Unmanned aerial vehicle systems: key management and intrusion response techniques

Reshma C. Sonawane[1], **A. Muthukrishnan**[2]
[1]Department of Computer Science and Engineering, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai, India
[2]Department of Electronics and Communication Engineering, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai, India

Article Info

Article history:

Received Jul 27, 2024
Revised Nov 14, 2025
Accepted Dec 15, 2025

Keywords:

Elliptic curve encryption
Energy consumption
Intrusion detection system
Malicious nodes
Pairwise key generation
Secure communication
Unmanned aerial vehicles

ABSTRACT

Protecting information is crucial for unmanned aerial vehicle (UAV) network communications, particularly during delicate tasks such as surveillance and reconnaissance. While encryption safeguards data privacy, managing and distributing keys in UAV settings poses significant challenges due to the vehicles' mobility and limited processing power. This research proposes an efficient key management scheme utilizing elliptic curve cryptography (ECC) and bilinear pairings, complemented by a lightweight intrusion detection system (IDS). The method employs behavior-based anomaly detection, using cluster-based watchdogs and trust assessment to identify and isolate harmful nodes. Additionally, applying compression techniques before encryption helps to reduce transmission load. Simulation in NS2 demonstrates performance improvements of 6-10% in throughput, 4-6% in packet delivery ratio (PDR), and a 13-17% reduction in delay compared to elliptic curve cryptography Diffie–Hellman (ECCDH) and pairwise encryption methods.

Corresponding Author:

Reshma C. Sonawane
Department of Computer Science and Engineering
Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology
Chennai, India
Email: reshmagold@gmail.com

1. INTRODUCTION

Unmanned aerial vehicles, also known as UAVs, are crucial for modern applications such as environmental monitoring, disaster response, and military activities [1], [2]. Nonetheless, their flexibility and reliance on wireless communication expose them to vulnerabilities such as data breaches, jamming, and node-level attacks [3], [4]. As a result, ensuring secure, efficient, and scalable communication protocols is critical to the dependability and resilience of UAV networks [5], [6]. Conventional cryptography algorithms, while efficient, are resource-intensive and unsuitable for UAVs with limited processor and energy capabilities [7], [8]. Lightweight encryption approaches, such as elliptic curve cryptography (ECC), strike a balance between efficiency and security [9], [10]. Nonetheless, merging key management and intrusion detection into a unified framework remains a substantial difficulty, which this study addresses by utilizing a dual-layered security approach. Another challenge with UAV networks is detecting harmful actions. Intrusion detection systems (IDS), specifically Watchdog methods, have been used to identify odd behavior in UAV systems. Nonetheless, these systems usually encounter difficulties when confronted with sophisticated or coordinated attacks, particularly in high-mobility scenarios where UAVs regularly shift positions [11], [12]. The most recent research has focused on IDS concepts based on clustering, in which cluster heads collect and analyze data to improve detection accuracy and response times [13], [14]. However, this strategy introduces a potential weakness: relying entirely on a single cluster head may result in a single failure point, reducing the network's resilience [15], [16].

To address these shortcomings, the I-Watchdog system was designed, which improves detection precision by combining cluster-based IDS with extra monitoring capabilities. This integrated strategy reduces mistake rates and improves the efficacy of intrusion detection [17], [18]. Nonetheless, a more comprehensive system is required to integrate key management and breach detection into a unified framework, which has been missed in previous research. The current study focuses on either primary management or independent violation detection, resulting in trade-offs between security and operational efficiency [19], [20]. This research addresses an existing gap by introducing a dual-layered security framework that combines lightweight key management with intrusion detection. While many earlier studies have tackled these issues separately, resulting in partial solutions, this new model integrates both aspects using bilinear pairing cryptography using elliptic curves, designed for low-power UAV settings and behavior-based detection within clustered UAV scenarios. This unified approach is crucial for applications that are resource-limited, mobile, and sensitive to delays [21], [22]. Additionally, this study builds on previous developments in key setup systems, which use a multi-step approach for safeguarding UAV communications. Each UAV node is assigned an identification number and pre-distributed digitally signed keys, allowing for mutual authorization through safe private key agreements. Regular key refreshes improve security over time by addressing potential weaknesses [23], [24]. However, the technique confronts difficulties such as the difficulty of early distribution of keys and significant computing costs, especially in flexible or ad hoc UAV systems. Likewise, stochastic key pre-distribution strategies improve scalability and robustness for node capture; nevertheless, they bring difficulties like key mismatch and communication cost during the crucial discovery phase [25], [26]. Although several writers offered integrated systems, there is still a demand for a more complete approach [27], [28]. These issues are addressed by a novel key administration strategy for UAVs, which may increase computing complexity. In order to improve the dependability and flexibility of UAV aerial communication networks, recent research has identified safe and portable key management techniques that frequently make use of blockchain-supported systems [29]. Furthermore, advancements in artificial intelligence-powered key management algorithms suggest that processing costs could be decreased while still meeting stringent safety standards for UAV communication networks [30], [31].

This study brings three important contributions: i) a more effective pairwise key administration protocol for UAV networks, ii) a modified I-Watchdog detection and prevention model based on UAV collections, and iii) verified improvements in performance via NS-all-in-one 2.35 (NS2) modeling, showing diminished delay, upgraded delivery of packets ratios, and lesser usage of energy in UAV interaction for changing security-critical usages. The following portions of this work are grouped as follows: section 2 discusses the proposed system, including the interaction and attacking models, as well as the algorithmic sketch. The section 3 provides a comparative evaluation of projected research and recent developments. The section 4 comprises the work's results and discussion, followed by a constructive conclusion in the section 5.

2. METHOD

This research aims to enhance the security and energy efficiency of ad hoc UAV networks, which typically employ IEEE 802.11 and 802.15.4 standards. Transport layer security (TLS) and internet protocol security (IPsec) are sophisticated protocols, but they are too demanding for resource-constrained UAV systems. Thus, this part provides the framework of the system's architecture (proposed system and conceptual perspective), including model details for encryption and attack detection. Our strategy combines a dynamic key management protocol based on elliptic curve pairing with a smart watchdog system to detect malicious UAV nodes via trust scoring and packet forwarding analysis using the I-Watchdog mechanism. The system has three stages: initial encryption at the source, intrusion detection using the watchdog, and energy-efficient communication. Each level is designed to improve security and network performance while keeping computational needs minimal. To aid in execution, these components are explained using stratified algorithms and visual representation via architectural models.

2.1. Proposed system

Here, we introduce an encryption method that utilizes a dual key creation system to protect UAV communications. Every network node receives a distinct identification code (ID), incorporating both MAC and IP addresses, which serve as crucial elements in the encryption procedure. The suggested method creates paired keys, enabling the source node to choose the following hop node and establish secure communication. This framework implements a combined encryption approach where ECC manages secure key negotiation, while symmetric encryption—such as advanced encryption standard (AES)—processes the primary data encryption. This blend successfully maintains equilibrium between the processing efficiency of symmetric algorithms and the strong key exchange capabilities of asymmetric techniques. When network capacity expands, obstacles like key synchronization, complexity control, and delays caused by packet loss may affect secure data transmission. To address these issues, redundancy verification is implemented to maintain synchronization. Enhanced encryption methods are also used to minimize processing times and performance restrictions. The encryption-driven communication framework is depicted in Figure 1. In this paradigm, the source node 'S_N' chooses the destination node. The encryption process is specified by (1).

$$M \leftarrow encrypt\ (msg, ID\ (D_N)), \tag{1}$$

Ensuring that only the destination node with the correct ID can decrypt the message using (2).

$$Msg \leftarrow decrypt\ (M, ID\ (Did)) \tag{2}$$

This technique prohibits unapproved nodes from obtaining data, hence maintaining secrecy. Maintaining stable node IDs and upgrading the key encryption in variable UAV scenarios with changing or momentarily unavailable nodes was a significant problem. To solve this, we developed an affordable identity verification technique that successfully protects node reputation integrity and improves system security under dynamic settings. Figure 1 demonstrates how compression is performed before encryption to reduce payload size and cut down on transmission delays by generating unique pairwise keys for communication between the source and destination UAV nodes, utilizing node IDs to ensure the safety of the exchanges.

