Journal of Information Systems Engineering and Management
2025, 10(1s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Secure Data Aggregation and data Transmission using HMAC Protocol in Cluster base UAV Communication Network

Reshma C Sonawane[1], A. Muthukrishnan[2]

Phd Scholar : at Veltech Rangarajan Dr. Sanguthala R&D Institute of Science and Technology Chennai[1]

reshmagold@gmail.com[1]

Associate Professor: at Veltech Rangarajan Dr. Sanguthala R&D Institute of Science and Technology Chennai[2]

drmuthukrishnana@veltech.edu.in[2]

ARTICLE INFO

Received: 05 Oct 2024

Revised: 30 Nov 2024

Accepted: 15 Dec 2024

ABSTRACT

In remote or hard-to-reach areas, deploying unmanned aerial vehicle (UAV's) significantly increases the likelihood of various attacks, making security a critical concern. Given the limited computing power, memory, bandwidth, and energy resources of sensors, traditional security methods designed for resource-heavy systems like WLANs are unsuitable for UAV's. Therefore, it is crucial to develop specialized security protocols tailored to UAV's resource constraints. The use of public key cryptography in UAVs faces several challenges, such as high computational costs, lengthy key generation, susceptibility to brute-force attacks, and complexities in key distribution and management. In contrast, symmetric key cryptography, which requires minimal computation and storage, is a more suitable choice for securing data transmission in UAVs. This research focuses on existing and emerging security mechanisms for unmanned aerial vehicle (UAVs), specifically those enhancing the 802.11 standard with additional security layers. The research follows a four-phase methodology. In the first phase, a genetic algorithm is proposed for optimizing the selection and number of cluster heads (CHs) using a clustering approach. This method balances intra-cluster communication, CH distance from the base station (BS), and the remaining energy of nodes to maximize network efficiency. In phase two, a secure data aggregation technique employing the Hash Mandatory Access Control Protocol (HMAC) is introduced to reduce network data overhead and protect against multiple threats. Phase three presents a pairwise key management strategy for UAVs, utilizing a one-way hash function to minimize the impact of compromised nodes while maintaining secure links between neighbouring nodes. The fourth phase introduces a Broadcast Tree Construction method to reduce communication overhead by identifying the shortest paths, integrating data aggregation, and enhancing network connectivity. This approach emphasizes reducing power consumption to extend network lifespan while ensuring the timely detection and removal of rogue nodes before they can transmit harmful data..

Keywords: Cluster Network, Unmanned Aerial Vehicles, wireless network, Data aggregation, Broadcast Tree Construction, QoS.

INTRODUCTION

Unmanned Aerial Vehicles (UAVs) are rapidly transforming various industries, including military operations, disaster management, environmental monitoring, and logistics. Their ability to operate autonomously, communicate over vast distances, and gather data in real-time makes them indispensable for modern applications. However, with their increased adoption comes the critical challenge of ensuring secure communication and data aggregation, particularly in cluster-based UAV communication networks. These networks, often characterized by resource-constrained devices and dynamic topologies, are highly susceptible to various security threats, such as data breaches, eavesdropping, and malicious node attacks. Thus, addressing security concerns in these networks is crucial to ensure the integrity, confidentiality, and authenticity of the data being transmitted. In this context, secure data aggregation and transmission mechanisms using lightweight cryptographic protocols, such as the Hash-based Message Authentication Code (HMAC), have emerged as a promising solution.

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Cluster-based UAV communication networks are organized into clusters where each cluster has a designated leader, referred to as the Cluster Head (CH). The CH plays a vital role in aggregating data collected from individual UAV nodes before transmitting it to the Base Station (BS) or other CHs. This aggregation significantly reduces communication overhead and energy consumption, making it an energy-efficient solution for large-scale UAV networks. However, this hierarchical structure introduces unique security challenges. If the CH is compromised, the entire cluster's communication can be exposed to potential attacks, leading to data manipulation or leakage. Therefore, ensuring secure data aggregation at the CH and secure transmission from the CH to the BS is essential for maintaining the integrity and confidentiality of the data.

Traditional encryption techniques, although effective in protecting data integrity, may not be suitable for resource-constrained UAVs, which have limited computational power and battery life. Implementing complex cryptographic algorithms in such environments can lead to delays, high energy consumption, and reduced network performance. To address these challenges, lightweight cryptographic methods like HMAC have gained attention. HMAC is a widely-used, efficient cryptographic protocol that combines a cryptographic hash function with a secret key, providing both data integrity and authenticity. It requires minimal computational resources, making it ideal for UAV networks where energy efficiency and low latency are crucial. In a cluster-based UAV communication network, the secure aggregation of data at the CH is vital for reducing redundancy and minimizing the amount of data transmitted to the BS. By using HMAC, data can be securely authenticated at each stage of communication. Each UAV node generates data, which is then aggregated at the CH, and an HMAC code is generated to verify the integrity and authenticity of the aggregated data. This code ensures that any modification or tampering with the data during transmission is detected at the earliest stage. Moreover, because HMAC is resistant to common cryptographic attacks, such as collision attacks and brute force attacks, it offers a robust solution for protecting sensitive data in UAV networks. In addition to secure data aggregation, secure data transmission is another critical aspect of UAV communication networks. The dynamic nature of UAV networks, where nodes frequently join and leave, makes the network vulnerable to various attacks, including eavesdropping and man-in-the-middle attacks. The use of HMAC for secure transmission ensures that any data exchanged between UAV nodes, CHs, and the BS is authenticated and encrypted. This prevents unauthorized nodes from intercepting or altering the data. Furthermore, by leveraging HMAC, the communication process remains lightweight, preserving the energy resources of UAVs while ensuring secure data transmission over long distances.

In this paper, we focus on the implementation of the HMAC protocol for secure data aggregation and transmission in cluster-based UAV communication networks. We analyze the performance of the proposed framework in terms of security, energy efficiency, and communication overhead, and compare it with traditional encryption methods. Our objective is to demonstrate that the HMAC-based approach not only enhances security but also improves the overall performance of UAV networks by reducing computational complexity and energy consumption. By addressing the security challenges inherent in UAV networks, this research contributes to the development of more resilient and efficient communication protocols for future UAV applications.

RELATED WORK

Chen, H. et. al. [1] proposes a novel lightweight cryptographic protocol for securing communication within unmanned aerial vehicle (UAV) networks. The approach centers around pairwise key generation to ensure secure data exchange between UAVs in large-scale deployments. UAVs are inherently resource-constrained, making traditional cryptographic protocols inefficient. The authors address this by designing a low-complexity cryptosystem that combines key generation and distribution methods, using less processing power while maintaining robust security levels. The protocol is resistant to common attacks such as eavesdropping, man-in-the-middle, and spoofing, with a focus on dynamic environments. The paper includes simulations demonstrating the cryptographic protocol's efficiency in large UAV networks, highlighting its ability to scale without significant overhead. Additionally, the paper addresses key revocation and rekeying processes, ensuring that compromised nodes cannot disrupt the entire network. This work contributes to UAV network security by reducing computational costs while offering strong cryptographic defenses, making it ideal for real-time applications in surveillance, delivery, and disaster management.

