Ingénierie des Systèmes d'Information
Vol. 30, No. 8, August, 2025, pp. 2175-2188
Journal homepage: http://iieta.org/journals/isi

A Lightweight Authentication and Resource Optimization Scheme for Secure Internet of Drones in Critical Applications

Ahmad Jamal Ahmed[1], Mohammed I. Khalaf [2*], Mahmood Alsaadi[2]

[1] Department of Electrical Engineering, College of Engineering, University of Anbar, Al Anbar 31001, Iraq
[2] Department of Computer Sciences, College of Science, University of Al Maarif, Al Anbar 31001, Iraq

Corresponding Author Email: m.i.khalaf@uoa.edu.iq

https://doi.org/10.18280/isi.300823

Received: 13 July 2025
Revised: 15 August 2025
Accepted: 21 August 2025
Available online: 31 August 2025

Keywords:
Internet of Drones (IoDs), unmanned aerial vehicles (UAVs) or drones, Lightweight Authentication (LA) mechanism, Resource Optimization (RO)

ABSTRACT

Internet of Drones (IoDs) is one among the trending technologies that interconnects the unmanned aerial vehicles (UAVs) or drones to perform confidential operations, which is used in critical applications. The increasing demands for drone capture the attention of both the industrial and academic sectors. The other applications where drones are employed such as traffic, environment, and natural calamity management, Internet of Things (IoT), and smart cities. Alternatively, data transmission among drones becomes a risky process due to the security threats at the time of sensitive message exchange between several applications. So, it is essential to develop a highly protective security prototype to secure the confidential data transmission among the network devices, such as sensors, UAVs, Access Points (APs), and the Server. Thus, we developed the Design of Lightweight Authentication (LA) Mechanism with Resource Optimization (DLARO) in IoD to guarantee stable and reliable communication. The experimentation DLARO-IoD is performed in platform called NS2, also it offers maximum security and efficiency than another earlier research, such as RUAM-IoD, RAMP-IoD, SLAP-IoD, and BDTC-IoD. The DLARO-IoD method improves IoD networks by using LA and better resource allocation. DLARO-IoD is better for efficiency, security, and reliable communication in IoD applications. Performance analysis involves energy efficiency, packet loss rate, communication cost, malicious detection rate, throughput, data success rate, computational time, and overhead. During comparative analysis, we illustrate that the suggested DLARO-IoD accomplishes maximum security with minimum energy utilization, and the communication cost and computational time are lower compared with the other authentication methods, and it highly suitable for the IoD-based critical applications.

1. INTRODUCTION

IoD technology is the improved version of the Internet of Things (IoT) technology, that helps in the exchange of data using the Internet. IoD is otherwise called flying IoT, which connects the flying device, namely UAVs, which are termed as drones. It is defined as a layer-based controlled architecture that can effectively communicate with each other in a certain coverage area by controlling of airspace. The drones are equipped with some of the devices, such as sensors, actuators, and processors (to build a wireless link), which help to perform a wide range of communication [1]. IoD is offered for several confidential applications like military rescue operations, traffic surveillance, and medical applications. The usage of drones in the industries has increased, which has made the monitoring and surveillance operations perform intelligently [2]. The architecture of IoD is demonstrated in Figure 1.

Recently in drones have been getting advanced with including the future 6G-enabled IoT devices in them. To perform communication, the drones follow the basic principle that they effectively cover their location and transmit beacon messages to the objects that are deployed in their coverage area, which consists of the details such as location and power of the devices. The main issue with drones communicating is finding the best route to send data to ground IoT devices while using minimal energy [3]. In addition to this, the second most important drawback in the existing drone-based communication is that it suffers from a lack of security during confidential message transmission. There are several safety threats alongside drones present in the real-time application, such as data hacking, eavesdropping, and data manipulation in the drone [4, 5]. So, it becomes very imperative to design a security mechanism to protect the network from these external threats [6-8]. The security threats of the IoD network are illustrated in Figure 2.

In response to the above-mentioned issues in the IoD environment, this research provides a proper energy utilization and network authentication for the sensors and the UAVs. For that purpose, in this paper LA mechanism with RO is concentrated. The main suggestion of this study is described below.

Key contributions of the Research:

- To advance the security and efficiency of the IoD communication in this research, an Enhanced LA with

RO is proposed. Hence, the IoD communication is surrounded by various network threads, such as a replay attack.

- To achieve effective resource utilization in specific loads, the proposed DLARO-IoD hybrid MAC model is used with the combination of CSMA and TDMA models so that effective communication with low congestion and delay can be achieved in the network.
- The proposed approach mainly concentrated on providing security to the network devices using an enhanced LA mechanism, as well as effective utilization of resources using a RO process.
- Using these methods, the accuracy and reliability of the IoD communication are highly increased.

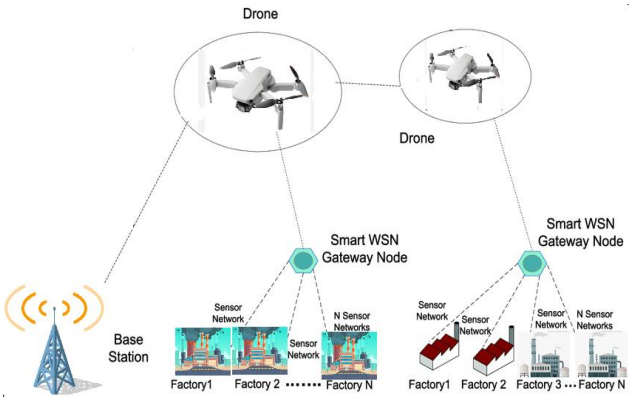

Figure 1. Architecture of IoD [5]