2.2. Attack identification model

The attack detection model identifies rogue sites in a network via a watchdog system equipped with UAV broadcast capabilities. Figure 2 illustrates the enhanced I-Watchdog model. In this setup, cluster leaders oversee data transmissions and detect harmful nodes by identifying behavioral anomalies through reports from UAV colleagues.

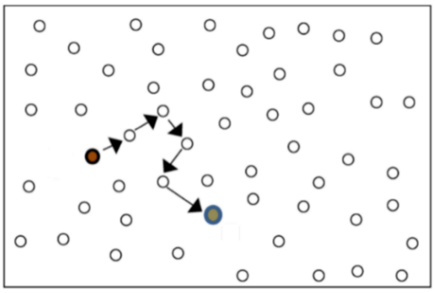


Figure 1. Secure data transmission model between source and destination UAV nodes

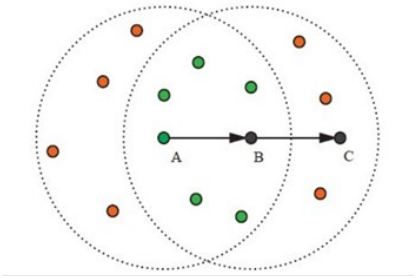


Figure 2. Proposed system model for detecting malicious nodes in UAV

2.3. Secure hybrid encryption and intrusion detection algorithm for UAV communications

2.3.1. Conceptual framework

As per the proposed framework, adaptive monitoring patterns and flexible packet routing mechanisms are used in UAV networks regarding precision, security, and adaptability. This approach reduces false alerts and wrong node classification significantly. Basically, the I-Watchdog system uses cluster heads as the main monitoring points that detect problems and isolate bad nodes. It's the same as having smart guards that watch for suspicious activity and block harmful elements. UAV networks have changing structures where nodes keep joining and leaving clusters, which surely makes it difficult to maintain stable cluster leadership. Moreover, this dynamic nature creates major challenges in ensuring reliable network management. To solve this problem, flexible re-clustering methods are used to change leadership roles automatically, which, to a greater extent, provides the network itself remains stable with less manual work. This flexibility actually supports safe communication and trust-based deals across all UAV nodes. The framework definitely uses a two-level system that combines secure data sending, real-time threat finding, and energy saving to make UAV networks stronger.

2.3.2. Algorithm

This section outlines the techniques used in the proposed safe hybrid encryption and IDS. Algorithm 1 focuses on hybrid encryption and energy-efficient communication, assigning each UAV node a unique identification and generating lightweight key pairs with ECC to enable safe data transfer. The embedded watchdog mechanism monitors all nodes for harmful activities. Algorithm 2 builds on this foundation by integrating key management and improved watchdog detection. It assesses intermediate nodes in clustered UAV networks using a trust-based technique, allowing for dependable network operations. Cluster chiefs are constantly updating trust scores to ensure safe communication and balance energy usage. Together, these algorithms create a lightweight security architecture that improves data integrity, dependability, and energy economy. Elliptic curve cryptography Diffie–Hellman (ECCDH) is used for safe pairwise key creation, whereas bilinear pairings provide group keys for trustworthy nodes in each cluster, allowing for scalable and secure operations. The Algorithm 1 securely transfers messages across UAV nodes while using very little energy. The next algorithm combines ECC-based key generation and trust-based anomaly detection.

Algorithm 1. Hybrid encryption with ECC and energy-efficient communication

```
Input: Source node (S), Destination node (D), Message (msg)
Output: Encrypted message (M), Decrypted message (msg)
Phase 1: Setup
1. Give every UAV node a distinct identifier (ID), like an IP or MAC address.
2. Choose source node S and destination node D.
Phase 2: Message encryption at source
3. Create a pairwise key K utilizing the destination node's identity (ID_D).
4. Encode the message msg with the created key K: M ← Encrypt (msg, K).
5. Send the encoded message M from S to D.
Phase 3: Message decryption at destination
6. Destination node D obtains the encoded message M.
7. Decode M with key K: msg ← Decrypt(M, K).
8. Extract the original message msg.
Phase 4: Threat detection (I-Watchdog)
9. Node A transmits data to node C through node B.
10. Node A observes whether B relays the packet to C.
11. If B relays properly → label as trustworthy.
12. Otherwise → label as malicious and alert cluster head.
13. Cluster head removes flagged nodes from the network.
Phase 5: Energy management
14. Communication gets redirected through low-energy-cost routes identified using remaining energy tables.
15. Repeat steps 3–14 regularly to preserve security and energy balance
```

Algorithm 2. Trust-based watchdog detection with enhanced key management

```
Input: Source node (S), Destination node (D), Message (msg), Cluster head (CH)
Output: Protected communication, malicious node removal
Encryption and transmission
16. Set up S and D with distinct IDs.
17. Create a pairwise key K utilizing ID_D.
18. Encode data: M ← Encrypt(msg, K).
19. Transfer M from S → D.
Decryption
20. Destination node D obtains M.
21. Decode: msg ← Decrypt(M, K).
22. Deliver the decoded message.
Enhanced watchdog detection
23. Node A transmits data to node B meant for node C.
24. Node A monitors B's relaying behavior.
25. If B relays → label B as reliable.
26. Otherwise → label B as questionable.
27. Cluster head assesses overall trust ratings.
28. If trust rating < limit → remove the node.
29. Share the updated cluster table to preserve routing reliability
```

2.4. Simulation and experimental setup

The simulations using a network simulator 2 (NS2, ver 2.35) on a Linux platform showed the efficacy of the proposed safe hybrid encryption as well as intrusion detection solution. The simulation intended to replicate a clustered UAV ad hoc network with varying node mobility. The transmission ranges were varied to evaluate the proposed method in actual operational conditions.

2.4.1. Simulation topology

A preliminary setup of 30 UAV nodes was built, with plans to extend to a scalable arrangement up to 500 nodes. The nodes were randomly arranged throughout a 1000×1500 m area. Each UAV featured a wireless interface that followed the IEEE 802.11 MAC protocol and used the two-ray ground propagation model to replicate realistic signal behavior. Adhoc on-demand distance vector (AODV), along with destination-sequenced distance vector (DSDV) algorithms for routing, were used for the discovery of routes and maintenance during communication.

2.4.2. Traffic configuration

The UAV network was simulated using constant bit rate (CBR) and Poisson bit rate (PBR) traffic models to reflect different communication demands. The packet size was set to 1000 bytes. Every simulated scenario was run for 25 seconds to ensure constant tracking of system performance across varied traffic patterns.

