BANDA: A Novel Blockchain-Assisted Network for Drone Authentication

Simeon Okechukwu Ajakwe, Igboanusi Ikechi Saviour, Jung-Hyeon Kim, Dong-Seong Kim, Jae Min Lee
Department of IT Convergence Engineering, Kumoh National Institute of Technology, Gumi, South Korea
(simeonajlove, ikechisaviour)@gmail.com, (trizkim, dskim, ljmpaul)@kumoh.ac.kr

***Abstract*—The development of a comprehensive and decisive drone defense integrated control system (DDS) that can provide maximum security is crucial for smart aerial mobility to sustain the emerging drone transportation system (DTS) for priority-based logistics and mobile communication. This study developed a robust drone defense control system that uses blockchain technology to verify and authenticate the legitimacy of a drone operation and verify its package delivery to forestall possible disruption of aerial vehicular mobility, malicious attacks, and invasions. The system accepts inputs about the drone information and attached package in real-time over the cloud and verifies them using a proof of authority algorithm and smart contract and authenticates them using a decentralized application that is deployed on the drone, the ground control station, and the DDS before executing the appropriate neutralization response. To maintain a proper balance between scalable authentication, security, and speed of responsiveness in taking action, the legacy and the proposed blockchain-assisted approach run in parallel, and the disparity in the result is adjudged a perceived illegitimate aerial mobility intention in real-time. With the deployment of the BANDA on three (3) public networks, the Avalanche Fuji achieved a 97.7 ms authentication latency adjudging it an efficient and effective drone defense security approach for ensuring the sustainability of DTS as an autonomous vehicle for mobility.**

***Index Terms*—Anti-drone, Authentication, Blockchain, Drone transportation system, Security, UAV.**

I. Introduction

In recent times, there have been several reports of increased disruption and violation of the airspace due to the polarization of drone usage and their associates, otherwise known as unmanned aerial vehicles (UAV) [1]. Precisely, according to reports from the US Federal Aviation Authority (FAA), there were 14178 cases of UAV-related airspace smart city security violations across the US from January 2016 to December 2022 [2] which is almost 200% astronomical increase as compared to the 8124 cases recorded in 2015 by authors [1]. Drone defense systems (DDS) are hard real-time cyber-physical systems (CPS) that run on fault-tolerant networks (FTN) to monitor and supervise the activities and operations of drones from invasive and malicious usage such as spying, network jamming, reprisal attacks, espionage, etc. [3]. The importance of developing DDS technologies cannot be overemphasized, as it has become an essential technology for society, from the need to protect major key facilities to the purpose of protecting individual privacy and property. Nowadays, drone usage for priority-based logistics is gaining gradual momentum and wide acceptability, albeit with several security issues [4] which threaten the viability of civilian drone usage.

Despite the advancement in DDS, the persistent security problems in drone operations especially for logistics cut across tracking drone user intention [1], drone user-identity theft management [5], drone communication hijacking, drone user authentication [6], [7], drone operator authorization [8], drone package delivery verification and accountability [9], [10], and dynamic drone engagement and neutralization based on environmental impact assessment [3]. These problems suggest inadequacy in the capacity of the artificial intelligence (AI)-driven defense approaches [3]. Blockchain technology offers a safe, traceable, decentralized, and tamper-proof platform for storing, transmitting, and validating the source of sensitive data [11], which has the potential to revolutionize data security in drone transportation. However, the deployment of blockchain technology in DDS is somewhat in its infancy due to the need for a trade-off between security, speed, and scalability, which has remained an issue in blockchain-assisted designs.

The current drawbacks in secured drone authentication approaches remain latency (speed) issues for real-time transmission and communication in checking and mitigating security vulnerabilities imposed by malicious drone deployment. Generally, authentication approaches can be in the form of scalable secret-free authentication, scalable and secure key agreement, and scalable continuous authentication. There have been few attempts to address these persistent security issues using blockchain and allied technologies. For drone authentication, authors [3], [12], [13] developed AI-based and trusted computing approaches to authenticate drones in flight. These frameworks have privacy issues, sensor-fusion complexities, overhead costs, and a lack of mutual authentication since blockchain was incorporated to ensure transparency. To introduce transparency and enhance trustworthiness for verifiable drone user/ownership authentication, authors [14]–[16] formulated blockchain-based drone ownership verification frameworks with impressive results in terms of throughput and latency. However, the overhead cost of these frameworks makes them porous, susceptible to malicious cyber attacks, and unfit for DDS to provide maximum security.

