



Cybersecurity in UAVs: An Intrusion Detection System Using UAVCAN and Deep Reinforcement Learning

Md Rezanur Islam¹, Kamronbek Yusupov¹, Ibrokhim Muminov², Mahdi Sahlabadi³,
and Kangbin Yim³(✉)

¹ Department of Software Convergence, Soonchunhyang University, Asan, Korea
{arupreza, yuskamron}@sch.ac.kr

² Department of Computer Software Engineering, Soonchunhyang University, Asan, Korea
theibrokhim@sch.ac.kr

³ Department of Information Security Engineering, Soonchunhyang University, Asan, Korea
sahlabadi@ieee.org, yim@sch.ac.kr

Abstract. Unmanned Aerial Vehicles (UAVs) are increasingly used in military operations, disaster management, and urban planning. Nevertheless, its susceptibility to cyber-attacks has generated substantial cybersecurity apprehensions. The UAVCAN protocol, widely employed for UAV communication, is vulnerable to sophisticated threats such as message spoofing, replay, and Denial of Service (DoS) assaults. This research presents an Intrusion Detection System (IDS) that uses deep reinforcement learning to safeguard UAVCAN networks against cyber threats. The suggested IDS utilizes artificial intelligence (AI) techniques to safeguard against emerging attack patterns. These systems provide robust defense mechanisms specifically designed to address the distinct problems UAVCAN offers. The system's detection accuracy has been extensively validated through experiments, showing remarkable performance in identifying various attack situations. This dramatically improves the cybersecurity and resilience of UAV communication networks. This study focuses on specific IDS requirements in UAVs. This solution presented in the study makes a valuable contribution to the field of UAV cybersecurity by effectively and promptly addressing sophisticated cyber-attacks.

1 Introduction

Unmanned Aerial Vehicles (UAVs) are becoming increasingly crucial in a wide range of applications, such as military operations, agricultural monitoring, disaster management, and urban planning [1]. Nevertheless, UAVs are now more susceptible to cyberattacks due to their increased use [2]. Consequently, there is a demand for strong security protocols to safeguard these systems. UAVCAN is a lightweight and open-source communication protocol specifically created for vehicle networks like UAVs. Its purpose is to provide dependable and instantaneous data exchange [3]. Although UAVCAN has its benefits, its intricate nature and deployment in safety-critical settings render it vulnerable to sophisticated cyber threats, including message spoofing, replay assaults, and Denial of Service (DoS) attacks.

The current IDS developed for the CAN [4, 5] primarily targets the automotive and heavy-duty vehicle sectors [6, 7]. They do not use UAVCAN, a protocol designed specifically for UAVs. UAVCAN operates at the application layer, in contrast to classical CAN, which functions at the data link layer. It allows for immediate, direct contact between individuals with a high level of dependability and a redundant modular structure [3]. Existing IDS are insufficient to deal with the unique security challenges presented by this discrepancy, as well as the use of UAVCAN in safety-critical scenarios. Therefore, we must specifically tailor a dedicated IDS for UAVCAN. The integration of AI into UAV security, primarily through machine learning (ML) and deep learning (DL), offers promising solutions. Recent advancements in AI-based IDS, specifically those utilizing RL, have shown potential in effectively identifying and minimizing various types of cyber threats. As a result, these systems enhance the security and resilience of UAV communication networks.

