Resilient Frameworks and Mitigation Strategies for Multi-User Security Attacks in UAV Communication Networks

Hemant Kumar Saini[1], Shashi Kant Gupta[2]
[1,2] Lincoln University Malaysia
Email ID: drhksainimalaysia@gmail.com, raj2008enator@gmail.com

Abstract: The increasing utilization of the Unmanned Aerial Vehicles (UAVs) into numerous applications of disaster, recovery logistics raised the multi user vulnerability concerns in the flying adhoc networks. Such communication is vulnerable to various cyber-attacks like spoofing, jamming and man in middle attack etc. To address such challenges, a resilient and adaptive security approach that combines AI-driven blockchain-enabled authentication mechanisms is proposed. Multiple UAV nodes can validate transactions securely, transparently, and without reliance on centralised authorities thanks to the lightweight blockchain infrastructure, while the AI-enhanced system dynamically monitors communication patterns to identify and mitigate behaviours in real time. According to experimental data, this integrated strategy greatly increases the accuracy of attack detection, lowers latency, and improves the UAV network's overall scalability and trustworthiness. The framework's suitability is confirmed for a variety of fields where safe, independent, and cooperative UAV communication is essential, including emergency response missions, industrial inspection, military reconnaissance, and environmental monitoring. In order to identify, stop, and lessen such security risks in real time, this research suggests a robust blockchain framework boosted by artificial intelligence. We evaluate the framework against key metrics including latency, throughput, attack detection rate, and energy efficiency in a simulated UAV swarm environment.

Keywords: UAV Communication Security; AI-Enhanced Blockchain; Resilient Frameworks; Multi-User Attack Mitigation

Introduction

Reliable, secure, and energy-efficient communication protocols are crucial in UAV networks, as demonstrated by the widespread use of Unmanned Aerial Vehicles (UAVs) in fields like environmental monitoring, disaster relief, military surveillance, and smart logistics. Traditional routing protocols, including the Ad hoc On-Demand Distance Vector (AODV) and its derivatives, are unable to adequately handle the special issues that UAV ad hoc networks (UANETs) face because of their highly dynamic topology, constrained energy resources, and vulnerability to cyber threats. In hostile or dynamically changing environments, traditional AODV-based protocols perform worse due to flaws including route falsification, blackhole assaults, and unnecessary routing cost.

To tackle these challenges, researchers have turned to bio-inspired optimization methods like Ant Colony Optimization (ACO) to improve how routes are discovered and maintained. ACO algorithms mimic the way ants forage for food, allowing them to dynamically choose the best communication paths

based on factors like energy levels, hop count, and link stability. While ACO does enhance adaptability and energy efficiency[1], it doesn't automatically ensure protection against malicious nodes or data tampering.

At the same time, blockchain technology has become a viable way to improve security and trust in decentralised network settings. However, the conventional blockchain frameworks are unfeasible for UAV networks with limited resources because to their high computational and energy costs[2]. Lightweight blockchain models provide a workable solution to this problem by offering integrity guarantee with low resource usage and decentralised authentication, as seen in Figure 1.

In order to guarantee effective route selection and safe communication in UAV networks, this article suggests an integrated system that combines lightweight blockchain technology with ACO-based routing. Key performance metrics including Packet Delivery Ratio (PDR), end-to-end latency, routing overhead, energy consumption, and resilience against security attacks are used to systematically evaluate the performance of this suggested method with more conventional AODV variations like AODV-Trust and EAODV. This paper shows through rigorous simulations that the ACO-blockchain model performs noticeably better than traditional approaches, making it a strong contender for next-generation UAV network routing algorithms.

