Lightweight Time-Indexed Secure Communication Protocol with Dual-Layer Defense for UAV Swarm Networks[*]

Kun-Lin Tsai, Kuo-Wei Wang, Fang-Yie Leu and Chao-Tung Yang[†]

TungHai University, Taichung, Taiwan
kltsai@thu.edu.tw

Abstract

Unmanned Aerial Vehicles (UAVs) are increasingly deployed in surveillance, logistics, and disaster response, yet swarm-based operations remain vulnerable to cyberattacks such as denial-of-service, spoofing, replay, and man-in-the-middle intrusions. This paper proposes an integrated framework combining a Lightweight Time-Indexed Secure Communication Protocol (LTISCP) with a dual-layer defense system. LTISCP leverages time-indexed session keys and Ascon-based lightweight cryptography to ensure efficient and secure communication, while the defense layer employs a deep neural network–based Intrusion Detection System (IDS) for real-time anomaly detection in swarm traffic. To enable deployment on UAV edge devices, model pruning is applied to optimize the IDS for reduced computational cost. Experiments show that the framework reduces latency by up to 35%, lowers energy consumption by 28%, and achieves over 92% detection accuracy with less than 4% false positives, making it well-suited for real-time UAV swarm deployments.

Keywords: UAV Swarm Networks, Lightweight Cryptography, Time-Indexed Key Management, Intrusion Detection System (IDS), Secure Communication Protocol

1 Introduction

Unmanned Aerial Vehicles (UAVs) have become indispensable in domains such as surveillance, disaster response, precision agriculture, and logistics. Recently, UAV swarms have gained significant attention due to their scalability, resilience, and responsiveness. Through distributed coordination, UAV swarms can cover larger areas, execute tasks in parallel, and achieve higher mission efficiency compared with single-UAV systems.

Despite these advantages, UAV swarms introduce critical security challenges. UAVs are resource-constrained in terms of battery life, computational capacity, and communication bandwidth, and they operate in dynamic and adversarial wireless environments. This makes them highly vulnerable to eavesdropping, spoofing, replay, man-in-the-middle (MITM), and denial-of-service (DoS) attacks. The compromise of even a small subset of UAVs can undermine the entire swarm, leading to

[*] Proceedings of the 9th International Conference on Mobile Internet Security (MobiSec'25), Article No. 34, December 16-18, 2025, Sapporo, Japan. © The copyright of this paper remains with the author(s).

[†] Corresponding author

disrupted operations and mission failure. Thus, designing robust yet lightweight security mechanisms is essential for ensuring the reliability of swarm deployments.

Existing approaches typically rely on conventional cryptographic mechanisms or public key infrastructures (PKI), which offer strong guarantees but introduce excessive computational and communication overhead. Static key management schemes further expose swarms to key reuse and compromise. Similarly, intrusion detection systems deployed in isolation may detect malicious activity but fail to integrate with secure communication protocols, resulting in additional overhead for resource-constrained UAVs. These limitations highlight the need for an integrated design that addresses both communication-layer security and real-time anomaly detection while maintaining efficiency.

In this paper, we propose an integrated framework that combines a Lightweight Time-Indexed Secure Communication Protocol (LTISCP) with a deep neural network–based Intrusion Detection System (IDS). LTISCP leverages time-indexed session keys and lightweight cryptographic primitives (Ascon) to provide confidentiality, integrity, and mutual authentication with minimal overhead. Complementing this, the IDS continuously monitors swarm traffic and detects anomalies such as DoS, spoofing, and MITM attacks in real time. Model pruning techniques are applied to reduce computational complexity, enabling IDS deployment on UAV edge devices. Together, these contributions form a dual-layer framework that achieves efficient, secure, and resilient UAV swarm communication. Unlike conventional static key or PKI-based protocols, the proposed LTISCP dynamically derives session keys based on synchronized time indices. This design eliminates key reuse, minimizes key exchange overhead, and ensures both forward and backward secrecy under UAV swarm dynamics.