UAVCAN utilizes a Data Structure Description Language (DSDL) to precisely specify intricate data types and guarantee data integrity by means of CRC verification [3]. The UAV network bus maintains UAVCAN v0, whereas Cyphal has developed UAVCAN v1. Figures 1(a), 1(b), and 1(c) illustrate the three primary categories of UAVCAN ID frames, each fulfilling specific objectives [3]. The UAVCAN Message Frame is the designated frame for transferring orders or data from a node with an allocated ID, making it appropriate for a wide range of communication duties. Nodes that do not have an assigned ID use the UAVCAN Anonymous Message Frame. Generally, nodes use this during dynamic ID allocation or for broadcasting messages [8], where the sender's ID is not necessary. These frames have limited utility because they lack a source ID. These frames use distinct fields, such as discriminator, to identify messages. Specifically designed to facilitate bidirectional communication between nodes, the UAVCAN Service Frame enables service requests and responses. This is especially important when querying sensor data or delivering control commands is required. CAN and UAVCAN exhibit notable disparities in terms of their functioning and capabilities. The CAN, which operates at the data link layer, provides fundamental frame structures, error detection, and peer-to-peer communication. People commonly use simple, hierarchical networks [9]. There are advanced features in UAVCAN, such as advanced data structures using DSDL, multi-frame transmissions, and a peer-to-peer network without a central bus master [3]. It operates at the application layer. While the CAN has a maximum restriction of 8 bytes per frame, the UAVCAN allows for greater data transmissions [3]. This makes UAVCAN well-suited for real-time, high-reliability systems such as UAVs and robotics. Figure 1 illustrates the architectural differences between UAVCAN and CAN identifiers, highlighting the structural variations in their data transmission techniques. UAVCAN surpasses CAN in terms of its increased capabilities to manage intricate data types and longer frames, making it more suitable for complicated UAV applications. Although UAVCAN has made significant progress, its intricate nature and involvement in safety-critical systems make it vulnerable to cybersecurity risks that conventional CAN-based IDS may not adequately mitigate. It is essential to have a specialized IDS that is capable of managing the advanced features of UAVCAN and identifying complex assaults, such as message spoofing and replay attacks. This is necessary to ensure the security and dependability of systems that rely on this protocol.

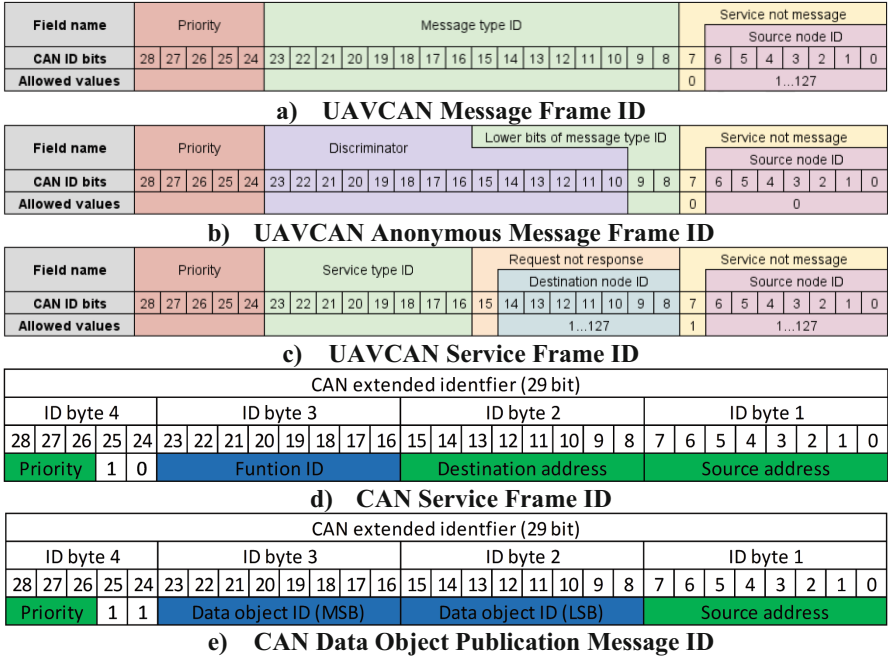


Fig. 1. Comparative layout between UAVCAN and CAN on Identifier [10, 11]

This study addresses a gap in knowledge by introducing a sophisticated IDS that utilizes deep reinforcement learning. We specifically designed the IDS to meet UAVCAN's unique security requirements. This system employs sophisticated artificial intelligence approaches to adaptively safeguard against evolving threat environments, offering a robust defense against intricate cyber-attacks aimed at unmanned aerial vehicle communication networks. This technique improves UAV system security and addresses the unique issues presented by the UAVCAN protocol.

2 Related Work

Recent years have seen major developments in the field of intrusion detection for UAVs, with a particular emphasis on the CAN bus protocol. Numerous studies have proposed various protection strategies to counteract cyberattacks. These studies have investigated various methodologies, including machine learning and deep learning approaches, to improve the security of UAV communication networks.