2.4.3. Performance metrics

The suggested framework's usefulness was evaluated using four key performance metrics: end-to-end delay, packet delivery ratio (PDR), throughput, and energy consumption. These parameters assess the reliability, responsiveness, and energy efficiency of UAV communication using secure hybrid encryption. The proposed solution was compared to existing approaches, such as random key, pairwise key, and ECCDH, to demonstrate improvements in various assessment measures.

i) End-to-end delay (ms): end-to-end delay is the average time it takes for a data packet to go from its origin UAV node to its destination over the network. It accounts for all potential delays, including the transfer, propagation, processing, plus queuing at the intermediate nodes. In UAV communications, a shorter end-to-end latency suggests a more agile system, which is critical for real-time operations like surveillance and reconnaissance. The proposed hybrid encryption and IDS reduces latency by using lightweight encryption, improved routing, and fewer retransmissions. In secure UAV ad hoc networks, the optimal end-to-end delay for each hop is less than 1 millisecond, with a total network delay of 10-20% less than traditional ECC-based systems.

ii) PDR (%): the PDR is the proportion of data packets that are successfully received at the destination relative to the total number of packets sent from the source. It assesses the reliability and efficacy of the exchange of information protocol. Maintaining a high PDR in UAV networks ensures data integrity and robust connections, even during node movement or external disturbances. The proposed system improves PDR by combining adaptive forwarding of data, trustworthy intrusion detection, and reliable key management, which decreases packet losses caused by hostile acts or transmission problems. A PDR greater than 95% is considered remarkable for UAV communication systems, indicating dependable and resilient to loss data transmission.

iii) Throughput (bps): throughput is the average speed at which information is successfully transferred via a communication connection, measured in bits per second (bps). It represents the efficacy of bandwidth use when securely sending data. In this study, throughput is impacted by factors such as encrypting overhead, route effectiveness, and traffic across the network. The recommended hybrid encryption solution increases speed by compressing data before encryption and reducing needless communications between UAV clusters. A constant growth in production over time indicates increased efficiency. For secure communication with UAVs, the throughput should be more than 0.9 bps (the normalized value) or demonstrate a 6-10% improvement over standard ECCDH-based techniques.

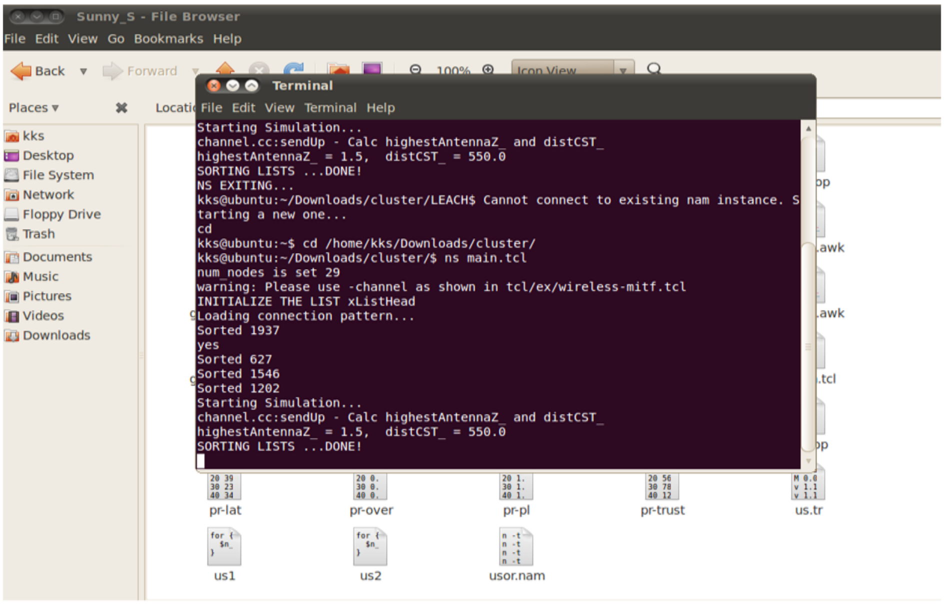
iv) Energy consumption (pJ): energy consumption is the total energy consumed by the UAV node for transmitting information, reception, encryption, and detecting of intrusions, measured in picojoules (pJ). It indicates the UAV network's sustainable operation and energy efficiency. UAVs rely on limited mid-board energy; therefore, lowering power consumption immediately increases flying endurance and missions' length. The proposed strategy achieves significant energy savings by improving key management, utilizing energy-conscious routing, and decreasing transmission via compression. To produce energy-efficient UAV devices, overall energy use must be decreased, to save 35-55% over traditional encryption methods such as ECCDH or pairs of key approaches.

2.4.4. Simulation environment parameters

Table 1 compiles all of the setting parameters for the model used in this research. Sample pictures are also provided in Figures 3 to 6 to depict the entire simulation environment, including node layout, communication relationships, and cluster leadership interactions. These pictures serve to clarify the experimental layout and its operational process.

Table 1. Parameters and values

Parameters	Values
Simulation duration	25 seconds
Type of channel type	Wireless
Propagation system	2 ray ground
Standard	MAC/802.11
Simulation dimension	1,000×1,500 m^2
Maximum packet size	1,000 bytes
Adhoc routing	DSDV, AODV, dynamic source routing (DSR), secure AODV (SAODV)
Traffic	PBR, CBR



```
Starting Simulation...
channel.cc:sendUp - Calc highestAntennaZ_ and distCST_
highestAntennaZ_ = 1.5,  distCST_ = 550.0
SORTING LISTS ...DONE!
NS EXITING...
kks@ubuntu:~/Downloads/cluster/LEACH$ Cannot connect to existing nam instance. S
tarting a new one...
cd
kks@ubuntu:~$ cd /home/kks/Downloads/cluster/
kks@ubuntu:~/Downloads/cluster/$ ns main.tcl
num_nodes is set 29
warning: Please use -channel as shown in tcl/ex/wireless-mitf.tcl
INITIALIZE THE LIST xListHead
Loading connection pattern...
Sorted 1937
yes
Sorted 627
Sorted 1546
Sorted 1202
Starting Simulation...
channel.cc:sendUp - Calc highestAntennaZ_ and distCST_
highestAntennaZ_ = 1.5,  distCST_ = 550.0
SORTING LISTS ...DONE!
```

Figure 3. Initial start of the simulation environment

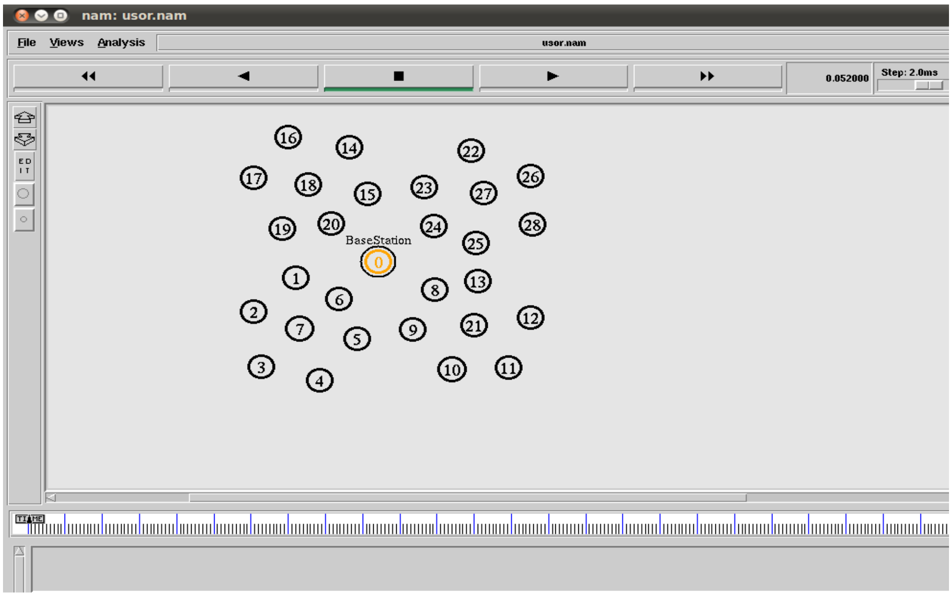
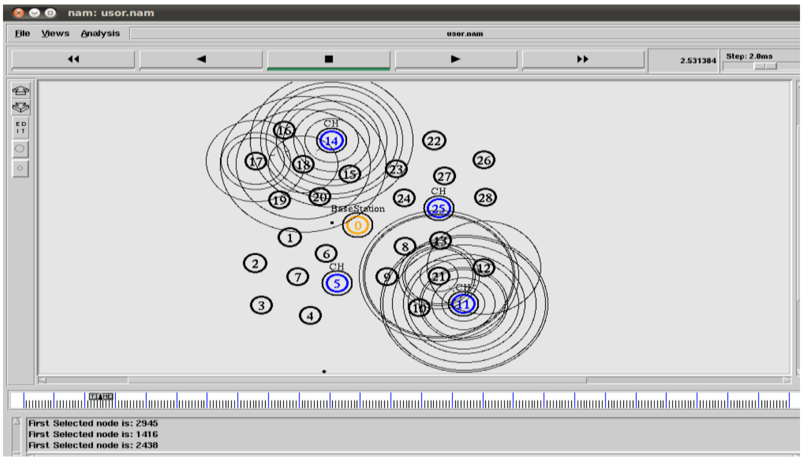
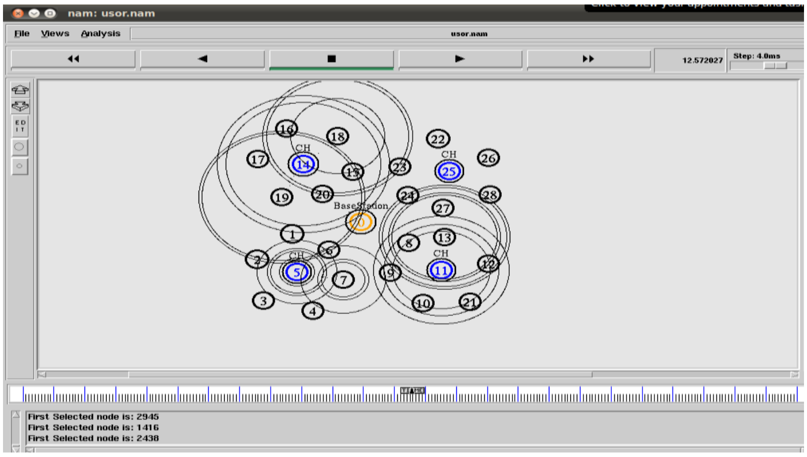