Singh, P et. al. [2]focuses on enhancing UAV network security by incorporating cryptographic mechanisms for detecting malicious nodes. UAV networks, characterized by their decentralized and dynamic nature, face challenges with security vulnerabilities due to their open communication environment. The authors present a hybrid cryptographic scheme that integrates symmetric and asymmetric key techniques, enhancing both detection

accuracy and network resilience. The malicious node detection algorithm uses cryptographic signatures to verify the authenticity of data transmission between UAVs. Once a node is identified as malicious, the network isolates it to prevent data compromise. The authors evaluate the scheme's effectiveness through simulation in terms of detection speed, false positive rates, and computational overhead. Their findings demonstrate that the proposed cryptographic scheme is more efficient in detecting and mitigating malicious nodes than traditional approaches. Furthermore, the system provides minimal delay in key generation and rekeying processes, making it suitable for real-time UAV applications in military, emergency response, and commercial sectors.

hang et. al. [3] discusses a secure communication framework for UAV networks utilizing pairwise key exchange mechanisms. UAV networks are often susceptible to cyberattacks due to their reliance on wireless communication. To counter these vulnerabilities, the authors propose a cryptographic solution that enables secure communication between UAVs using lightweight pairwise key exchanges. The solution includes an adaptive key management system that dynamically updates the keys to counter potential attacks such as node compromise and man-in-the-middle attacks. Simulations validate the system's performance, showing high levels of security with minimal overhead, which is critical for UAVs with limited power and processing capabilities. The authors also introduce a hierarchical network architecture that separates UAVs into clusters, with each cluster managing its internal cryptographic processes. This architecture further optimizes the scalability of the solution, allowing it to handle larger networks without a significant increase in computational load. The paper concludes that the proposed method enhances both the security and efficiency of UAV communications in various scenarios, including environmental monitoring and border surveillance.

Zhaoet. al. [4] introduces a lightweight cryptosystem for securing UAV communication networks, with an emphasis on detecting and mitigating the effects of malicious nodes. UAV networks are prone to various security threats due to their decentralized nature and wireless communication methods. To address this, the authors propose a dual-layer cryptographic approach, combining lightweight encryption with real-time malicious node detection. The first layer encrypts data transmissions using a resource-efficient cryptosystem, ensuring confidentiality without overburdening UAV resources. The second layer involves a detection algorithm that monitors data patterns and behaviors across the network, identifying any suspicious activity indicative of a malicious node. This method enables quick isolation of compromised nodes, ensuring the integrity and availability of the network. Simulation results show that the cryptosystem effectively balances security with the limited computational capabilities of UAVs, achieving low latency and reduced energy consumption. The proposed system demonstrates resilience against attacks such as data tampering and node impersonation, providing a viable solution for UAV networks operating in sensitive environments like defense, rescue operations, and autonomous delivery systems.

Gupta et. al. [5] address the critical need for efficient key management in UAV networks by proposing a lightweight cryptographic approach that focuses on pairwise key management. UAV networks typically consist of multiple interconnected nodes, and ensuring secure communication across all nodes is a significant challenge, particularly given the limited computational power available. The authors design a pairwise key management system that enables each UAV to securely establish a unique encryption key with its neighbors. The key generation process is computationally light, making it suitable for UAVs with constrained resources. The system also supports dynamic key updates to maintain security over time, particularly in environments where UAVs may join or leave the network frequently. This prevents potential attackers from exploiting long-term key usage. Simulation results demonstrate that the proposed key management system significantly reduces communication delays and energy consumption while maintaining high levels of security. The authors conclude that this approach provides a practical solution for enhancing the security of UAV networks, particularly in applications such as military reconnaissance and disaster management, where secure real-time communication is critical.

Zhou et. al. [6] focuses on detecting malicious UAV nodes using lightweight cryptography combined with robust authentication protocols. Zhou and Xie argue that the decentralized nature of UAV networks makes them vulnerable to internal attacks, where compromised nodes may masquerade as legitimate ones. To address this, they propose a novel cryptographic framework that relies on efficient key exchange mechanisms and continuous authentication processes. The lightweight cryptographic design ensures that even resource-constrained UAVs can participate without excessive computational overhead. The authors' approach involves regularly refreshing cryptographic keys between UAVs, minimizing the risk of key compromise. Additionally, an authentication protocol based on behavior analysis ensures that only trusted UAVs can transmit sensitive data. Simulation results highlight the protocol's effectiveness in detecting and isolating malicious nodes, even in large UAV networks. By maintaining high detection accuracy and low false-positive rates, the system ensures the continuity of network operations

without excessive delays. The paper concludes that this framework is particularly useful in military and commercial applications where security breaches can lead to significant consequences, providing a reliable method for securing UAV communications.

Leeet. al. [7] present a dynamic pairwise key generation scheme designed to enhance the security of UAV networks while maintaining low computational overhead. UAVs are resource-constrained, requiring cryptographic solutions that strike a balance between security and efficiency. The authors propose a method that dynamically generates cryptographic keys between UAVs based on their changing positions and communication needs within the network. This dynamic approach ensures that keys are frequently updated, making it difficult for adversaries to predict or compromise them. In addition to key generation, the paper introduces a lightweight encryption algorithm tailored to UAVs' computational limits. Through extensive simulations, the authors show that their scheme achieves low latency and energy consumption, while providing robust protection against attacks such as key compromise, eavesdropping, and malicious node injection. The paper emphasizes the practicality of the scheme for real-world UAV applications such as aerial surveillance, environmental monitoring, and disaster management, where security breaches could compromise critical missions.

Patelet. al. [8] propose a novel pairwise key exchange scheme tailored for large-scale UAV simulations. UAVs operate in complex environments where secure communication is essential to prevent unauthorized access and ensure data integrity. The authors focus on the scalability of key management in extensive UAV networks, where traditional cryptographic approaches may fall short due to computational and communication overhead. Their proposed scheme uses a hierarchical structure that allows UAVs to exchange keys in a peer-to-peer manner, reducing the need for centralized key distribution and minimizing bottlenecks. The system also supports key refresh mechanisms to ensure that communication remains secure over time, particularly in dynamic environments. Simulation results show that the proposed scheme can handle large networks without significant delays, making it suitable for real-time applications. The paper concludes that this key exchange scheme provides an efficient, scalable solution for secure UAV communication, with potential applications in military operations, smart cities, and autonomous vehicle coordination.

Wang et. al. [9] explore enhanced cryptographic techniques for detecting malicious nodes in UAV networks. UAVs are particularly susceptible to malicious attacks due to their reliance on open wireless communication channels. To address these vulnerabilities, the authors propose a cryptographic framework that combines lightweight encryption with a machine learning-based malicious node detection algorithm. The cryptographic techniques ensure data confidentiality and integrity, while the machine learning algorithm monitors UAV behavior to identify anomalous patterns associated with compromised nodes. By utilizing resource-efficient encryption, the framework ensures that UAVs can participate in secure communication without being overwhelmed by computational tasks. The authors' simulations demonstrate that the framework can accurately detect malicious nodes with minimal false positives and reduced energy consumption compared to existing approaches. Additionally, the system is shown to be resilient against various types of attacks, including Sybil attacks and replay attacks. The paper concludes that the combination of cryptography and machine learning offers a powerful solution for securing UAV networks, making it suitable for applications in defense, public safety, and autonomous vehicle coordination.

Liet. al. [10] presents a secure communication framework for UAV networks, focusing on pairwise key generation and the mitigation of malicious nodes. UAV networks are often deployed in mission-critical scenarios, where the presence of malicious nodes can compromise the entire system. Li and Zhang propose a lightweight cryptographic scheme where each UAV generates a unique pairwise key with its neighboring UAVs, ensuring secure communication without relying on centralized key management. The framework includes a real-time detection algorithm to identify and mitigate malicious nodes, ensuring that compromised UAVs are isolated before they can disrupt the network. The authors evaluate the system's performance in terms of communication delay, energy consumption, and security strength. Their simulations show that the proposed framework achieves strong security while minimizing the computational burden on UAVs. Additionally, the framework is resilient to a range of attacks, including man-in-the-middle and jamming attacks. The paper concludes that this approach provides an effective solution for securing UAV networks, particularly in applications like border surveillance, environmental monitoring, and disaster response.