A significant addition in this field is the study [12], which presented a Dynamic Intrusion Detection Framework (DIDF) specifically tailored for the UAVCAN protocol. This system uses a Long Short-Term Memory (LSTM) neural network to detect and categorize attacks such as flooding, fuzzy, and replay attacks, which exploit flaws in the CAN bus protocol. The LSTM model analyzes important characteristics such as timestamps, CAN IDs, and data payloads, resulting in a detection accuracy of 99.73%.

Nevertheless, the study acknowledges the limitation of concentrating on a specific group of attacks, indicating the need for additional research to tackle more intricate and diverse attack situations.

A major paper [13] introduced a new model, known as a diverse ensemble model. This model uses Shapley Additive Explanations (SHAP) to find different types of cyberattacks on UAVCAN, such as DoS, spoofing, and replay attacks. This model combines Long Short-Term Memory (LSTM) and decision trees to assess payload data. SHAP values enhance interpretability by emphasizing important traits that are suggestive of an assault. The ensemble model demonstrated a high level of effectiveness in detecting various attack types, achieving an accuracy rate of around 97%.

A study by [14] focused on developing an exhaustive distributed intrusion detection system (E-DIDS) specifically for UAVs. This system allocates the intrusion detection tasks across numerous networked IDS units inside the UAV network. This strategy not only improves the accuracy of detection but also decreases the complexity of the system. The E-DIDS system analyzes data from flight records, sensors, and communication protocols to detect aberrant behaviors with a precision rate of 98.6%. Nevertheless, the paper acknowledges the possible requirement for additional comprehensive training data to tackle the varied setups observed in UAV operations.

The following study demonstrates the continuous efforts to improve the security of UAVCAN and associated protocols by utilizing modern intrusion detection systems. The models we have proposed, especially those that employ deep reinforcement learning approaches, have attained impressive levels of accuracy in detecting, highlighting their potential efficacy in practical scenarios. Nevertheless, these models also emphasize the difficulties in safeguarding against a wider array of attack categories and varied operational situations. It is essential to tackle these difficulties in order to make future progress in UAV cybersecurity. This establishes the foundation for future investigation and innovation in order to provide stronger security solutions for UAV communication networks.

3 Feature Extraction and Model Specification

3.1 Feature Extraction

Feature extraction is crucial in cybersecurity to enhance system efficiency. Adding irrelevant features can cause a rise in both the rate of false positive outcomes and the amount of processing resources needed. However, opting for only the most crucial and relevant components decreases the intricacy of the system and the processing resources needed. Under the UAVCAN framework, the system typically generates data that adheres to predetermined boundaries and conforms to specific patterns. Nevertheless, when a malicious entity carries out an illegal intrusion, as demonstrated in this research by executing DoS, fuzz, and replay attacks at varying frequencies, it disturbs regular patterns, particularly in the CAN ID sequence and time intervals, as depicted in Fig. 2. The sequence of CAN IDs and the intervals between them, as shown in Fig. 1, provide unequivocal evidence of this. Usually, the system exhibits a regular and repetitive pattern. However, in the event of an intrusion, the attacker's manipulation of UAVCAN IDs completely interrupts this regularity, resulting in disruptions to both the order and timing of the

IDs. As a result, the most persuasive characteristic of IDS in UAVCAN is its ability to monitor ID sequences and time intervals between them. This concept provides a reliable approach to identify and mitigate potential security vulnerabilities.