To address drone content and package delivery verification, authors [17] proposed a secure distribution of protected content

in information-centric networking for drone goods delivery authentication to validate the source of the package but the approach suffers from insufficient mobility support and lacks decentralization. To address decentralization in drone package verification, authors [10] and [3] developed a multimodal conveyed object verification and neutralization using visual object detection and assisted learning. However, these studies did not incorporate blockchain technology, cannot verify sealed content, and lacks transparency. Finally, authors [18] proposed a drone user-route assessment to validate the authorization and legality of a drone operator within a jurisdiction. However, this proposal has authentication issues, high computational complexity, and low communication efficiency.

How can the security risk, uncertainty, and perceived threat associated with the polarization of drone usage as an aerial vehicular logistics delivery enabler be curtailed? How can the intent and behavioral tendencies of aerial autonomous vehicles be checked intrinsically? How can we align algorithmic decision-making with ethical principles in the design of mobility-friendly and secured autonomous aerial vehicles? Designing a DDS that can guarantee maximum security against malicious drone mobility as an aerial smart vehicular technology for freight operations (especially in smart cities) therefore requires an inclusive robustness that blends scalability with speed and security in carrying out real-time (timely), scenario-specific (tactile), traceable (tractable), and trustworthy(transparent) countermeasure operations.

Therefore, this study is motivated by the need to improve the existing DDS architectures through the incorporation of blockchain technology to enhance its performance capacity in curtailing malicious drone deployment and accelerate the DTS as the next-generation vehicular mobility choice for value chain logistics with less security botheration. To improve the timeliness and efficiency of the network, an off-chain transaction strategy is adopted and runs concurrently with the legacy drone authentication approach. To the best of our knowledge, no research has been carried out to encapsulate drone user authentication, operator authorization and legality, package delivery status verification, and dynamic scenario-specific neutralization using blockchain technology. Hence, the novelty of this study.

The specific contributions of this study are;

- To formulate an approach for comprehensive verification, authorization, and authentication of drones and their attached package before triggering dynamic neutralization,
- To design a transparent blockchain network and develop a decentralized application that runs on the edge for validation of authentication parameters,
- To deploy the developed blockchain network and application on the drone defense system to check the legitimacy and authority to operate as a smart mobility vehicle.

The rest of the paper is organized as section II for problem formulation, section III for system design and experimental setup, section IV for result presentation and discussion, and section V to conclude the paper.

II. PROBLEM FORMULATION: SCALABLE AUTHENTICATION

The modeling of a DDS for dynamic and comprehensive drone engagement problems for secured smart aerial mobility, especially for logistics, is complex and multifarious (otherwise called "np-problem") because different interlining system components and controlled parameters are intuitively considered before a final time-sensitive automated decision/response is taken. Using the principles of the kinematic model of an autonomous mobile robot based on Ackermann steering, a drone usually moves in a 2D coordinate system as shown in Fig. 1,

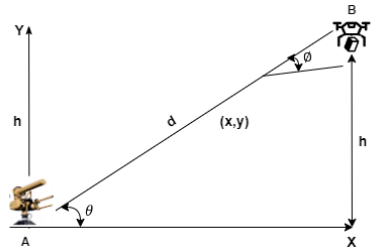

Fig. 1. Kinematics of a Typical DDS Authentication Procedure for Dynamic Engagement of a Drone within its Detection Line of Sight