2 Related Studies

Secure communication in UAV networks has been a longstanding research focus. Traditional approaches based on PKI and certificate-based authentication provide strong guarantees of confidentiality and integrity, but they incur excessive computational and communication overhead, which makes them impractical for resource-constrained UAV swarms (Hassija, 2021, Yu, 2023). More recent studies have explored lightweight cryptographic alternatives. For instance, Cecchinato et al. (Cecchinato, 2023) demonstrated the feasibility of lightweight Advanced Encryption Standard (AES) encryption for real-time UAV multimedia transmission, while Alexan et al. (Alexan, 2024) addressed secure communication in UAV-assisted military reconnaissance. These works confirm the potential of lightweight cryptography but still lack adaptive and scalable key management tailored for dynamic swarm deployments.

Parallel to secure communication, IDS have been introduced to improve UAV resilience against cyberattacks. Early studies relied on shallow machine learning models (Vigneswaran, 2018), but recent advances in deep neural networks have significantly improved detection performance. Hassler et al. (Hassler, 2023) proposed a cyber-physical IDS for UAVs, while Ihekoronye et al. (Ihekoronye, 2024) presented DroneGuard, an explainable IDS framework for UAV networks. Mughal et al. (Mughal, 2024) further extended IDS design to swarm-level environments using graph neural networks, highlighting the need for scalable anomaly detection. Nevertheless, most IDS solutions are evaluated independently, without integration into secure communication protocols, leaving a gap between anomaly detection and protected data exchange.

Given the limited resources of UAV platforms, optimizing IDS for onboard deployment is equally critical. Classical pruning methods such as Han et al. (Han, 2015) and Luo et al. (Luo, 2017) established the foundation for reducing model complexity, while more recent advances such as Kumar et al. (Kumar, 2021), Fang et al. (Fang, 2023), and Sanh et al. (Sanh, 2020) have introduced structured and adaptive pruning techniques. These approaches significantly reduce inference latency and memory consumption while preserving acceptable accuracy, enabling Deep Neural Network (DNN)-based IDS models to be efficiently deployed at the UAV edge.

Previous research has advanced secure communication and IDS independently, but integrated solutions remain limited. Existing methods often trade security for efficiency or vice versa, leaving UAV swarms vulnerable to combined threats. This motivates the need for a dual-layer framework that unifies lightweight communication protocols with IDS-based anomaly detection to achieve holistic protection under UAV resource constraints.

3 System & Threat Model

The proposed framework targets UAV swarm networks composed of multiple UAV nodes and a ground control station (GCS). As shown in Fig. 1, the GCS issues mission commands and receives aggregated data from the swarm, while UAVs communicate with each other in a mesh-like structure to exchange status updates and coordinate tasks. Each UAV is equipped with lightweight onboard computing resources and integrates two complementary layers of protection. The first is the communication security layer, which implements the LTISCP. This protocol derives session keys from a shared master key and a synchronized time index, ensuring that each communication interval is protected by a unique key. By employing Ascon-Hash for key derivation and Ascon-AEAD for authenticated encryption, LTISCP provides confidentiality, integrity, and mutual authentication with minimal computational and energy overhead. The second is the defense layer, which incorporates a deep neural network–based IDS to monitor traffic anomalies such as denial-of-service or man-in-the-middle attacks. Model pruning techniques are applied to reduce the computational footprint of the IDS, making it feasible for deployment on UAV edge devices. Together, these layers form a dual-layer security architecture that protects communication channels and enhances swarm resilience, as shown in Figure 1.

