Grenze International Journal of Engineering and Technology, June Issue

Energy-Aware Adaptive Federated Cyber Defense for Internet of Drones using Multi-Objective Reinforcement Learning

Praveen Kumar C[1] and Sophia S[2]
[1-2]Division of Artificial Intelligence and Machine Learning, Karunya Institute of Technology and Sciences, Coimbatore, India
Email: praveenkumarpk14307@gmail.com, sophia@karunya.edu

***Abstract*— The Internet of Drones (IoD) enables cooperative aerial applications but introduces significant cybersecurity risks due to open wireless communication, distributed coordination, and limited onboard energy resources. Existing federated learning–based security approaches emphasize privacy but lack energy-aware and adaptive defense mechanism. This paper proposes an Energy-Aware Adaptive Federated Cyber Defense (EA-AFCD) framework that integrates lightweight local intrusion detection with customized federated learning and a multi-objective reinforcement learning controller. The controller dynamically manages drone participation, aggregation frequency, and model update strategies by jointly optimizing detection accuracy, energy consumption, and communication overhead. A non-IID federated environment is simulated using a benchmark intrusion detection dataset to reflect realistic IoD conditions. Experimental results show that EA-AFCD achieves higher detection accuracy 98.5% significantly reducing energy usage and communication cost. The framework also extends network lifetime and improves learning convergence. The findings demonstrate that adaptive, energy-aware federated defense enhances scalability and practicality for real-world IoD deployments.**

***Keywords*— Internet of Drones; Federated Learning; Cybersecurity; Energy Efficiency; Intrusion Detection; Reinforcement Learning.**

I. INTRODUCTION

The rapid advancement and development of unmanned aerial vehicles have led to the growth of the Internet of Drones (IoD), whereby autonomous drones coordinate and interact with each other through wirelessly facilitated communication and distributed sensing, followed by intelligent decision-making. The development of IoD has enabled diverse applications, such as disaster response, precision farming, traffic control, border control, and smart city services [1]. However, IoD is extremely susceptible and prone to various types of cyber attacks, such as denial-of-service, spoofing attacks, data falsification, and botnet attacks, owing to its open communication nature, decentralized architecture, and resource-constrained environment, which could adversely affect safety [2].

Conventional centralized cybersecurity solutions are no longer appropriate for the changing IoD environment due to their associated communication costs, single-point failure vulnerabilities, and concerns about privacy.

Grenze ID: 01.GIJET.12.2.620_26

To mitigate the abovementioned shortcomings, the concept of a distributed intelligence approach referred to as FL has gained prominence. FL achieves the paradigm of collaborative learning without sharing the raw data among the devices [3]. FL has shown much promise in terms of the preservation of privacies and scalability in the context of large-scale deployments. Nevertheless, the adoption of traditional FL-based frameworks directly to drone networks introduces significant challenges related to energy consumption, communication cost, and adaptive cyber defense [4].

One important factor considered as a limitation in IoD is energy efficiency. Drones are battery-powered and are subject to a number of activities, such as sensing, communicating, as well as computational activities. Recent research indicates that a number of cybersecurity activities, such as learning-based intrusion detection and model training, are contributing to faster battery consumption, as indicated in a study by Chen et al. [5]. Engagement in many rounds of federated learning contributes to increased energy consumption, thereby inhibiting the battery life of the drone. Therefore, energy efficiency is considered a priority research challenge in UAVs and IoD, as indicated in a study by Li & Zhao [6].

Meanwhile, the cyber-defense approach in IoD systems might depend on static approaches, e.g., setting thresholds, aggregation periods, and client engagement strategies. This may offer some degree of convenience in implementing these solutions but may not suit evolving IoD environments marked by high mobility, divergent states of battery drain, and varying rates of attacks [7]. Using static cyber-defense strategies may not help to improve adaptability to changing environments and threats.

Currently, research has highlighted the significance of joint optimization for the security of IoD systems, which needs to optimize the precision of intrusion detection systems, communication costs, and energy costs jointly and not in isolation [8]. However, the majority of the available methods optimize only one or two objectives and do not perform optimally when employed for IoD systems in real-world scenarios. Intelligent decision schemes that optimize varied objectives in real-time are areas yet to be researched concerning the cybersecurity of federated IoD systems.

To bridge the gap, the authors of the current paper develop a framework dubbed Energy-Aware Adaptive Federated Cyber Defense (EA-AFCD) for IoD systems. The framework includes a tailored federated learning process for IoD systems, as well as the inclusion of lightweight intrusion detection for each drone. Additionally, the authors introduce a multi-objective reinforcement learning (MORL) controller for the management of the federated learning process to ensure adaptability in the cyber defense of IoD systems. The controller, moreover, optimizes the attack detection, residual energy, communication costs, and the observed attack behaviors to ensure adaptability in the cyber defense of IoD systems [9].