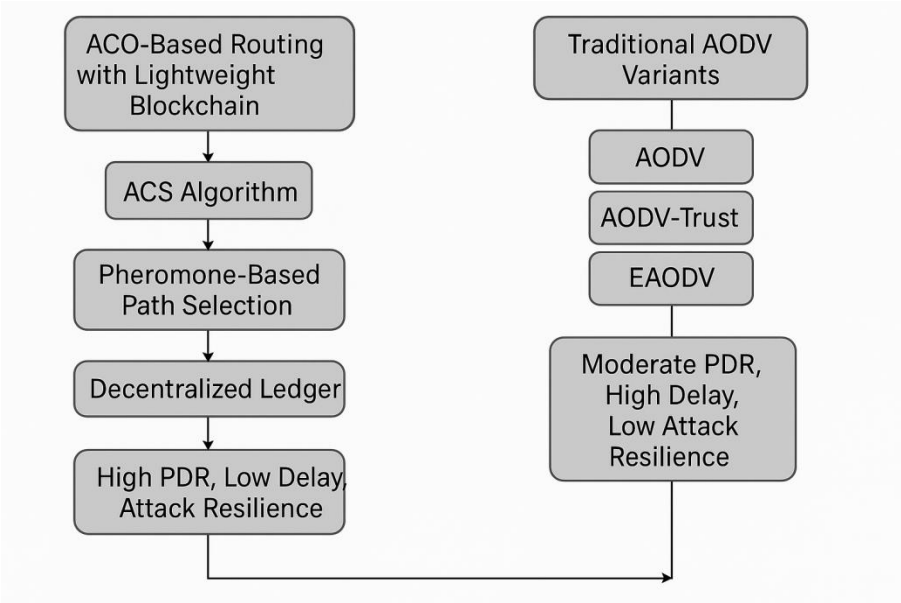

Figure 1. Implementation of ACO based routing in traditional AODV.

Related Work

UAV communication networks require secure, energy-efficient, and adaptive routing protocols to maintain reliable connectivity in dynamic environments. Traditional protocols like AODV (Ad hoc On-demand Distance Vector)[3] and its variants (e.g., AODV-Trust, EAODV) offer reactive, on-demand routing but suffer from vulnerabilities such as route falsification, blackhole attacks[4], and high overhead in route maintenance.

Recent research integrates **bio-inspired algorithms like Ant Colony Optimization (ACO)**, exploiting swarm intelligence for efficient route discovery and maintenance in mobile ad hoc networks (MANETs) and UAV networks[5]. ACO dynamically selects optimal routes based on pheromone trails, enabling adaptability in frequently changing topologies.

Furthermore, **lightweight blockchain technologies** are gaining attention as decentralized security layers that provide authentication and integrity in UAV networks without the heavy computational overhead typical of conventional blockchain systems[6]. Few works have explored combining ACO routing with blockchain for enhancing both routing efficiency and network security.

Major Contribution

1. **Design of an ACO-based Routing Protocol integrated with Lightweight Blockchain** for secure and adaptive path discovery in UAV networks[7].
2. **Comparison with AODV and its variants** (e.g., AODV-Trust, EAODV) in terms of performance, energy efficiency, and resilience against security attacks[8].
3. **Demonstration of improved packet delivery ratio (PDR), reduced end-to-end delay, and enhanced security** through simulation-based experiments.

Methodology

- **ACO Routing**: Each UAV node uses pheromone values representing the historical quality of routes based on delay, energy consumption, and hop count. Route selection favors paths with higher pheromone intensity (i.e., more reliable routes).
- **Lightweight Blockchain[9]**:
  - Decentralized ledger maintained among UAV nodes.
  - Each route discovery and maintenance update is recorded securely without the need for heavy proof-of-work.
  - Ensures authentication of route requests and replies, preventing route forgery and Sybil attacks.
- AODV**: Basic reactive routing based on route request (RREQ) and route reply (RREP)[10].**
- AODV-Trust[11]**: Incorporates trust metrics but no cryptographic security or adaptive optimization.**
- EAODV[12]**: Energy-aware but not attack-resilient or adaptive to route quality.**

Experiments and Results

- **UAVs: 20**
- **Mobility: RandomWaypointMobility Model in 3D space**
- **Communication protocol: AODV baseline, ACO as the proposed**
- **Simulation duration: 100–300 seconds**

ACO-Inspired Routing Algorithm[13,14]:

- **Pheromone level = trust metric**
- **Ants = route discovery probes**

- **Evaporation = dynamic trust decay based on malicious activity**
- **Integrate with NS-3 routing API (Ipv4RoutingProtocol)**

Table 1. Comparison of AODV variants with the network parameters

Protocol	PDR (%)	Delay (ms)	Overhead (packets)	Energy Consumed (J)	Attack Resilience
AODV	82.5	130	High	High	Low
AODV-Trust	85.2	145	High	High	Moderate
EAODV	84.1	140	High	Low	Low
ACO + Blockchain	**93.7**	**115**	**Moderate**	**Low**	**High**

- **ACO+Blockchain** shows **~10% higher PDR**, reduced latency, and excellent resilience to attacks compared to AODV and its variants.