Figure 4. Before the cluster generation scenario



```
First Selected node is: 2945
First Selected node is: 1416
First Selected node is: 2438
```

Figure 5. Cluster generation scenario



```
First Selected node is: 2945
First Selected node is: 1416
First Selected node is: 2438
```

Figure 6. Communication between nodes and cluster head

3. COMPARATIVE LITERATURE REVIEW

Several novel approaches are being explored to improve the security and communication efficacy of UAV and internet of things (IoT) systems. Xu *et al.* [29], developed a blockchain-based intrusion detection solution for drone systems that is tamper-resistant but restricted by consensus delays. Further researchers suggested an efficient key exchange mechanism that uses ECC to improve performance on resource-constrained devices, such as those prevalent in UAV networks [30]. This theme is modified by the designer of a blockchain-based reinforcing learning framework to improve key administration efficiency in IoT networks while ensuring resilience and security [31]. The glimpse of glow glowworm swarm optimization approach to optimize the blockchain-based framework in industrial IoT situations is presented in [32]. While an artificial intelligence-based key administration system for scalability, multi-tier detection of intrusion in UAV networks is depicted in detail by [33]. Researchers worked on enhancing dependability and tolerance for faults in sensor networks that are wireless for industry UAV applications, tackling the difficulties of continuous interaction and energy efficiency [34]. In comparison, our suggested strategy prioritizes security and conserving energy by combining ECC-based encryption with behavior-based I-Watchdog detection, resulting in the highest throughput and savings on energy without the computational cost of blockchain. As a result, this study fills a need by combining ultralight ECC encryption with a trustworthy IDS developed for ad hoc UAV networks.

4. RESULTS AND DISCUSSION

In this part, we assess both current and planned systems based on a complete examination of numerous performance parameters such as throughput, PDR, end-to-end delay, and energy consumption.

The evaluation was carried out with the NS2 simulations tool (version 2.35), which is known for its accuracy. The simulations used an infrastructure-based network architecture based on some parameters, as shown in Table 1, to provide a stable wireless network, while we executed the complete recommended plan in tool command language (TCL) coding inside of the NS 2 framework. The EvalVid Foundation was used to capture connection data messages using its connection patterns file, us1. Effectiveness statistics are produced using the NS2.tr trace file, allowing both vector and scalar assessment of data.

As indicated in Table 1, we carefully chose our simulation settings to adequately evaluate the recommended system's performance. Nevertheless, our data gathering was limited by the UAV's power consumption and information coverage. To solve these issues, we improved connection times and implemented an emergency node system, resulting in increased battery life and reliable data collection. In addition, we preserved network integrity by constantly revising for external variables like as physical impediments and interference with signals. Theoretical issues developed in reconciling security needs with the energy economy, especially given the restricted computational capacity in UAV networks. To address these difficulties, we created a hybrid security system that combines lightweight cryptography with flexible key management. This strategy additionally enhanced the confidentiality of information, but also decreased processing times. These early difficulties and answers serve as a foundation for our conclusions, which are graphically illustrated against key parameters based on data provided by us. The findings show that the proposed system outperforms existing solutions in terms of efficiency and efficacy in UAV network scenarios. Our data gathering was restricted by the UAV's lasting power and the amount of data covered. To address this, we improved connection times and implemented an alternate node system, resulting in longer battery life and reliable data collection. In addition, network integrity was preserved by periodic recalibration for external elements such as physical impediments and signal disruption. Theoretical issues have also developed, particularly in reconciling security needs with energy economy in UAV networks having limited processing capability. We created a combination security architecture that combines lightweight encryption and flexible control of keys to improve data security while decreasing processing times. These early obstacles and solutions provide context for analyzing our findings, taking into account the practical and theoretical limits inherent in UAV network settings. We begin by calculating the transmission time necessary to transfer information from the originating to the destination. Table 2 shows recorded values.

Table 2. End-to-end packet delay

Time (seconds)	Random key [24]	Pairwise key [25]	ECCDH [26]	Proposed method
5	1.35	2.15	1.25	1
10	1.8	2.4	1.45	0.9
15	1.9	2.25	1.15	0.8
20	2	3.05	1.05	0.92

This research provides a statistical analysis of throughout its entirety packet delays for four key control methods at periods of 5, 10, 15, as well as 20 seconds. This review sheds light on each scheme's effectiveness under various network situations, notably in UAV systems, in which high data transmission rates frequently result in obstacles and delays. To address these difficulties, time efficiency and sophisticated encryption techniques were applied, resulting in a 13-17% decline in average latency over previous key-generation procedures, as depicted in Figure 7. The data shows that the randomized key approach encounters growing delays, beginning at 1.35 seconds and then escalating to a duration of two seconds before reaching the 20-second point, indicating a decrease in effectiveness as network demand develops. The pairwise key approach exhibits significantly greater delays, ranging from 2.15 to 3.05 seconds, indicating increased computational expenses and inefficiencies. ECDH algorithm or ECCDH works better, with latencies ranging from 1.25 to 1.5 seconds, although it falls short of the proposed approach in terms of efficiency. The suggested approach stands out for its continuously low latency, which begins at 1 second and gradually decreases to a duration of 0.8 seconds by fifteen seconds, proving its potential for instantaneous communication. Figure 3 is displayed to facilitate comprehension of the collected table information.

Figure 7 depicts these variations visually, with the provided approach's latency bars constantly lower compared to the other approaches, demonstrating its efficacy even as the data amount rises. In comparison, the pairwise key method has the greatest delay in development, suggesting inefficiency. Both ECCDH and random key techniques function satisfactorily; however, they fall short of the proposed method's ideal performance. The simulation evaluated the methods of random key [24], pairwise key [25], and ECCDH [26] as opposed to the proposed method. The NS2.35 simulation was configured with different routing protocols, such as DSDV and AODV, and utilized a realistic terrain measuring 1,000 by 1,500 square meters. Statistical investigation demonstrates that the offered method decreases packet delay by 13-17%.