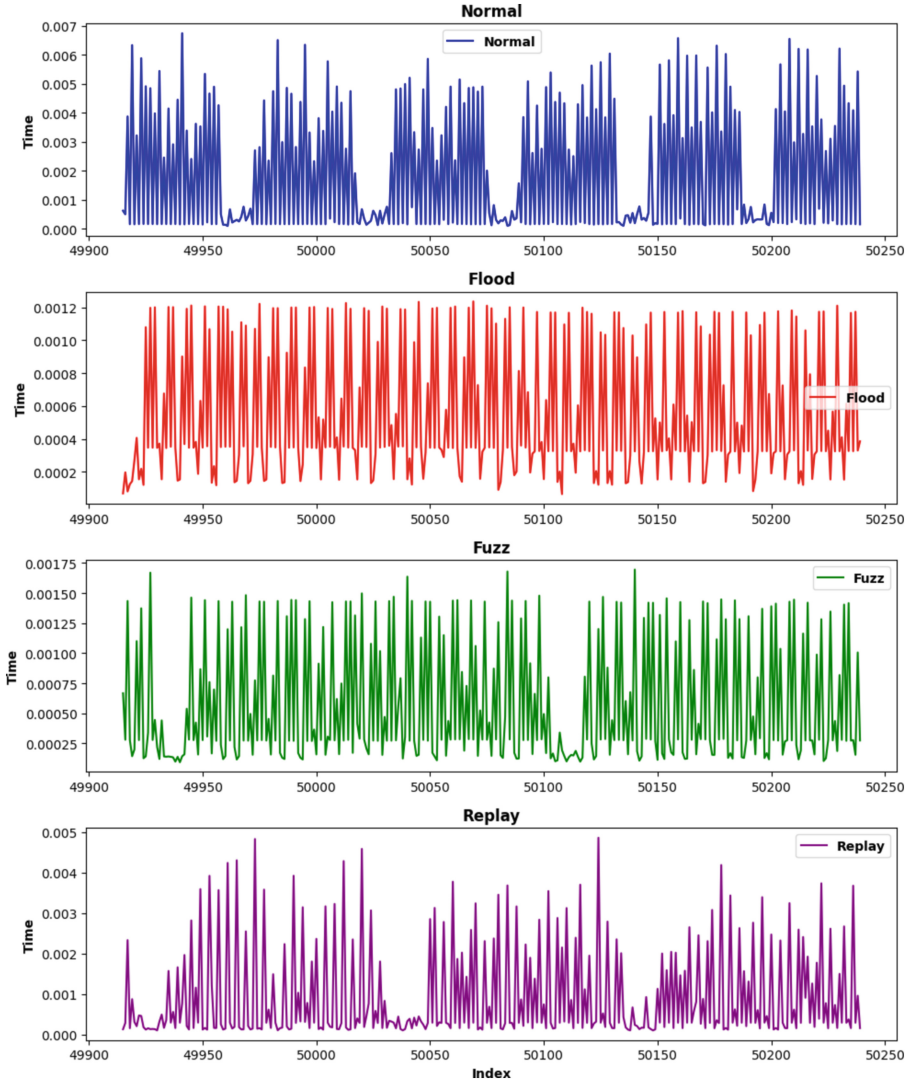


Fig. 2. Time interval analysis on UAVCAN

3.2 Model Specification

The model employs a reinforcement learning framework, leveraging an experience replay buffer to preserve and sample previous interactions. During the training process, the

agent actively investigates the environment, gathering valuable information such as the current state, the action taken, the reward received, the resulting next state, and whether the episode has ended. The model can learn from different and uncorrelated data kept in the buffer, which improves stability and performance. The Bellman equation revises the Q-values by incorporating anticipated future rewards into the estimates. Using the mean squared error (MSE) loss function and an Adam optimizer, the training process tries to narrow the gap between the predicted and target Q-values. In order to achieve a balance between exploration and exploitation, the model employs an epsilon-greedy strategy. Epsilon undergoes deterioration over time, transitioning from an exploratory state to an exploitative state. The target network regularly adjusts the model's weights to reduce variability and establish a stable learning process. This iterative process persists until the agent acquires an optimal policy that maximizes rewards within the given environment.

In order to estimate the Q-value function, we designed the Q-Network model as a feedforward neural network. The Q-value function is critical for decision-making in reinforcement learning. The architecture and hyperparameters outlined in Table 2 start with an input layer that handles the current state of the environment. We represent this state as a 2D array with dimensions of (10, 2), which we then flatten into a 20-dimensional vector. The network then feeds the input into two completely connected layers, each containing 64 neurons. A series of dense layers transforms the input data into higher-level features, which the network then uses to forecast Q-values. The hidden layers use the ReLU activation function to create non-linearity, which enables the network to capture intricate patterns and correlations in the input. The output layer comprises two neurons, each representing a potential action that the agent can execute, indicating a binary decision-making process. The function of these neurons is to generate Q-values, which are estimates of the predicted total reward for each possible action. Because the model does not have an activation function in the output layer, it can generate a wide range of Q-values, which is critical for making precise decisions even when negative values are involved. This design efficiently assigns states to Q-values, allowing the agent to choose behaviors that optimize its anticipated rewards through training and experience.

