SemanticBlock: Blockchain-Assisted Secure and Energy-Aware UAV-BS Deployment Leveraging Semantic Learning

Mohtasin Golam
ICT Convergence Research Center
Kumoh National Institute of Technology
Gumi, Republic of Korea
gmoh248@kumoh.ac.kr

Esmot Ara Tuli
ICT Convergence Research Center
Kumoh National Institute of Technology
Gumi, Republic of Korea
esmot@kumoh.ac.kr

Jae-Min Lee
Networked Systems Laboratory
Kumoh National Institute of Technology
Gumi, Republic of Korea
ljmpaul@kumoh.ac.kr

Dong-Seong Kim
Networked Systems Laboratory (NSLab. Inc.)
Kumoh National Institute of Technology
Gumi, Republic of Korea
dskim@kumoh.ac.kr

Abstract

Unmanned aerial vehicles (UAVs) are emerging as flexible, rapid-deployment platforms for wireless communication, particularly in remote or disaster-affected areas. However, effective UAV-based base station (UAV-BS) deployment faces two major challenges: limited flight energy and communication security. This paper presents SemanticBlock, a blockchain-assisted framework that leverages semantic learning to enable secure, energy-aware UAV-BS deployment. The proposed system integrates a context-aware deep learning model, a long short-term memory (LSTM) network that learns semantic relationships among environmental and operational parameters, such as temperature, wind speed, battery state, and payload, to accurately predict UAV energy consumption for flight duration. These predictions guide UAV-BS positioning and migration decisions to maintain service continuity and energy efficiency. To address security vulnerabilities, a blockchain network is introduced to authenticate UAVs, ensure trustworthy communication, and prevent malicious access without centralized control. The joint use of semantic learning and blockchain provides a robust mechanism for both intelligent energy management and decentralized security. Simulation results demonstrate that SemanticBlock achieves 93.7% prediction accuracy, surpassing state-of-the-art models while reducing communication latency, confirming its potential for reliable UAV-BS deployment in dynamic, disaster-prone environments.

Keywords

Blockchain, energy prediction, semantic learning, secure communication, and unmanned aerial vehicles (UAVs).

ACM Reference Format:
Mohtasin Golam, Esmot Ara Tuli, Jae-Min Lee, and Dong-Seong Kim. 2025. SemanticBlock: Blockchain-Assisted Secure and Energy-Aware UAV-BS Deployment Leveraging Semantic Learning. In *The 9th International Conference on Algorithms, Computing and Systems (ICACS 2025), December 12–14, 2025, Bangkok, Thailand.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3789418.3789446

ACM ISBN 979-8-4007-1961-5/25/12
https://doi.org/10.1145/3789418.3789446

1 Introduction

Unmanned aerial vehicles (UAVs) have become a vital component of modern airborne systems due to their flexibility, mobility, and cost efficiency. They are increasingly used in civilian, industrial, and defense applications such as disaster management, aerial imaging, search and rescue (SAR), traffic monitoring, and environmental surveillance [2, 3, 13]. In emergency or infrastructure-compromised scenarios, UAVs can be rapidly deployed as aerial base stations (UAV-BS) to extend wireless coverage and restore communication services [16]. Their adaptability makes them a promising solution for next-generation wireless networks, particularly in areas with limited or damaged ground infrastructure.

Despite their advantages, UAV-BS deployment faces two critical challenges: high energy consumption and communication security risks. The limited onboard battery capacity of UAVs restricts flight duration and network service time, directly affecting their usability in large-scale or long-duration operations [13]. Simultaneously, UAV-BSs are vulnerable to diverse cyber threats, including jamming, eavesdropping, GPS spoofing, hijacking, and denial-of-service (DoS) attacks, which can disrupt mission-critical operations [1, 10]. Hence, achieving both energy efficiency and secure communication is essential for reliable UAV-BS deployment.

1.0.1 Background Studies. Several research efforts have explored energy-efficient UAV deployment strategies. In [11], an Artificial Bee Colony algorithm was developed for optimal UAV-BS placement, focusing on trajectory optimization but overlooking energy efficiency. A Software Defined Networking (SDN)-based scheme was proposed in [14] for location-aware UAV-BS deployment to minimize the number of aerial nodes. In contrast, [5] introduced an adaptive UAV-BS movement strategy driven by voting mechanisms to improve coverage. However, these heuristic and optimization-based approaches often neglect dynamic environmental conditions such as wind, temperature, or user mobility, which significantly affect UAV energy consumption. More recent studies, such as [15], employed machine learning (ML) models to predict UAV behavior and optimize placement. Still, these models are limited by shallow architectures that fail to capture complex contextual relationships. Convolutional neural networks (CNNs), with their superior feature extraction capabilities, have demonstrated improved performance in modeling UAV energy patterns compared to conventional ML techniques [4].