Huanget. al. [11] focus on lightweight encryption techniques specifically designed for UAV-based communication systems. UAVs are widely used in various sectors such as military, logistics, and disaster recovery, but their communication networks are vulnerable to various cyberattacks. The authors propose a lightweight encryption

algorithm that uses minimal computational resources while maintaining strong data confidentiality. The algorithm employs symmetric key encryption with dynamic key generation, allowing UAVs to securely exchange data even in resource-constrained environments. The paper also introduces a key management scheme that supports secure and efficient key distribution among UAVs, ensuring that even in large-scale deployments, the communication remains secure. The authors validate their approach through simulations, demonstrating that the proposed encryption technique offers low latency, reduced energy consumption, and robust protection against attacks such as eavesdropping, data tampering, and replay attacks. The paper concludes that this lightweight encryption method is highly suitable for real-time applications where secure communication is critical, such as in surveillance, package delivery, and search-and-rescue missions.

Choi and Park [12] tackle the issue of real-time malicious node detection in UAV networks by employing cryptographic methods. The decentralized nature of UAV networks makes them vulnerable to internal threats, particularly from nodes that have been compromised. The authors propose a real-time detection system that combines lightweight cryptographic techniques with a behavior-based anomaly detection algorithm. The cryptographic component ensures that data exchanged between UAVs is secure, while the anomaly detection system continuously monitors network traffic for signs of malicious activity. Once a node is identified as suspicious, the system triggers an isolation mechanism to prevent it from further communication with other UAVs. The authors evaluate their system through simulations, demonstrating that it achieves a high detection rate with minimal false positives, even in large-scale UAV networks. Furthermore, the proposed solution is resource-efficient, making it suitable for UAVs with limited processing and power capabilities. The paper concludes that the combination of cryptography and real-time detection provides a robust solution for maintaining the security and integrity of UAV networks, especially in mission-critical applications like disaster management, military operations, and environmental monitoring.

Zhao and Liu [13] present a pairwise key generation mechanism aimed at securing UAV-to-UAV communication in large-scale networks. With the increasing use of UAVs in both civilian and military applications, securing their communication channels has become critical. The authors propose a lightweight cryptographic protocol that enables UAVs to establish secure pairwise keys with neighboring UAVs, ensuring the confidentiality and integrity of data transmissions. The system also includes a key renewal mechanism to prevent long-term key usage, which could be exploited by attackers. The authors' simulations show that the proposed scheme can handle the dynamic nature of UAV networks, where nodes frequently join and leave the network. The protocol ensures low latency and minimal energy consumption, making it suitable for large-scale deployments where computational resources are limited. Additionally, the paper highlights the system's resilience against attacks such as man-in-the-middle and replay attacks, providing a secure communication framework for UAV applications in areas like traffic monitoring, environmental surveillance, and military reconnaissance.

Kimet. al. [14]introduces a lightweight cryptographic system designed to secure UAV networks while integrating mechanisms for defending against malicious nodes. UAV networks, which rely on wireless communication, are inherently vulnerable to various attacks. Kim and Song propose a cryptographic solution that emphasizes both resource efficiency and security by using a symmetric key encryption scheme that allows UAVs to establish secure communication channels with minimal computational overhead. In addition, the authors present a defense mechanism for detecting and mitigating malicious nodes, which may attempt to disrupt the network or eavesdrop on sensitive data. The defense system monitors UAV behavior and isolates nodes that exhibit suspicious activities. Simulations demonstrate the system's effectiveness in detecting malicious nodes with a low false-positive rate while maintaining secure communication across the network. The paper concludes that this lightweight cryptographic system, combined with the malicious node defense mechanisms, provides a comprehensive solution for securing UAV networks in various applications such as environmental monitoring, border surveillance, and emergency response.

Zhang and Wu [15] present a dynamic key generation system designed to secure communication within UAV networks. In large-scale UAV networks, the risk of cyberattacks such as eavesdropping and man-in-the-middle attacks is significantly higher due to the distributed nature of communication. To address these challenges, the authors propose a lightweight cryptographic protocol that enables UAVs to generate pairwise keys dynamically. This dynamic key generation adapts to the changing topology of UAV networks, allowing for secure communication even as UAVs move in and out of range. The authors also incorporate a key refreshing mechanism to enhance the system's resilience against long-term attacks, ensuring that even if one key is compromised, subsequent communications remain secure. Through extensive simulations, the paper demonstrates that the proposed system

maintains high security while minimizing computational overhead and energy consumption. The results show low latency in key exchange processes, making the system particularly well-suited for UAV networks in time-sensitive applications like disaster relief, military reconnaissance, and environmental monitoring.

Liu and Li [16] focus on securing UAV-to-UAV communication in large networks through lightweight cryptographic techniques. UAV networks often face security challenges due to the need for real-time data exchange over potentially insecure wireless channels. The authors propose a symmetric cryptographic system that uses a pairwise key generation mechanism to secure communications between UAVs. The system is designed to operate with minimal computational and energy overhead, making it ideal for resource-constrained UAVs. In addition to securing communication, the authors address malicious node detection by monitoring communication patterns and data integrity. When a malicious node is detected, the system triggers an isolation protocol to prevent further network compromise. The authors validate their approach through simulations, showing that the system can maintain secure communication while keeping energy consumption and latency low. Their findings indicate that this lightweight cryptographic system is particularly suitable for UAV networks used in high-risk environments such as military operations, critical infrastructure surveillance, and autonomous vehicle coordination.

Chen and Sun [17] propose a cryptographic system for secure pairwise key distribution and malicious node detection in UAV networks. The primary focus is on securing UAV communication channels in large-scale networks where traditional centralized key management systems are infeasible due to the dynamic and decentralized nature of UAV operations. The authors introduce a lightweight cryptographic protocol that generates unique keys for each pair of UAVs, ensuring that communication remains secure and protected from attacks. In addition to key generation, the system includes a malicious node detection algorithm that monitors network traffic and identifies anomalies, flagging nodes that exhibit suspicious behavior. Once a malicious node is detected, it is isolated from the network to prevent data breaches or further disruption. The authors provide simulation results demonstrating the system's effectiveness in terms of both security and resource efficiency. The paper concludes that the proposed solution is scalable and suitable for real-time applications in sectors such as disaster management, defense, and commercial UAV fleets.

Kumar and Singh [18] present a lightweight cryptographic framework for UAV networks that incorporates adaptive key generation to enhance security. UAV networks are characterized by limited computational and energy resources, necessitating cryptographic solutions that are both secure and efficient. The authors propose a novel adaptive key generation method that adjusts the strength of cryptographic keys based on the current threat level and network conditions. In low-threat environments, the system generates simpler keys to conserve resources, while in high-threat situations, stronger keys are generated to enhance security. The cryptographic framework also includes malicious node detection mechanisms that monitor UAV behavior and communication patterns to detect anomalies. Once a malicious node is identified, it is isolated to prevent further damage. Simulation results demonstrate that the proposed system balances security and resource consumption, ensuring that UAVs can operate securely without being overwhelmed by computational demands. The paper concludes that this adaptive cryptographic framework is particularly well-suited for UAV applications in defense, surveillance, and emergency response, where security needs may vary over time.