Within this context, it is possible to assess the viability of the suggested framework through a set of evaluations, using a benchmark intrusion detection problem and under a non-IID distribution within the simulated federated IoD system. For this purpose, some metrics concerning the resulting network, such as detection accuracy, energy consumption, convergence, and network lifetime, are considered. The key contribution

- Designing an energy-aware federated cyber defense environment geared towards IoD.
- Integration of multi-objective reinforcement learning to allow adaptation of security and learning.
- Joint optimization of intrusion detection accuracy, energy efficiency, and communication overhead.
- A comprehensive experimental validation of improved performance and extended network lifetime.

The rest of this paper is structured as follows. Section II is the review of the related literature on edge-based cardiac monitoring and Transformer models. The third section (III) gives the system architecture. Part IV describes the experimental arrangement, then results and discussion respectively. Lastly, Section V provides a conclusion of the paper and outlines future research directions.

II. LITERATURE REVIEW

The high rate of the Internet of Drones (IoD) development has opened up the potential of critical applications (disaster response, smart transportation, militarization, and smart cities) but the dynamic nature of communications and extreme resource demands of IoD systems renders it extremely vulnerable to cyber-attacks. These attacks include spoofing, denial-of-service (DoS), malware injection, data interception, and unauthorized access, which significantly affect the reliability and operational stability of IoD environments.The recent studies have thus been directed towards coming up with foolproof, scaled, and energy efficient cyber defense mechanisms of distributed drone networks. A hybrid security model proposed by Pandey et al[10] is a machine learning–based user behavior analysis with an authentication system based on cryptography, which consumes less energy but cannot provide centralized and adaptive decision-making. Survey studies conducted by Derhab[11], indicate that although the current IoD security solutions are focused on high attack detection rates,

energy-saving and dynamically evolving defense mechanisms are under explored. The study further emphasizes the necessity of intelligent and autonomous cyber defense mechanisms capable of adapting to rapidly changing drone network conditions in real time.Likewise, Aldweesh[12] surveyed the lightweight and energy-conscious authentication schemes, and observed that the majority of them are fixed and do not support dynamic network behaviour or incorporate learning-based intrusion detection. Furthermore, many lightweight authentication schemes fail to dynamically adjust security policies according to drone mobility, residual battery power, and varying attack intensities. Intrusion Detection Systems (IDS) have also attracted interest and Ajakwe et al[13] suggest a multihop intruder detector to enhance scalability and energy consumption but it is not scalable because it does not use collaborative learning and privacy preservation [14]. In large-scale IoD deployments, collaborative and privacy-aware learning mechanisms are essential for ensuring scalable and intelligent intrusion detection across distributed drone nodes.Federated learning (FL) has become a potential solution to facilitating distributed and privacy-aware intelligence in IoD, but the majority of current FL-based systems use the fixed-aggregate strategies like FedAvg[15], lacking the ability to consider different energy levels, the severity of attacks, and adaptive cyber-defense. Additionally, existing FL-based security frameworks rarely integrate reinforcement learning or multi-objective optimization strategies to support adaptive cybersecurity decision-making under dynamic IoD conditions. In general, a significant gap in the literature lies in the creation of intelligent, energy-conscious, and dynamically adaptive federated frameworks of security of IoD.

A. Research Gap

Overall, existing studies primarily focus on individual objectives such as attack detection accuracy, energy efficiency, or communication optimization independently, rather than proposing a unified cybersecurity framework capable of simultaneously balancing these conflicting requirements in real-time IoD environments. By critically examining recent literature in this area, several gaps in Internet of Drones (IoD) cybersecurity research can be identified. First, existing federated learning-based IoD security frameworks highly emphasize preserving privacy and leveraging decentralization but fail to incorporate an energy-aware system of adapting learning and cyber defense processes, which is of immense importance in battery-constrained networks like drones [10], [14]. This limitation reduces the operational lifetime and adaptability of drones operating in highly dynamic and mission-critical environments. Secondly, existing intrusion detection and authentication methodologies are largely designed around conventional static defense paradigms, such as failing to adapt to changing security levels according to available residual energies in the drones, attack severity, and varying network environments [12], [13]. As a result, these approaches cannot effectively respond to continuously evolving cyber threats and heterogeneous drone communication patterns. Lastly, existing works on optimized Internet of Drones-based security cover either the enhancement of security functionalities, power efficiency, and excellence in detection and communication overheads individually, without providing a unified approach in this regard, as proposed in recent works like [15]. Moreover, current works in this area Existing optimization-driven IoD security frameworks also fail to jointly optimize security performance, communication latency, energy consumption, and attack response efficiency within a single adaptive model.hardly incorporate real-time aspects of Internet of Drones environments, such as varying speeds and battery characteristics, which weaken existing cyber defense solutions. Therefore, there is a strong need for an intelligent, energy-aware, and adaptive federated cyber defense framework capable of dynamically optimizing cybersecurity performance while minimizing energy and communication overhead in Internet of Drones environments.

