Extended Literature Review on Zero Trust Architecture and Machine Learning for Military UAV Security

Yadunandan N
School of Computer Engineering
Manipal Institute of Technology, Manipal, India
Email: yadunandan1.mitmpl2025@learner.manipal.edu

Deepak Parashar
Associate Professor, School of Computer Engineering
Manipal Institute of Technology, Manipal, India
Email: deepak.parashar@manipal.edu

***Abstract*—Unmanned Aerial Vehicles represent critical assets in modern military operations, bestowed with enhanced reconnaissance, surveillance, and communication capabilities. However, their deployment in the IoBT introduces new challenges to cybersecurity. Traditional perimeter-based security models cannot protect UAV systems in dynamic and decentralized networks. This work extends the literature review on the application of Zero Trust Architecture and Machine Learning to UAV security. The review analyzes the foundational concepts, discusses very recent implementations, including the 2024 IEEE Access paper from Alquwayzani and Albuali [6], and analyzes how ZTA enhances IoBT resilience through continuous verification, access control, and ML-driven threat detection. It also pinpoints architectural frameworks that underpin secure IoBT systems and identifies gaps for future research.**

***Index Terms*—Zero Trust Architecture, UAV Security, Cybersecurity, Machine Learning, Internet of Battlefield Things (IoBT), Access Control, Defense Networks**

I. Introduction

Unmanned Aerial Vehicles represent a transformative element in defense, enabling autonomous intelligence, surveillance, and tactical support. However, their integration into IoBT infrastructures exposes them to advanced cyber threats. Spoofing, data manipulation, and signal jamming are some of the attacks that make mission-critical operations vulnerable [13], [14]. The traditional network security approaches relying on static perimeters and implicit trust are inadequate for these dynamic environments.

It calls for continuous authentication and verification, replacing implicit trust.*"never trust, always verify"*,principle, ZTA enforces contextual access decisions and least-privilege policies across all entities [1], [2]. In UAV networks, the use of ZTA ensures secure communications among drones, control centers, and battlefield nodes. The recent research, as represented by the 2024 IEEE Access study by Alquwayzani and Albuali [6], includes the integration of ZTA with ML in the IoBT environment for military-grade object detection, response, and adaptation.

II. Foundational Development of Zero Trust Architecture

John Kindervag introduced the concept of Zero Trust in 2010 to fix the shortcomings of perimeter-based defense models for any organization [1]. NIST came up with an authorized edition of this model in SP 800-207 [2], which introduced three main elements:

- **Policy Engine (PE)** – evaluates trust levels and makes access decisions.
- **Policy Administrator (PA)** – enforces authentication and authorization.
- **Policy Enforcement Point (PEP)** – manages data flow between entities.

These components work together in ensuring that access to system resources has continuous verification. DeCusatis et al. [3] extended ZTA to cloud systems by embedding verification at multiple layers. Phiayura and Teerakanok [4] later proposed a migration framework for organizations adopting ZTA in distributed infrastructures.

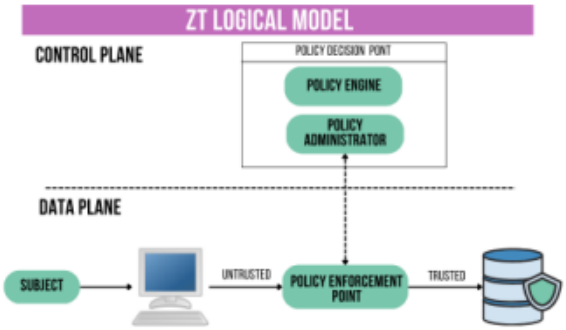

Fig. 1. Zero Trust Logical Model illustrating core components: Policy Engine (PE), Policy Administrator (PA), and Policy Enforcement Point (PEP).

In the military context, these principles translate into dynamic, role-based access for UAV fleets. Each UAV and command node is authenticated in real time, with trust recalculated based on mission context and communication integrity.

III. ZTA in IoBT and Edge Environments

IoBT ecosystems consist of interconnected UAVs, sensors, and edge computing devices that collectively enable situational awareness on the battlefield. As these nodes often operate in contested environments, they require continuous identity verification and secure data routing. Ferretti et al. [5] proposed survivable Zero Trust systems that can self-recover during attacks. Alagappan et al. [4] showed how ZTA improves resilience in distributed power systems, principles that similarly apply to UAV networks.

In Alquwayzani and Albuali's 2024 review [6], ZTA integration into UAV networks was mapped through three levels: device-level trust, network segmentation, and behavioral analytics. They demonstrated that adaptive policy enforcement significantly reduces vulnerabilities caused by insider threats and spoofed commands.

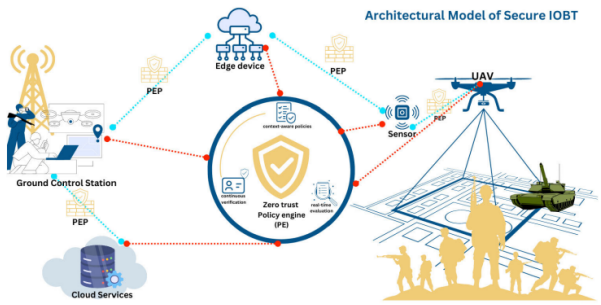

Fig. 2. Architectural model of Secure IoBT integrating UAVs under a Zero Trust framework.