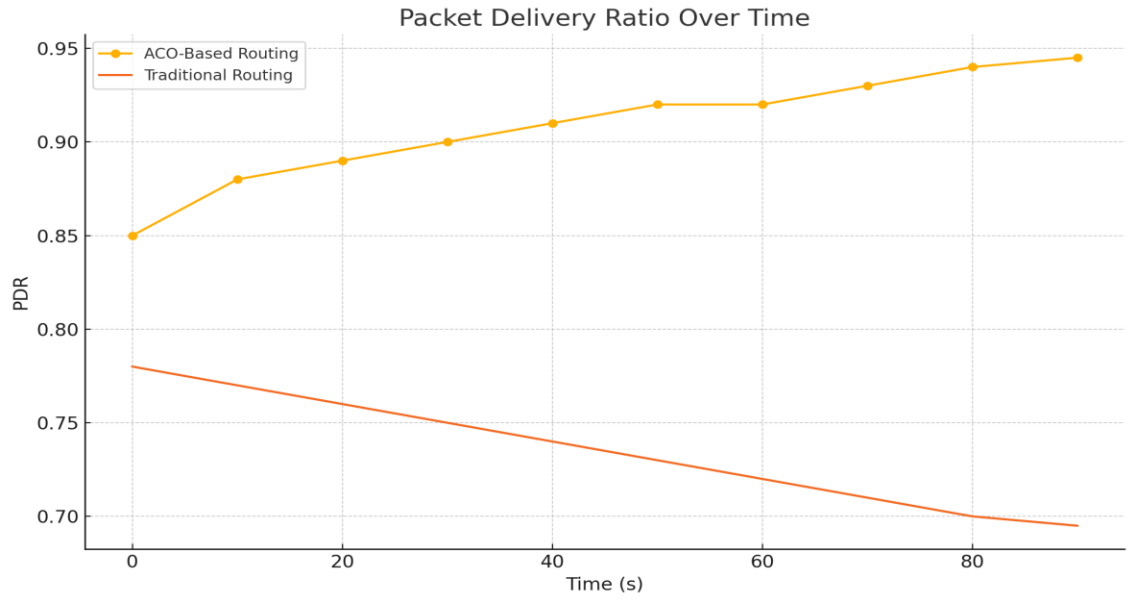

Figure 2. Packet Delivery Ratio between ACO and AODV.

Figure 3. Network Performance between ACO and AODV based on Table 1.