III. METHODOLOGY

The proposed methodology develops an Energy-Aware Adaptive Federated Cyber Defense Framework for the Internet of Drones. The system aims to concurrently optimize cybersecurity and energy consumption to optimize high accuracy of intrusions and maximize network longevity. Instead of sending raw data, the proposed methodology uses a customized federated learning approach, where drones engage with a lightweight model based on local observations. The traditional approach to protecting drone networks from intrusions would involve using static approaches to detect intrusions, or using a federated learning approach without considering energy levels. However, the proposed methodology incorporates a multi-objective reinforcement learning approach. The proposed methodology uses a reinforcement learning approach to dynamically control the federated learning process in real-time based on energy levels, intrusions, and communication costs. Therefore, it is different from traditional approaches for securing communications within the Internet of Drones. Unlike conventional federated cybersecurity frameworks, the proposed methodology jointly optimizes intrusion detection accuracy, residual drone energy, communication overhead, and adaptive defense response through a

unified Multi-Objective Reinforcement Learning (MORL) controller. This enables intelligent real-time cyber defense adaptation in highly dynamic IoD environments.

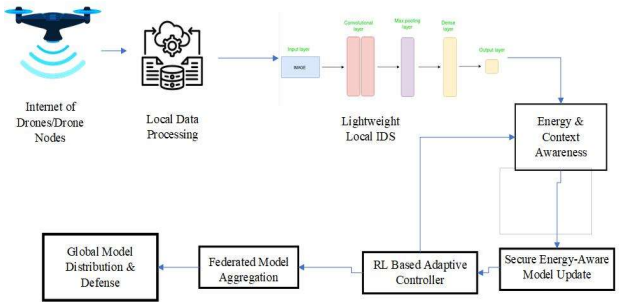

Fig 1. Proposed block Diagram

The proposed architecture consists of distributed drone nodes, lightweight local intrusion detection models, an energy-aware federated aggregation server, and a MORL-based adaptive decision controller that continuously adjusts learning and defense parameters according to network conditions.

A. Local Data Collection and Feature Representation

This ensures that computationally costly raw data processing is not done at the drone level. The extracted features are the most important statistical and temporal features. This process minimizes the processing time and the energy consumption of the system. Additionally, lightweight feature engineering reduces computational complexity and enables faster intrusion analysis suitable for resource-constrained drone platforms. Further, the compact feature representation facilitates rapid learning and inference, which is necessary in the wild cyber scenes characterized by the drone network. The drone d_ic continuously monitors the behavior of the local communication and operations. The raw data that the drone d_ic extracts are the raw data denoted by the raw data characterization.

Let the raw data that has been gathered by the drone be expressed as in eqn.(1):

$$\mathcal{D}_i = \{x_1, x_2, \ldots, x_n\} \quad (1)$$

Feature extraction is applied to transform raw data into a compact feature vector:

$$\mathrm{f}_i = \phi(\mathcal{D}_i) \quad (2)$$

where ϕ(·)represents lightweight preprocessing and feature extraction functions. The extracted features include communication frequency, packet transmission behavior, latency variations, abnormal access attempts, and energy utilization statistics for accurate intrusion characterization.

B. Lightweight Local Intrusion Detection Model

Also, local intrusion detection enables drones to react to potential threats instantly rather than awaiting a decision from a central entity. The usage of lightweight models makes the approach feasible for drones, given that they possess limited CPU and memory resources. Furthermore, local learning is helpful in achieving robustness as it enables each drone to adapt to its specific environment and risk exposure. Each drone is associated uniquely with a lightweight model of IDS, given by the model M_i parameterized by parameters θ_i. The model in consideration is predictive with regards to normal/malicious behaviors. The localized IDS framework improves response latency by enabling drones to identify suspicious activities independently before federated aggregation occurs. The local prediction is given by eqn. (3):

$$\hat{y}_i = M_i(\mathbf{f}_i; \theta_i) \quad (3)$$

The training loss at drone di is defined as in enq. (4)

$$\mathcal{L}_i(\theta_i) = \frac{1}{|\mathcal{D}_i|} \sum_{j=1}^{|\mathcal{D}_i|} \ell(y_j, \hat{y}_j) \quad (4)$$

where $l(\cdot)$is a classification loss function

The local optimization process minimizes classification error while maintaining low computational overhead to preserve drone battery life.