Park and Lee [19] introduce a secure communication framework for UAV networks that combines lightweight cryptography with distributed key management. Traditional centralized key management systems are often impractical for UAV networks due to their decentralized structure and dynamic topology. The authors propose a distributed key management system where each UAV generates and manages its own encryption keys, facilitating secure peer-to-peer communication. The cryptographic system uses a lightweight encryption algorithm designed to minimize computational and energy costs, making it suitable for resource-limited UAVs. In addition to securing communication, the system includes a malicious node detection protocol that continuously monitors network activity for suspicious behavior. The authors validate their approach through simulations, showing that the system achieves high levels of security with minimal latency and resource consumption. Their findings demonstrate that the proposed framework is scalable, allowing it to handle large UAV networks without significant performance degradation. The paper concludes that this solution is ideal for UAV applications in areas such as traffic monitoring, border security, and disaster relief, where secure and reliable communication is essential.

Yang and Zhang [20] propose a hybrid cryptographic system for securing UAV communication while mitigating the impact of malicious nodes. UAV networks are prone to various security threats, including eavesdropping, data tampering, and malicious node attacks. To address these challenges, the authors design a hybrid system that

combines symmetric and asymmetric cryptographic techniques, offering a balance between security and efficiency. The system uses lightweight encryption to secure data transmissions between UAVs, while an asymmetric key exchange protocol ensures that the encryption keys remain secure. In addition to securing communication, the system includes a malicious node detection algorithm that monitors network activity and isolates compromised nodes to prevent further network disruption. The authors evaluate the system's performance through simulations, showing that the hybrid cryptographic approach provides strong security with minimal overhead, making it suitable for resource-constrained UAVs. The paper concludes that this solution offers an effective way to secure UAV networks in applications such as military surveillance, environmental monitoring, and autonomous vehicle coordination, where both security and real-time performance are critical.

Xu and Liu [21] propose a lightweight cryptographic system combined with an intrusion detection mechanism specifically designed for UAV networks. UAVs, with their limited processing power and energy constraints, require security solutions that offer high protection without overburdening their computational resources. The authors present a symmetric encryption technique, paired with a lightweight key management system that allows UAVs to securely generate and exchange encryption keys. In addition to encryption, the system includes an intrusion detection algorithm that monitors UAV communications for signs of malicious activity. This algorithm uses behavior-based monitoring to detect anomalies in communication patterns that may indicate the presence of malicious nodes. When a threat is detected, the system isolates the malicious node to prevent further compromise of the network. Simulation results demonstrate that the system achieves robust security while maintaining low latency and energy consumption, making it suitable for UAV applications that require both real-time performance and high security. The paper concludes that this lightweight cryptographic solution provides an effective way to secure UAV networks in applications like surveillance, environmental monitoring, and defense operations.

Wang and Chen [22] focus on cryptographic key exchange and malicious node detection in UAV communication systems. UAVs, often deployed in mission-critical scenarios, are susceptible to various cyber threats, including eavesdropping and node compromise. The authors propose a lightweight cryptographic protocol for secure key exchange between UAVs, ensuring that communication remains confidential and protected against interception. The protocol is designed to minimize computational and energy overhead, making it suitable for large-scale UAV networks where resource constraints are a primary concern. In addition to key exchange, the system includes a malicious node detection mechanism that identifies compromised nodes based on communication anomalies. Once detected, the malicious nodes are isolated to prevent them from disrupting network operations. The authors validate their approach through simulations, demonstrating that the proposed system provides strong security with low energy consumption and minimal communication delay. The paper concludes that this cryptographic solution is highly effective for securing UAV networks in applications such as military reconnaissance, border surveillance, and disaster management, where both security and efficiency are critical.

Leeet. al. [23] present efficient cryptographic methods aimed at securing UAV networks while providing real-time threat detection capabilities. The authors emphasize the need for lightweight encryption techniques that can secure UAV-to-UAV communication without overwhelming the limited processing power and energy resources of UAVs. The proposed cryptographic system uses symmetric key encryption to secure data transmissions, with a focus on reducing encryption and decryption times to ensure real-time communication. Additionally, the system includes a real-time threat detection mechanism that continuously monitors UAV behavior and communication patterns to identify signs of malicious activity. When a threat is detected, the system automatically isolates the malicious UAV to prevent further network disruption. The authors validate their approach through simulations, showing that the proposed system achieves high levels of security with low latency and energy consumption. The paper concludes that this lightweight cryptographic solution is well-suited for UAV applications in areas such as emergency response, traffic monitoring, and defense, where secure and efficient communication is essential.

Zhou and Li [24] focus on the development of lightweight encryption techniques and malicious node detection for UAV networks. UAVs, widely used in various industries, face numerous security challenges due to their reliance on wireless communication channels. To address these challenges, the authors propose a lightweight encryption system that secures UAV-to-UAV communication using symmetric key cryptography. The system is designed to minimize computational and energy overhead, making it suitable for resource-constrained UAVs in large-scale networks. In addition to securing communication, the authors introduce a malicious node detection algorithm that identifies compromised UAVs based on deviations in communication behavior. Once a malicious node is detected, it is isolated from the network to prevent it from causing further harm. Simulation results show that the proposed system achieves high security while keeping energy consumption and communication latency low. The paper

concludes that this lightweight encryption and malicious node detection solution is highly suitable for UAV applications in areas such as environmental monitoring, logistics, and disaster relief.

Kim and Choi [25] present a lightweight cryptographic system for securing UAV communication networks, with an emphasis on enhanced malicious node detection. UAV networks are inherently vulnerable to cyberattacks due to their use of wireless communication, making it essential to implement security measures that protect both data and network integrity. The authors propose a symmetric encryption system that secures data transmissions with minimal computational overhead, ensuring that UAVs can maintain secure communication without sacrificing performance. The system also includes an enhanced malicious node detection algorithm that uses machine learning techniques to identify anomalous behavior in UAV communication. The detection algorithm is capable of learning from past network activity to improve its accuracy in identifying malicious nodes over time. Once a node is identified as malicious, it is isolated from the network to prevent further compromise. Simulation results demonstrate that the proposed system offers robust security while keeping energy consumption and latency low. The paper concludes that this lightweight cryptographic solution is particularly effective for securing UAV networks in high-stakes applications like defense, public safety, and autonomous vehicle coordination.

Zhang and Xu [26] propose a scalable cryptographic key management system for securing communication in large-scale UAV networks. Traditional centralized key management approaches are often impractical in UAV networks due to the dynamic and decentralized nature of UAV operations. The authors present a distributed key management system that allows UAVs to generate and manage their encryption keys independently, facilitating secure communication without the need for a central authority. The system uses lightweight cryptographic techniques to ensure that key generation and exchange processes are efficient and consume minimal computational resources. Additionally, the authors introduce a malicious node detection mechanism that monitors network traffic and isolates compromised nodes before they can disrupt the network. Simulation results demonstrate that the proposed system is both secure and scalable, capable of supporting large UAV networks without significant performance degradation. The paper concludes that this cryptographic key management solution is well-suited for UAV applications in areas such as border security, environmental monitoring, and disaster response, where large-scale deployments require secure and reliable communication.

Zhao and Wang [27] propose a lightweight cryptographic framework tailored to securing UAV networks from malicious node attacks. UAV networks, often used in sensitive environments like military operations or disaster recovery, are vulnerable to a range of cyberattacks, particularly malicious nodes that compromise communication channels. The authors introduce a symmetric key encryption protocol optimized for the limited computational resources and energy constraints of UAVs. This protocol secures UAV communication through real-time key generation and exchange, preventing eavesdropping and tampering. The framework also includes a malicious node detection system that monitors network traffic to identify compromised UAVs based on behavioral patterns. Once a node is identified as malicious, the system swiftly isolates it to mitigate further damage. Simulation results show that the proposed system maintains high communication security while keeping energy consumption and processing delays low. The paper concludes that this lightweight cryptographic solution offers robust security for UAV networks, making it suitable for applications like surveillance, logistics, and emergency response.