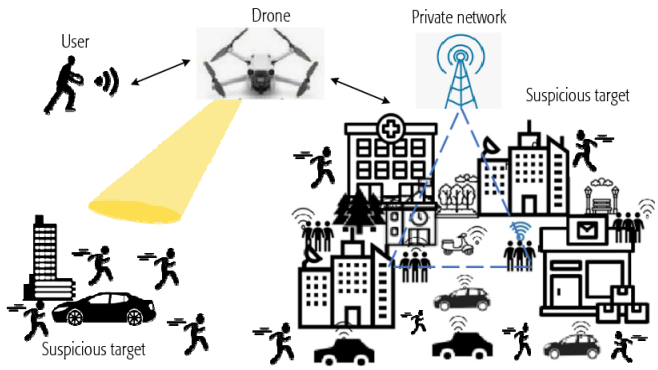

Figure 2. IoD security threats [9]

This paper is summarized as follows in this study. Section 2, The review of some related works about the earlier authentication methods is discussed. Section 3 describes the preliminaries of the research, such as the network model and attack model. In Section 4, the proposed LA mechanism RO is elaborated, while in Section 5, the results and discussion are presented. Section 6 presents the conclusion with the future direction.

2. LITERATURE REVIEW

Singh et al. [9] developed a blockchain-based security process for cyber-physical systems to ensure the safe transmission of data between drones. Though it provides security with minimum computational cost, the Communication cost, the rate of transactions per unit of time is limited. Lei et al. [10] proposed an authentication protocol to optimize the authentication process for UAV networks. Though this protocol offers security, the computational cost is high. Nguyen et al. [11] developed an advanced drone-based system to overcome the limitations like energy inefficiency, quality of service, shortages of automation, and security issues in SAR systems. In addition, offloading approaches are used to enhance the energy efficiency and minimize the system latency. This proposed system achieves security requirements, but it increases the operational time. Chaudhry et al. [12] designed a generic certificate based on an access control scheme in an IoD environment. The RoR model is used to perform the security analysis. This scheme provides security, but it has limitations in computational and communication efficiency.

Bera et al. [13] proposed a blockchain-based authentication and control scheme to identify the unauthorized UAVs in the Internet of Drone environment. The RoR model helps to prevent various attacks in the IoD. The performance of ACSUD-IoD has high efficacy in computational and communication overhead, but the operational time has increased. Nikooghadam et al. [14] proposed an authentication technique for elliptic curve cryptography for Drones in the modern city. Though this technique provides security but the computation process is complex. Qureshi et al. [15] introduced an innovative Trust and Priority-based Drone Assisted Internet of Vehicles (TPDA-IoV) method to eliminate any serious problems in the network. This solution obtains high performance in the packet delivery ratio. Zhang et al. [16] propose a LA and Key Agreement scheme to resolve the security problems. This method achieves security with low communication cost, but the packet delivery ratio is moderate. The study by Bera et al. [17] focuses on enabling highly secure communication and solving privacy problems in drone-to-drone communication. In Addition, Oracle Model resists the various attacks. This scheme offers low communication and computational cost but a delay in operational time.

Hussain et al. [18] proposed an enhanced scheme to overcome the existing Wazid et al.'s scheme, which provides security issues against server and drone attacks. Though this scheme prevents attacks, but computational cost is high. Bera et al. [19] developed a unique blockchain-based to provide secure communication for IoT IoT-based agricultural environment. It provides better security, lower communication costs, but the functional features are complex. Ever et al. [20] developed a verification method in association with an elliptic curve to provide effective and efficient resilience against attacks for the WSN network. It consumes less energy with security, but the computational cost is high. Ch et al. [21] proposed a Blockchain Techniques (BCT)-dependent solution for improving privacy and security. In Addition, the Ganache platform is utilized to provide data security and privacy. The efficiency and security features perform well, but they increase the complexity of the computational process. Hussain et al. [22] developed an authentication scheme to prevent communication attacks between a user and a flying drone. Additionally, the Random oracle method is used for security analysis. This scheme provides high security, but the trade-off between security and efficiency is moderate.

Tanveer et al. [23] proposed a robust user authentication mechanism to improve the security in IoTs. The core idea of this mechanism random oracle model, which provides informal security against different pernicious security attacks. This method achieves low communication and computational cost. However, due to a lack of effective resource allocation,

the consumption of energy and other resources is high in this method. Tanveer et al. [24] especially developed a security method for the IoD network called a robust AKM protocol. This protocol combines certain authentication methods such as lightweight cryptography and elliptic-curve cryptography. Using this method, the communication and computational overheads are reduced, but even though the energy consumption and delay produced during communication are high in this network model. In the study [25], the author presented a Secure and LA Protocol to improve the security and efficiency of the IoD-based modern metropolitan area. The core idea of the proposed protocol is that a physical unclonable function (PUF). For that purpose, in this paper, a Design of LA Mechanism with RO is proposed, which concentrates on both network security and effective resource allocation to attain efficient and effective communication in IoD. The earlier research analysis is illustrated in Table 1.