A typical DDS over a cloud will detect drone(s) within its detection range, identify the attached object, measure the drone distance/proximity ($\overline{AB}$), estimate the drone altitude ($\overline{BX} \equiv \overline{AY}$), the direction of arrival estimate (θ), and estimate speed (ϕ), based on the drone's registration information, the transmitted GCS information, and other acquired sensor parameters. Much research effort has been put into this area using AI [1], [3], [19]. This work focuses on authenticating the outcome of these procedures using blockchain. Mathematically, the DDS engagement for drone authentication problems can be defined by a linear transformation function as expressed in equation (1):

$$D \mapsto d_X, \tag{1}$$

at a current timestamp (t); where d_X represents the constituent of the authentication input variable of the elements (i.e., all pairs of $(x, f(x))$ for $x \in X$) needed for determining the overall drone authentication function expressed in equation (1)

$$D = \begin{bmatrix} A_1 & A_2 & ... & A_n \\ B_1 & B_2 & ... & B_n \\ C_1 & C_2 & ... & C_n \end{bmatrix}_{t+1} \tag{2}$$

where A = drone-user status;
B = drone-source status;
C = drone-package status;
$t+1$ = current timestamp;and
n = total number of drones within the detection range.

Therefore, the objective function of the blockchain-assisted DDS engagement is to optimize the drone authentication target

function (D) for every input variable (x) subject to time (t) and other network and control input (ψ) constraints.

Theorem 1: ***At any given instance*** *(i)****, the dynamic engagement of a DDS*** *(D)* ***for authenticating a targeted logistics-based drone*** *(d)****, with changing distance/proximity*** *(s)* ***and altitude*** *(h)****, measured in real-time*** *(t)* ***over a secured cloud-based network, is a function of the drone-user state*** *(d_u)****, drone-source identity*** *(d_i)****, and drone-package delivery status*** *(d_p)* as expressed in equation (3):

$$D_l = f_d(u_t, i_t, p_t), \tag{3}$$

where D_l = Legacy DDS engagement determinant at the current time-stamp, and u_t, i_t, and p_t are the control input vectors at the current timestamp for drone user state, source, and package status. By expanding equation (3) to factor in drone proximity to the DDS (in terms of distance and altitude), we have:

$$D_l = \oint_{k=1}^{n} \{d_{u_t}, d_{it}, d_{p_t}\}.\{d_{st}, d_{ht}\}, \tag{4}$$

where d_{st} and d_{ht} is the drone proximity values to the DDS.

The incorporation of blockchain technology into the network to enhance the DDS decision-making mechanism (as seen in Fig. 1) will undoubtedly increase the overall complexity of the system, which inadvertently affects its responsiveness as an increase in complexity is inversely proportional to system scalability and speed. To circumvent this problem, our approach ensures that the proposed blockchain-assisted DDS network model (D_α) runs independently for the dynamic engagement of drones from the typical legacy approach as seen in Fig 2.

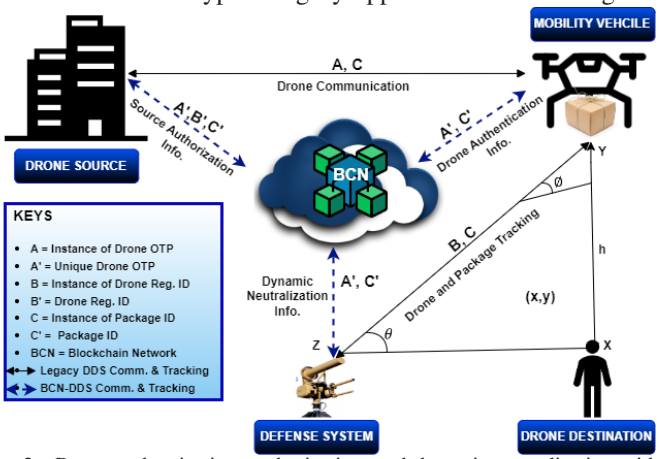

Fig. 2. Drone authentication, authorization, and dynamic neutralization with Blockchain Technology at center for traceability, transparency, and trustworthy DTS operations and DDS security

Hence, the blockchain-assisted drone authentication problem is transformed into equation (5).

