10, 2021.

[23] Y. Ren *et al.*, "A dynamic trust model for wireless sensor networks," *IEEE Transactions on Wireless Communications*, vol. 6, no. 8, pp. 2956–2964, 2007.

[24] M. H. Ibrahim and A. Gani, "Lightweight trust models in iot: Recent advances and research challenges," *IEEE Internet of Things Journal*, vol. 7, no. 7, pp. 5971–5984, 2020.

[25] J. Wang *et al.*, "Blockchain-based trust management in vehicular networks: A survey," *IEEE Internet of Things Journal*, vol. 8, no. 2, pp. 1492–1505, 2021.

[26] A. Hamza, A. Nait-Sidi-Moh, and A. Gueroui, "Fuzzy logic-based trust management framework for drone networks," *Journal of Network and Computer Applications*, vol. 160, p. 102631, 2020. [Online]. Available: https://doi.org/10.1016/j.jnca.2020.102631

[27] M. H. Ibrahim and A. Gani, "Lightweight trust models in iot: Recent advances and research challenges," *IEEE Internet of Things Journal*, vol. 7, no. 7, pp. 5971–5984, 2020. [Online]. Available: https://doi.org/10.1109/JIOT.2020.2975392

[28] N. Komninos *et al.*, "Survey in intrusion detection for the internet of things," *Journal of Network and Computer Applications*, vol. 66, pp. 37–57, 2016.

[29] Z. Qin *et al.*, "When things matter: A survey on data-centric internet of things," *Journal of Network and Computer Applications*, vol. 64, pp. 137–153, 2016.

[30] M. K. Sigaroli, M. Nagar, and M. K. Jhariya, "Investigation of clock synchronization techniques and its performance impact in manet," *International Journal of Current Trends in Engineering & Technology (IJCTET)*, vol. I, no. VII, pp. 183–189, Nov. 2015, prof. Mithlesh Kumar Sigaroli et al.

[31] H. M. Omar, "Hardware-in-the-loop simulation of time-delayed anti-swing controller for quadrotor with suspended load,"

Applied Sciences, vol. 12, no. 3, p. 1706, 2022, highlights HIL integration gaps with PX4 firmware v1.12.3.

[32] Anonymous, "A step-by-step guide to creating a robust autonomous drone," *arXiv preprint arXiv:2506.11400*, 2025, section 2.2 highlights hardware integration latency on PX4/ArduPilot HIL systems. [Online]. Available: https://arxiv.org/abs/2506.11400

[33] A. Liu *et al.*, "Low-latency trust evaluation for iot devices," *Computer Networks*, vol. 149, pp. 245–259, 2019.