In terms of communication security, existing approaches include threshold-based intrusion detection, WPA2-based encryption, and physical-layer authentication mechanisms [12]. While effective in specific cases, these methods generally depend on centralized management and static key distribution, which introduce latency and single points of failure. To overcome these issues, blockchain (BC) technology offers a decentralized and tamper-resistant alternative for securing UAV networks. BC enables trustless authentication and immutable data storage, ensuring data integrity and preventing unauthorized access during UAV-BS operations.

1.0.2 Motivation and Contributions. This paper proposes *SemanticBlock*, a blockchain-assisted framework that leverages *semantic learning* to enable secure and energy-aware UAV-BS deployment. Unlike conventional ML or heuristic methods, semantic learning in this work refers to a context-aware deep learning approach that captures semantic relationships among UAV operational and environmental features, such as payload, wind speed, temperature, and battery usage, to accurately predict flight energy consumption. These predictions are used to dynamically guide UAV-BS placement and migration decisions. Furthermore, a permissioned blockchain network is integrated to authenticate UAVs and manage secure communication between distributed aerial and ground nodes. The combination of semantic learning and blockchain ensures both intelligent energy optimization and decentralized network security. The key contributions of this paper are summarized as follows:

- Proposes a hybrid architecture, *SemanticBlock*, combining semantic learning and blockchain for secure and energy-efficient UAV-BS deployment.
- Develops a semantic learning-based prediction model that captures the contextual relationships among UAV and environmental parameters to estimate flight duration and energy consumption.
- Designs a permissioned blockchain authentication mechanism to ensure secure, tamper-proof, and low-latency communication among UAV nodes.
- Evaluates the proposed system through extensive simulations, demonstrating its superior energy prediction accuracy and security performance compared to conventional methods.

2 Proposed Architecture

The SemanticBlock architecture, shown in Fig. 1, facilitates communication between UAVs and a central station (CS) while connecting remote areas. The CS oversees the execution of deep learning (DL) models to predict UAV energy usage and records the data on a blockchain (BC) ledger. Each remote area is managed by a local server (LS), which handles authentication, migration, and communication between UAVs through the BC network. This decentralized peer-to-peer network ensures secure data exchange across zones. Additionally, the BC network is used to authenticate UAVs when they enter or migrate between zones. UAV migration is based on remaining energy, which can be predicted from UAV energy consumption patterns.

2.1 Dataset Description

The dataset used for predicting UAV energy consumption consists of data collected from five different UAV types (DJI Mavic Pro, DJI Phantom 4 Pro, DJI Inspire 2, Parrot Anafi, and Parrot Bebop). The dataset includes meteorological variables such as temperature, humidity, pressure, wind speed, and wind direction, gathered by UAV sensors during flight. Additionally, flight-related information provided by the UAV controller includes fixed speed (15 m/s), altitude (80 m), total flight time, and battery utilization (ranging from 100% to 15% at 5-minute intervals). The dataset also incorporates environmental factors, such as time of day (morning, afternoon, and evening) and month (July to October), to improve prediction accuracy, with all UAVs flying for at least 20 minutes under standard conditions and at maximum payload capacity.

2.2 Network Architecture of Proposed Model

The proposed model uses a Long Short-Term Memory (LSTM) network to predict UAV energy consumption based on a set of meteorological and operational data [6]. The LSTM model is trained on the collected dataset, which includes variables such as temperature, humidity, wind speed, and UAV-specific data, including speed, altitude, and battery usage. One of the main challenges in this task is extracting meaningful features from the diverse datasets, as each has distinct properties. To address this, the model leverages LSTM's ability to extract relevant features by using its memory cells, which store historical data and enable context-aware predictions of energy consumption. The network consists of an input layer with 128 neurons, a hidden layer with 64 neurons, and an output layer that produces the predicted energy consumption.