$$D_\alpha = \oint_{k=1}^{n} \{d_{u_t'}, d_{it}^{'}, d_{p_t}^{'}\}.\{d_{st}, d_{ht}\}, \tag{5}$$

where $d_{u_t'}$ = A‘ $\equiv$ Unique Drone OTP aside other details; $d_{it}^{'}$ = B‘$\equiv$ Drone Registration ID to track the drone source; and $d_{p_t}^{'}$ = C‘ $\equiv$ Package ID used for tracking and verifying the conveyed object legitimacy and destination. A disparity between the response capacity and behavioral tendencies for dynamic engagement of (D_l) and (D_α) within an allowable timeframe indicates a security breach in defense against malicious drones. Hence, $D_\alpha \neq D_l$ signals an authentication flaw in the dynamic engagement routine of the legacy DDS; while a $D_\alpha \equiv D_l$ suggests a trustworthy routine for dynamic engagement. Therefore, a scalable authentication for improved defense security against the malicious deployment of drones for smart mobility is defined as:

$$D_{max} = \Sigma(D_\alpha - D_l) \equiv \eta_b, \tag{6}$$

subject to a maximum allowable response time threshold, which is $\leq$ 100 milliseconds for a legacy DDS. Before smart aerial mobility, the drone source registration details, user/operator identity information, and package delivery data are sent to the cloud represented by A', B', C' as indicated in Fig 2 which is utilized by the DDS for authentication during flight operation. During smart mobility operation, the legacy DDS (D_l) engages the drone by acquiring these pieces of information (A, B, C) via GCS sensing based on its underlying defense technology characterization, which is diametrically insufficient. Contrariwise, the proposed blockchain-assisted DDS (D_α) retrieves all information associated with the drone within line of sight from the cloud and verifies its authenticity via the BCN before responding intuitively. At any instance, if any of the values of the legacy DDS (D_l) parameters differ from the blockchain-assisted DDS (D_α) parameters, a perceived danger meta-heuristic analysis and procedure are launched depending on the scenario-specifics.

III. BANDA SYSTEM DESIGN AND METHODOLOGY

Aligning algorithmic decision-making with ethical principles is critical to securing autonomous vehicle innovation designs and guaranteeing their sustainability. For the system modeling, the authors made the following assumptions:

- That the drone detection and identification algorithm is intact,
- That there is an authorization body that regulates the airspace operations, and
- That every drone used for smart mobility has the license to operate and is duly registered as either a freight operator or hobby-drone user with the authorized regulator.

The proposed model is designed using a public blockchain architecture that runs on an Ethereum network using a proof of authority (PoA) consensus algorithm and smart contracts (SM) to accept only data as input, verify its authenticity through mining activities in the block within a specified block time, and generate feedback via the decentralized application (DApp) which serves as the output that is utilized by the DDS in taking the appropriate neutralization response (either active or passive) by triggering its jammers, spoofers, drone shooters, etc. Fig. 3 is the system design logic diagram summarizing the input, process, and output of the proposed approach.

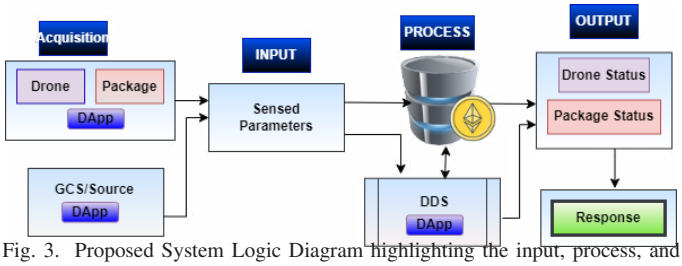

Fig. 3. Proposed System Logic Diagram highlighting the input, process, and output flow and activities of the DDS for drone authentication before dynamic neutralization

The drone input consists of a time-synchronized one-time password (OTP); a unique security token (D_{mac}) representing the mac address of the drone and a hash value, i.e. a one-time password (D_{otp}) for the drone that is sent by the source into the blockchain network, the acquired GCS signal information (D_{gcs-x}, D_{gcs-y}) for the drone used to check the mac address and drone source, a soft token for the package delivery (P_{st}) sent by the source into the cloud, and an RFID tag in the form of a hard token (P_{ht}) embedded and attached to the delivery package by the source which can be sensed and retrieved by the DDS from the drone in flight within its detection range. These six (6) data constitute the system input parameters that the DDS utilizes for authentication before deciding the appropriate neutralization call.