C. Energy Consumption Modeling at Drone Level

Precise energy modeling forms the basis of informed adaptation decisions. Explicit quantification of the energy cost of computation and communication allows the framework to prevent unnecessary participation of low-energy drones. This modeling also provides the balancing of security effectiveness with operational longevity. The energy-aware framework dynamically prevents low-energy drones from excessive communication participation, thereby improving the sustainability of the overall IoD network. The total energy consumption of drone modeled as in eqn. (5).

$$E_i = E_i^{\text{comp}} + E_i^{\text{comm}} + E_i^{\text{idle}} \quad (5)$$

Where E_i^{comp}: Energy for local computation, E_i^{comm}: Energy for communication, E_i^{idle}: Baseline operational energy. Communication energy is estimated as in eqn. (6).

$$E_i^{\text{comm}} = P_i \times T_i \quad (6)$$

where P_i is transmission power and T_i is transmission time.

D. Energy-Aware Federated Learning Update

Selective participation ensures that only drones that have the necessary energy left and a stable connection are able to contribute to the process. This eliminates redundant communication attempts that might otherwise cause these drones to be drained of their energy. With the weighted aggregation approach, fairness persists while convergence is guaranteed to happen. Fig 2 shows the federated learning schema.

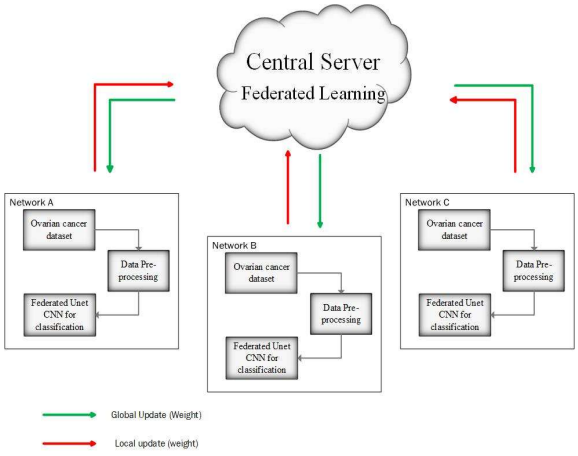

Fig 2. Federated Learning

Rather than sending data, drones send their local model updates as in eqn. (7).

$$\Delta\theta_i = \theta_i^{(t)} - \theta^{(t-1)} \quad (7)$$

Only a subset $\mathcal{S}_t \subseteq \mathcal{N}$ of drones participates in round t, selected based on energy and context. The global model update is computed as:

$$\theta^{(t)} = \sum_{i \in \mathcal{S}_t} w_i \cdot \theta_i^{(t)} \quad (8)$$

The weighted aggregation strategy prioritizes drones with stable connectivity and sufficient residual energy, thereby improving federated learning convergence and reducing communication instability.

Multi-Objective Reinforcement Learning Controller

This step represents the core intelligence embedded in the proposed framework. As mentioned before, the MORL agent will learn the optimal trade-off between detection accuracy and energy efficiency. Unlike control policies designed using fixed approaches, this RL-based approach will adjust continuously. This allows the system to adapt efficiently to changing patterns of attack and other network conditions. Unlike static optimization approaches, the proposed MORL controller continuously learns optimal cybersecurity strategies by balancing multiple conflicting objectives, including attack detection accuracy, communication cost, energy

preservation, and network responsiveness. The proposed MORL agent can be framed based on the following Markov Decision Process (MDP) model a sin eqn. (9)

$$s_t = [\bar{E}_t, A_t, C_t, L_t \quad (9)$$

Where $\bar{E}_t$: Average residual energy, A_t: Detection accuracy, C_t: Communication cost, L_t: Observed attack intensity

Action Vector is given by the eqn. (10) $a_t \in$
{"Drone selection","FL interval","Compression level", "IDS sensitivity"} (10)
Reward function is given by the eqn. (11)

$$R_t = \alpha A_t - \beta \bar{E}_t - \gamma C_t - \delta L_t \quad (11)$$

The reward function enables adaptive policy learning by maximizing cybersecurity performance while penalizing excessive energy consumption and communication overhead.
The policy is updated as in eqn. (12)

$$\pi^*(s) = \arg\max_{\pi} \mathbb{E}\left[\sum_{t=0}^{\infty} \gamma^t R_t\right] \quad (12)$$

Through continuous interaction with the IoD environment, the MORL agent progressively improves decision-making policies for adaptive drone participation, intrusion sensitivity adjustment, and federated communication scheduling.