The LSTM network consists of three layers: an input layer, a hidden layer, and an output layer. Consequently, the hidden layer regulates the input features via memory blocks comprising a forget gate, an input gate, and an output gate. The time-variant input sequence of a memory block is expressed as $\{i(1), i(2), \ldots i(X)\} \epsilon \mathbb{R}^{F \times X}$, where $i(t) \epsilon \mathbb{R}^{F}$, is the input feature vector at the instant of time, t. Let us assume that a complete memory block consists of n memory cells. Hence, an input feature $i(t) \epsilon \mathbb{R}^{F}$ will update for X times. Each update of feature vectors also updates the memory blocks as a result of the current state vector as $s(t) \epsilon \mathbb{R}^{n}$. Basically, the current output vector $y(t) \epsilon \mathbb{R}^{n}$ of input sequence depends on the previous step cell state vector $s(t-1) \epsilon \mathbb{R}^{n}$ and output vector $y(t) \epsilon \mathbb{R}^{n}$. The forget gate layer $f_g(t) \epsilon \mathbb{R}^{n}$ performs a decision operation through a sigmoid function as follows:

$$f_g(t) = \sigma\left[w_f i(t) + u_f y(t-1) + b_f\right], \quad (1)$$

The upgradation of the current cell state is decided by the input layer $i_g(t) \epsilon \mathbb{R}^{n}$, using a sigmoid operation as follows,

$$i_g(t) = \sigma\left[w_i i(t) + u_i y(t-1) + b_i\right], \quad (2)$$

Consequently, a thin layer (ϕ) compute an intermediate cell state $\hat{s}(t) \epsilon \mathbb{R}^{n}$ as follows,