Instantiating the verification, authorization, and authentication procedure begins with a transaction request made by the drone source into the BCN indicating that a drone is about to begin a delivery operation within the network with the D_{mac} and D_{otp} into the cloud. Then, the drone source initiates a transaction with a fee. The miners in the network carry out mining. The DDS retrieves the hash value and cross-examines it with the acquired GCS signal information D_{gcs-x}. If the value agrees, it authenticates and recursively continues this procedure until a disparity is encountered as summarized by the flow chart in Fig 4. The gas cost and time taken for the completion of the transaction are recorded.

Similarly, it carries out a one-time comparison of the value of D_{mac} retrieved from the cloud with the D_{gcs-y} acquired from the GCS for disparity and authenticates it accordingly. Finally, it also performs a one-time cross-examination of the package delivery P_{st} retrieved from the cloud with the P_{ht} value acquired via sensing. These three (3) processes run concurrently in real-time and each authentication meta-heuristic value is utilized for the eventual decision-making.

Once a disparity occurs, then an appropriate neutralization response is triggered by the DDS depending on the value of the environmental impact assessment, and other characterizations from the detection and identification routines such as detection range estimate, object detection visual representation, detection accuracy, etc. (not covered in this work). Generally, the neutralization response can be either destructive (destroy) by shooting down the drone or non-destructive (disarm or re-route)

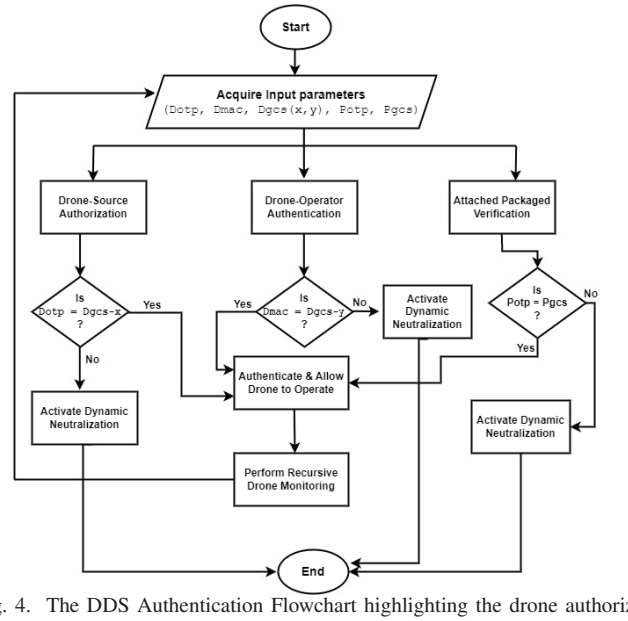

Fig. 4. The DDS Authentication Flowchart highlighting the drone authorization, and package verification process

through jamming or spoofing [3], [10], [20]. Algorithm 1 is the abridged form of the scalable authentication procedure.

Algorithm 1: DDS Scalable Continuous Authentication D_{max}

Input: Acquire variables: D_{otp}, D_{mac}, D_{gcs-x},...P_{otp};
Edge server executes & interact with blockchain layer;
while *True* **do**
    Check Drone Source Authorization(D_{otp}=D_{gcs-x});
    Check Operator Authentication(D_{mac}=D_{gcs-y});
    Check the attached package verification using RFID tag(P_{otp}=P_{gcs});
    if *Steps 4, 5, and 6 ==* ***True*** **then**
        Authenticate & Allow Drone to Operate;
        Perform Recursive Monitoring;
    end
    else
        Activate Dynamic Neutralization;
        Report & Document drone information;
    end
    return D_{max}
end

A. Experimental Setup

The summary of the proposed system design implementation platform and parameters are highlighted in Table I. The choice of a public Ethereum network ensures that the proposed approach performs authentication efficiently in real-time.