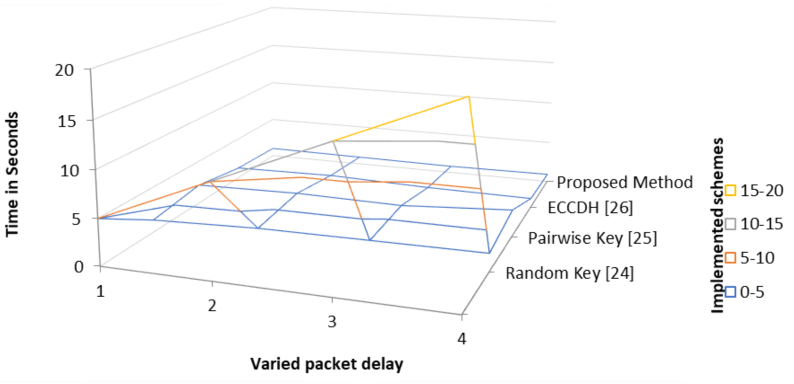


Figure 7. Comparative end-to-end packet delay between well-known key management methods

This increase is critical for networks that need low latency, including UAV infrastructure, applications for the IoT, and real-time interaction platforms, since it immediately improves connection speed and packet delivery dependability, which are significant indications of network efficiency. Ultimately, the findings, confirmed by both Table 2 and Figure 7, show that the suggested strategy greatly surpasses existing strategies in terms of delay reduction, making it the best alternative for outstanding performance communication. The combination of robust encryption and delay reduction algorithms assures efficient, minimal latency data transport, rendering the suggested technique an important step forward in future research on reliable and successful communication networks. After finishing the delay analysis operation, we examine the data packet delivery percentage. The packet delivering ratio is an internet performance metric that assesses the reliability and efficacy of transmitting information over a network. It is determined as the fraction of the entire data packets conveyed to the receiver divided by the total quantity of packets sent by the sender. Table 3 displays the PDR, an important statistic that quantifies the share of the information packets that are successfully delivered to their destination of choice compared to the total quantity of data assigned by the initial source, to feed four different key administration strategies: random key [24], pairwise key [25], ECCDH [26], and the proposed method. Four separate periods—5, 10, 15, and 20 seconds—are employed to gather the metrics.

Table 3. Packet delivery ratio

Series	Time (seconds)	Random key [24]	Pairwise key [25]	ECCDH [26]	Proposed method
1	5	88.5	91	92.2	95.5
2	10	89	90.5	92.8	95.8
3	15	89.7	91.2	93	95.3
4	20	90	91.8	93.3	95.7

The research compares the ratio of PDR of several important management techniques, offering insights into their reliability and effectiveness across wireless systems such as the IoT and UAV networking [32]–[37]. Maintaining a high PDR in such systems is critical for ensuring timely and correct data transmission in the face of obstacles like as interference-induced loss of packets and integrity of signals, particularly in applications involving UAVs. To address these challenges, a unique adaptive packet-oriented transfer technique was developed that effectively decreases interference while maintaining high packet delivery rates. A random key approach had the lowest PDR, indicating limited effectiveness and staying below 90% despite slight improvements over time. The pairing key scheme performed significantly better, but fell short of sophisticated techniques like ECCDH. ECCDH maintained a consistent PDR of more than 92%, but fell short of the suggested method's profitability. The proposed approach regularly produced the greatest PDR, beginning at 95.5% and increasing marginally to 95.8%, resulting in an especially dependable alternative for critical interaction networks. When compared to these alternatives, the randomized key synthesis methodology had a starting PDR of 88.5%, suggesting inadequate transmission efficacy due to large packet losses. The pairing keys generation approach improved marginally, with an initial PDR of around 91%, although it still showed inefficiencies. ECCDH improved significantly from about 92.2% to 93.3%, beating randomized and pairing key approaches but falling short of the suggested method's dependability. The suggested technique regularly excelled, with a PDR ranging from 95.3% to 95.8%, representing a 4-6% increase and demonstrating its appropriateness for applications that are fast processing with little data loss. The radar spectrum map graphically illustrates these results, with the suggested technique showing on the outermost portion to highlight its better data transfer capacity. ECCDH follows close behind by 2-3%, but the random and pairs key approaches stay in the deepest layers, revealing their inefficiency. Figure 8 illustrates the PDR for different encryption schemes over simulation time. The proposed technique demonstrates the highest delivery rate across all intervals, reflecting its resilience and reliability.

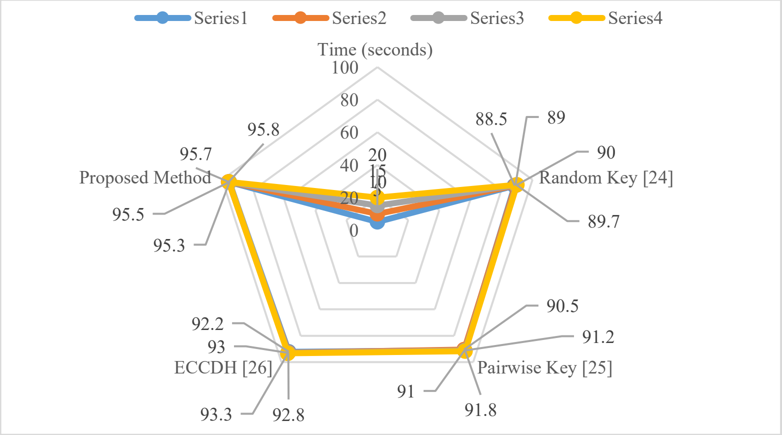


Figure 8. PDR for various key management techniques

Empirical study confirms the proposed method's benefits, demonstrating a constantly elevated PDR, which decreases packet degradation and renders it perfect for extreme-reliability applications like UAV interaction, when data loss might cause major interruptions. The random and pairing key approaches are more susceptible to packet loss, whilst ECCDH provides moderate benefits but falls shy of our proposal. These findings have significant implications for developing dependable systems of communication. The provided method's better PDR, when paired with an adaptable packet-based reissue mechanism, reduces retransmissions, improves communication efficiency, and assures effective information delivery. This makes it ideal for sensitive applications such as UAVs and IoT devices. Overall, the analysis shows that the suggested strategy improves PDR by 4-6% compared to other ways, making it the best option for improving the effectiveness of immediate, high-reliability network interactions. Table 4 displays the median throughput figures for four key administration plans: random key [24], pairing key [25], along with ECCDH [26], as well as the proposed approach. The information is taken at four different time intervals: 5, 10, 15, and 20 seconds. Throughput, expressed as bps, is some data successfully transmitted from the emitter to the recipient in a particular length of time.

Table 4. Throughput (bps) achieved with the proposed system

Time (seconds)	Random key [24]	Pairwise key [25]	ECCDH [26]	Proposed method
5	0.8	0.83	0.75	0.88
10	0.9	0.74	0.78	0.92
15	0.85	0.8	0.79	0.93
20	0.88	0.79	0.81	0.94

Throughput is an important statistic for measuring the transfer of information effectiveness within communication systems, especially in applications that need fast speeds and dependable transfer of information, like wireless networks for UAV interactions and IoT settings. Ensuring adequate throughput whilst balancing energy usage and avoiding network congestion presents significant problems, particularly in areas with significant traffic. To overcome these issues, the suggested technique includes an evolving throughput management mechanism. This method optimizes energy consumption while improving throughput, assuring the reliability of the system even during high-volume data transfer. The random keys production technique begins with an initial throughput of around 0.8 bps, temporarily jumping to 0.9 following 10 seconds before gradually decreasing, indicating inadequate reliability over time.