Bera et al. [7] developed the ACPBS-IoT protocol, enforcing Zero Trust-based access for UAVs in battlefield operations. Blockchain-enhanced ZTA models [8] provide immutable records of authentication events, preventing replay and impersonation attacks.

IV. Machine Learning Integration in ZTA Systems

Machine Learning (ML) strengthens ZTA by enabling real-time anomaly detection and adaptive decision-making. Nour [9] introduced an ML-based intrusion detection system for Zero Trust IoT networks, while Ramezanpour and Jagannath [10] developed an intelligent ZTA (i-ZTA) capable of context-aware trust scoring.

Kurunathan et al. [11] reviewed ML's impact on UAV operations and noted that algorithms such as Random Forest, XGBoost, and SVMs effectively detect deviations in network behavior. Alquwayzani and Albuali [6] found that ML-based ZTA models in UAV networks improved detection accuracy to 99.8% while maintaining operational speed. However, they also highlighted computational trade-offs, noting that continuous ML inference can strain UAV resources and energy consumption.

V. Comparative Insights and Research Gaps

Although the literature validates ZTA's value in UAV security, certain challenges remain:

- **Computational Constraints:** Continuous verification demands high processing power.
- **Latency and Scalability:** Applying ZTA across UAV swarms can introduce delays.
- **Standardization:** Lack of common protocols for defense-grade IoBT integration.
- **Empirical Validation:** Few real-world deployments exist due to classified military environments.

Future directions include energy-efficient trust computation, federated ML frameworks for distributed UAVs, and formal standardization of military ZTA policies. Alquwayzani and Albuali's findings [6] recommend adopting dynamic trust models and lightweight cryptographic systems tailored for IoBT.

VI. Conclusion

Zero Trust Architecture, supported by Machine Learning, represents the next frontier of UAV cybersecurity. The combination provides robust, adaptive, and self-learning defense mechanisms that protect UAV networks in real time. Research over the past decade confirms that ZTA reduces the risk of insider and external attacks while enhancing situational awareness and operational integrity. The 2024 IEEE Access study by Alquwayzani and Albuali [6] underscores that future defense systems must adopt ZTA as a core security framework within IoBT. Integrating ML-based analytics, decentralized access control, and context-driven trust scoring will be critical for achieving secure, autonomous UAV operations.

References

[1] J. Kindervag, "Build security into your network's DNA: The zero trust network architecture," Forrester Research Report, 2010. [2] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero trust architecture," *NIST Special Publication 800-207*, 2020. [3] A. Decusatis, P. Liengtiraphan, M. Morales, and R. Chothia, "Zero trust access control for cloud networks," *IEEE Cloud Computing*, vol. 3, no. 5, pp. 44–53, 2016. [4] P. Phiayura and S. Teerakanok, "A comprehensive framework for migrating to zero trust architecture," *IEEE Access*, vol. 11, pp. 19487–19511, 2023. [5] L. Ferretti, F. Magnanini, M. Andreolini, and M. Colajanni, "Survivable zero trust for cloud computing environments," *Computers & Security*, vol. 110, p. 102419, 2021. [6] A. A. Alquwayzani and A. A. Albuali, "A Systematic Literature Review of Zero Trust Architecture for Military UAV Security Systems," *IEEE Access*, vol. 12, pp. 176033–176051, Dec. 2024, doi: 10.1109/ACCESS.2024.3503587. [7] P. Bera, A. Majumdar, and A. Das, "ACPBS-IoT: An access control protocol for battlefield UAV operations in IoT environments," *IEEE Access*, vol. 11, pp.

147232–147244, 2023. [8] S. M. Awan et al., “A blockchain-inspired attribute-based zero-trust access control model for IoT,” *Information*, vol. 14, no. 2, p. 129, 2023. [9] M. Nour, “An ML-based intrusion detection system for zero trust in 5G/IoT environments,” *IEEE Internet of Things Journal*, vol. 9, no. 12, pp. 10834–10845, 2022. [10] A. Ramezanpour and J. Jagannath, “Intelligent zero trust architecture (i-ZTA) for secure 5G/6G military networks,” *Proc. IEEE MILCOM*, 2023. [11] H. Kurunathan et al., “Machine learning-aided operations and communications of unmanned aerial vehicles: A contemporary survey,” *IEEE Commun. Surveys & Tutorials*, vol. 26, no. 1, pp. 496–533, 2023. [12] S. Waharte and N. Trigoni, “Supporting search and rescue operations with UAVs,” in *Proc. Int. Conf. Emerging Security Technologies*, 2010, pp. 142–147. [13] R. L. Finn and D. Wright, “Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications,” *Computer Law & Security Review*, vol. 28, no. 2, pp. 184–194, 2012. [14] S. Keshavarz, M. Ramezanpour, and J. Jagannath, “Cybersecurity challenges and threats to UAVs in defense environments,” *IEEE Access*, vol. 9, pp. 125891–125905, 2021. [15] A. Albuali, T. Mengistu, and D. Che, “ZTIMM: A zero-trust-based identity management model for volunteer cloud computing,” in *Cloud Computing—CLOUD 2020*, Springer, 2020, pp. 287–294.