IV. Result and Discussion

By analyzing the results of the implementation, we demonstrate that the BANDA model improves drone/anti-drone net-

works. The smart contract was developed using our "pure wallet" framework.

TABLE I
IMPLEMENTATION PARAMETERS

Acronym	Meaning
Network	Ethereum public testnet (Goerli)
Consensus	Proof of Authority (PoA)
Smart contract language	Solidity (0.7.6+committ.7338295f)
Dapp Language	Dart (flutter)
Device	MacBookAir
Chip/RAM	M1/16GB
OS	macOS Ventura (Version 13.2)

Specifically, the result analysis focuses on the blockchain aspect of the implementation, especially time (t) which is a performance metric that validates the timeliness or latency in the responsiveness of the DDS while guaranteeing security for smart aerial mobility against abusive drone usage. Fig. 5 is the underlying smart contract interface where the input parameters are entered, retrieved, processed, and transmitted in the network. These automated parameters are manipulated and utilized for authentication.

Fig. 5. The interface of the smart contract deployed on remix IDE with the Smart Contract procedures for Authorization of Drones and Authentication of Attached Package to the Drone

The time it takes to communicate between the drone source or logistics company and the drone is the time the system takes to detect discrepancies between the data sent over the regular network and the blockchain network. The model takes a stream of data from the logistics company and stores it on the blockchain network. The drone listens to the blockchain network and retrieves the value of the data from the blockchain smart contract.

Fig. 6 highlights the authentication latency performance of the BANDA on three (3) different public networks in verifying the legitimacy of a detected drone and the attached object. **Network Time** represents the time taken between the company (drone source) sending the data and the drone receiving the data. On the other hand **Dapp Time** is when the smart contract receives the company's data and the time it releases it to the drone.

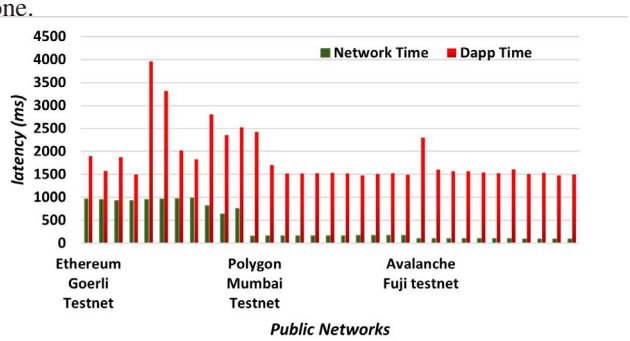

Fig. 6. BANDA authentication performance in terms of network time and Dapp time on Polygon Mumbai Testnet and Ethereum Georli Testnet respectively.

In practice, this time determines represents the authentication time required by the BANDA-controlled DDS to confirm and validate a drone's legitimacy and its attached object via the blockchain network. The values in Table II show the performance of the BANDA in terms of latency for confirming the legitimacy of a drone and the attached package before triggering the appropriate neutralization

A. Evaluation of Proposed Approach Authentication Latency

The performance evaluation is carried out on three (3) public networks namely Ethereum Goerli, Polygon Mumbai, and Avalanche Fuji, and compared with a legacy DDS as shown in Table II

TABLE II
AVERAGE AUTHENTICATION LATENCY ON DIFFERENT NETWORKS

Sno.	Network Name	Average Network (ms)	Average Dapp Time (ms)
1.	Ethereum Goerli	893	2326
2.	Polygon Mumbai	1632	1607.6
3.	Avalanche Fuji	97.7	160.6
4.	Legacy DDS	100	100