Table 1. Earlier research summary

Ref.No	Methodology Details	Cryptography Technique	Advantages	Limitations	Application Context
[9]	Blockchain-based Security Mechanism for Cyber-Physical Systems	RES Cryptography	Computational Resources are Maximum	Time Consumption is Maximum	Safe data transmission between drones
[10]	Optimized Identity Authentication Protocol	Double Data Encryption Standard (2DES)	Computing Resource and Security are Maximum	Communication Cost is Maximum	UAV network authentication
[11]	Blockchain and Artificial Intelligence	AES256 and ChaCha20	Authentication and Tolerance are Maximum	Time Consumption is Maximum	Search and Rescue (SAR) systems
[12]	A Certificate-based Generic Access Control Scheme	Elliptical Curve Cryptography (ECC)	Computation and Communication Efficiency is Maximum	Computation and Communication Cost is Maximum	IoD environment
[13]	Access Control Scheme for Unauthorized UAV Detection and Mitigation	Elliptical Curve Cryptography (ECC), AES-128	Network Efficiency and Robustness are maximum	Time Consumption is Maximum	Unauthorized UAV detection in IoD
[14]	Secure Authentication Scheme Based on Elliptic Curve	Elliptical Curve Cryptography (ECC) with hash operations	Computation and Communication costs are Minimum	Time Consumption is Maximum	Drones in a modern city
[15]	Drone-Assisted Internet of Vehicles based on Trust and Priority	Trust Model	Moderate delay and Routing Overhead	Communication and Computation Cost is high	Internet of Vehicles
[16]	LA	AKA schemes	Computation and Communication Cost is Minimum	Packet Delivery Ratio is Moderate	UAV security problem resolution
[17]	Blockchain-based Access Control Scheme	Elliptical Curve Cryptography (ECC)	Computation and Communication Cost is Minimum	Time Consumption is Maximum	Privacy and secure UAV communication
[18]	Secure And Lightweight User Access Model	Secure Hash Standard (SHA-1)	High Authentication and Low Packet Loss	Energy and Time consumption are Maximum.	UAV and server communication security
[19]	Private Block-Chain Envisioned Authentication Scheme	Elliptical Curve Cryptography (ECC)	Communication Cost is Minimum	Time Consumption is Maximum	IoT-based agricultural environment
[20]	A Secure Authentication Scheme Framework	AES-128, ECC Scheme and SHA-1	Data Confidentiality, Mutual Authentication,	High Computational Time	Wireless Sensor Networks
[21]	Blockchain Technology-based Secure Communication	Secure Hash Standard (SHA-1)	Efficiency and Security are Maximum	Communication and Computation Cost is high	Privacy and security improvement
[22]	An ECC-Based Authentication Scheme	Elliptical Curve Cryptography (ECC)	Security is Maximum	High Delay and Energy Consumption	User-drone communication attacks
[23]	Robust User Authentication Mechanism for The IoD	AKA schemes	Computation and Communication Cost is Minimum	Energy Consumption and Resource Utility are Maximum	IoT security improvement
[24]	A Robust and Resource-Efficient AKM Protocol.	Elliptical Curve Cryptography (ECC)	Computation and Communication Overhead is Minimum	Storage is minimal	IoD network security
[25]	Secure and LA Protocol	Secure Hash Standard (SHA-1)	Efficiency and Security are Maximum	Communication and Computation Cost is high	IoT-based agricultural environment
[26]	Bio-inspired dynamic trust.	Dynamic Trust Model	Computation and Communication Overhead is Minimum	Energy Consumption and Resource Utility are Maximum	IoD modern metropolitan area communication

3. PRELIMINARIES

3.1 Node deployment in the network

The UAV sensing network consists of several kinds of nodes in its architecture, such as servers, Access Points (APs), UAVs, and Sensors. The server is the main processing sector, and it is equipped with maximum computing power and computing resources. The AP is used to perform complex operations in the network, where it also consists of high-power and computing resources. UAVs are used as data collectors, and they hold high power. A sensor is used to perform simple calculations with limited power and resources. The network model is hierarchically described in Figure 3, which includes the server, APs, UAVs, and sensors.

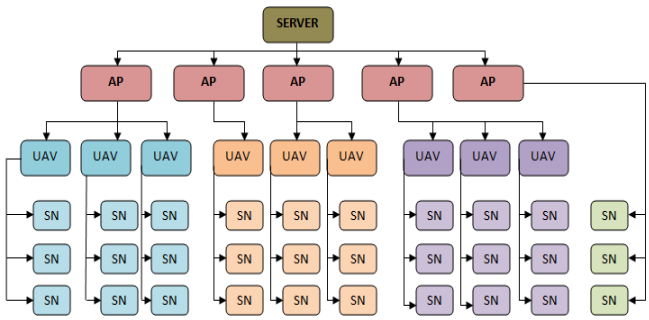

Figure 3. Hierarchical network model

The network is designed in a way that the entire network is equipped with hierarchically equipped in the IoD system. To achieve feasible and secure communication, the deployment of nodes is structured in provisions of disjoint clusters. To accomplish effective results, the transmission is not performed in the order of the hierarchical network model rather follows a certain structure. The nodes are divided into certain clusters, and two or more clusters are controlled by the UAVs. In the first case, through UAVs, the APs gather the data from a large number the sensors, then forward it to the server. In the second case, through the APs, the server collects the information of the UAVs without the presence of the sensors. In the final case, without any presence of UAVs, the APs gather the data from a variety the sensors directly and then transfer it to the server. This communication model is mainly encouraged to achieve the security requirements of IoDs in a critical application. This kind of network communication is suitable for providing authentication effectively, and the authentication procedure of this network is illustrated in the next section.

3.2 Attack model

We demonstrate in this section the most important features related to the attack model as follows:

1. Relay Attack – It is a kind of attack that creates eavesdropping on the communication channel, which results in huge data loss during communication. The proposed work is developed to increase the difficulty for the attacker to hack the data, where each sensor consists of a valid authentication in it. Reply attack mainly happens during the transmission between the sensors and the UAVs, so that the authentication of these devices is highly concentrated in the proposed model.

2. Traceability Attack – In this attack model, the attackers find the internal state of the sensor with the help of the transmission history (previous data) and its unavailable values. Using the proposed authentication process, the sensors' IDs and Passwords become highly secured so that the data of each sensor is highly authenticated and secure.

3. Denial of Service (DoS) Attack – In this kind of attack, the attacker frequently blocks the communication channel between the sensors and the UAVs. So, the UAVs lost communication with the sensors. Our proposed authentication process secures the communication channel from attackers using its secret key generation.

4. Man-In-The-Middle Attack – Using this attack, fake data packets are received by the UAVs, which greatly increase the energy consumption and delay, likewise reducing the resource utilization during communication. Using the proposed authentication process, the server authentication the secret keys to the sensors and the UAVs so that the fake sensors can be easily identified by the UAVs.