E. Secure and Energy-Efficient Model Aggregation

Model compression helps reduce the size of communication payload. This is efficient as it saves bandwidth and energy. Secure aggregation is effective as it maintains the confidentiality of all the models. In this sense, it provides robust protection of the system against inference and poisoning attacks. This step promotes efficiency and security together.
Secure aggregation further protects local model privacy and minimizes the risk of model poisoning and inference-based cyber attacks during federated communication..For efficiency, the gradient compression is employed as in eqn.(13)

$$\widetilde{\Delta\theta}_i = \mathcal{C}(\Delta\theta_i) \quad (13)$$

where $C(\cdot)$denotes compression. The compressed updates are securely aggregated to form the global model.

F. Global Model Dissemination and Continuous Learning

The process of continuous updates helps drones improve their capabilities in mitigating intrusions. Whenever threats arise, the framework improves as energy levels change, making it a reliable cyber defense platform for long-lasting IoD duties. The updated global model θ^((t))is broadcast to participating drones:

$$\theta_i^{(t+1)} \leftarrow \theta^{(t)} \quad (14)$$

Consequently, the proposed framework achieves adaptive, privacy-preserving, and energy-efficient cyber defense for highly dynamic Internet of Drones environments while maintaining scalable federated intelligence.

IV. Result and Discussion

In this section, a thorough evaluation of the proposed Energy Aware Adaptive Federated Cyber Defense (EA-AFCD) framework for internet of drones environments is provided. The performance of the proposed method is evaluated by utilizing a benchmark dataset for intrusion detection under a simulated environment considering non-IID distributed data and heterogeneous drone energy profiles. In this context, performance metrics such as detection accuracy, precision, recall, energy efficiency, communication, convergence speed, and network lifetime are considered in the proposed method. The performance of the proposed framework is comprehensively evaluated and compared with existing approaches such as centralized, centralized standard federated learning, and energy-aware approaches.
The results are presented using various tables and figures to describe the trends and behavior of the proposed system. The results show that EA-AFCD always outperforms the state-of-the-art approaches and significantly improves the performance of the system in terms of energy, which validates the proposed innovative scheme for an adaptive approach to the proposed federated cyber defense.

A. Intrusion Detection Accuracy Comparison

The fig 3 presents a comparison of the accuracy of intrusion detection using the proposed framework, i.e., 'EA-AFCD,' with respect to existing methodologies. The results obtained using the proposed framework indicate high accuracy, demonstrating the effectiveness of adaptive federated learning with reinforcement learning for improving the accuracy of heterogeneous IoD detection.

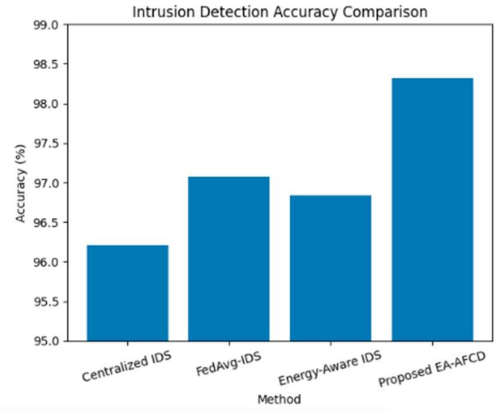

Fig 3. Intrusion Detection Accuracy Comparison

The Fig 4 depicts the proportionate distribution of attack categories present within CICIDS data. The categories have been represented outside the donut, while the calculated percentages have been represented inside each section to maintain quantitative clarity. The use of colors has ensured that there is no overlapping effect, making this visualization usable within double-column journal space. The varied nature of attack types indicates that this data possesses heterogeneity, enabling extensive evaluation of proposed energy-aware federated cyber defense.