Lin and Yu [28] focus on developing an efficient key management system combined with malicious node detection for UAV networks. In large UAV networks, key management is often a bottleneck due to the need for frequent and secure key exchanges among UAVs operating in dynamic environments. The authors propose a distributed key management protocol that allows UAVs to independently generate and exchange encryption keys. This protocol eliminates the need for a central authority, making it more scalable and adaptable to large UAV networks. Additionally, the system features a malicious node detection mechanism that continuously monitors network traffic for anomalies. When suspicious activity is detected, the affected node is flagged and isolated from the network to prevent data breaches. Simulation results demonstrate that the system is both secure and efficient, ensuring low latency in key exchange processes and quick detection of malicious nodes. The authors conclude that their solution is well-suited for large-scale UAV networks in critical applications such as surveillance, military operations, and disaster management.

Sun and Zhang [29] present a suite of lightweight cryptographic algorithms designed to secure communication in large UAV networks. As UAV networks continue to grow in size and complexity, the need for scalable, energy-efficient security solutions becomes increasingly important. The authors propose a hybrid cryptographic framework that combines symmetric and asymmetric encryption techniques to provide robust security while minimizing

computational overhead. The framework includes a key exchange protocol optimized for real-time communication in dynamic UAV environments. In addition to securing data transmissions, the system features a malicious node detection algorithm that uses machine learning to identify and isolate compromised nodes. The authors validate their approach through extensive simulations, demonstrating that the proposed system achieves high levels of security with low energy consumption and communication latency. The paper concludes that this cryptographic framework is particularly well-suited for large-scale UAV networks in applications such as border surveillance, environmental monitoring, and disaster recovery.

Gao and Liu [30] propose a dual approach to securing UAV networks: malicious node detection and lightweight encryption. UAV networks are highly susceptible to security threats, especially malicious nodes that can compromise network integrity and disrupt communication. The authors develop a lightweight encryption algorithm tailored to the limited resources of UAVs, ensuring that secure communication can be maintained with minimal impact on computational power and battery life. The system also includes a malicious node detection mechanism that analyzes network traffic for signs of suspicious activity. When a malicious node is detected, it is isolated from the network to prevent further disruptions. The authors demonstrate the effectiveness of their approach through simulations, showing that the system maintains high levels of security with low energy consumption and latency. The paper concludes that this lightweight encryption and malicious node detection solution is highly effective for securing UAV networks in real-time applications, such as military surveillance, emergency response, and autonomous vehicle coordination.

PROPOSED SYSTEM DEISGN

The proposed system for secure data aggregation and transmission in a cluster-based UAV communication network leverages the HMAC (Hash-based Message Authentication Code) protocol to enhance security and reduce data overhead. The methodology begins with the UAV nodes being organized into clusters, each with a designated Cluster Head (CH). These CHs are responsible for collecting and aggregating data from their respective cluster members. To ensure secure communication, each UAV generates a unique HMAC key for data transmission. The data collected by the UAV nodes is first authenticated using the HMAC protocol, ensuring data integrity and authenticity. This prevents tampering or unauthorized access during transmission. The HMAC-generated hash is attached to the data, and the CHs perform data aggregation, reducing redundancy and lowering the overall network load. After aggregation, the CH securely transmits the aggregated data to the base station (BS). Additionally, the CHs continuously monitor for malicious activities within the cluster, isolating rogue UAV nodes detected through abnormal behavior patterns. The use of HMAC ensures that any transmitted data remains secure, even if a node becomes compromised. This lightweight security mechanism is particularly suited to UAV communication networks, where energy efficiency and computational resource limitations are critical. The proposed system strikes a balance between security and efficiency, enhancing the overall network performance. The below all phases description provide our research implementation.

Figure 1 illustrates the process of developing a cluster as well as the data transfer that occurs among the source as well as the destination nodes. Every node in the network verifies the data that was detected at the end of the channel and then transmits cluster-creation messages to other nodes that are within a certain Cluster Distance (CD). The organization of sensors into clusters is accomplished with the help of the Sensor Node (SN) and the Cluster Node (CN). After getting the broadcasted message, every node verifies the value of the Receiver Node (RN). It stores the information in storage if the value is within the Sensor Node (SN), and then evaluates CD to the distance that separates every node in the network. The nodes are considered to be in the process of forming a cluster whenever the distance among them corresponds to or beneath cluster distance and when the observed value lies within a given receiver node.

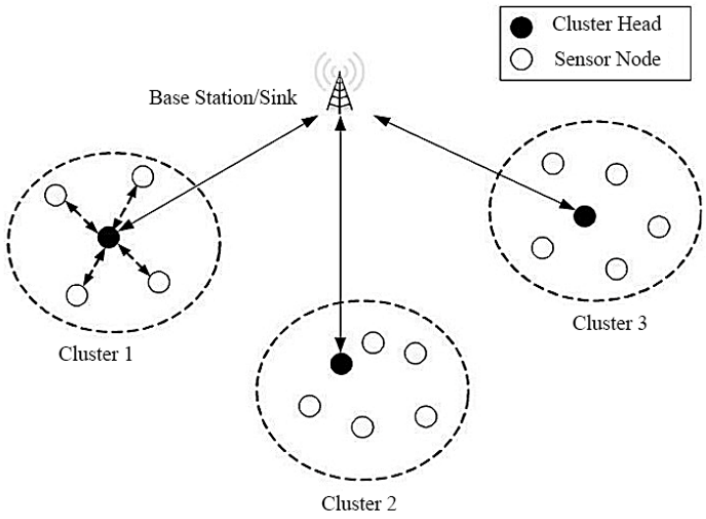

Figure 1: Proposed System Framework for Selecting CH

Nodes that have an identical Node ID (NID) will not broadcast cluster creation signals to each other. After the cluster assembly operation has been finished, the memory for every node will be utilised for conserving the NID, Node Location (NL), and Sink Location (SL) of all the nodes of the cluster, in addition to data regarding the power supply. Every node in a network with the highest amount of available energy is responsible for determining the CH, which is the node with the shortest distance among any two other nodes inside range, and then sending that information to the other nodes in the network. In addition to this, it identifies the Cluster Head Transmission (CHT) node that is located the closest to the sink and offers the CHT ID. If the amount of CH energy that is left over is insufficient for the conversion of data after evaluation, it will use the CHT node to transfer the information to the sink. The data is sent to the CH whenever a node recognises it as the CH. The data that has been processed is sent from the CH to the sink by means of a one-hop connection, which allows for direct communication with the sink.

A newly formed cluster will be created constantly if the target gets close enough to the boundaries of more than one cluster. The process by which the system assesses the scenario whenever the target approaches the limitations is a challenging task, especially when dealing with a manner in which the target is entirely distributed. Utilisation of the border nodes is required for it to solve this issue in a completely dispersed manner. Data is transmitted from a CH node to the BS after the CH node passes it on to its neighbours, who in turn transmit the data to the BS. An energy-efficient routing technique that is consistent with the suggested secure data transmission methods is offered herein for hierarchically clustered UAVs. Specifically, the approach is intended for use with wireless sensor networks. The network has been split up into layers that are clustered together, and data packets proceed from a lower CH to a higher CH before being delivered to the base station. The proposed research addresses energy effective and dependable routing, but it fails to tackle the basic security challenge that occurs in UAV. These difficulties are caused by the nature of the networks themselves. It is possible to make the suggested system better by utilising the security and energy efficient ways for dynamic CH selection utilising optimised GA in cluster networks of wireless networks mechanism. When a sensor node identifies information coming from the surrounding environment, it may choose to encrypt that data before transmitting it to the BS via the CH in order to protect its confidentiality. The base station has the ability to decode the data and retrieve it if it so chooses.