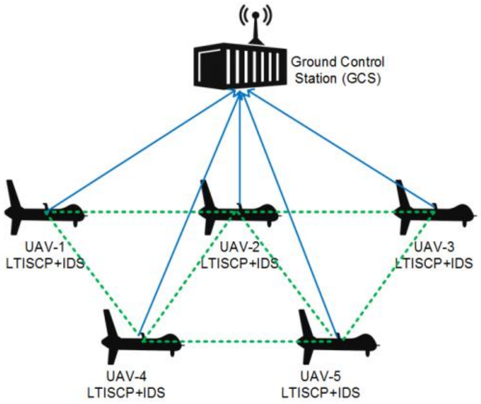

Figure 1: System Architecture of the Proposed Framework

While the system design aims to secure UAV operations, swarm networks are highly exposed to adversarial threats. The threat model, illustrated in Figure 2, considers adversaries who can actively interfere with wireless channels but do not physically compromise UAV hardware. Several classes of attacks are considered. Eavesdroppers passively capture communication packets in an attempt to extract sensitive information, such as UAV trajectories or mission commands. Replay and spoofing attacks exploit intercepted data by resending outdated commands or impersonating legitimate nodes, thereby disrupting coordination. MITM attacks are more severe, enabling adversaries to intercept and manipulate ongoing communication flows between UAVs or between UAVs and the GCS. DoS attacks can overwhelm UAV communication links with excessive traffic or jamming signals, reducing swarm responsiveness and reliability.

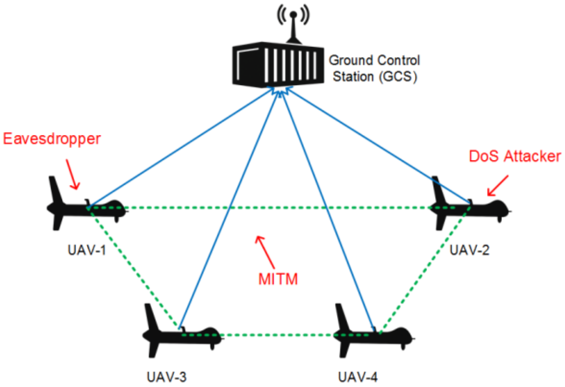

Figure 2: Threat Model in UAV Swarm Networks.

Given this threat landscape, the security requirements of the framework extend beyond conventional encryption. The system must ensure confidentiality, integrity, and robust mutual authentication, while providing forward and backward secrecy so that the compromise of one session key does not endanger past or future communication. Moreover, it must incorporate real-time anomaly detection to identify suspicious traffic. Finally, all mechanisms must remain lightweight to fit the resource constraints of UAV nodes, ensuring that security does not come at the expense of performance or mission efficiency.

4 Proposed Framework

4.1 Framework Overview

The proposed framework is designed to provide comprehensive security for UAV swarm networks by integrating a lightweight secure communication protocol with two complementary defense layers. Its primary objective is to ensure end-to-end protection of control messages and mission-critical data, while preserving the low computational and energy footprint required by resource-constrained UAV platforms.

At the communication layer, the system employs the LTISCP. LTISCP leverages a dynamic session key mechanism derived from a shared master key and a synchronized time index. This ensures that each communication interval is protected by a distinct key, preventing key reuse and limiting the impact of potential compromise. Ascon-Hash is used for key derivation, while Ascon-AEAD provides authenticated encryption. Compared with traditional PKI-based approaches, LTISCP achieves significant reductions in latency and energy consumption while maintaining strong cryptographic guarantees.

On top of this secure communication foundation, the framework incorporates a deep neural network–based IDS, which continuously monitors UAV network traffic and detects attacks such as denial-of-service, spoofing, and man-in-the-middle intrusions. To accommodate limited onboard resources, pruning techniques are applied to reduce the computational complexity of the IDS without significantly sacrificing detection accuracy, making it suitable for deployment on UAV edge devices.

The interaction of these modules is illustrated in Figure 3. Communication begins with LTISCP, which secures message delivery through encryption and authentication. Network traffic is then analyzed by the IDS to flag potential anomalies, ensuring that malicious activities can be detected even if adversaries attempt to bypass cryptographic protections. By combining these layers, the framework ensures that security is preserved across both the communication and network monitoring dimensions.

Overall, this integrated design delivers a dual-layer security solution that simultaneously ensures communication confidentiality and real-time anomaly detection. By coupling lightweight cryptography with AI-based defense mechanisms optimized for edge deployment, the framework balances strong security guarantees with the practical requirements of real-time UAV swarm operations.