4. PROPOSED DLARO-IOD APPROACH

The proposed approach in this research is developed to provide authentication and proper resource utilization of UAVs to achieve high performance in an IoD environment. This section is divided into two segments: the improved LA mechanism and RO. The model of the DLARO-IoD Approach is shown in Figure 4.

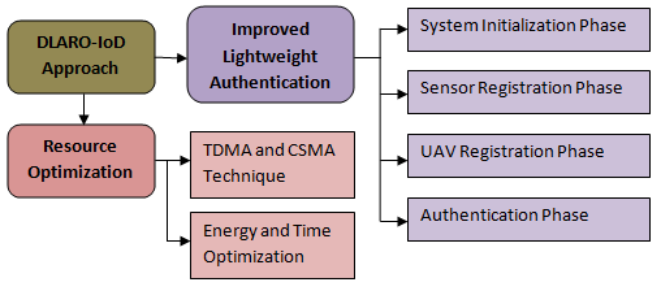

Figure 4. Workflow of the proposed DLARO-IoD approach

4.1 Improved Lightweight Authentication mechanism

Table 2. Notations

Notation	Definition
MSK	Master Private Key
PSK	Primary Shared Key
Q_i	Larger prime number with i {1,2,3,4}
MK	Mask Key
$PSKID_S$	PSK-based sensor Identity
SID_i	Initial sensor Identity
SK	Secret Key
$s(U_{\downarrow}(i,)Q_{\downarrow}i)$	Sensor Representation
SPW_i	Sensor Password
PSK_i	Prime number representation $Q_3 * Q_4$
PSK_j	Prime number representation $Q_1 * Q_2$
$UAV\ (U_{j,}Q_j)$	UAV Representation
θ_i and θ_j	Master Private Keys

The authentication process in our improved LA mechanism is divided into three sections: the first Phase, the Sensor and UAVs process Stage. In the initialization phase, the primary security activities for each sensor are performed in IoD. In the sensor and UAVs registration phase, essential security parameters are constructed according to the hierarchical

network architecture. In the authentication phase, continuous authentication is applied for all types of transmissions in the network. The definitions of the notations are shown in Table 2.

4.1.1 Initialization phase

During this phase, the server produces its master private key (MSK) and other essential parameters for each sensor. Before generating the MSK, the server produces four private keys $Q_1, Q_2, Q_{3,}$ and Q_4. The other process is followed below.

1. Primary shared keys (PSK) are generated using large prime numbers Q_i, and $i = \{1,2,3,4\}$. These PSKs are present in the memory of all devices in the network, such as sensors, UAVs, APs, and servers (S).
2. Server selects a 160-bit MSK at random, a 160-bit mask key MK, and the PSK with prime Q_i.
3. S selects a high security based one-way hash function which includes PSK where $h: \{0,1\}^* \rightarrow Z_n^*$, its identity ID and computes $PSKID_S = h(SID_S \| MK)$.
4. S stores $(MSK, MK, PSK, Q{\downarrow}i)$ in a confidential manner to publish $(h, s, PSKID_S, Q_i)$.

4.1.2 Sensor registration phase

In this phase, sensor $s(U_{i,}Q_i)$, which is equipped with respective Q_i enters the IoD environment with its unique identity, which gets registered with the server S, and collects its SK through a secure channel.

Here, they can communicate with each other securely after the establishment of their session key.

In this phase, sensor $s(U_{i,}Q_i)$, which is equipped with respective $Q_{i,}$ enters the IoD environment with its unique identity, which gets registered with the server S, and collects its SK through a secure channel.

5. Here, the sensor is represented as $s(U_{i,}Q_i)$ randomly chooses its identity SID_i and password SPW_i, then sends by transmitting the registration request to S.
6. Receiving the request packets from evaluates $PSKID_i = h(SID_i \| MK)$, $\theta{\downarrow}i = h(S[ID]{\downarrow}i \| MSK \| PSK \| Q{\downarrow}i)$, and stores $(S[ID]{\downarrow}i, \theta{\downarrow}i, [PSKID]{\downarrow}i)$ in list L_S securely. Then S sends (θ_i, PID_i, PID_j) to $s(U_{i,}Q_i)$ through a secure channel.
7. PSK is divided into two sections with the help of four large prime numbers $Q_1, Q_2, Q_{3,}$ and $Q_{4,}$ where $PSK_i = Q_3 * Q_4$ and $PSK_j = Q_1 * Q_2$.
8. $s(U_{i,}Q_i)$ receives $(\theta_i, PSKID_i, PSKID_j, PSK_i, PSK_j)$ and computes $\theta_i^m = h(SID_i \| SPW_i) \oplus \theta_i$, $PSKID_i^m = h(SID_i \| SPW_i) \oplus PSKID_i$. Finally, $s(U_{i,}Q_i)$ stores θ_i^m. The local memory of the $s(U_{i,}Q_i)$ is responsible for storing these details.

4.1.3 UAVs registration phase

In this, UAV admits its ID to S to obtain its secret key. The procedure for this process is described below.

1. UAV $(U_{j,}Q_j)$ randomly selects its identity ID_i and sends it with a registered request to S.
2. S evaluates $PSKID_j = h(SID_j \| MK)$, $\theta_t j = h(PS[ID]{\downarrow}j \| MSK \| PSK \| Q{\downarrow}i)$, and stores $(SID_j, \theta_j, PSKID_j)$ in list L_S securely. Finally, to UAV $(U_{j,}Q_j)$ through a secure channel.
3. PSK is divided into two sections with the help of four large prime numbers $Q_1, Q_2, Q_{3,}$ and $Q_{4,}$ where $PSK_i = Q_3 * Q_4$ and $PSK_j = Q_1 * Q_2$.
4. UAV $(U_{j,}Q_j)$ receives and confidently stores them. The local memory of the UAV $(U_{j,}Q_j)$. It is responsible for storing these details.