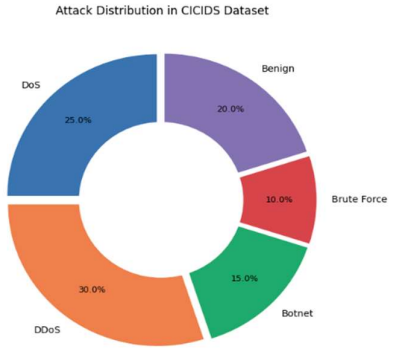

Fig 4. Attack Type Distribution

Figure 5 shows a histogram of the distribution of intrusion detection latency in the simulated federated Internet of Drones environment. Detection latency is defined as the time it takes between when traffic arrives at a drone and when a corresponding decision is generated by the local intrusion detection system. As presented in the results above, it is clear that the majority of the detection events are spread across a small range of latency values, thus indicating that the variance is less and the response time for each of the drone nodes is stable in nature. This demonstrates the effectiveness of the proposed energy-aware adaptive federated cyber defense framework by ensuring timely detection in response to the learning process for each of the fusion nodes. The absence of the long-tailed delays further reveals that the proposed mitigation achieves effectiveness in this regard.

Fig 5 low latency is achieved by exploiting the benefits of lightweight local intrusion detection systems, federated updates scheduled asynchronously and selectively, along with energy-aware participation and gradient compression. From the histogram itself, it can be concluded that the proposed framework satisfies the requirements for IoD systems without compromising responsiveness.

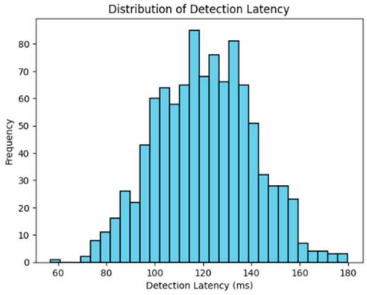

Fig. 5 distribution of intrusion detection latency

Figure 6 representing the relationship between energy consumption and intrusion detection accuracy. From the figure, the proposed framework EA-AFCD also shows high accuracy in detection at lower levels of energy consumption. This demonstrates the appropriateness and efficiency of the proposed energy-aware control in a manner that balances security and resource consumption for drone batteries.

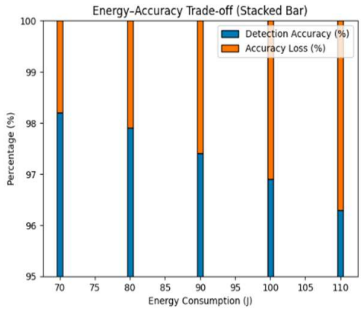

Fig 6. Relationship between energy consumption and intrusion detection accuracy

Table 1 suggested EA-AFCD attains the least average energy expenditure (72 J) through optimized node involvement and minimizing the number of communications. As compared with FedAvg-IDS (112 J) and Energy-Aware IDS (96 J), significant energy efficiency is gained, and it is well suited for IoT-based intrusion detection systems as shown in table I.

TABLE I. AVERAGE ENERGY CONSUMPTION PER DRONE

Method	Avg. Energy Consumption (J)
FedAvg-IDS	112
Energy-Aware IDS	96
Proposed EA-AFCD	72

Figure 7 shows how convergent federated learning behaves at successive rounds of training. From the highlighted diagram, it is evident that the suggested EA-AFCD approach converges quickly and attains better accuracy compared to other approaches, which is attributed to better stability in the global update process.

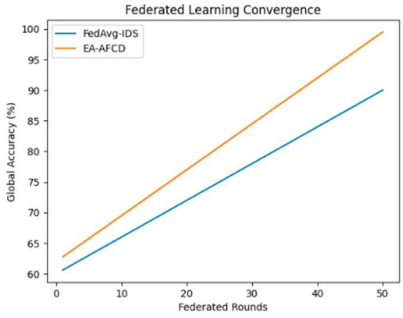

Fig 7. Federated learning Convergence

From fig 8, can see the residual energy distribution of the drones for different methods at the end of federated learning. Compared to the baseline, the proposed framework achieves a higher median residual energy and a smaller interquartile range, which means the drones have more balanced residual energies. Moreover, the smaller variance and the absence of extreme low residual energies in the plot reveal the effect of the proposed framework, which prevents premature battery drain for the drones. The balanced energy consumption for the drones leads to a longer lifetime for the Internet of Drones networks.

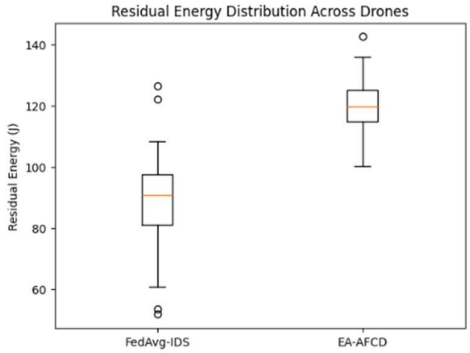

Fig 8. Energy distribution

From the area plot depicted in Figure 9, the cumulative communication overhead during the process for different techniques can be determined. It can be noted from the plot that while the number of rounds increases, the communication cost also increases accordingly for different techniques. Nevertheless, the growth rate for the proposed EA-AFCD framework is significantly low compared to other techniques. This reduction can be attributed to the reduced participation of the drones during the communication process for the new framework. This reduction can be noted as a major factor for the efficient bandwidth utilization for the proposed framework, which promotes reduced energy consumption for communication. Therefore, based on the plotted graph, the advantage of the adaptive federated control can be determined while considering the communication process for different techniques.