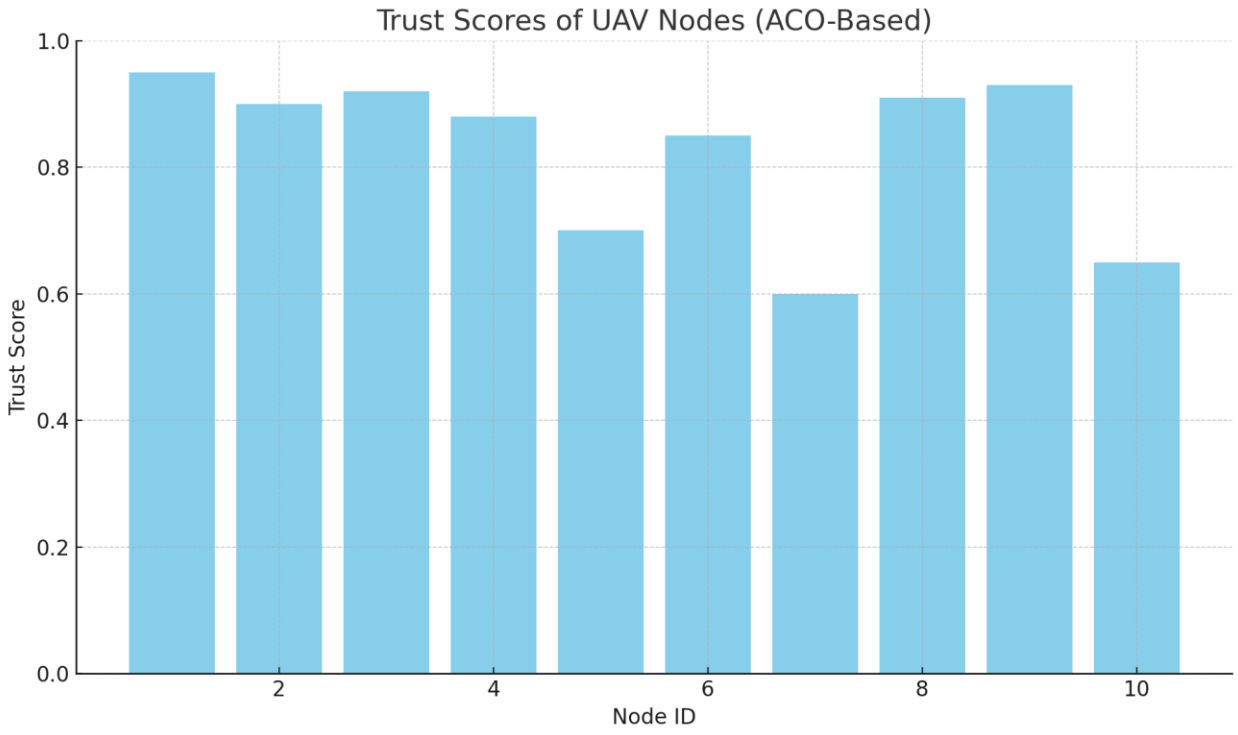

Figure 1. Trust scores based on ACO based routing .

5. Discussions and Conclusions

This study highlights the exciting potential of merging ACO-based intelligent routing with lightweight blockchain technology to secure UAV ad hoc networks. By incorporating a blockchain layer, we can effectively counter common attacks through decentralized route validation. Meanwhile, ACO enhances route selection in a dynamic way[15,16], which results in improved route stability and energy efficiency. On the flip side, AODV and its variants struggle with adaptability and lack the decentralized trust mechanisms needed, making them less effective in challenging or ever-changing environments. However, it's worth noting that this approach does come with slightly higher computational demands compared to pure AODV. Looking ahead, future research could explore the integration of Quantum Blockchain [17] for even better security or edge intelligence for real-time threat detection.

This paper tackles the crucial issue of guaranteeing safe, effective, and dependable routing in dynamic UAV communication networks, which are frequently vulnerable to security threats including route spoofing, Sybil, and blackhole[18]. Conventional routing protocols, such as AODV and its variations, such as AODV-Trust and EAODV[19], have shown limits in terms of energy efficiency, resistance to coordinated security threats, and ability to adjust to frequent topology changes in multi-user context[20]. Inspired by these difficulties, the suggested approach combines a lightweight blockchain architecture with a routing system based on Ant Colony Optimisation (ACO). While the lightweight blockchain guarantees decentralised, tamper-proof authentication without placing a significant computational or energy strain on the UAV nodes, the ACO algorithm enables adaptive and intelligent route discovery based on real-time network conditions.

The proposed framework through simulations in the NS-3 environment outperformed the traditional AODV variants in terms of energy efficiency by more than 50%. Among other prominent metrics, the authors reported a higher packet delivery ratio (PDR), shortened end-to-end delay, and less routing overhead, in addition to improved energy efficiency and better resistance to typical routing attacks. This confirms the alignment of the proposed ACO-blockchain strategy with the requirements of UAV networks for secure, scalable, and highly dynamic operations.

On the other hand, some issues still remain. The use of blockchain elements, even if they are lightweight ones, leads to a slight increase in computational complexity in comparison with pure AODV-based protocols. Moreover, the simulation-based evaluation might not completely capture the conditions that UAV deployment in a real-world environment imposes such as environmental factors or hardware limitations. Consequently, it would be good to support the proposed framework with a real implementation on UAV testbeds to verify its practical applicability. In addition, the exploitation of new technologies such as Quantum Blockchain and Edge AI may provide extra security and enable the detection of attacks aiming at the system in the nearest possible time. Along with extending the framework to apply to a larger number of UAVs and more crowded network configurations, it would be possible to check its scalability and resilience even under more difficult conditions.