4.1.4 Authentication phase

The two registered sensors and UAV are $s(U_{i,}Q_i)$ and UAV $(U_{j,}Q_j)$ are considered in this authentication process. Here, they can communicate with each other securely after the establishment of their session key.

1. s $(U{\downarrow}(i,)Q{\downarrow}i)$ first inputs identity SID_i and password SPW_i and the it will evaluate $[PSKID]{\downarrow}i = [PSKID]{\downarrow}i^{\uparrow}m \oplus h(S[ID]{\downarrow}i \| [SPW]{\downarrow}i \| Q{\downarrow}i)$, $\alpha{\downarrow}i = h(S[[ID]]{\downarrow}i \| [[SPW]]{\downarrow}i \| Q{\downarrow}i) \oplus \theta{\downarrow}i^{\uparrow}m$. The function $r_1 \in Z_n^*$ is randomly selected and consists of 160 bits, and the current time stamp ST_1. Lastly, the authentication request packets $(RP_{1,}\, RP_{2,}\, RP_{3,}\, RP_4)$ to S through a public channel are transmitted.

$$RP_1 = h(PSKID_S \| ST_1 \|) \oplus PID_i \quad (1)$$

$$RP_2 = h(PSKID_i \| PSID_S \| \theta_i) \oplus r_1 \quad (2)$$

$$RP_3 = h(PSKID_i \| PSID_S \| \theta_i \| r_1 \| Q_i \| PSK_i) \oplus PSID_j \quad (3)$$

$$RP_4 = h(PSKID_i \| PSID_S \| PSID_j \| \theta_i \| r_1 \| Q_i \| Q_j \| PSK_i \| PSK_j) \quad (4)$$

2. After receiving the authentication packet $(RP_{1,}\, RP_{2,}\, RP_{3,}\, RP_4)$ from $s(U_{i,}Q_i)$, S first checks the validation at each instant of time, where $t_{i,2} - T_{i,1} \leq \Delta T$ is the maximum threshold time to accept the packets and $t_{i,2}$ implies the time taken to receive the request packets. If it is true, S starts the main authentication process; else, authentication packets were neglected by S. Then it computes.

$$RP_1 \oplus h(PSKID_S \| ST_1 \| Q_i \| PSK_i) \quad (5)$$

And retrieves α_i' in the list of $L_{S,}$ then S computes,

$$r_1' = RP_1 \oplus h(PSKID_i' \| PSKID_S \| \theta_i' \| PSK_i) \quad (6)$$

$$PID_j' = RP_3 \oplus h(PSKID_i' \| PSKID_S \| \theta_i' \| r_1' \| Q_i \| PSK_i) \quad (7)$$

$$RP_4' = h(PSKID_i' \| PSKID_j' \| \theta_i' \| r_1' \| Q_i \| Q_j \| PSK_i \| PSK_j) \quad (8)$$

3. S checks the validation of $RP_4' = RP_4$. If they are equal, S can authenticate $s(U_{i,}Q_i)$ and retrieve θ_j' in the list L_S through $PSKID_j'$, then continue to do the following process. Else S neglects the request packet. At last, S sends request packets $(RP_{5,}\, RP_{6,}\, RP_7, RP_8)$ to UAV $(U_{j,}Q_j)$ via public channel.

$$RP_5 = h(PSKID_j' \| \theta_j' \| PSK_i) \oplus r_1' \quad (9)$$

$$RP_6 = h(PSKID_j' \| PSKID_S \| \theta_j' \| r_1' \| Q_i` \| PSK_i) \oplus PID_i' \quad (10)$$

$$RP_7 = h\left(PID_i' \,\|\, PID_j' \,\|\, PID_S \|\theta_j' \|r_1'||Q_i||Q_j||PSK_i||PSK_j\right) \quad (11)$$

4. After receiving message (RP_5, RP_6, RP_7) from S, $UAV\ (U_j Q_j)$ proceeds.

$$r_1'' = RP_5 \oplus h\left(PSKID_j \|\theta_j ||PSK_i\right) \quad (12)$$

$$PSKID_i'' = SK_6 \oplus h\left(PSKID_j \,\|\, PSKID_S \|\theta_j \|r_1''||PSK_j\right) \quad (13)$$

$$RP_7' = h\left(PSKID_i'' \,\|PSKID_j \,\|\, PSKID_S \|\theta_j \|r_1'' ||PSK_i||PSK_j\right) \quad (14)$$

5. $UAV\ (U_j Q_j)$ checks the validation of $RP_7' = RP_7$. If it does not hold, $UAV\ (U_j Q_j)$ rejects the request packet. Else $UAV\ (U_j Q_j)$ authenticate S and it chooses the function $r_2 \in Z_n^*$, which is 160 bits. Then the following steps are processed. Finally, $UAV\ (U_j Q_j)$ sends packets $(RP_8, RP_{10})\ to\ \mathrm{s}(U_i Q_i)$ via public channel.

$$RP_8 = h\left(\| PSKID_j \|PSKID_i'' \|r_1''||PSK_i||PSK_j\right) \oplus r_2 \quad (15)$$

$$RP_8 = h(r_1''\|r_2) \quad (16)$$

$$SK_{ji} = h\left(\|PSKID_j \,\|\, PSKID_S \|RP_9||PSK_i||PSK_j\right) \quad (17)$$

$$RP_{10} = h\left(\|PSKID_j \,\|\, PSKID_S \|r_1''\|r_2 \|PSK_i||PSK_j||RP_9\right) \quad (18)$$

6. When $s(U_i Q_i)$ receives message (RP_8, RP_{10}) verifies the validation of $(RP_{10}' = RP_{10})$. If they are equal, $s(U_i Q_i)$ can authenticate $UAV\ (U_j Q_j)$ and calculate the common session key.

