SCIENCE CHINA
Information Sciences

• LETTER •

May 2024, Vol. 67, Iss. 5, 159103:1–159103:2
https://doi.org/10.1007/s11432-023-3984-7

CoDetect: cooperative anomaly detection with privacy protection towards UAV swarm

Teng LI[1*], Weiguo LIN[1], Ruichen MA[1], Zhuo MA[1], Yulong SHEN[2] & Jianfeng MA[1]

[1]*School of Cyber Engineering, Xidian University, Shaanxi* 710071*, China;*
[2]*School of Computer Science and Technology, Xidian University, Shaanxi* 710071*, China*

Received 1 July 2023/Revised 12 January 2024/Accepted 19 March 2024/Published online 22 April 2024

As mission scenarios grow more complex, the role of a single unmanned aerial vehicle (UAV) is limited. The UAV swarm, surpassing the single UAV, dynamically establishes temporary communication networks, ensuring high transmission rates and expansive communication coverage [1]. Unlike a single UAV, a swarm faces increased security risks, requiring specific capabilities. (1) Anomalies detection. Heterogeneous interference factors in unknown environments make the hardware and flight control system susceptible to failure. To ensure the seamless progression of missions, the swarm must possess anomaly detection capabilities. (2) Swarm intelligence collaboration. Heterogeneous interference factors in unknown environments make the hardware and flight control system susceptible to failure. Ensuring the seamless progression of missions requires the swarm to possess anomaly detection capabilities. (3) Data privacy preserving. Communication and data transmission within the swarm occur through a wireless network, vulnerable to invasion by malicious nodes. The data transmission process also introduces the risk of privacy disclosure during missions, demanding the implementation of a robust data protection scheme [2]. Therefore, it is crucial for the swarm to ensure data privacy while facilitating self-anomaly detection. However, achieving this balance between self-anomaly detection and privacy protection is challenging. Collaborative efforts among drones are necessary for effective anomaly identification and resolution. During this process, data exchange is inevitable, introducing the potential risk of information leakage within swarm networks, especially in the presence of internal malicious nodes. This leakage could raise significant concerns for personal and national security, particularly for drones carrying user identity or military mission information.

In this study, we propose a collaborative anomaly detection framework with integrated privacy protection to address the mentioned issues. It aims to balance self-detection during the dynamic adjustment of swarm structure with individual drone privacy. To overcome challenges, we introduce the following innovations.

(1) Efficient swarm dynamic authentication. The swarm dynamically adjusts its network structure for mission scenarios. To prevent infiltration of malicious nodes during recombination, it is necessary to conduct preliminary screening of legitimate nodes [3]. Typical schemes use real-time session keys from ground control station (GCS) for dynamic authentication. Those employing key sharing also rely on GCS resources for key management, hindering efficient authentication in distant missions. Our proposed membership authentication ensures UAV node legitimacy and anonymity amidst internal malicious nodes. Specifically, to realize mutual authentication between UAVs, GCS must make some agreement during UAV registration, which can help the UAV complete the detection of UAV identity legitimacy when it is far away from the GCS. It provides a unique identity id_i and its key chain KC_i extracted from the Merkle tree for Node_i. The key chain is used to verify the legal identity of each UAV. When the swarm conducts cooperative detection through mutual communication, any UAV in the swarm is able to initiate the information of the inquiry data header, and all nodes complete the collection of basic data at the same time.

(2) Decentralized swarm self-detection. After authenticating legitimate nodes, it is impossible to completely eliminate the risk of legitimate drones being invaded and controlled by adversaries. These drones may disrupt the mission by deviating from norms, resulting in Byzantine failures, and these anomalous nodes are referred to as Byzantine nodes. Detecting such abnormal nodes and taking measures to limit their behaviors are necessary. Some schemes introduce a trusted third party as an intermediary [4]. However, seeking a trusted third party for each mission is impractical due to unknown mission scenarios. Therefore, we propose a collaborative anomaly detection scheme based on a consensus algorithm, identifying and addressing Byzantine nodes through self-proof and challenge mechanisms. Initially, the GCS generates a Merkle tree for the entire swarm, with each leaf node storing a GCS-verified legal UAV. Once the UAV swarm is established, the scheme trains an anomaly detection model to identify hardware or system anomalies in individual UAVs. Utilizing GCS-authenticated UAV flight data as training data, during missions, individual UAVs use the trained model to assess their states. In cases of a negative judgment, indicating abnormalities, the affected UAV follows the temporary-departure protocol to exit the swarm network. For malicious nodes concealing negative judgments, the framework incorporates a cooperative de-

* Corresponding author (email: tengli@xidian.edu.cn)

tection module and consensus mechanism to address this issue. In the inquiry phase, a legal swarm node initiates regular queries. Subsequently, UAV B scrutinizes UAV A upon receiving self-prove messages from various UAVs in the self-prove phase. If UAV A is deemed abnormal, it enters the challenge phase, transmitting pertinent evidence to other UAVs. Other nodes assess whether UAV A is a Byzantine failure node through calculations. During the commit stage, the swarm achieves consensus and enforces appropriate punitive measures for the Byzantine node.