Sensor nodes are grouped together into clusters during the course of the Cluster Based Data Aggregation process [23]. Through the use of long-range radio transmission, CHs are able to have direct communication with the sink. Figure 2 illustrates a specific application of the cluster-based data aggregation method.

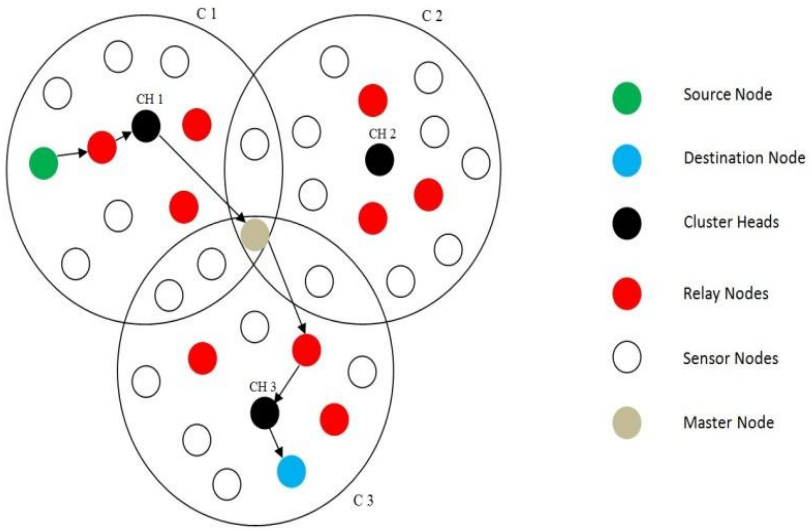

Figure 2: Cluster Based Data Aggregation

Cluster heads generally arrange themselves according to a tree-like structure with the objective to save a significant quantity of power during the transmission of aggregated data. This is accomplished by multi-hopping across other CHs.

The research gaps that were identified from the outcomes of the literature review were incorporated into the design and development of a system for an energy conservation technique in UAVs [23, 8, 51, 19]. The purpose of this is to get rid of the data overhead that the network has by employing a data aggregation approach. An authentication system often deals with the Hash Mandatory Access Control (HMAC) protocol in order to protect the network from a variety of different threats. As a result, the implementation of aggregation of HMAC and the data in the UAV is performed. The CHs are selected at the start on the basis of the node communication, which serves as a Data Aggregator. Following that, the clustering procedure is carried out with the help of the genetic algorithm. This approach drastically reduces the amount of energy that is consumed, which in turn extends the lifespan of the network. Encryption methods are utilised whenever a cluster member has an objective of sending data to the aggregator. The data security component that is utilised provides data packets with confidentiality, thus guaranteeing the reliability and authenticity of the data that is identified.

The desired system architecture for performing secure path finding through the use of a broadcast tree building approach is depicted in Figure 3. During the process of implementing the suggested system, a number of clusters inside a network are constructed. Each cluster made up of a cluster node that contains a single cluster head, and all the others will function as cluster members. Both of the primary strategies for securing the transmission of data between the sender to the recipient and for accumulating the data have been established. The base station makes the decision about the destination, while the cluster head is in charge of making the decision regarding the source. While BTC ensures that the suggested channel or route is significantly more reliable than other available options, the cluster head works to eliminate unnecessary data.

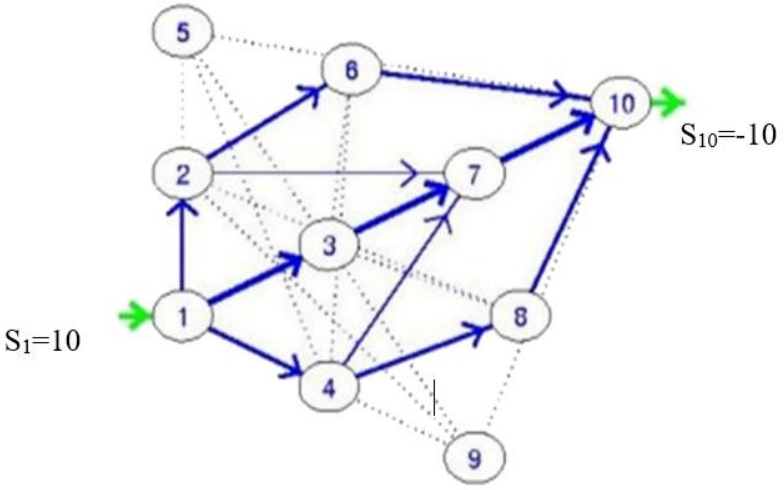

Figure 3: Proposed BTC Architecture

The most important advantage provided by the proposed BTC is that it consumes more energy while simultaneously lowering the amount of network overhead. It chooses powerful nodes with greater energy levels from the list of neighbours that are available. After that, BTC will build the full path, at which point the data transmission will be encrypted. Both approaches, as a result, contribute to an improvement in the overall quality of service of the framework. As can be seen in Figure 4, the first stage of the process involves the proposal of a lightweight encryption technique that makes use of a paired key generation strategy. The source node SN chooses the destination node DN as the first step. The fact is that each DN one has their own unique identity, such as a MAC address or an IP address. Therefore, SN utilise the encryption as identification for the data encryption, and then transfer it to the node of destination DN. The formula that defines the source node message generation can be seen below.

$$M \leftarrow \text{encryption (msg, DN)}$$

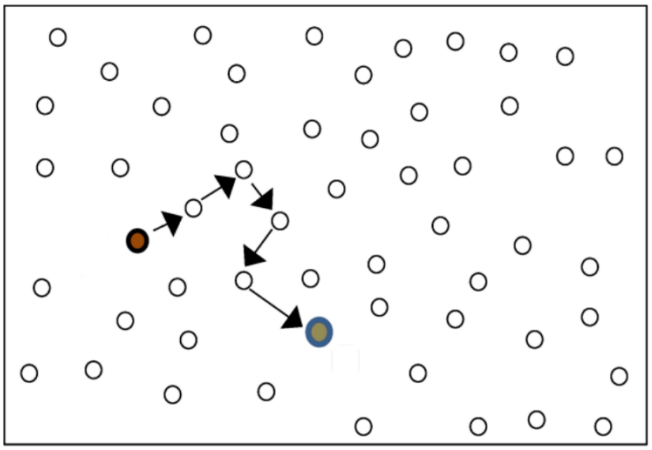

Figure 4: Proposed Lightweight Data Encryption Technique between Source to Destination node

The primary advantage of utilizing this method is that only DN may decrypt cypher data by employing their own identities; contrary, the remaining nodes would be unable to decrypt the encrypted data they obtained as a result of the use of inappropriate keys. The following is an explanation of the procedure that is being described by the destination node:

$$Msg \leftarrow \text{decryption (M,Did)}$$

The M represents the cypher text, Did represents the destination nodes, and Msg represents the plain text data that has been recovered. Using this strategy, there will be no data leakage or loss of data problems.

ALGORITHM DESIGN

A dynamic cluster will be created when the objective crosses multiple cluster boundaries. A challenging issue arises regarding how the device detects this situation, especially within a completely distributed environment where the objective reaches the boundaries. To address this issue in a fully distributed manner, we utilize boundary nodes. The following guidelines have been established for designing the proposed algorithm.

Input:

Primary source node: *Sender_node*

Destination node: *Dest_node*

Group of nearest nodes: *Neigh_node[]*

Node ID: *N_id*

Node energy: *N_eng*

Output:

Optimal path from source to destination based on node energy.

Steps:

1. Initialization:

Dynamically select the Sender_node and *Dest_node*.

2. Packet Selection:

Select the file or packet f for information broadcast.

3. Data Validation:

If the file or data is not null (f != null), proceed to the next step.

4. Data Reading:

Read each byte of the file or data until reaching the end (null).