$$\hat{s}(t) = \phi\left[w_s i(t) + u_s y(t-1) + b_s\right], \quad (3)$$

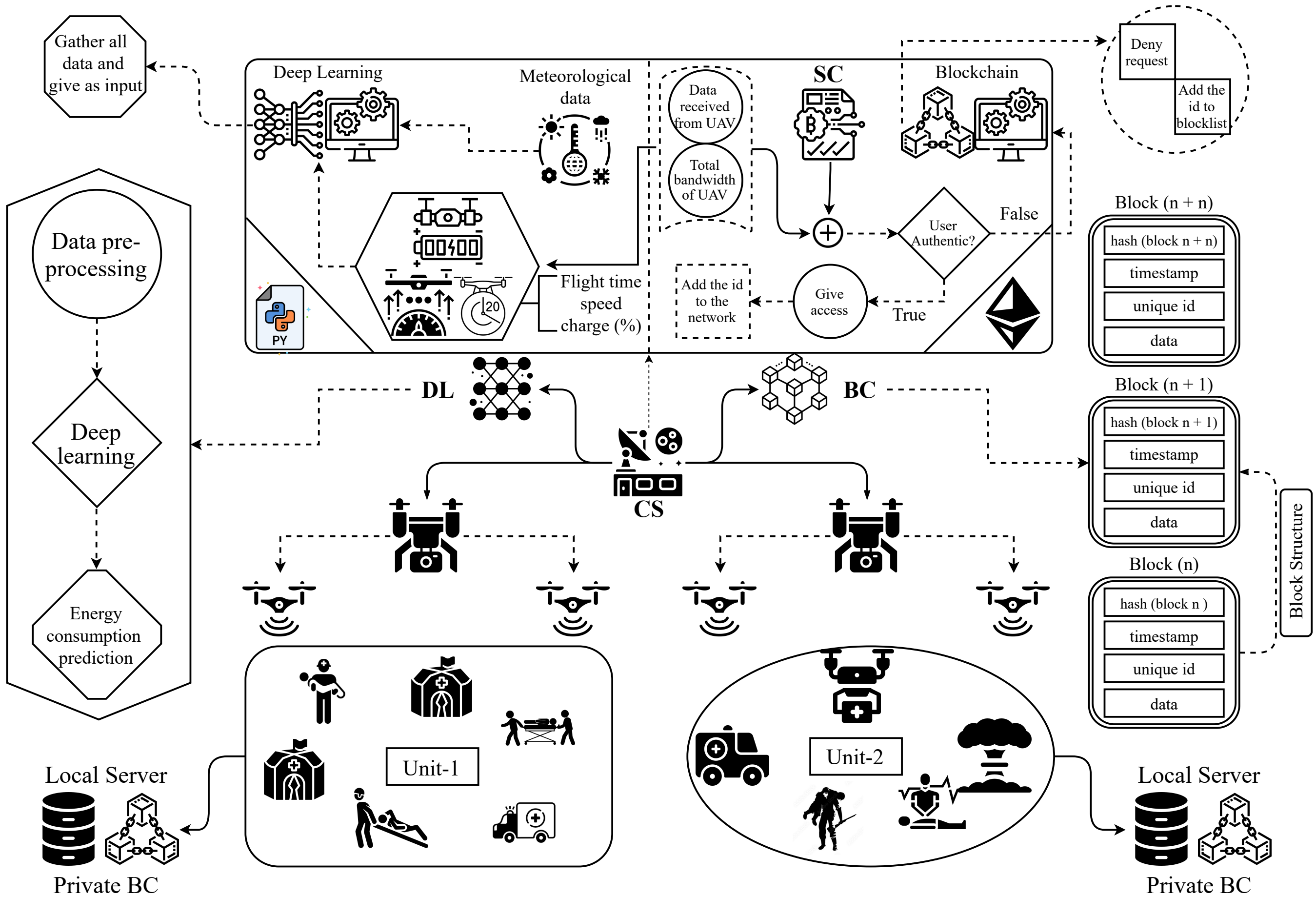

Figure 1: Proposed architecture of SemanticBlock

In the next step, the current cell state $s\,(t)\,\epsilon\mathbb{R}^n$ is updated depending on the information coming from the previous cell state $s\,(t-1)\,\epsilon\mathbb{R}^n$ as follows,

$$s\,(t) = f_g\,(t) \odot s\,(t-1) + i_g\,(t) \odot \hat{s}\,(t)\,, \tag{4}$$

Finally, the output gate performs a sigmoid function (σ) to decide what part of the previous cell state is going to be output as follows,

$$o_g\,(t) = \sigma\left[w_o i\,(t) + u_o y\,(t-1) + b_o\right], \tag{5}$$

Lastly, the current output vector $y\,(t)\,\epsilon\mathbb{R}^n$ is of a memory block at time step (t) is formulated as follows,

$$y\,(t) = o_g\,(t) \odot \phi\left[s\,(t)\right]. \tag{6}$$

here $\odot$ represents the elementwise multiplication while in Equations (4) to (9) $w_f i\,(t)$, $w_i i\,(t)$, $w_o i\,(t)$ are the weight metrics and b_f, b_i and b_o are the bias of forget, input and output gate respectively.

The model's input consists of meteorological data and UAV operational parameters, which are processed and normalized to predict energy consumption. The dataset includes three days' worth of meteorological data collected at 5-minute intervals and uses Min-Max scaling to normalize the feature vectors to the range [0, 1]. The dataset is split into training and test sets, and the time-series length is adjusted to match the prediction horizon. The LSTM-based model is employed to predict energy consumption by learning the sequential relationships between UAV operational data (e.g., speed, battery level) and environmental factors (e.g., wind, temperature). This allows the model to adjust UAV-BS positioning and optimize energy usage during deployment dynamically.

The architecture of the SemanticBlock model consists of a single LSTM input layer and a Leaky ReLU activation function, designed to process input features effectively. Additionally, the model includes two more LSTM layers, Leaky ReLU layers, a dropout layer to combat overfitting, and a dense layer to improve prediction accuracy. The LSTM network extracts key features from the input data by learning dependencies from previous time steps, using its memory cells. Each input feature vector is sequentially fed to the LSTM, which updates its memory block at each time step, retaining information to predict future energy consumption accurately.

For feature extraction, the dataset is formatted as a series of historical meteorological data points, denoted as $Q = \{q(t{-}X), q(t{-}X+1), \ldots, q(t-1)\} \in \mathbb{R}^X$. These input features are concatenated into a matrix $W \in \mathbb{R}^{6\times X}$, where each variable represents different weather parameters, and the sequence captures data over the past X time steps. The model then uses these features to predict the next set of values $F \in \mathbb{R}^{6\times X}$, which corresponds to future energy consumption.

The memory block in the LSTM network updates at each time step using the previous time step's output vector, enabling continuous learning of temporal dependencies. The network's final output is denormalized to yield the predicted UAV energy consumption for the next flight. To improve performance, a Leaky ReLU activation function is used, scaling negative values proportionally while leaving positive values unchanged. This function helps the network to avoid vanishing gradients during training, ensuring that the model learns effectively. A dropout layer is incorporated to reduce overfitting by randomly setting some input elements to zero during training. The model's predictions provide valuable insights for UAV energy management, which are essential for optimizing UAV-BS deployment in dynamic environments.