$$SK_{ij} = h\left(\|PSKID_j \,\|\, PSKID_S \,\|r_1''\|r_2 \,\|PSK_i||PSK_j||RP_9'\right) = SK_{ji}$$

Else, $\mathrm{s}(U_i Q_i)$ rejects the request.

$$r_2' = h\left(PSKID_i \|PSKID_j \,\|r_1||PSK_i \,||PSK_j\right) \oplus RP_8 \quad (19)$$

$$RP_9 = h(r_1||r_2) \quad (20)$$

$$RP_{10}' = h\left(PSKID_i' \,\|PSKID_j \,\|PSKID_S\|r_1 \,\|r_2'||PSK_j||PSK_i \,||\, Q_i||Q_j\right) \quad (21)$$

$$SK_{ij} = h\left(PSKID_i \|PSKID_j \,\|PSKID_S\|RP_9'||PSK_j||PSK_i||\, Q_i||Q_j\right) \quad (22)$$

4.1.5 Forward authentication

After the process of authentication, this mechanism updates the parameters used. Each round follows a unique model in this process. In case the current round data packets are leaked, then the authentication becomes highly secured in the next rounds. So that it can able to support both the forward and backward security in the IoDs. Based on the attackers, such as replay attack, traceability attack, man-in-the-middle attack, and denial of service attack, the attacker model's capability is analyzed.

4.2 Resource Optimization

In the case of the uplink scenario, in which sensors send data to the server carried by the UAV. To serve all sensors, UAV employs Carrier Sense Multiple Access (CSMA) and the Time Division Multiple Access (TDMA) technologies. According to this technology, all the sensor utilizes the energy from a common source with a total E_t Watt budget. The functional application of this energy budget consists of certain features, such as Priority transmitters (PTXs) with solar panels, sensors that are linked to a single energy source, and distributed antenna systems (DASs), in which different antennas are positioned at various locations and are connected to the server through the wired medium. According to the spectral efficiency in bits per second per hertz (bps/Hz), the $\mathrm{s}(U_i Q_i)$ communication with $UAV\ (U_j Q_j)$ is mathematically expressed for SNR calculation, as given in Eq. (1).

$$S_{Eff} \triangleq \{0,1\}\log_2 [[(1+\gamma_i]]) = \{0,1\}\log_2 [[(1 + E_i g_i/\sigma^2]]) \quad (23)$$

In Eq. (23), the S_{Eff} implies the spectral efficiency, E_i implies the energy allocated to the sensors $\mathrm{s}(U_i Q_i)$, $\forall_i \varepsilon T_0$ implies the block duration according to the time factor, and g_i implies the input gain. To perform effective resource allocation and to transmit the data packets to the $UAV\ (U_j Q_j)$ from the $\mathrm{s}(U_i Q_i)$, the spectral efficiency (S_{Eff}) of the sensor has to be greater than its threshold rate (T_{rate}), which is $S_{Eff} > T_{rate}$. To achieve our main objective, which is effective resource allocation to sensors, the UAV has to serve the maximum number of sensors with energy and time resources in a satisfying manner. All kinds of sensors (Users) are considered here with a varying range of data utility, and it gets prioritized with the help of the TDMA and CSMA technology. The sensor with the maximum data rate transmits the data using the TDMA technique, and the sensor with a low data rate uses the CSMA technique for data transmission.

As a result, downlink communication can also benefit from coverage analysis and joint optimization. In the downlink situation, the UAV is responsible for allocating the entire energy budget E_t to each sensor. For periodic events, UAVs are deployed in terrestrial base stations. They can also be utilized as flying base stations for public safety situations. In such circumstances, the main objective is to provide as many sensors with the available energy resources in a feasible manner. With the help of priority-based data transmission, effective performance is achieved in the IoD communication in critical applications.

5. SIMULATION ENVIRONMENTS AND PERFORMANCE ANALYSIS

The performance of the DLARO-IoD approach was evaluated using NS-2 simulation and the SUMO mobility model. Key parameters analysed include end-to-end delay, communication cost, data success rate, malicious detection rate, packet loss rate, energy efficiency, throughput, and

overhead. Additionally, the suggested DLARO-IoD approach is contrasted with more recent techniques such as RUAM-IoD [23], RAMP-IoD [24], DLARO-IoD [25], and BDTC-IoD [26]. Two scenarios—varying node counts and speed variations—are used to conduct the performance analysis. In essence, NS2 is an event-driven simulator that uses both the back-end language (C++) and the front-end language. Table 3 illustrates the input simulation, which focused in the parameters that are applied in the simulation process.

5.1 Comparative performance analysis by number of devices

This section measures the simulation results based on the number of nodes and provides a graphical description of the results for methods such as RUAM-IoD, RAMP-IoD, SLAP-IoD, BDTC-IoD, and the planned DLARO-IoD. End-to-end latency, energy efficiency, packet loss rate, data success rate, communication cost, malicious detection rate, throughput, and overhead are the parameters utilized in performance evaluation.

Table 3. Input simulation parameters

Parameters	Values
Simulator	NS2
Drone Mobility Model	SUMO
Time	500 ms
Network Coverage	2000m*2000m
Number of Devices	100 devices
Number of Drones	10 Drones [SLoDT][26]
Drone Transmission Range	5 Km [SLoDT][26]
Antenna Type	Omni-directional Antenna
UMTS Threshold	-94 dBm [SLoDT][26]
Queue Type	DropTail
Maximum Iteration	50 [8]
Drone Bandwidth	50 Mbps
Transmission Power	0.500 Joules
Receiving Power	0.050 Joules
Sending Rate	1HZ [8]

5.1.1 Computation of end-to-end delay

With the support of a LA process, the packet loss and forwarding rate are reduced. On the other hand, due to the resource allocation process, the delay is reduced. The high performance of the proposed DLARO-IoD approach is based on the combination of optimized resource allocation and authentication. For this purpose, the proposed solution is much better for the IoD environment in Figure 5.