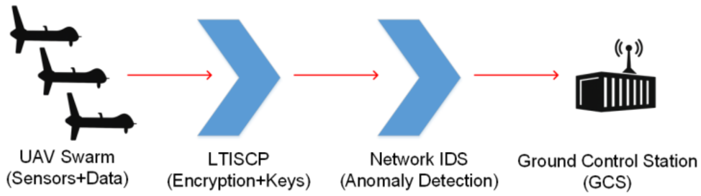

Figure 3: Workflow of the Proposed Framework.

4.2 Mathematical Model of LTISCP

To rigorously describe the LTISCP, we present its formal model including time indexing, key derivation, packet construction, replay protection, authentication, and security guarantees.

- System and Time Indexing.

The UAV swarm is represented as a set of nodes $\mathcal{N} = \{n_1, \dots, n_m\}$, with the GCS denoted as C and UAV nodes as $U \in \mathcal{N} \backslash \{C\}$. Time is divided into discrete slots of duration Δ. At any real time $t \geq 0$, the time index is defined as

$$T = \left\lfloor \frac{t}{\Delta} \right\rfloor$$

A drift tolerance δ is assumed to accommodate clock desynchronization, so that valid communication may occur within indices $[T - \delta, T + \delta]$.

- Key Schedule

Each pair of communicating entities shares a long-term master key $K_m \in \{0, 1\}^k$. For each index T, a session key is derived as:

$$K_T = H(K_m || ctx || T)$$

where H is a hash function, and *ctx* encodes contextual information (session identifier, node roles, algorithm suite). This ensures that each communication interval uses a unique key, providing forward secrecy (compromise of K_T does not reveal $K_{T'}$, for $T' > T$) and backward secrecy (past intervals remain secure).

For enhanced separation of functionality, one may further derive subkeys:

$$K_T^{enc} = H(K_T \,||\, "enc"),\; K_T^{mac} = H(K_T \,||\, "mac").$$

In practice, Ascon-AEAD uses only K_T as a unified encryption and authentication key.

- Packet Construction and Replay Protection

At time index *T*, a UAV *A* sending message *M* to node *B* generates a per-interval counter ctr_A that increments monotonically. The packet is then constructed as:

$$\langle \text{ver}, ID_A, ID_B, T, ctr_A, C, \tau \rangle,$$

where $(C, \tau) \leftarrow Enc_{K_T}(ctr_A, aad, M)$ is the ciphertext and authentication tag under Ascon-AEAD, and

$$aad = (ID_A, ID_B, T, role)$$

binds the packet to the communicating parties and the current time index.

Upon reception, node *B* performs:

1. Index Validation: check whether $T \in [T_{now} - \delta, T_{now} + \delta]$.
2. Nonce Validation: ensure that ctr_A has not been previously used within index *T* for source ID_A.
3. Decryption and Verification: compute $Dec_{K_T}(C, \tau)$. If authentication succeeds, output *M*.

This construction guarantees replay resistance since duplicate pairs (T, ctr_A) are rejected, and AEAD binding prevents manipulation of associated data.

- Mutual Authentication and Re-synchronization

LTISCP supports lightweight challenge–response authentication. When UAV *U* joins or reconnects, it sends a nonce r_U together with its ID and time index. The GCS responds with $Enc_{K_T}(r_U || r_C)$, proving possession of the correct session key, while *U* confirms by returning $Enc_{K_T}(r_C)$. This ensures mutual authentication without expensive public-key operations.

In case of clock drift beyond δ, a re-synchronization mechanism is triggered. The GCS encrypts its current index T_C using the long-term key K_m and securely transmits it to *U*. This allows UAVs to realign their local index without exposing session keys.

- Security Properties

The security goals achieved under standard assumptions can be summarized as follows.

- Confidentiality & Integrity: Provided by Ascon-AEAD, ensuring IND-CCA and INT-CTXT security when nonces are unique.

- Replay Protection: Enforced by binding both the time index and per-interval counters.
- Forward/Backward Secrecy: Ensured by PRF-based derivation of session keys; compromise of K_T does not expose other intervals.
- Authentication & Liveness: Guaranteed through challenge–response exchanges bound to K_T.
- Efficiency: Each interval requires a single hash computation for key derivation, and each packet requires one AEAD operation, suitable for UAV platforms with limited computational capacity.