The measurement of the time taken to communicate between the logistics company and the drone varies after every trial. Hence, the average value of the experiment is assumed to be the standard time for transacting through blockchain. The results show in Table II that by deploying the proposed approach on Avalanche Fuji Testnet, it takes an average network time of 97.7ms and an average Dapp time of 160.6ms for drone authentication to occur in the BANDA framework. The 97.7ms network authentication latency achieved by the Avalanche Fuji Testenet on the BANDA for DDS operation is within the legacy DDS network authentication benchmark of 100 ms which signifies that the proposed blockchain authentication approach for the DDS nearly outperforms the standard legacy DDS. However, on the Polygon Mumbai and Goerli networks, the authentication latency is a bit higher than the authentication latency for the legacy DDS. this implies that the authentication

latency is a function of the intrinsic characterizations of the public Ethereum network on which the BANDA is deployed rather than the approach itself. Although time cannot be considered real-time in a drone network, the BANDA architecture does not degrade the experience of using the network since the legacy network takes the proactive data to the target user's destination, until blockchain data arrives at the drone. Since the time value sometimes changed significantly after each iteration, we assume that the number of transactions (n) in the network contributed to this behavior. Also, since the off-chain transaction runs concurrently with the DDS legacy approach to drone authentication, the issue of timely drone authentication is also taken care of. Widespread testing of the proposed model on different blockchain networks will help to further validate the speed of authentication. For proof concept validity, our smart contract simulation for the implementation of the authentication model can be accessed online via [21]. Finally, in the future, the model will be tried and tested on other different blockchain networks to obtain how the authentication time changes in relation to the network on which the BANDA model is deployed.

V. Conclusion

This study proposed a blockchain-assisted authentication approach that enhances the scenario-specific and dynamic neutralization capacity of drone defense systems against the malicious deployment of UAVs to disrupt aerial autonomous vehicular mobility and endanger the sustainability of drone transportation systems. The approach verifies the legitimacy of the drone information within its detection range as well as the harmful status of the conveyed delivery package using a proof of authority algorithm, and smart contract and authenticates the output based on the decentralized application deployed on the drone, the ground control station, and the defense system. The experimental result proves that incorporating blockchain technology into a drone defense system leads to improved security and scalability, with timely response necessary for a time-sensitive cyber-physical system in responding to dynamic scenarios to ensure the continuity of drone usage as a preferable aerial smart mobility solution for prioritized logistics in smart cities. In the future, we intend to improve the system's security capacity by incorporating federated policy control to achieve zero trust and increase responsiveness since future security networks demand antifragile capacity where the performance of a security architecture is measured by the probability of the reduction of deception.

Acknowledgment

This research was supported by Priority Research Centers Program through NRF funded by MEST (2018R1A6A1A03024003), NRF-2022R1I1A3071844, and the Grand Information Technology Research Center support program (IITP-2023-2020-0-01612) supervised by the IITP by MSIT, Korea.

References

[1] V. U. Castrillo, A. Manco, D. Pascarella, and G. Gigante, "A Review of Counter-UAS Technologies for Cooperative Defensive Teams of Drones," *Drones*, vol. 6, no. 3, 2022.

[2] F. A. Administration. (2023, 01) UAS Sightings Report. [Online]. Available: https://www.faa.gov/uas/resources/public_records/uas_sightings_report

[3] S. O. Ajakwe, V. U. Ihekoronye, D.-S. Kim, and J.-M. Lee, "ALIEN: Assisted Learning Invasive Encroachment Neutralization for Secured Drone Transportation System," *Sensors*, vol. 23, no. 3, 2023.

[4] A. Gohari, A. B. Ahmad, R. B. A. Rahim, A. Supa'at, S. Abd Razak, and M. S. M. Gismalla, "Involvement of Surveillance Drones in Smart Cities: A Systematic Review," *IEEE Access*, 2022.

[5] S. O. Ajakwe, D.-S. Kim, and J. M. Lee, "Drone Transportation System: Systematic Review of Security Dynamics for Smart Mobility," *IEEE Internet of Things Journal*, pp. 1–1, 2023.

[6] P. Mehta, R. Gupta, and S. Tanwar, "Blockchain envisioned UAV Networks: Challenges, Solutions, and Comparisons," *Computer Communications*, vol. 151, pp. 518–538, 2020.