2.3 Blockchain-based Authentication Process

UAV-based base station (UAV-BS) deployment faces significant security challenges, including eavesdropping, jamming, GPS spoofing, and hijacking. To address these threats, the SemanticBlock architecture employs blockchain (BC) technology, providing a decentralized, tamper-proof solution for securing UAV communications [8]. Blockchain enables secure, peer-to-peer exchanges without third-party involvement, providing the reliability and security required for UAV-BS applications [9].

To prevent unauthorized access, the proposed architecture integrates a BC-based peer-to-peer (P2P) network that facilitates secure authentication and communication [4]. Each UAV is provided with a unique public/private key pair, enabling it to securely join the network. The system uses a permissioned BC, which allows predefined UAV nodes to interact, share information, and authenticate each other without relying on centralized control [7]. This is crucial, as UAV-BS are computationally constrained and cannot afford the high processing costs typically associated with traditional consensus mechanisms.

In the SemanticBlock architecture, each block in the blockchain contains essential data, including a unique UAV identifier (v_{id}) and MAC address ($\bar{mac}_{ad}$) for authentication. When a UAV joins a unit or migrates between units, its identity is verified using the unique ID stored in a local server (LS). To optimize efficiency, UAVs can migrate between zones without undergoing full authentication each time, thereby reducing latency.

If a UAV exceeds the LS's capacity by making excessive join requests, its activity is flagged as malicious, triggering a security action. The LS then rejects the UAV's participation in the unit, and the CS blocks its MAC address and unique ID, distributing this information across all units in the BC network to prevent further unauthorized attempts. This approach ensures security without sacrificing latency or scalability in a dynamic, decentralized UAV network. Additionally, when a UAV migrates to a new unit, it sends a join request, which is verified against the unit's unique ID before access is granted.

3 Performance Evaluation

This section presents the performance evaluation of the SemanticBlock architecture, which combines deep learning (LSTM) and blockchain (BC) technologies. To assess the efficiency of the proposed model, we conducted simulations using Google Collaboratory for deep learning and Ethereum for blockchain operations. The deep learning model, based on an LSTM, was implemented using Keras with TensorFlow as the backend and the Adam optimizer. The experiments were conducted on a system with a 3.00 GHz Intel processor, an NVIDIA GeForce RTX 2060 SUPER GPU, and 16 GB of RAM. The dataset used for training and testing consisted of 26,256 samples collected from four UAVs at 5-minute intervals, with an 80:20 training-test split. Each batch contained 26 entries, and training was conducted over 100 epochs. For the blockchain-based authentication mechanism, we analyzed key performance metrics, including authentication time, key processing time, and throughput. The blockchain network was tested for its ability to handle UAV authentication and communication in a decentralized manner.

3.1 Performance Evaluation of the LSTM-Based Context-Aware Model

Table 1 presents the key performance metrics for the LSTM-based deep learning model used to predict UAV energy consumption. The table highlights the number of model parameters (127,937), which reflects the complexity of the LSTM network, including its input and hidden layers. The inference time of 139 ms demonstrates the model's efficiency in making predictions, a crucial factor for real-time UAV operations. The 1,907 ms training time reflects the time required to process one batch during training, further indicating the model's computational feasibility for deployment. The LSTM model's 93.74% prediction accuracy indicates its effectiveness in predicting UAV energy consumption, surpassing that of other models such as GRU and SVM. The error metrics Mean Absolute Error (MAE), Mean Squared Error (MSE), and Root Mean Squared Error (RMSE) provide further insight into the model's precision. The MAE of 0.042 indicates the average absolute deviation from the actual values, while the MSE and RMSE metrics show the squared and root errors, respectively. The computational complexity is low, as indicated by the fast inference time and the optimized network architecture, making this model suitable for real-time prediction tasks in UAV deployment.