In comparison, the pairing key approach fluctuates, beginning at 0.83 bps at 5 seconds and dropping to 0.74 in 10 seconds, indicating inefficiencies over long durations. Meanwhile, ECCDH shows a modest and constant improvement, beginning at 0.75 bps and reaching 0.81 at 20 seconds, showing reasonable but limited dependability. Conversely, the suggested technique continuously outperforms conventional strategies, starting with an average throughput of 0.88 bps at 5 seconds and rapidly increasing to 0.94 by 20 seconds, indicating enhanced reliability and information dependability. The random key extraction approach performs decently overall, reaching a high of 0.9 bps at 10 seconds before declining, indicating instability difficulties. Whereas the pairing key approach initially outperforms the random key strategy, starting at 0.83 bps, it drops to 0.74 bps after ten seconds, exposing difficulties in sustaining continuous data transmission. ECCDH improves steadily from 0.75 to 0.81 bps, ensuring stable but moderate throughput reliability. In contrast, the proposed method achieves and maintains the best throughput throughout all periods, culminating at 0.94 bps. This technology provides a 6-10% boost over existing systems, proving its ability to provide efficient data transfer even under demanding situations. Figure 9 shows a graphical study of the effectiveness of each key leadership approach over various periods, featuring the proposed approach constantly demonstrating superior results via higher bars, emphasizing its efficiency.

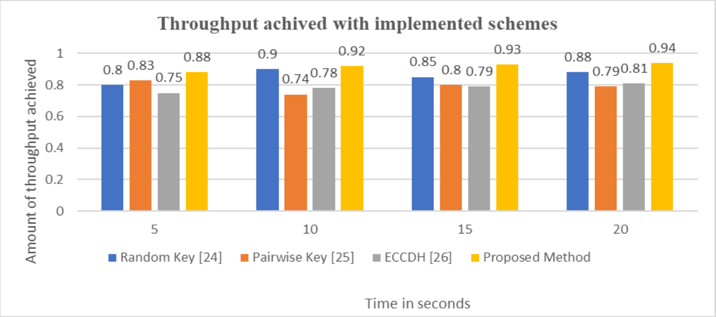


Figure 9. Throughput of the proposed system compared to the well-known system

ECCDH's effectiveness is shown by relatively high bars, indicating reliability, but with a lesser throughput than the proposed method. The randomized key and pairing key approaches have substantially lower throughput, with overall performance dropping after 10 seconds, highlighting their respective inefficiency. The proposed method's improved throughput is due in part to its buffer-throughput regulation (BTC) technique, which enhances transmission rates by lowering packet degradation and network expenses while protecting against data-related concerns such as storage overflow. This method solves issues like as power use and network overload by constantly improving throughput while decreasing the use of energy. The suggested method is 6 to 10% more successful than previous systems due to the Bitcoin algorithm's ability to preserve throughput effectiveness and continuously manage energy, which is a crucial enhancement for applications that need high throughput, such as aerial vehicle networks and immediate time data from IoT transfers. The next bar chart depicts the rise in throughput with greater effectiveness.

The proposed method's performance throughout time intervals suggests greater effectiveness in sharing information, with fewer missed packets and quicker rates of transmission. Its capacity to maintain excellent speed for extended periods exhibits resilience in continuing communication settings, which is critical for applications with continuous or large-volume data needs. This increased performance increases the entire network efficiency by lowering latency and handling higher traffic loads while maintaining privacy and delivery speed. As a result, the proposed approach is ideal for services that require huge amounts of information or rapid communication. In closing, the proposed method greatly improves throughput in contrast to existing techniques, including random key extraction, pair key creation, and ECCDH. The 6 to 10% throughput boost shown in Table 4 and substantiated by visual evaluation demonstrates the method's capacity to provide effective and safe data transfer. This capability is especially useful for high-speed, dependable communication demands, such as UAVs and safe networks of wireless sensors. Lastly, adaptive message forwarding and a reduction of redundant cluster transmissions enhanced the efficient management of energy. This approach contributes to prolonging battery life during long-range UAV missions, as depicted in the form of Table 5. It compares the energy consumption of four different key management systems as the simulation duration increases: randomized key [24], paired key [25], ECCDH [26], and the suggested method. The number of resources used is monitored at intervals of 5, 10, 15, and 20 seconds.

Table 5. Energy consumption (in pJ) with the vehicle node over time

Time (seconds)	Random key [24]	Pairwise key [25]	ECCDH [26]	Proposed method
5	580	640	720	400
10	780	850	780	550
15	1,150	1,350	1,700	740
20	1,420	1,600	2,000	920

Energy efficiency is critical when developing communication systems, particularly for portable or uncontrolled nodes like as UAVs and vehicle networks. Excess utilization of energy can result in fewer resources, reduced service life, and greater operating costs. However, attaining this efficiency is difficult, particularly when it comes to maintaining information secrecy during periods that have significant network activity. A comprehensive strategy for energy management is required to support these elements. Various key management techniques have been developed, such as the random key approach, which begins with 580 pJ and progressively increases over time. The by pair key approach begins at 640 pJ and requires the greatest energy, especially after 10 seconds. ECCDH expends much more power, hitting 2000 pJ following 20 seconds. The offered method, which commences at 400 pJ but only grows to 920 pJ following 20 seconds, uses 35-55% less energy than competing solutions. The suggested technique's success stems from a developing energy conservation mechanism that adjusts power consumption in real-time. This system solves the energy-data privacy trade-off by dynamically adjusting power use based on network requirements. Throughout idle periods, the protocol lowers energy usage, preserving power for critical transfers and preventing unnecessary pulls. Then, the proposed technique reduces internal node communication, lowering the likelihood of energy holes, or areas of a network wherein nodes rapidly drain their power, jeopardizing data and operational security. Figure 10 displays the energy consumption profile of UAV nodes under different key management strategies over a 20-second simulation. It shows that the proposed method uses significantly less energy, demonstrating a 35-55% efficiency improvement compared to random key, pairwise key, and ECCDH protocols. This confirms its suitability for energy-constrained UAV environments. Consequently, the proposed strategy preserves 35-55% annually by restricting connections to critical nodes, thus altering network lifetime. This increase in energy efficiency has a direct impact on network lifetime, which is crucial in scenarios like vehicle networks with UAV connections, where energy resources are restricted. Lower energy consumption enables more hours of work, which reduces the need for frequent refilling or battery replacements.

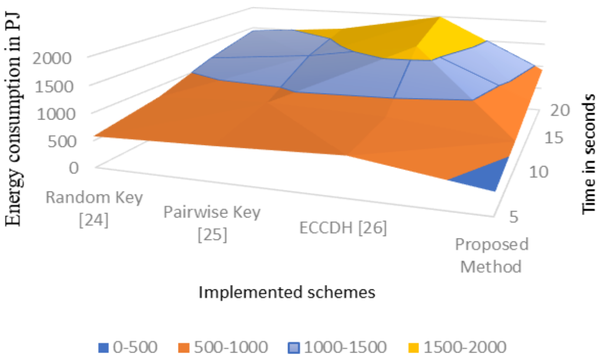


Figure 10. Energy consumption by the vehicle node with simulation time

This investigation also fills important research holes by maximizing key performance parameters required for high-performing UAVs and connected devices. The results show continuous and considerable enhancements, notably a 13-17% decrease from beginning-to-end packet latency, a 4-6% rise in the PDR, as well as a 6-10% boost in throughput. In addition, energy usage was significantly lowered. To solve data-collecting issues, transmission intervals were improved to increase the lifespan of the battery, and an additional node mechanism was installed to ensure continuous data gathering. Environmental conditions, including signal interference as well as impediments, have an impact on network integrity, requiring regular nodes and a new calibration. A mixed security architecture was created that combines compact encryption with reactive control of keys, reducing time to process while increasing data security. These targeted mitigations were critical to delivering considerable gains in network speed and dependability, allowing the suggested method to outperform established techniques.