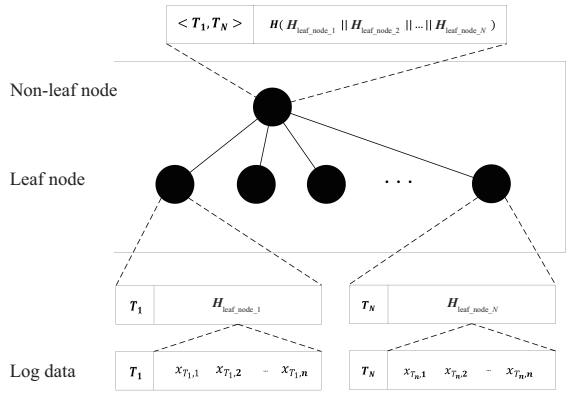

Figure 1 Unit of Merkle tree.

(3) Privacy preserving in self-detection. During authentication and cooperative anomaly detection, UAVs communicate via a vulnerable wireless network. External eavesdroppers and internal malicious nodes necessitate the swarm to safeguard privacy and sensitive data. Some schemes rely on random key generation and secure key storage, ensuring the difficulty for external attackers to eavesdrop or tamper with communication data [5]. However, these schemes fall short in addressing internal malicious nodes during the self-detection process. To tackle this issue, we introduce a privacy data protection scheme based on the Merkle tree, covering both internal and external malicious nodes. Instances of data tampering by malicious nodes trigger feedback to the cooperative detection framework for appropriate processing. Our verification occurs in the self-prove phase of the consensus process. First, the sensor data is arranged in chronological order, and each data group will contain a specific unit called the timestamp T_i. Each unit in the Merkle tree $H_{\text{leaf\_node\_}i}$ will be generated in binary $\{T_i, H_{\text{leaf\_node\_}i}\}$. To ensure efficient processing of data blocks, we branch in periods and build a Merkle tree in the form of a multi-branch tree which is shown as Figure 1. The leaf node of the tree is the log data at each time point, the non-leaf node is the log data at each period, and the period is the time range of its first and last child nodes.

Environment setup. We implement our framework using Java, Python, and C++ programming languages. Additionally, we utilize the open-source ALFA dataset for anomaly detection. This dataset showcases various types of faults on the UAV control surface for fault detection and isolation (FDI) and anomaly detection (AD) research. We also acquire datasets from a real UAV entity equipped with a Pixhack V3 flight controller and UBLOX NEO-M8N GPS module. Utilizing the MAVLink protocol, we obtain attitude angle data by writing a program through the Raspberry Pi 4B. The data from 16000 sampling points are used to detect two anomalies: drift failure and step failure.

Exploratory experimental evaluation. We calculate the runtime of common mathematical and cryptographic operations, including XOR, PRNG, hash (SHA-1, consistent with other schemes for comparative evaluation), HMAC (SHA-1), and concatenation. We assess computational and communication consumption during authentication. Next, we analyze the authentication algorithm's security using high-level protocol specification language (HLPSL). We instantiate roles and create channels to simulate message exchange. Safety objectives are defined to analyze safety aspects. Finally, we simulate the consensus process and evaluate our framework's performance in two aspects: (1) performance comparison with existing consensus schemes and (2) different attack strategies from Byzantine nodes. Reproducing the consensus processes of Tendermint and EPBFT schemes and comparing them with ours, we verify a 40% improvement in the efficiency of the consensus algorithm under the same timeout, iteration times, node proportion, and swarm size.

Conclusion. In this study, we introduce a novel framework for cooperative anomaly detection in UAV swarms. The scheme integrates an anomaly detection model, consensus algorithm, and lightweight communication authentication algorithm. Tailored to address external eavesdroppers and malicious Byzantine nodes, it effectively manages and mitigates Byzantine behavior while safeguarding internal communication. Simultaneously, the framework incorporates a lightweight authentication scheme designed to verify node legitimacy and enhance swarm scalability. Compared with existing schemes, it demonstrates competitiveness in communication, computing costs, and consensus algorithm efficiency. Consequently, we assert that the proposed framework is effective and feasible for swarm anomaly detection. However, in more intricate scenarios, there is room for further refinement. Therefore, delineating attack dictionaries and formulating defense strategies emerge as noteworthy future directions for this work.

Acknowledgements This work was funded by National Key Research and Development Program of China (Grant No. 2023YFB2904000), National Natural Science Foundation of China (Grant Nos. 62272370, U21A20464), Fundamental Research Funds for the Central Universities (Grant No. QTZX23071), Young Elite Scientists Sponsorship Program by CAST (Grant No. 2022QNRC001), China 111 Project (Grant No. B16037), and Qinchuangyuan Scientist + Engineer Team Program of Shaanxi (Grant No. 2024QCY-KXJ-149).

References

1 Li T, Zhang J, Obaidat M S, et al. Energy-efficient and secure communication toward UAV networks. IEEE Internet Things J, 2022, 9: 10061–10076
2 Zhang S, Ray S, Lu R, et al. Towards efficient and privacy-preserving interval skyline queries over time series data. IEEE Trans Dependable Secure Comput, 2023, 20: 1348–1363
3 Khalid H, Hashim S J, Hashim F, et al. HOOPOE: high performance and efficient anonymous handover authentication protocol for flying out of zone UAVs. IEEE Trans Veh Technol, 2023, 72: 10906–10920
4 Kim S, Kim B J. On the Byzantine-fault-tolerant consensus in blockchain built on Internet of vehicles. In: Proceedings of International Conference on Electronics, Information, and Communication (ICEIC), 2022. 1–4
5 Wang H, Fan K, Yu C, et al. LSPSS: constructing lightweight and secure scheme for private data storage and sharing in aerial computing. IEEE Trans Serv Comput, 2024. doi: 10.1109/TSC.2023.3333347