3.2 Performance Evaluation of the Blockchain Authentication Mechanism

Table 2 summarizes the performance metrics for the blockchain component of the SemanticBlock architecture, which ensures secure, decentralized communication among UAVs. The 43 ms authentication time is the time required for a UAV to authenticate and join the network, which is critical for minimizing latency during operation. The key processing time of 12 ms reflects the time required to process the public/private key pairs used in authentication, ensuring the blockchain can securely handle UAV nodes in a time-sensitive manner. The energy consumption for blockchain operations accounts for 14% of the total UAV energy, reflecting the computational overhead of integrating blockchain into UAV operations while maintaining energy efficiency. The throughput

Table 1: Performance Metrics for the LSTM-Based Deep Learning Model

Metric	Value
Number of Parameters	127,937 (LSTM model with 128 neurons in input layer, 64 in hidden layer)
Inference Time	139 ms (time taken for each prediction)
Training Time	1,907 ms (time to process a batch of 26 entries)
Prediction Accuracy	93.74% (overall accuracy of the model)
Mean Absolute Error (MAE)	0.042 (average absolute error in predictions)
Mean Squared Error (MSE)	0.0045 (average squared error in predictions)
Root Mean Squared Error (RMSE)	0.0619 (square root of MSE, error in predictions)
Computational Complexity	Low (optimized with fewer parameters and fast inference time)

Table 2: Performance Metrics for Blockchain in the SemanticBlock Architecture

Metric	Value
Authentication Time	43 ms (time taken for UAV to authenticate and join the network)
Key Processing Time	12 ms (time to process public/private keys during UAV authentication)
Energy Consumption for Blockchain	14% (average energy spent on BC operations)
Throughput	836 transactions per second (TPS)
Communication Latency	48 ms (average latency for UAVs to communicate across units)
Number of Malicious UAVs Blocked	92.82% (unauthorized UAVs successfully blocked)
False Positive Rate	2% (rate at which legitimate UAVs are falsely flagged as malicious)
Reauthentication Latency	63 ms (time to verify and reauthenticate a UAV

of 836 transactions per second (TPS) demonstrates the blockchain network's ability to handle multiple UAVs and their real-time communication needs. The 48 ms communication latency indicates the delay between UAVs and local servers within the blockchain network, indicating how quickly the system can relay data. The blockchain system also demonstrated strong security, blocking 92.82% of unauthorized UAVs and achieving a false-positive rate of only 2%, ensuring that legitimate UAVs can still operate without undue interruptions. The reauthentication latency of 63 ms is the time it takes the blockchain to verify a UAV as it migrates between zones, ensuring the migration process is efficient and secure.

4 conclusion

This paper presents SemanticBlock, an integrated framework that combines semantic learning and blockchain technology to enable energy-efficient, secure deployment of UAV-based base stations (UAV-BS). The proposed architecture effectively addresses two major challenges in UAV communication systems: energy consumption prediction and network security. By integrating deep learning for energy optimization and blockchain for secure communication, SemanticBlock provides a practical solution for UAV-BS management in dynamic, disaster-prone environments. The LSTM-based deep learning model achieved 93.7% prediction accuracy, with low error rates (MAE = 0.042, MSE = 0.0045, RMSE = 0.0619) and minimal inference time, demonstrating its effectiveness in predicting UAV energy consumption during dynamic operations. Meanwhile, the blockchain system ensured secure communication through fast authentication, efficient key processing, and high throughput, while successfully blocking 92.82% of malicious UAVs with a false-positive rate of 2%. The SemanticBlock framework established a balance between intelligent energy management and strong security, both of which are critical for modern UAV-BS networks. The integration of semantic learning allowed the system to make context-aware decisions, while the permissioned blockchain provided trust, transparency, and resilience against malicious activity. Together, these contributions make SemanticBlock a scalable and reliable architecture suitable for real-world UAV-BS communication systems, particularly in scenarios where both energy optimization and data security are vital.

Acknowledgments

This work was partly supported by the Innovative Human Resource Development for Local Intellectualization program through the Institute of IITP grant funded by the Korean government (MSIT) (IITP-2025-RS-2020-II201612, 50%) and by the Priority Research Centers Program through the NRF funded by the MEST (2018R1A6A1A03024003 50%).

References

[1] Aly Sabri Abdalla, Keith Powell, Vuk Marojevic, and Giovanni Geraci. 2020. UAV-assisted attack prevention, detection, and recovery of 5G networks. *IEEE Wireless Communications* 27, 4 (2020), 40–47.