[7] K. Belwafi, R. Alkadi, S. A. Alameri, H. Al Hamadi, and A. Shoufan, "Unmanned Aerial Vehicles' Remote Identification: A Tutorial and Survey," *IEEE Access*, vol. 10, pp. 87 577–87 601, 2022.

[8] G. Lykou, D. Moustakas, and D. Gritzalis, "Defending Airports from UAS: A Survey on Cyber-Attacks and Counter-Drone Sensing Technologies," *Sensors*, vol. 20, no. 12, 2020.

[9] J.-P. Yaacoub, H. Noura, O. Salman, and A. Chehab, "Security Analysis of Drones Systems: Attacks, Limitations, and Recommendations," *Internet of Things*, vol. 11, p. 100218, 2020.

[10] S. Okechukwu Ajakwe, V. Ukamaka Ihekoronye, D.-S. Kim, and J.-M. Lee, "Tractable Minacious Drones Aerial Recognition and Safe-Channel Neutralization Scheme for Mission Critical Operations," in *2022 IEEE 27th International Conference on Emerging Technologies and Factory Automation (ETFA)*, 2022, pp. 1–8.

[11] Z. Wang, J. Lin, Q. Cai, Q. Wang, D. Zha, and J. Jing, "Blockchain-based Certificate Transparency and Revocation Transparency," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 1, pp. 681–697, 2022.

[12] S. Mandal, B. Bera, A. K. Sutrala, A. K. Das, K.-K. R. Choo, and Y. Park, "Certificateless-Signcryption-Based Three-Factor User Access Control Scheme for IoT Environment," *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 3184–3197, 2020.

[13] Z. Lv, "The Security of Internet of Drones," *Computer Communications*, vol. 148, pp. 208–214, 2019.

[14] S. Jangirala, A. K. Das, and A. V. Vasilakos, "Designing Secure Lightweight Blockchain-Enabled RFID-Based Authentication Protocol for Supply Chains in 5G Mobile Edge Computing Environment," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 11, pp. 7081–7093, 2020.

[15] G. Cho, J. Cho, S. Hyun, and H. Kim, "SENTINEL: A Secure and Efficient Authentication Framework for Unmanned Aerial Vehicles," *Applied Sciences*, vol. 10, no. 9, p. 3149, 2020.

[16] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, H. Karimipour, G. Srivastava, and M. Aledhari, "Enabling Drones in the Internet of Things with Decentralized Blockchain-based Security," *IEEE Internet of Things Journal*, vol. 8, no. 8, pp. 6406–6415, 2020.

[17] M. Bilal and S. Pack, "Secure Distribution of Protected Content in Information-Centric Networking," *IEEE Systems Journal*, vol. 14, no. 2, pp. 1921–1932, 2020.

[18] A. Gumaei, M. Al-Rakhami, M. M. Hassan, P. Pace, G. Alai, K. Lin, and G. Fortino, "Deep Learning and Blockchain with Edge Computing for 5G-enabled Drone Identification and Flight Mode Detection," *Ieee Network*, vol. 35, no. 1, pp. 94–100, 2021.

[19] S. Ajakwe, R. Akter, D. Kim, and J. Lee, "Lightweight CNN Model for Detection of Unauthorized UAV in Military Reconnaissance Operations," in *Korean Institutes of Communications and Information Sciences Conference*, vol. 1, 2021, pp. 1–3.

[20] S. Ajakwe, R. Akter, D. Kim, G. Mohatsin, D. Kim, and J. Lee, "Anti-drone systems design: Safeguarding airspace through real-time trustworthy ai paradigm," in *Proceedings of the 2nd Korea Artificial Intelligence Conference (KAIC 2021), Da Nang, Vietnam*, 2021, pp. 27–28.

[21] S. O. Ajakwe, I. S. Igboanusi, D.-S. Kim, and J. M. Lee, "BANDA Implementation Code," 2023. [Online]. Available: http://nsl.kumoh.ac.kr/include/sub.php?m=134&mode=Write&com_id=bi0001&menu_cd=30&class_cd=106&Page_Num=&left=&item=&find=&m=134