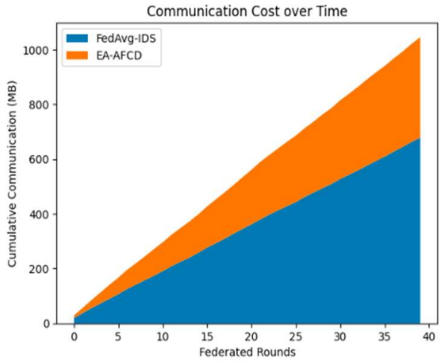

Fig 9. Communication overhead

It can be observed from the results that FedAvg-IDS has the highest volume of data transmission, which is around 820 MB because of frequent full model updates. Compressed FL can reduce the communication overhead by 610 MB using model compression techniques. On the other hand, the proposed EA-AFCD achieves the minimum data transmission, about 460 MB, via adaptive client selection and efficient update aggregation, hence significantly reducing the communication cost as shown in table II.

TABLE II. COMMUNICATION OVERHEAD COMPARISON

Method	Total Data Transmitted (MB)
FedAvg-IDS [15]	820
Compressed FL [11]	610
Proposed EA-AFCD	460

Figure 10 below presents a pie chart representing the contribution of each of these elements in the proposed energy-aware adaptive federated cyber defense system. The elements considered in this proposed system are represented by reinforcement learning controller, energy-aware selection of drones, model compression, and intrusion detection system. It can be observed from the figure that RL controller contributes the maximum to this proposed system, thereby illustrating its significance in adapting to minimize all three factors of security, power, and overhead.

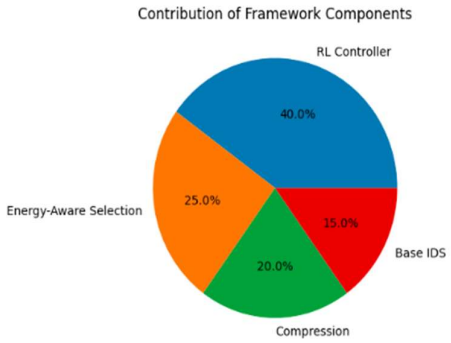

Fig 10. Contribution of each element

B. Discussion

The experimental results can well illustrate the effectiveness of this proposed Energy-Aware Adaptive Federated Cyber Defense Framework (EA-AFCD) in the IoD networks. Compared to the traditional centralized and static characteristic of federated networks, this proposed framework can always maintain better performance in terms of intrusion detection while reducing energy consumption and communication costs. The improvement in performance can also well illustrate the effectiveness of applying adaptive federated learning with intelligent controllability to solve problems with non-i.i.d. data and varying attack experiences on individual drone nodes, which are inherent in IoD systems. Another key conclusion from these results is the effectiveness of this proposed method in terms of energy consumption, through which we can clearly see the improvement in total energy consumption and network lifetime, illustrating that this reinforcement learning approach to determining node participation can prevent some drones with low energy from excessive computation and communication. This problem is also critical with regards to IoD systems.

V. Conclusion

This study proposed an energy-aware adaptive federated cyber defense system for ensuring Internet of Drones networks are secured under practical constraints. With the fusion of local intrusion detection systems, federated learning approaches, and multi-objective reinforcement learning methods, this proposed system aims to improve intrusion detection, energy usage, and communication overhead simultaneously. Through extensive experiments using a benchmarking intrusion detection dataset, it has been shown that this proposed system outperforms other state-of-the-art and competitive cyber defense systems, including traditional centralized, federated, and/or energy-aware systems. This proves the adaptability and viability of this proposed system in securing Internet of Drones networks under different criteria. There are various ways to augment and enhance this proposed system in future. First, it may involve exploring an Internet of Drones implemented in real-world drones to assess the adaptability and viability of this proposed system. Moreover, various state-of-the-art techniques using reinforcement learning may improve adaptability by involving deep reinforcement learning and multi-agent reinforcement learning. Third, integrating trust management and blockchain-based reputation is another possible enhancement, especially against insider and poisoning attacks. Finally, leveraging this framework for cross-domain federated learning across heterogeneous aerial and ground IoT devices is an interesting track for next-generation intelligent cyber defense systems.