[2] Rubina Akter, Van-Sang Doan, Thien Huynh-The, and Dong-Seong Kim. 2021. RFDOA-Net: An Efficient ConvNet for RF-based DOA Estimation in UAV Surveillance Systems. *IEEE Transactions on Vehicular Technology* (2021).

[3] Rubina Akter, Van-Sang Doan, Jae-Min Lee, and Dong-Seong Kim. 2021. CNN-SSDI: Convolution neural network inspired surveillance system for UAVs detection and identification. *Computer Networks* (2021), 108519.

[4] Rubina Akter, Mohtasin Golam, Van-Sang Doan, Jae-Min Lee, and Dong-Seong Kim. 2022. Iomt-net: Blockchain-integrated unauthorized uav localization using lightweight convolution neural network for internet of military things. *IEEE Internet of Things Journal* 10, 8 (2022), 6634–6651.

[5] Mingzhe Chen, Mohammad Mozaffari, Walid Saad, Changchuan Yin, Mérouane Debbah, and Choong Seon Hong. 2017. Caching in the sky: Proactive deployment of cache-enabled unmanned aerial vehicles for optimized quality-of-experience. *IEEE Journal on Selected Areas in Communications* 35, 5 (2017), 1046–1061.

[6] Mohtasin Golam, Rubina Akter, Jae-Min Lee, and Dong-Seong Kim. 2021. A long short-term memory-based solar irradiance prediction scheme using meteorological data. *IEEE Geoscience and Remote Sensing Letters* 19 (2021), 1–5.

[7] Mohtasin Golam, Rubina Akter, Revin Naufal, Van-Sang Doan, Jae-Min Lee, and Dong-Seong Kim. 2022. Blockchain inspired intruder uav localization using lightweight cnn for internet of battlefield things. In *MILCOM 2022-2022 IEEE Military Communications Conference (MILCOM)*. IEEE, 342–349.

[8] Mohtasin Golam, Md Mahinur Alam, Dong-Seong Kim, and Jae-Min Lee. 2024. BLM-Chain: AI-Driven Blockchain for UAV Threat Resistance in IoBT. In *2024 15th International Conference on Information and Communication Technology Convergence (ICTC)*. IEEE, 1609–1613.

[9] Ikechi Saviour Igboanusi, Kevin Putra Dirgantoro, Jae-Min Lee, and Dong-Seong Kim. 2021. Blockchain side implementation of Pure Wallet (PW): An offline transaction architecture. *ICT Express* 7, 3 (2021), 327–334.

[10] Hoon Lee, Subin Eom, Junhee Park, and Inkyu Lee. 2018. UAV-aided secure communications with cooperative jamming. *IEEE Transactions on Vehicular Technology* 67, 10 (2018), 9385–9392.

[11] Jialiuyuan Li, Dianjie Lu, Guijuan Zhang, Jie Tian, and Yawei Pang. 2019. Post-disaster unmanned aerial vehicle base station deployment method based on artificial bee colony algorithm. *IEEE Access* 7 (2019), 168327–168336.

[12] Gaurav Kumar Pandey, Devendra Singh Gurjar, Ha H Nguyen, and Suneel Yadav. 2022. Security threats and mitigation techniques in UAV communications: A comprehensive survey. *IEEE Access* 10 (2022), 112858–112897.

[13] Hazim Shakhatreh, Ahmad H Sawalmeh, Ala Al-Fuqaha, Zuochao Dou, Eyad Almaita, Issa Khalil, Noor Shamsiah Othman, Abdallah Khreishah, and Mohsen Guizani. 2019. Unmanned aerial vehicles (UAVs): A survey on civil applications and key research challenges. *Ieee Access* 7 (2019), 48572–48634.

[14] Sahil Vashisht, Sushma Jain, and Ravinder Singh Mann. 2019. Software Defined UAV-Based Location Aware Deployment Scheme for Optimal Wireless Coverage. In *2019 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech)*. IEEE, 907–912.

[15] Zhe Wang, Lingjie Duan, and Rui Zhang. 2019. Adaptive deployment for UAV-aided communication networks. *IEEE transactions on wireless communications* 18, 9 (2019), 4531–4543.

[16] Nan Zhao, Weidang Lu, Min Sheng, Yunfei Chen, Jie Tang, F Richard Yu, and Kai-Kit Wong. 2019. UAV-assisted emergency networks in disasters. *IEEE Wireless Communications* 26, 1 (2019), 45–51.