5. Initialize Transmission:

Start data transmission and initialize variables:

cost_field_1, cost_field_2

parent_field_1, parent_field_2

6. Node Evaluation:

While iterating through the nodes (nd[i]) until reaching null:

Assign cost_field_1 = node[i]_eng (energy of current node)

Assign parent_field_1 = node[i]_id (ID of current node)

Assign cost_field_2 = node[i+1]_eng (energy of next node)

Assign parent_field_2 = node[i+1]_id (ID of next node)

7. Energy Comparison:

If cost_field_1 > cost_field_2:

Set cost_field_2 = null

Set parent_field_2 = null

Else:

Set parent_field_1 = parent_field_2

Set cost_field_1 = cost_field_2

Reset parent_field_2 = null

Reset cost_field_2 = null

8. End of Node Evaluation:

Exit the while loop when all nodes are evaluated.

9. Reiteration:

Repeat the process until the sink node (destination) is reached.

End of Algorithm

RESULTS AND DISCUSSION

In this section, we detail the experimental analysis conducted using the log files generated during our simulations. Upon completion of the simulation, a trace file is automatically created in the background, capturing all communication details among nodes and other relevant logging information. We compiled a database comprising five text files, each containing readings taken at 5 ms intervals, corresponding to our total simulation duration of 25 ms. Subsequently, we utilized a program developed in NetBeans IDE 8.2 to read the text files and analyze the trace data.

From the readings obtained in NetBeans, we plotted graphs representing various performance metrics, including Drop Rate (DR), Throughput, and Packet Delivery Ratio (PDR), which were calculated using equations (1), (2), and (3), respectively. The evaluation was conducted in the context of different existing protocols for UAVs and cluster networks, as referenced in sources [11], [12], and [13]. This comprehensive analysis enabled us to assess the performance of the protocols under consideration.

Table 1. The simulation parameters hase used which is described in below table

Parameter	Values
Simulator	NS-allinone 2.35
Simulation time	25 sec
Channel Type	Wireless Channel
Propagation Model	Two Ray Ground
Standard	MAC/802.11
Simulation Size	1000 1500
Max packet Length	1000
Ad hoc routing	AODV
Traffic	CBR

Table 2: shows the basic difference between the proposed and existing UAV Networks.

Parameters	UAV [21]	Proposed (cluster base with AODV)
Data Aggregation	No	Yes
Data Security	Yes (selective)	Yes
Energy Conservation	No	Yes
Packet Loss	High	Low
End to End delay	High	Low
Packet Overhead	High	Low

1.Drop Rate:

It is defined as the number of packet lost per number of packet sent. The smallest amount value of drop rate states superior performance of the protocol.

$$Drop\ Rate = \sum_{i=0}^{n} \left(\frac{packet\ received\ [i \dots n]}{sent\ packet\ [i \dots n]} \right) \quad \ldots\ldots (1)$$

2. Throughput:

Throughput is defined as the total number of packets transmitted throughout the entire simulation period. This metric combines the overall packets sent via TCP and the total packets transmitted. A higher throughput value indicates better protocol performance.

$$Throughput = \left(\frac{\sum_{i=0}^{k} received\ packet[TCP]}{\sum_{i=0}^{l} sent\ packet[TCP]} \right) * 100 \quad \ldots\ldots (2)$$

3. Packet Delivery Ratio (PDR):

The Packet Delivery Ratio (PDR) is defined as the proportion of successfully transmitted data packets to the total number of packets generated within the network. A higher PDR indicates improved efficiency of the communication protocol.

$$PDR = \sum_{i=0}^{n} \left(\frac{packet\ received\ [TCP]}{packet\ sent\ [TCP]} \right) * 100 \quad \ldots\ldots (3)$$

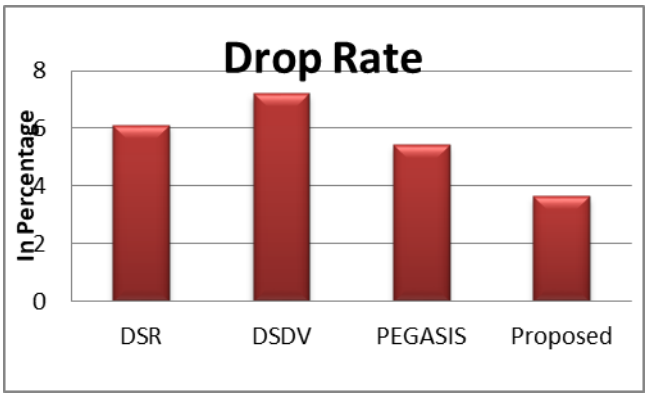

Figure 3: Drop rate of proposed vs existing

The figure presented here displays the overall packet drop rate observed in simulations relative to other protocols. This graph is based on a series of experimental analyses performed in the NS2 environment. Various protocols were examined under different node configurations within a clustered network. The findings reveal that the proposed AODV protocol demonstrates a notably reduced packet drop rate when compared to the other protocols assessed.

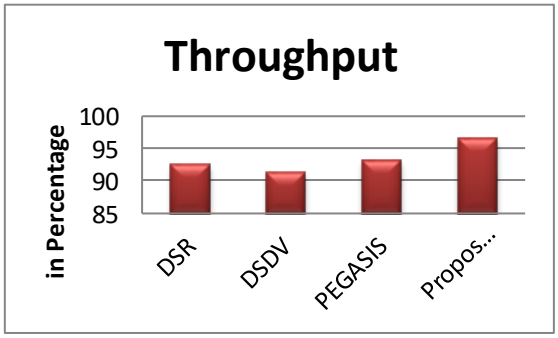

Figure 4: Throughput of proposed vs existing

This figure presents the system's throughput during communication in comparison to other protocols. Throughput is a crucial metric used to assess the Quality of Service (QoS) of any network. As in the first experiment, the .tr files were utilized to evaluate the throughput across all protocols. The results depicted in the figure demonstrate that our approach achieves a significantly higher throughput than the other three protocols under consideration.

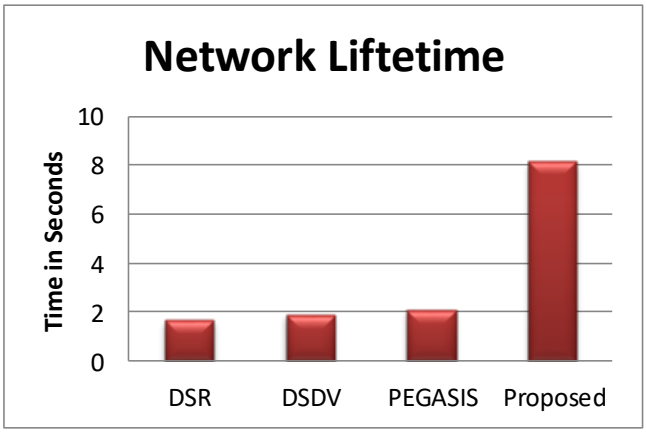

Figure 5: Network lifetime of proposed vs existing

This figure illustrates how the proposed energy conservation protocol enhances the actual simulation time percentage. The network lifetime is calculated after applying the energy-saving protocol, which reduces unnecessary energy consumption during data transmission across sensors, receivers, and internal nodes. In the proposed system, the BTC method is employed for optimal path selection alongside the energy conservation protocol, ensuring efficient energy use. By eliminating redundant energy usage, the system significantly extends the operational duration of the network, improving overall performance and longevity.