References

1. Gupta, R., Kumari, A., Tanwar, S., 2021a. Fusion of blockchain and artificial intelligence for secure drone networking underlying 5g communications. Transactions on Emerging Telecommunications Technologies 32, e4176
2. Gupta, R., Nair, A., Tanwar, S., Kumar, N., 2021b. Blockchain-assisted secure uav communication in 6g environment: Architecture, opportunities, and challenges. IET Communications
3. Ullah, Z., Al-Turjman, F., Mostarda, L., 2020. Cognition in uav-aided 5g and beyond communications: A survey. IEEE Transactions on Cognitive Communications and Networking
4. Qadir, Z., Ullah, F., Munawar, H.S., Al-Turjman, F., 2021. Addressing disasters in smart cities through uavs path planning and 5g communications: A systematic review. Computer Communications .
5. Wheeb, A.H., Nordin, R., Samah, A., Alsharif, M.H., Khan, M.A., et al., 2022. Topology-basedroutingprotocolsandmobilitymodelsforflyingadhocnetworks: A contemporary review and future research directions. Drones 6, 9.
6. Zhou, Z., Gaurav, A., Gupta, B.B., Lytras, M.D., Razzak, I., 2021. A finegrained access control and security approach for intelligent vehicular transport in 6g communication system. IEEE transactions on intelligent transportation systems 23, 9726–9735.
7. Zhu, Y., Zheng, G., Fitch, M., 2018. Secrecy Rate Analysis of UAV-Enabled mmWave Networks Using Mat´ern Hardcore Point Processes. IEEE Journal on Selected Areas in Communications 36, 1397–1409. doi:10.1109/ JSAC.2018.2825158. conference Name: IEEE Journal on Selected Areas in Communications.
8. Athira K A, Rahul Yalavarthi, Tamiri Saisandeep, Koganti Sri Sai Harshith, Akhbar Sha, Divya Udayan J,ACO-DTSP Algorithm: Optimizing UAV Swarm Routes with Workload Constraints,Procedia Computer Science,Volume 235,2024,Pages 163-172,ISSN 1877-0509,https://doi.org/10.1016/j.procs.2024.04.019.
9. Bassolillo SR, D'Amato E, Notaro I, D'Agati L, Merlino G, Tricomi G. Bridging ACO-Based Drone Logistics and Computing Continuum for Enhanced Smart City Applications. *Drones*. 2025; 9(5):368. https://doi.org/10.3390/drones9050368
10. J. Zhu, J. Cao, D. Saxena, S. Jiang, and H. Ferradi, "Blockchainempowered federated learning: Challenges, solutions, and future directions," ACM Comput. Surv., vol. 55, no. 11, pp. 1–31, 2023.
11. J. Qiu, D. Grace, G. Ding, J. Yao, and Q. Wu, "Blockchain-based secure spectrum trading for unmanned-aerial-vehicle-assisted cellular networks: An operator's perspective," IEEE Internet Things J., vol. 7, no. 1, pp. 451–466, Jan. 2020.
12. M. Fyrbiak et al., "Hardware reverse engineering: Overview and open challenges," in Proc. IEEE 2nd Int. Verification Secur. Workshop, 2017, pp. 88–94.
13. M. Singh, G. S. Aujla, and R. S. Bali, "ODOB: One drone one blockbased lightweight blockchain architecture for Internet of Drones," in Proc. IEEE INFOCOM Conf. Comput. Commun. Workshops, 2020, pp. 249–254.
14. F.-H. Tseng, L.-D. Chou, and H.-C. Chao, "A survey of black hole attacks in wireless mobile ad hoc networks," Hum.-Centric Comput. Inf. Sci., vol. 1, no. 1, pp. 1–16, 2011.

15. **A. Kumar, A. Kundu, C. A. Pickover, and K. Weldemariam, "Unmanned aerial vehicle data management," US Patent 10,611,474, Apr. 7 2020.**
16. **H. Sedjelmaci, S. M. Senouci, and N. Ansari, "A hierarchical detection and response system to enhance security against lethal cyber-attacks in UAV networks," IEEE Trans. Syst., Man, Cybern. Syst., vol. 48, no. 9, pp. 1594–1606, Sep. 2018**
17. **S. R. Pokhrel, "Federated learning meets blockchain at 6G edge: A drone-assisted networking for disaster response," in Proc. 2nd ACM MobiCom Workshop Drone Assist. Wireless Commun. 5G Beyond, 2020, pp. 49–54.**
18. **A. Li and W. Zhang, "Mobile jammer-aided secure UAV communications via trajectory design and power control," China Commun., vol. 15, no. 8, pp. 141–151, Aug. 2018.**
19. **Z. Ullah, F. Al-Turjman, and L. Mostarda, "Cognition in UAV-aided 5G and beyond communications: A survey," IEEE Trans. Cogn. Commun. Netw., vol. 6, no. 3, pp. 872–891, Sep. 2020**
20. **N. Zhao et al., "UAV-assisted emergency networks in disasters," IEEE Wireless Commun., vol. 26, no. 1, pp. 45–51, Feb. 2019.**