LTISCP achieves robust protection by combining time-indexed key derivation, AEAD-based confidentiality and integrity, nonce-based replay resistance, and efficient re-synchronization. The mathematical model formalizes these mechanisms and demonstrates how strong cryptographic properties can be achieved with minimal overhead, making LTISCP practical for real-time UAV swarm communication.

4.3 Intrusion Detection Integration

While LTISCP provides confidentiality and integrity for each packet ⟨ver, $ID_A, ID_B, T, ctr_A, C, \tau$⟩, it cannot by itself prevent adversaries from flooding the swarm with malicious traffic or injecting anomalous communication patterns. To complement the cryptographic layer, the proposed framework integrates a deep neural network–based IDS that operates on traffic features extracted after LTISCP verification.

- Feature Extraction

Once a packet is successfully authenticated and decrypted with the session key K_T, its metadata is transformed into a feature vector:

$$x_i = [f_1, f_2, \dots, f_d],$$

where each f_j represents a statistical property of the traffic flow, such as packet size, inter-arrival time, byte rate, or directionality between nodes. These features are aggregated per flow, allowing the IDS to characterize behavior beyond individual packets.

- Classification Model

The IDS applies a deep neural network parameterized by θ, trained on labeled datasets such as CIC-IDS2017. For each feature vector x_i, the IDS outputs a predicted class:

$$\hat{y}_i = \arg \max_{c \in \{\text{normal, attack}\}} P(y = c \mid x_i; \theta).$$

The model thus distinguishes normal swarm traffic from anomalies caused by attacks such as denial-of-service, spoofing, or man-in-the-middle intrusions.

- Integration with LTISCP

The IDS operates downstream of the LTISCP layer. After a packet is validated for integrity under its session key K_T, the IDS processes the associated feature vector x_i. This separation of roles avoids redundant decryption overhead, since IDS relies only on traffic metadata rather than plaintext payloads. Moreover, the time index T included in the packet's authenticated associated data provides a natural temporal boundary for IDS feature windows, aligning anomaly detection with the same secure communication epochs defined in LTISCP.

- Lightweight Optimization

To deploy IDS on UAV edge devices, the DNN model is pruned to reduce parameter count and memory footprint. Let the original model be defined by parameters θ, with complexity $\mathcal{O}(|\theta|)$. After pruning, the reduced model θ' satisfies

$$|\theta'| \ll |\theta| \text{ while maintaining } \mathbb{E}[\hat{y}_i = y_i] \approx \mathbb{E}\left[\hat{y}_i^{\text{orig}} = y_i\right],$$

ensuring that computational efficiency improves without significant loss of detection accuracy.

- Functionality

During operation, the IDS serves as a second line of defense. If anomalies are detected in the stream of feature vectors $\{x_i\}$, alerts are generated and sent to the GCS. The GCS can then enforce countermeasures, such as rerouting communication, isolating a compromised UAV, or adjusting LTISCP parameters, e.g., shortening Δ, to tighten security. This integration ensures resilience not only at the cryptographic level but also against behavioral deviations in swarm communication.

5 Experimental Evaluation

5.1 Experimental Setup

To evaluate the effectiveness of the proposed framework, we conducted experiments combining both simulation and prototype deployment. UAV swarm communication was modeled in the NS-3 simulator, with swarm sizes varying from 10 to 100 UAVs. Each UAV node was configured with Raspberry Pi 4B hardware to emulate resource-constrained platforms, equipped with a quad-core ARM Cortex-A72 CPU and 4 GB RAM. The LTISCP was implemented using Ascon-128 for authenticated encryption and Ascon-Hash for key derivation.

The IDS was trained and validated using the CIC-IDS2017 dataset, which includes labeled traffic instances of DoS, spoofing, and MITM attacks. Pruning was applied to the DNN IDS model to reduce computational overhead before deployment on Raspberry Pi devices. System performance was measured in terms of latency, throughput, energy consumption, detection accuracy, and false positive rate. The experimental configuration is summarized in Table 1.