References

[1] Y. Zhang, X. Liu, M. Chen, and Q. Li, “Security and Privacy Challenges in Internet of Drones: A Comprehensive Survey,” IEEE Communications Surveys & Tutorials, vol. 24, no. 3, pp. 1839–1876, 2022, doi: 10.1109/COMST.2022.3167894.

[2] J. Wang and X. Lu, “Cyber Threats and Defense Mechanisms for Unmanned Aerial Vehicle Networks,” IEEE Network, vol. 37, no. 2, pp. 44–51, 2023, doi: 10.1109/MNET.011.2200187.
[3] D. C. Nguyen, M. Ding, P. N. Pathirana, and A. Seneviratne, “Federated Learning for Internet of Things: A Comprehensive Survey,” IEEE Communications Surveys & Tutorials, vol. 25, no. 1, pp. 162–198, 2023, doi: 10.1109/COMST.2022.3200626.
[4] M. A. Khan, I. Ullah, S. Nisar, and D. H. Kim, “Federated Learning-Enabled Security for UAV-Assisted IoT Networks,” IEEE Internet of Things Journal, vol. 9, no. 23, pp. 24139–24151, 2022, doi: 10.1109/JIOT.2022.3178496.
[5] S. Chen, Y. Wang, and H. Zhang, “Energy-Efficient Learning and Communication Strategies for UAV Networks,” IEEE Transactions on Green Communications and Networking, vol. 8, no. 1, pp. 120–132, 2024, doi: 10.1109/TGCN.2023.3310245.
[6] Z. Li and N. Zhao, “Energy-Aware Security Design for Unmanned Aerial Vehicle Networks,” IEEE Transactions on Aerospace and Electronic Systems, vol. 59, no. 4, pp. 3461–3473, 2023, doi: 10.1109/TAES.2023.3247715.
[7] A. Al-Hourani, S. Kandeepan, and A. Jamalipour, “Modeling Air-to-Ground Path Loss for Low Altitude Platforms in Urban Environments,” IEEE Transactions on Wireless Communications, vol. 21, no. 6, pp. 3936–3949, 2022, doi: 10.1109/TWC.2021.3126948.
[8] J. Park, S. Samarakoon, M. Bennis, and M. Debbah, “Wireless Network Intelligence at the Edge: Multi-Objective Learning and Optimization,” IEEE Journal on Selected Areas in Communications, vol. 42, no. 1, pp. 55–69, 2024, doi: 10.1109/JSAC.2023.3324197.
[9] Y. Sun, H. Yu, Q. Liu, and S. Xie, “Multi-Objective Reinforcement Learning for Resource Management in Edge Computing Systems,” IEEE Transactions on Network and Service Management, vol. 20, no. 2, pp. 1641–1654, 2023, doi: 10.1109/TNSM.2023.3241128.
[10] P. Pandey, R. Mishra, and D. Singh, “A Lightweight and Secure Framework for Internet of Drones Using Machine Learning and Cryptographic Techniques,” Big Data and Cognitive Computing, vol. 9, no. 3, p. 61, 2025, doi: 10.3390/bdcc9030061.
[11] A. Derhab, “Internet of Drones Security: Taxonomies, Open Issues, and Countermeasures,” Journal of King Saud University – Computer and Information Sciences, vol. 35, no. 2, pp. 512–528, 2023, doi: 10.1016/j.jksuci.2022.05.010.
[12] A. Aldweesh, “Authentication Techniques in the Internet of Drones: A Comprehensive Review,” Future Internet, vol. 14, no. 3, p. 57, 2025, doi: 10.3390/fi14030057.
[13] S. O. Ajakwe, C. E. Okwara, and C. C. Udeze, “MINDS: A Multihop Intruder Node Detection Scheme for Autonomous Drone Networks,” IET Intelligent Transport Systems, vol. 19, no. 4, pp. 700–712, 2025, doi: 10.1049/itr2.70080.
[14] Z. Xi, Y. Chen, H. Wang, and J. Liu, “An Enhanced Cybersecurity Framework for Unmanned Aerial Systems,” IET Information Security, vol. 19, no. 1, pp. 1–13, 2025, doi: 10.1049/ise2.9637334.
[15] A. Derhab, “Internet of Drones Security: Taxonomies, Open Issues, and Countermeasures,” Journal of King Saud University – Computer and Information Sciences, vol. 35, no. 2, pp. 512–528, 2023, doi: 10.1016/j.jksuci.2022.05.010.