4 Result Evaluation and Discussion

4.1 Result Evaluation

We evaluated the model's effectiveness in identifying instances as "Attack" or "Attack Free" using a range of metrics and visualizations presented in Fig. 3, and Table 1. The classification report demonstrates excellent performance, with precision, recall, and F1 scores of 0.97 for the "Attack Free" category and 0.93 to 0.94 for the "Attack" category. Additionally, the classification has a total accuracy of 0.96. The confusion matrix provides more evidence to support these findings, showing that 96.93% of occurrences labeled "Attack Free" and 93.93% of instances labeled "Attack" were accurately classified, with only a few misclassifications. In addition, the ROC curve, with an AUC of 0.99, demonstrates the model's exceptional capacity to differentiate between the two classes. These measures collectively validate the model's excellent efficacy and reliability in classification tasks.

Table 1. Classification Report and Performance Metrics

Class	Precision	Recall	F1-Score	Support
Attack Free	0.97	0.97	0.97	456
Attack	0.93	0.94	0.94	214
Accuracy	0.96			
Macro Avg	0.95	0.95	0.96	670
Weighted Avg	0.96	0.96	0.96	670

Table 2. Q-Network Hyperparameters and Neural Network Architecture

Hyperparameter/Layer	Value/Details
Batch_size	32
Gamma	0.99
Epsilon_start	1.0
Epsilon_end	0.1
Epsilon_decay	0.995
Learning_rate	0.001
Memory_size	10000
Targer_update	10
Num_episodes	1000
Neural Network Layers	Details
Input Layer	Input shape: (10, 2)
Dense Layer 1	Input: 20, Output: 64
Activation 1	ReLu
Dense Layer 2	Input: 64, Output: 64
Activation 2	ReLu
Output Layer	Input: 64, Output: 2

4.2 Discussion

The study demonstrates the efficacy of deep reinforcement learning in enhancing the security of UAV communication networks, particularly those utilizing the UAVCAN protocol. The proposed IDS successfully detects and reliably differentiates various forms of assault from regular operating activity, as demonstrated by the assessment metrics. The model demonstrates the ability to acquire knowledge and defend against several types of attack scenarios, including DoS, fuzz, and replay attacks. This emphasizes the adaptability of reinforcement learning in cybersecurity.

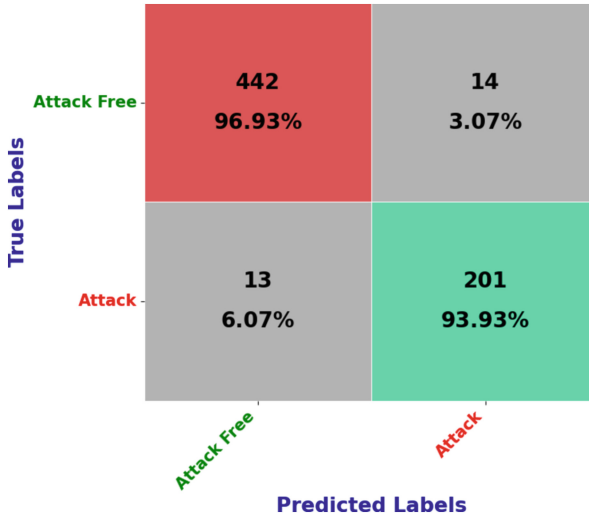


Fig. 3. Confusion Matrix in the Classification Report for Intrusion Detection

While this work has demonstrated some achievements, future research must address the significant obstacles. The IDS underwent extensive testing utilizing testbed data, which, although valuable, must accurately represent the intricacies of real-world events. In order to obtain more reliable results, it is critical to validate the IDS against real-world data in various settings. UAVs have different duties and operational contexts, so a more diverse dataset is required in order to design a dependable IDS. To make sure that the IDS can correctly spot possible threats in a lot of different real-life situations, it is important to combine data from different kinds of UAVs and operational settings. This emphasizes the importance of having diverse end datasets in order to improve the strength and usefulness of the IDS in real-world applications.