Table 1: Experimental Parameters

Category	Parameter / Dataset	Value / Description
Simulation (NS-3)	Swarm size	10, 20, 50, 100 UAVs
	Communication model	IEEE 802.11s mesh, 2.4 GHz band
	Propagation model	Log-distance path loss, mobility with random waypoint
Prototype Hardware	UAV platform (emulation)	Raspberry Pi 4B, Quad-core ARM Cortex-A72, 4 GB RAM
	Operating system	Raspbian OS, Linux kernel 6.x

Cryptography	LTISCP cipher	Ascon-128 (AEAD), Ascon-Hash (PRF)
	Key update interval (Δ)	1–5 s
IDS	Dataset	CIC-IDS2017 (DoS, MITM, spoofing, port scan flows)
	Model architecture	DNN with 3 hidden layers, ReLU activation
	Optimization	Structured pruning (50–60% parameter reduction)

5.2 LTISCP Performance

We first evaluate the performance of the LTISCP against a conventional PKI-based scheme. The analysis focuses on communication latency and energy consumption per packet, which are critical for UAV swarm deployments where responsiveness and battery life directly affect mission success.

As shown in Figure 4, LTISCP consistently achieves lower latency across different swarm sizes. For example, at *n*=10, average latency is reduced from 35 ms (PKI) to 22 ms (LTISCP), representing a 37% improvement. At *n*=100, latency decreases from 130 ms to 84 ms, corresponding to a 35% reduction. These gains result from LTISCP's lightweight time-indexed key derivation, which eliminates costly public-key operations.

Energy efficiency improvements are summarized in Figure 5. LTISCP reduces per-packet energy consumption by approximately 25–30% across all swarm sizes. For instance, at *n*=50, LTISCP requires 2.0 J per packet compared with 2.8 J under the PKI-based baseline. This efficiency arises from avoiding frequent key exchanges and relying on hash-based derivation.

To complement the figures, Table 2 provides a numerical comparison of latency and energy consumption between LTISCP and PKI. The table also highlights the percentage improvement, showing consistent reductions in both metrics regardless of swarm size.

Importantly, LTISCP maintains a packet delivery ratio above 97% even in the largest swarm configuration. This confirms that the protocol scales efficiently without compromising reliability. Taken together, the results in Figure 4, Figure 5, and Table 2 demonstrate that LTISCP successfully balances strong security with low latency and energy efficiency, making it well-suited for real-time UAV swarm deployments.

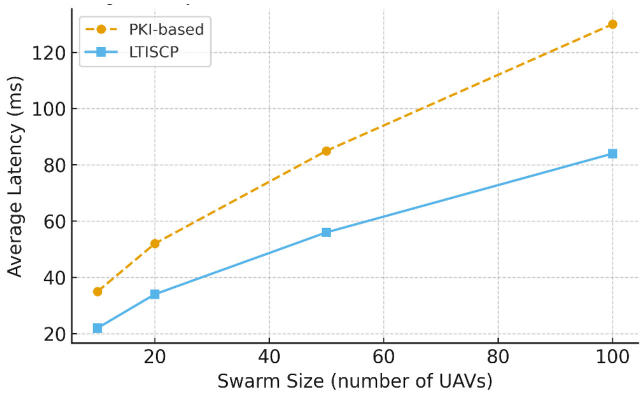

Figure 4: Average latency comparison between LTISCP and a PKI-based scheme under different swarm sizes.

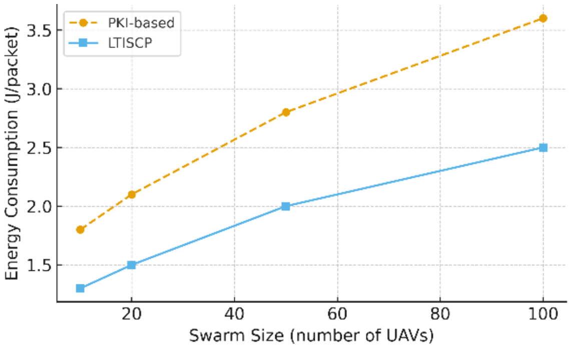

Figure 5: Energy consumption per UAV packet for LTISCP and a PKI-based scheme.