The previous methods mainly focus on security, neglecting other important aspects like RUAM-IoD, RAMP-IoD, SLAP-IoD, and BDTC-IoD. For that reason, the energy consumption of the high-speed UAVs is increased during communication because of improper resource allocation. When UAVs move faster, it increases the delay and overcomes in the earlier solutions. To overcome this drawback in the proposed solution, with an enhanced authentication process, RO is also performed, which greatly helps to improve the performance of the IoD communication.

5.1.2 Communication cost calculations

The communication cost performance is illustrated in Figure 6. The DLARO-IoD technique offers the lowest communication cost compared to other methods. In addition to that, the improved LA is producing secret keys using a highly secure one-way hash key. Using this secret key, the transmission between the sensors and the UAVs becomes highly secure and confidential. So, the network produces low delay, overhead, and packet loss during transmission of the data packets, which reflects in the reduction of communication cost when compared with the earlier research. Alternatively, by the use of resource allocation in the network, the energy and time consumption in the network is reduced even which will also help in the maintenance of minimum communication cost until the end of the simulation.

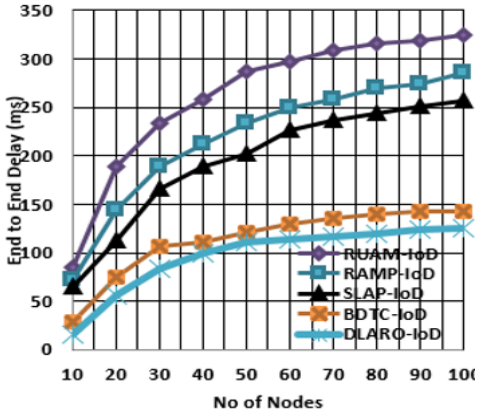

Figure 5. End-to-end delay

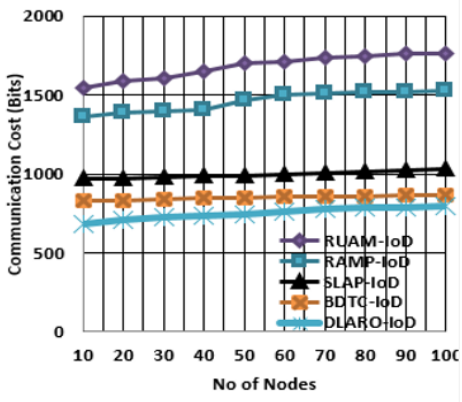

Figure 6. Communication cost

5.1.3 Malicious detection rate calculations

Figure 7 shows that the DLARO-IoD method has the highest detection rate for malicious behavior in network data transmission. In contrast, quicker solutions like RUAM-IOD, RAMP-IOD, SLAP-IOD, and BDTC-IoD have only moderate detection ratios. Hence, the performance of these solutions is not highly suitable for high-speed IoD communication. The proposed DLARO-IoD approach performs optimal sensor reliability by effectively detecting the malicious activities qualitatively and quantitatively.

5.1.4 Estimation of packet loss ratio

The hybrid MAC model combines TDMA and CSMA. Figure 8 shows that DLARO-IoD has less packet loss compared to others. Hence, the packet transmission from the source to the destination is separated according to the congestion level. The packet is tremendously reduced, which reflects in the increase of the delivery ratio and throughput of the networks when compared with the earlier methods like

RUAM-IOD, RAMP-IOD, SLAP-IOD, and BDTC-IoD.

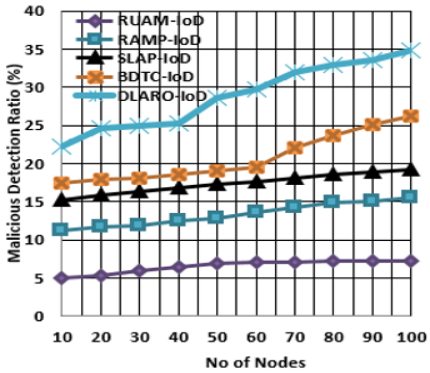

Figure 7. Malicious detection rate

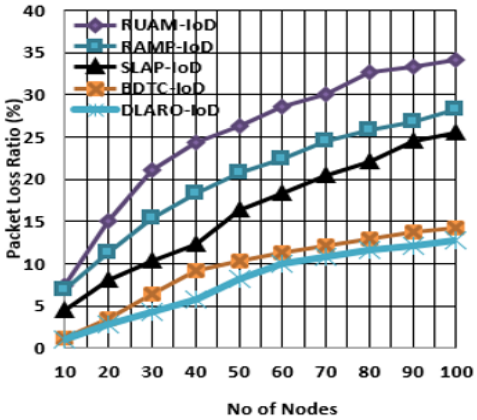

Figure 8. Packet loss rate

5.1.5 Estimation of data delivery success ratio

The suggested solution offers better data success due to efficient LA and RO, as shown in Figure 9. The maximum success rate in data transmission is achieved by the proposed solution with the help of the enhanced authentication and RO process. Using this method, the network efficiency and security are highly increased, and likewise, the energy and time consumption are reduced. The network architecture is designed in the way that to achieve the highest energy efficiency. All these parameters are connectively helped to help achieve maximum data success rate in the suggested DLARO-IoD approach.