5 Conclusion

This study aims to improve the security of UAV communication networks by developing an IDS based on deep reinforcement learning using the UAVCAN protocol. The suggested IDS effectively detects and mitigates many sophisticated cyber-attacks, such as message spoofing, replay attacks, and DoS attacks. It has a remarkable degree of precision in identifying potential dangers. This research makes a substantial contribution to the field of UAV cybersecurity by explicitly addressing the unique challenges posed by UAVCAN. Nevertheless, further investigation is necessary to validate the IDS by utilizing actual data from real-world situations and testing it in different operational settings. This will ensure that the IDS remains robust and effective in diverse UAV environments. The study lays the groundwork for future research that seeks to develop more comprehensive and resilient cybersecurity frameworks for UAV systems.

Acknowledgments. This research was supported by the MSIT(Ministry of Science and ICT), Korea, under the Convergence security core talent training business support program(IITP-2024-2710008611) supervised by the IITP(Institute for Information & Communications Technology Planning & Evaluation).

References

1. Mohsan, S.A.H., et al.: Towards the unmanned aerial vehicles (UAVs): a comprehensive review. *Drones* **6**(6), 147 (2022). <https://doi.org/10.3390/drones6060147>
2. Tilili, F., Ayed, S., Fourati, L.C.: Advancing UAV security with artificial intelligence: a comprehensive survey of techniques and future directions. *Internet of Things* **27**, 101281 (2024). <https://doi.org/10.1016/j.iot.2024.101281>
3. Kim, D., et al.: Uavcan dataset description. arXiv preprint [arXiv:2212.09268](https://arxiv.org/abs/2212.09268) (2022)
4. Islam, M.R., et al.: CF-AIDS: comprehensive frequency-agnostic intrusion detection system on in-vehicle network. *IEEE Access* **12**, 13971–13985 (2024)
5. Kamronbek, Y., et al.: Time series mean normalization for enhanced feature extraction in in-vehicle network intrusion detection system. In: Barolli, L. (ed.) *Advances on Broad-Band and Wireless Computing, Communication and Applications: Proceedings of the 18th International Conference on Broad-Band and Wireless Computing, Communication and Applications (BWCCA-2023)*, pp. 302–311. Springer Nature Switzerland, Cham (2024). https://doi.org/10.1007/978-3-031-46784-4_29
6. Yusupov, K., et al.: Security assessment of in-vehicle network intrusion detection in real-life scenarios. In: SPTM, AIS, SOENG, AMLA, NLPA, IPPR, CSIT – 2024, pp. 01–10. CS & IT – CSCP 2024. <https://doi.org/10.5121/csit.2024.141101>
7. Thien-Nu Hoang, M., Islam, R., Yim, K., Kim, D.: CANPerFL: improve in-vehicle intrusion detection performance by sharing knowledge. *Applied Sciences* **13**(11), 6369 (2023). <https://doi.org/10.3390/app13116369>
8. Cui, J., et al.: Lightweight encryption and authentication for controller area network of autonomous vehicles. *IEEE Trans. Vehicular Technol.* **72**(11), 14756–14770 (2023)
9. CAN Specification. Bosch. Robert Bosch GmbH. Postfach **50**,15 (1991)
10. ThingSet. Thingset can bus specification v0.2 - service message (2024). Accessed 13 Aug 2024
11. UAVCAN: Can bus transport layer -uavcan specification (2024). Accessed 13 Aug 2024
12. Tilili, F., Ayed, S., Chaari Fourati, L.: Dynamic intrusion detection framework for UAVCAN protocol using AI. In: *Proceedings of the 18th International Conference on Availability, Reliability and Security* (2023)
13. Hong, Y.-W., Yoo, D.-Y.: Multiple intrusion detection using shapley additive explanations and a heterogeneous ensemble model in an unmanned aerial vehicle's controller area network. *Appl. Sci.* **14**(13), 5487 (2024)
14. Tilili, F., Ayed, S., Fourati, L.C.: Exhaustive distributed intrusion detection system for UAVs attacks detection and security enforcement (E-DIDS). *Comput. Secur.* **142**, 103878 (2024). <https://doi.org/10.1016/j.cose.2024.103878>