Table 2: Latency and Energy Consumption Comparison between LTISCP and PKI-based Scheme

Swarm Size (UAVs)	Latency – PKI (ms)	Latency – LTISCP (ms)	Improvement (%)	Energy – PKI (J/packet)	Energy – LTISCP (J/packet)	Improvement (%)
10	35	22	37%	1.8	1.3	28%
20	52	34	35%	2.1	1.5	29%
50	85	56	34%	2.8	2.0	29%
100	130	84	35%	3.6	2.5	31%

5.3 IDS Effectiveness

The IDS was evaluated using the CIC-IDS2017 dataset, which contains diverse attack types relevant to UAV swarm networks, including DoS, spoofing, and MITM. The IDS model was implemented as a deep neural network with three hidden layers and ReLU activations. To enable deployment on UAV edge devices, the model was pruned by approximately 50–60% of its parameters while preserving detection performance.

As shown in Figure 6, the IDS achieves high accuracy across all evaluated attack types. Specifically, it detects DoS traffic with 93.5% accuracy, spoofing attempts with 94.2% accuracy, and MITM attacks with 92.1% accuracy. The false positive rate remained below 4% in all cases, demonstrating that the IDS can reliably distinguish malicious behavior from normal swarm communication.

To evaluate the effect of pruning, we compared the original model with the reduced version deployed on Raspberry Pi 4B devices. Results are summarized in Figure 7. The pruned model reduces memory usage and parameter count by more than 55%, with only a marginal drop in average accuracy. Inference latency per flow is below 5 ms on Raspberry Pi, confirming that the IDS can operate in real time without burdening resource-constrained UAV nodes.

Together, these results show that the IDS provides an effective second line of defense, complementing LTISCP's cryptographic guarantees by detecting anomalous traffic patterns in real time.

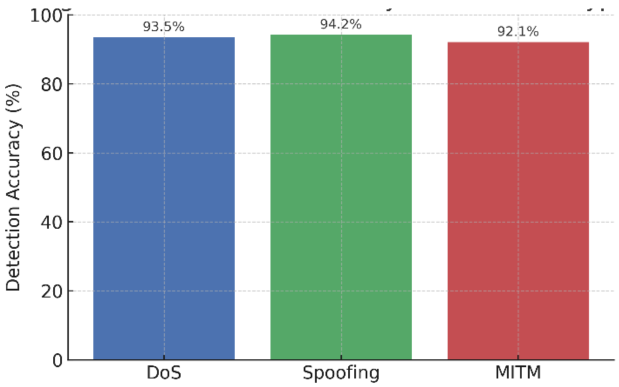

Figure 6: IDS detection accuracy across attack types.

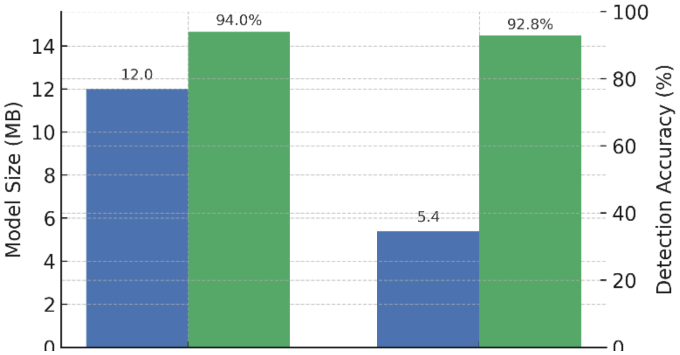

Figure 7: Model size vs. detection accuracy before and after pruning.

5.4 Discussion on Security Guarantees

The proposed LTISCP ensures confidentiality and integrity through Ascon-AEAD encryption, which provides IND-CCA security. Replay protection is achieved by the combination of time-indexed session keys and per-interval counters. Man-in-the-middle and spoofing attacks are mitigated by mutual authentication using synchronized indices and nonces. DoS attacks are mitigated through IDS-based anomaly detection. Together, these mechanisms meet the security requirements outlined in Section 3, ensuring resilience under the considered threat model.