4.1. Summary of results section

The performance of the proposed hybrid encryption and IDS was compared to existing techniques such as random key, pairwise key, and ECCDH. Key network measures, such as PDR, throughput, energy usage, and end-to-end latency, were examined to quantify improvements. The comparative findings are described in Table 6. Key observations from Table 6 are listed as follows:

i) The proposed approach has the greatest PDR and increases dependability by 4-6%.
ii) Throughput is increased by 6% to 10%, suggesting more efficient data transfer.
iii) Energy usage is greatly decreased, with savings of 35-55% over alternative approaches.
iv) The end-to-end delay is reduced by 13-17%, indicating quicker communication performance.

These findings support the suggested framework's usefulness in improving both the reliability and efficiency of UAV network operations [36]–[39].

Table 6. Performance parameter comparison with various key management methods

Metric	Random key	Pairwise key	ECCDH	Proposed method	% Improvement
Packet delivery ratio	88.5–90%	90–91.8%	92–93.3%	95.3–95.8%	4–6
Throughput (bits/s)	0.8–0.9	0.74–0.83	0.75–0.81	0.88–0.94	6–10
Energy consumption (pJ)	580–1,420	640–1,600	720–2,000	400–920	35–55
End-to-end delay (ms)	–	–	–	Reduction in 13–17%	

5. CONCLUSION

This study presents a powerful hybrid encryption and intrusion detection solution to increase data security and reliability in large UAV networks. The architecture decreases human participation while increasing network self-sufficiency by combining effective bidirectional key generation with adaptive detection of harmful activity. Simulation results show considerable improvements, including a 6-10% increase in throughput, a 4-6% increase in PDR, and a 13-17% reduction in latency, all while reducing energy consumption. These findings support the model's potential to deliver secure, efficient, and robust communication when compared to current approaches such as random key, pairwise key, and ECCDH. To further improve system resilience, future research will focus on adaptive encryption approaches, energy efficiency, and practical validation over a wide range of threat and traffic situations. Upcoming endeavors will evaluate its performance in complex security scenarios, extend its use to large UAV swarms using federated AI technologies, and investigate multi-layered encryption schemes. These developments will increase model flexibility and make it easier to deploy automatic security functions in UAV networks, paving the way for more widespread commercial applications.

FUNDING INFORMATION

This study did not receive any specific support from public, commercial, or non-profit entities.

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
Reshma C. Sonawane	✓	✓	✓	✓	✓	✓		✓	✓		✓		✓	
A. Muthukrishnan					✓	✓	✓			✓		✓		

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 there is no conflict of interest regarding the publication of this paper. The authors have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this article.

INFORMED CONSENT

Informed consent was not applicable for this study as it does not involve human participants or identifiable personal data.

ETHICAL APPROVAL

Ethical approval was not required for this study as it does not involve human subjects or animal experiments.

DATA AVAILABILITY

The authors confirm that the data supporting the findings of this study are available within the article and its supplementary materials.

REFERENCES

[1] T. Mazhar *et al.*, “Analysis of IoT security challenges and its solutions using artificial intelligence,” *Brain Sciences*, vol. 13, no. 4, Apr. 2023, doi: 10.3390/brainsci13040683.

[2] H. Wu *et al.*, “Blockchain for finance: A survey,” *IET Blockchain*, vol. 4, pp. 101–123, 2024, doi: 10.1049/blc2.12067.

[3] F. A. Shah *et al.*, “Applications, challenges, and solutions of unmanned aerial vehicles in smart city using blockchain,” *PeerJ Computer Science*, vol. 10, Feb. 2024, doi: 10.7717/peerj-cs.1776.

[4] F. Abdullayeva and O. Valikhanli, “A survey on UAVs security issues: attack modeling, security aspects, countermeasures, open issues,” *Control and Cybernetics*, vol. 52, no. 4, pp. 405–439, 2023, doi: 10.2478/candc-2023-0044.

[5] S. Sarkar, S. Shafaei, T. S. Jones, and M. W. Totaro, “Secure communication in drone networks: a comprehensive survey of lightweight encryption and key management techniques,” *Drones*, vol. 9, no. 8, 2025, doi: 10.3390/drones9080583.

[6] M. A. Sen, S. Al-Rubaye, and A. Tsourdos, “Securing UAV flying ad hoc wireless networks: authentication development for robust communications,” *Sensors*, vol. 25, no. 4, 2025, doi: 10.3390/s25041194.

[7] R. Aissaoui, J.-C. Deneuville, C. Guerber, and A. Pirovano, “A survey on cryptographic methods to secure communications for UAV traffic management,” *Vehicular Communications*, vol. 44, Dec. 2023, doi: 10.1016/j.vehcom.2023.100661.

[8] J. Kaur, A. C. Canto, M. M. Kermani, and R. Azarderakhsh, “A comprehensive survey on implementations, attacks, and countermeasures of NIST lightweight cryptography standard,” *arXiv:2304.06222*, 2023.

[9] B. Cordill, D. Fang, and S. Xu, “A comprehensive survey of security and privacy in UAV systems,” *IEEE Access*, vol. 13, pp. 117843–117866, 2025, doi: 10.1109/ACCESS.2025.3583985.

[10] D. He, Y. Song, M. Dai, S. Chan, L. Chen, and M. Guizani, “Trust-based authentication aided blockchain for distributed learning in AAV swarms: Challenges and solutions,” *IEEE Network*, vol. 39, no. 4, pp. 262–270, 2025, doi: 10.1109/MNET.2024.3510113.

[11] W. Ahmad, M. A. Almaiah, A. Ali, and M. A. Al-Shareeda, “Deep learning based network intrusion detection for unmanned aerial vehicle (UAV),” in *Proceedings of the 7th World Conference on Computer Communication Technologies (WCCCT)*, 2024, pp. 31–36, doi: 10.1109/WCCCT60665.2024.10541665.

[12] H. A. Hashim, “Advances in UAV avionics systems architecture, classification and integration: a comprehensive review and future perspectives,” *Results in Engineering*, vol. 25, Mar. 2025, doi: 10.1016/j.rineng.2024.103786.

[13] M. S. Islam, A. S. Mahmoud, and T. R. Sheltami, “AI-enhanced intrusion detection for UAV systems: a taxonomy and comparative review,” *Drones*, vol. 9, no. 10, 2025, doi: 10.3390/drones9100682.

[14] Y. Renu and V. Sarveshwaran, “Secure communication routing and attack detection in UAV networks using Gannet Walruses optimization algorithm and sheppard convolutional spinal network,” *Peer-to-Peer Networking and Applications*, vol. 17, pp. 3269–3285, 2024, doi: 10.1007/s12083-024-01753-4.

[15] R. -Sugranes, A. Razi, F. Afghah, and J. Chakareski, “A review of AI-enabled routing protocols for UAV networks: trends, challenges, and future outlook,” *Ad Hoc Networks*, vol. 130, May 2022, doi: 10.1016/j.adhoc.2022.102790.

[16] K. Seerangan *et al.*, “A novel energy-efficiency framework for UAV-assisted networks using adaptive deep reinforcement learning,” *Scientific Reports*, vol. 14, 2024, doi: 10.1038/s41598-024-71621-x.

[17] P. Saxena and G. M. Phade, “Deep reinforcement learning-based routing framework for bidirectional communication in UAV-UGV networks,” *Cognitive Robotics*, vol. 5, pp. 249–259, 2025, doi: 10.1016/j.cogr.2025.06.003.