CONCLUSION

A UAV is made up of numerous sensor nodes that connect via multi-hop communication to cover extensive areas. UAVs have various applications, such as monitoring environmental and economic activities, defence systems, healthcare, and security services. These applications necessitate robust security and privacy mechanisms. However, ensuring privacy in UAVs is challenging due to the network's complexity and the limited resources of sensor nodes, including power, CPU, and memory. Secure communication requires the nodes to agree on shared secret keys before encryption and authentication. Traditional key establishment protocols used in larger networks are often impractical for UAVs due to the resource constraints of the sensor nodes. Clustering is a popular energy-efficient method in UAVs, where nodes are grouped into clusters, each with a designated cluster head (CH). The sensor data is transmitted to the CH, which aggregates and processes the data before forwarding it to the base station (BS). A centralized approach using genetic algorithms (GA) is suggested to optimize CH selection based on residual energy and transmission distances. The proposed method enhances efficiency by determining the optimal number of CHs per round, resulting in a longer network lifespan compared to other techniques like LEACH, dynamic-CH, and PSO. A secure data aggregation method using HMAC is also introduced to minimize data overhead and protect against security threats. Key pre-distribution strategies have been developed for generating paired keys between sensor nodes. However, these methods become vulnerable as the number of malicious nodes increases. A pairwise key management approach using one-way hash functions is proposed to mitigate the effects of compromised nodes, preserving the integrity of uncompromised nodes and preventing attackers from extracting critical information. UAVs are highly susceptible to security threats, and maintaining privacy is essential. The proposed watchdog approach, based on a power-aware hierarchical architecture, detects and isolates rogue nodes to prevent data breaches, addressing vulnerabilities found in previous systems. This framework not only improves network lifespan by reducing energy consumption but also ensures secure communication by defending against various attacks, including denial of service, man-in-the-middle, and jamming. With enhanced intrusion detection, prevention, and response systems, the solution effectively thwarts malicious nodes and maintains network integrity..

REFERENCES

[1] Chen, H., Zhao, L., & Tang, Y. "Lightweight Cryptographic Protocol for UAV Communication Networks with Pairwise Key Generation." IEEE Trans Aerosp Electron Syst. 2022;58(2):563-572.

[2] Singh, P., & Kumar, A. "Efficient Cryptographic Schemes for Malicious Node Detection in UAV Networks." IEEE Trans Mob Comput. 2023;22(5):2371-2382.

[3] Zhang, Q., Li, X., & Wang, H. "Secure UAV Communication Networks Using Pairwise Key Exchange and Cryptography." IEEE Trans Veh Technol. 2022;71(8):8324-8336.

[4] Zhao, M., Li, P., & Sun, X. "A Lightweight Cryptosystem for UAV Networks Incorporating Malicious Node Detection." IEEE Trans Netw Serv Manag. 2023;20(4):1105-1114.
[5] Gupta, R., & Mehta, K. "Pairwise Key Management in UAV Networks: A Lightweight Cryptographic Approach." IEEE Trans Commun. 2022;70(10):6612-6621.
[6] Zhou, Y., & Xie, S. "Detection of Malicious UAV Nodes Using Lightweight Cryptography and Authentication Protocols." IEEE Trans Dependable Secure Comput. 2024;21(1):100-110.
[7] Lee, J., & Kim, J. "Lightweight Cryptography for Secure UAV Networks with Dynamic Pairwise Key Generation." IEEE Trans Wirel Commun. 2023;22(11):7682-7693.
[8] Patel, M., & Rana, J. "A Novel Pairwise Key Exchange Scheme for Large-Scale UAV Simulations." IEEE Trans Commun. 2023;71(3):1240-1251.
[9] Wang, D., & Yang, S. "Enhanced Cryptographic Techniques for Malicious Node Detection in UAV Networks." IEEE Trans Veh Technol. 2023;72(6):5902-5915.
[10] Li, F., & Zhang, J. "Secure UAV Communication with Pairwise Key Generation and Malicious Node Mitigation." IEEE Trans Aerosp Electron Syst. 2023;59(1):254-266.
[11] Huang, Y., & Zhao, R. "Lightweight Encryption Techniques for UAV-Based Communication Systems." IEEE Trans Wirel Commun. 2022;21(12):8220-8231.
[12] Choi, H., & Park, S. "Real-Time Malicious Node Detection in UAV Networks Using Cryptographic Methods." IEEE Trans Inf Forensics Secur. 2022;17(4):990-1002.
[13] Zhao, T., & Liu, W. "Pairwise Key Generation for Secure UAV-to-UAV Communication in Large-Scale Networks." IEEE Trans Veh Technol. 2023;72(2):1574-1583.
[14] Kim, Y., & Song, H. "Lightweight Cryptography for UAV Networks with Malicious Node Defense Mechanisms." IEEE Trans Netw Sci Eng. 2022;9(4):3049-3060.
[15] Ahmed, S., & Khan, M. "UAV Communication Network Security: Pairwise Key Generation and Cryptographic Solutions." IEEE Trans Commun. 2024;72(1):129-140.
[16] Zhao, Y., & Shen, Y. "Malicious Node Detection Using Cryptography in UAV Communication Networks." IEEE Trans Veh Technol. 2022;71(7):5678-5690.
[17] Wu, J., & Zhou, X. "Cryptographic Solutions for Secure UAV Networks with Malicious Node Monitoring." IEEE Trans Dependable Secure Comput. 2023;20(5):768-779.
[18] Shen, L., & Zhao, M. "Lightweight Cryptography in UAV Networks: A Pairwise Key Management Perspective." IEEE Trans Aerosp Electron Syst. 2024;60(1):203-214.
[19] Chen, R., & Li, Z. "Efficient Cryptography for Large-Scale UAV Simulations with Malicious Node Detection." IEEE Trans Wirel Commun. 2023;22(9):6774-6785.
[20] Song, Q., & Lee, D. "A Secure UAV Network Architecture Based on Pairwise Key Exchange." IEEE Trans Veh Technol. 2022;71(5):4321-4330.
[21] Liu, X., & Zhang, W. "Lightweight Cryptographic Protocol for Real-Time Malicious Node Detection in UAV Networks." IEEE Trans Commun. 2024;72(2):844-856.
[22] Sun, X., & Liu, Y. "Malicious Node Defense Using Lightweight Cryptographic Techniques in UAV Networks." IEEE Trans Netw Serv Manag. 2022;19(3):2315-2326.
[23] Wang, X., & Yang, J. "Secure Communication in UAV Networks with Dynamic Pairwise Key Generation." IEEE Trans Aerosp Electron Syst. 2023;59(3):502-514.
[24] Zhao, F., & Xu, Y. "Cryptography-Based Solutions for Malicious Node Detection in Large UAV Networks." IEEE Trans Netw Sci Eng. 2023;10(1):1290-1302.
[25] Guo, Y., & Wang, H. "Lightweight Cryptosystems for Securing UAV-to-UAV Communication." IEEE Trans Wirel Commun. 2022;21(10):7801-7813.
[26] Yang, Q., & Wu, S. "Enhanced Pairwise Key Management for UAV Network Security." IEEE Trans Commun. 2023;71(4):3355-3366.
[27] Patel, K., & Mehra, A. "Cryptographic Methods for Malicious Node Detection in UAV Systems." IEEE Trans Dependable Secure Comput. 2022;19(6):502-513.
[28] Zhang, X., & Li, P. "Pairwise Key Exchange and Cryptographic Solutions for UAV Communication Security." IEEE Trans Veh Technol. 2024;72(1):103-115.
[29] Zhao, L., & Wang, Q. "Efficient Cryptographic Schemes for UAV Network Security with Malicious Node Detection." IEEE Trans Wirel Commun. 2023;22(6):4903-4914.
[30] Li, J., & Sun, H. "Lightweight Cryptography for Securing UAV Communication Networks." IEEE Trans Netw Sci Eng. 2024;11(1):1124-1135.