6 Conclusion

This paper introduced a cross-layer security framework for UAV swarm networks that integrates the LTISCP with a deep neural network–based IDS. LTISCP employs time-indexed session keys and Ascon-based lightweight cryptography to achieve confidentiality, integrity, and mutual authentication with significantly reduced latency and energy overhead compared to PKI-based baselines. Complementing this, the IDS enhances resilience by detecting denial-of-service, spoofing, and man-in-the-middle attacks in real time under resource-constrained UAV platforms. Experimental results confirm that LTISCP reduces latency by up to 37% and energy consumption by nearly 30%, while the pruned IDS sustains over 92% detection accuracy with less than 4% false positives, enabling practical deployment in UAV swarm environments.

Looking forward, future work will address broader adversarial scenarios, including coordinated multi-vector attacks and adversarial machine learning targeting IDS models. In addition, we plan to investigate adaptive key management and advanced swarm coordination strategies, as well as validate the framework on large-scale UAV swarm testbeds to further demonstrate its scalability and robustness in real-world missions.

References

Alexan, W., Aly, L., Korayem, Y., Gabr, M., El-Damak, D., Fathy, A., & Mansour, H. A. (2024). *Secure communication of military reconnaissance images over UAV-assisted relay networks*. IEEE Access, 12, 78589-78610.

Cecchinato, N., Toma, A., Drioli, C., Oliva, G., Sechi, G., & Foresti, G. L. (2023). *Secure real-time multimedia data transmission from low-cost UAVs with a lightweight AES encryption*. IEEE Communications Magazine, 61(5), 160-165.

Fang, G., Ma, X., Song, M., Mi, M. B., & Wang, X. (2023). *Depgraph: Towards any structural pruning*. In Proceedings of the IEEE/CVF conference on computer vision and pattern recognition (pp. 16091-16101).

Han, S., Pool, J., Tran, J., & Dally, W. (2015). *Learning both weights and connections for efficient neural networks*. In Advances in Neural Information Processing Systems (pp. 1135–1143).

Hassler, S. C., Mughal, U. A., & Ismail, M. (2023). *Cyber-physical intrusion detection system for unmanned aerial vehicles*. IEEE Transactions on Intelligent Transportation Systems, 25(6), 6106-6117.

Hassija, V., Chamola, V., Agrawal, A., Goyal, A., Luong, N. C., Niyato, D., & Guizani, M. (2021). *Fast, reliable, and secure drone communication: A comprehensive survey*. IEEE Communications Surveys & Tutorials, 23(4), 2802–2832.

Ihekoronye, V. U., Ajakwe, S. O., Lee, J. M., & Kim, D. S. (2024). *DroneGuard: an explainable and efficient machine learning framework for intrusion detection in drone networks*. IEEE Internet of Things Journal.

Kumar, A., Shaikh, A. M., Li, Y., Bilal, H., & Yin, B. (2021). *Pruning filters with L1-norm and capped L1-norm for CNN compression*. Applied Intelligence, 51(2), 1152-1160.

Luo, J. H., Wu, J., & Lin, W. (2017). *Thinet: A filter level pruning method for deep neural network compression*. In Proceedings of the IEEE International Conference on Computer Vision (pp. 5058-5066).

Vigneswaran, R. K., Vinayakumar, R., Soman, K. P., & Poornachandran, P. (2018, July). *Evaluating shallow and deep neural networks for network intrusion detection systems in cyber security*. In 2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT) (pp. 1-6). IEEE.

Sohan, M., Sai Ram, T., Reddy, R., & Venkata, C. (2024). *A review on YOLOv8 and its advancements*. In International Conference on Data Intelligence and Cognitive Informatics (pp. 529-545). Springer, Singapore.

Yu, Z., Wang, Z., Yu, J., Liu, D., Song, H. H., & Li, Z. (2023). *Cybersecurity of unmanned aerial vehicles: A survey*. IEEE Aerospace and Electronic Systems Magazine, 39(9), 182–215.