[18] K. Vaithianathan, “Integrating machine learning and blockchain with UAV routing and navigation—challenges and potential solutions,” in *Fostering Machine Learning and IoT for Blockchain Technology*, Eds. Singapore: Springer, 2025, doi: 10.1007/978-981-96-4074-4_8.

[19] H. Peng, J. Cao, D. Yang, C. Li, T. H. Luan, and Z. Su, “Balancing energy efficiency and communication quality in UAV cargo delivery systems,” *IEEE Internet of Things Journal*, vol. 12, no. 16, pp. 34019–34034, 2025, doi: 10.1109/JIOT.2025.3577677.

[20] K.-Y. Tsao, T. Girdler, and V. G. Vassilakis, “A survey of cyber security threats and solutions for UAV communications and flying ad-hoc networks,” *Ad Hoc Networks*, vol. 133, Aug. 2022, doi: 10.1016/j.adhoc.2022.102894.

[21] W. J. Cho, S. Kim, Y. Kim, and Y. H. Moon, “Advanced co-simulation platform for UAV simulations under virtual wireless network environments,” *IEEE Access*, vol. 10, pp. 95498–95508, 2022, doi: 10.1109/ACCESS.2022.3201526.

[22] W. Jiang, H. Han, M. He, and W. Gu, “Network simulation tools for unmanned aerial vehicle communications: a survey,” *International Journal of Communication Systems*, vol. 37, no. 15, 2024, doi: 10.1002/dac.5878.

[23] M. S., M. Prabha, A. Farithkhan, G. Sivagurunathan, and M. Mahesh, “Decentralized control design for UAV swarms communication,” *Discover Applied Sciences*, vol. 7, 2025, doi: 10.1007/s42452-024-06408-w.

[24] Z. He, Y. Zheng, S. Chen, Z. Du, S. Liu, and K. Zhang, “Security-enhanced lightweight authentication key-agreement protocol for unmanned aerial vehicle communication,” *Applied Sciences*, vol. 15, no. 9, 2025, doi: 10.3390/app15094680.

[25] H. Tan, W. Zheng, and P. Vijayakumar, “Secure and efficient authenticated key management scheme for UAV-assisted infrastructure-less IoVs,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 6, pp. 6389–6400, Jun. 2023, doi: 10.1109/TITS.2023.3252082.

[26] H. J. Hadi, Y. Cao, S. Li, Y. Hu, J. Wang, and S. Wang, “Real-time collaborative intrusion detection system in UAV networks using deep learning,” *IEEE Internet of Things Journal*, vol. 11, no. 20, pp. 33371–33391, 2024, doi: 10.1109/JIOT.2024.3426511.

[27] Z. Li *et al.*, “A secure and efficient UAV network defense strategy: Convergence of blockchain and deep learning,” *Computer Standards & Interfaces*, vol. 90, 2024, doi: 10.1016/j.csi.2024.103844.

[28] Y. Zhang, “Research on optimization of UAV communication network security protection strategy based on advanced encryption technology,” *Journal of Cyber Security and Mobility*, vol. 13, no. 6, pp. 1379–1400, 2024, doi: 10.13052/jcsm2245-1439.1367.

[29] Y. Xu, X. Zhu, Y. Bai, Z. Chen and M. Sun, “A dynamic lightweight blockchain sharding protocol for autonomous collaborative combat of UAV swarms in denied environments,” *Scientific Reports*, vol. 15, 2025, doi: 10.1038/s41598-025-20359-1.

[30] Z. Amiri, A. Heidari, N. Jafari, and M. Hosseinzadeh, “Deep study on autonomous learning techniques for complex pattern recognition in interconnected information systems,” *Computer Science Review*, vol. 54, 2024, doi: 10.1016/j.cosrev.2024.100666.

[31] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, “Secure computation offloading in blockchain based IoT networks with deep reinforcement learning,” *IEEE Transactions on Network Science and Engineering*, vol. 8, no. 4, pp. 3192–3208, 2021, doi: 10.1109/TNSE.2021.3106956.

[32] K. Zanbouri, M. Darbandi, M. Nassr, A. Heidari, N. J. Navimipour, and S. Yalcin, “A GSO-based multi-objective technique for performance optimization of blockchain-based industrial internet of things,” *International Journal of Communication Systems*, vol. 37, no. 15, pp. 1–22, Jul. 2024, doi: 10.1002/dac.5886.

[33] M. A. O. Rabah, H. Drid, M. Rahouti, and N. Lazaar, “Empowering UAV communications with AI-assisted software-defined networks: A review on performance, security, and efficiency,” *Journal of Network and Systems Management*, vol. 32, 2024, doi: 10.1007/s10922-024-09866-0.

[34] R. Wang, Y. Tong, L. Tian, and D. Wang, “Reliability analysis of different fault-tolerant mechanisms in wireless sensor networks,” in *Proceedings of the 3rd International Conference on Applied Machine Learning (ICAML)*, 2021, pp. 250–256, doi: 10.1109/ICAML54311.2021.00060.

[35] Z. Amiri, A. Heidari, M. Zavvar, N. J. Navimipour, and M. Esmaeilpour, “The applications of nature-inspired algorithms in Internet of Things-based healthcare service: a systematic literature review,” *Transactions on Emerging Telecommunications Technologies*, vol. 35, no. 6, May 2024, doi: 10.1002/ett.4969.

[36] M. Asadi, M. A. J. Jamali, A. Heidari, and N. J. Navimipour, “Botnets unveiled: a comprehensive survey on evolving threats and defense strategies,” *Transactions on Emerging Telecommunications Technologies*, vol. 35, no.11, 2024, doi: 10.1002/ett.5056.

[37] M. K.-Sarakhsi, S. S. H. Shahabi, S. M. T. F. Ghomi, and E. Marchiori, “Deep learning for Alzheimer’s disease diagnosis: a survey,” *Artificial Intelligence in Medicine*, vol. 130, 2022, doi: 10.1016/j.artmed.2022.102332.

[38] A. Vakili *et al*., “A new service composition method in the cloud-based internet of things environment using a grey wolf optimization algorithm and MapReduce framework,” *Concurrency and Computation: Practice and Experience*, vol. 36, no. 16, May 2024, doi: 10.1002/cpe.8091.

[39] F. Kandah, T. Mendis, L. Medury, and H. Sherawat, “Navigating IoT security: architectures, emerging threats, and adaptive countermeasures,” *IEEE Access*, vol. 13, pp. 98888–98908, 2025, doi: 10.1109/ACCESS.2025.3576355.

BIOGRAPHIES OF AUTHORS

Reshma C. Sonawane is a research scholar at Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai, India, specializing in Computer Science and Engineering. She has a strong foundation in UAV-based systems, wireless sensor networks, artificial intelligence, the internet of things (IoT), data structures and algorithms, with research interests in natural language processing, machine learning, and computer vision. Her doctoral research focuses on UAV-based systems, contributing to advancements in intelligent and autonomous communication frameworks. She has participated in more than fifteen research projects, including both funded and unfunded initiatives. She can be contacted at email: reshmagold@gmail.com.

A. Muthukrishnan received his B.E. degree in Electrical and Electronics Engineering from RVS College of Engineering and Technology, India, in 2005, and his M.E. degree in VLSI design from Anna University, Coimbatore, in 2009. He earned his Ph.D. in Information and Communication Engineering from Anna University, Chennai, in 2016. He is currently working as a Professor in the Department of Electronics and Communication Engineering at Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai, India, with over fifteen years of teaching and research experience in information and communication engineering. His research interests include wireless sensor networks, the internet of things (IoT), VLSI design, and wireless communication systems. He received the best achiever award from Anna University Regional Campus, Madurai, in 2016, for his outstanding contributions to wireless sensor networks. He can be contacted at email: drmuthukrishnana@veltech.edu.in.