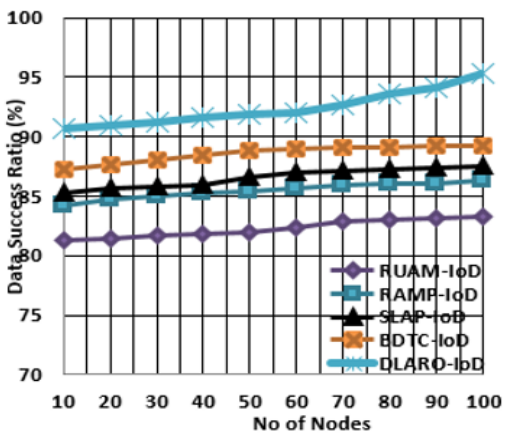

Figure 9. Data success rate

5.1.6 Overhead calculations

The DLARO-IoD method creates less overhead compared to current solutions, as shown in Figure 10. It offers the best performance through effective authentication and resource management. The structure of the network is better designed and well-connected to avoid the overhead occurrence in the network. On the other hand, RO is performed to achieve the highest energy efficiency during the communication between the UAVs and the sensors. The major disadvantages in the earlier solutions are a lack of resource allocation, and that issue is solved using our proposed solution in the IoD communication.

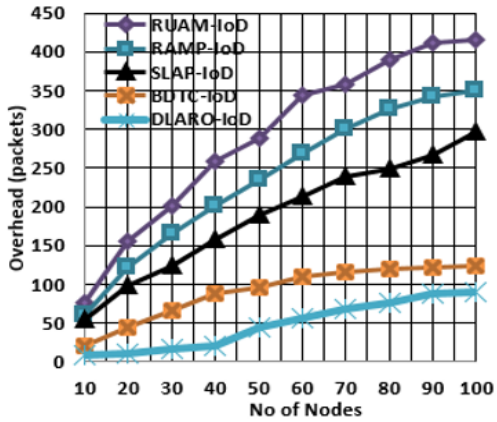

Figure 10. Overhead

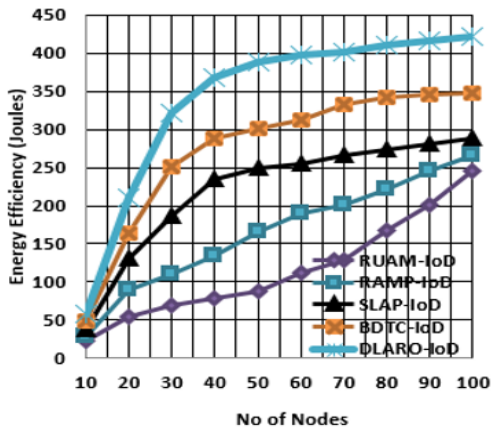

Figure 11. Energy efficiency

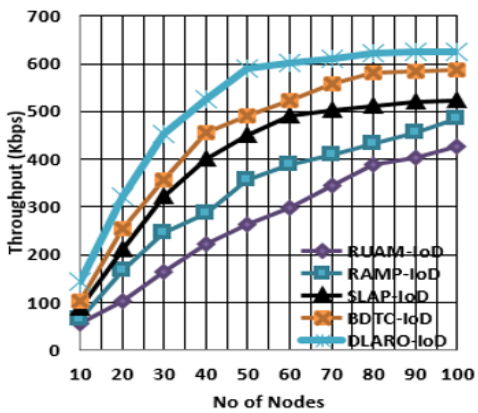

Figure 12. Throughput

5.1.7 Computation of energy efficiency

It is shown that the proposed DLARO-IOD outperforms the previous methods, such as RUAM-IOD, RAMP-IOD, SLAP-IOD, and BDTC-IoD. A graphical representation of the energy efficiency computation is shown in Figure 11. The proposed DLARO-IOD enhances efficiency by using effective authentication to lower data loss, latency, overhead, and energy use.

5.1.8 Calculation of system throughput

The research shows that the proposed DLARO-IOD achieves higher throughput than previous methods like RUAM-IOD, RAMP-IOD, SLAP-IOD, and BDTC-IoD in Figure 12. Using effective authentication and a hybrid MAC model, packet loss and routing overhead are greatly reduced, which leads a way to transmitting huge data in the network, that reflected in the increase of network throughput during communication.

5.2 Results and discussion

The simulation results are examined in detail in this section to analyse the effectiveness of the suggested DLARO-IOD strategy as well as techniques like RUAM-IoD, RAMP-IoD, SLAP-IoD, and BDTC-IoD. Performance evaluation metrics include malicious detection ratio, communication cost, data success rate, processing time, packet loss rate, overhead, energy efficiency, and throughput, as indicated in Tables 4 and 5.

Table 4. Data success ratio, communication expense, and malicious detection ratio are measured for performance

No of Nodes	RUAM-IoD	RAMP-IoD	SLAP-IoD	BDTC-IoD	DLARO-IoD	RUAM-IoD	RAMP-IoD	SLAP-IoD	BDTC-IoD	DLARO-IoD	RUAM-IoD	RAMP-IoD	SLAP-IoD	BDTC-IoD	DLARO-IoD
	Malicious Detection Ratio (%)					Communication Cost (Bits)					Data Success Ratio (%)				
10	4.96	11.28	15.2	17.45	22.31	1548	1358	968	828	681	81.26	84.2	85.2	87.19	90.75
20	5.34	11.67	15.8	17.94	24.65	1587	1387	972	834	711	81.38	84.6	85.6	87.64	91.01
30	5.99	11.93	16.3	18.08	24.94	1603	1399	978	839	726	81.64	84.9	85.8	87.99	91.23
40	6.42	12.45	16.8	18.64	25.31	1648	1408	985	845	738	81.86	85.2	85.9	88.45	91.64
50	6.97	12.86	17.2	18.97	28.66	1699	1467	989	849	746	81.99	85.3	86.5	88.86	91.91
60	7.08	13.66	17.6	19.54	29.68	1708	1501	999	856	757	82.42	85.6	86.9	88.91	92.05
70	7.11	14.22	18.1	22.15	32.01	1734	1509	1008	859	780	82.89	85.8	87.1	89.11	92.67
80	7.21	14.87	18.6	23.64	32.98	1745	1515	1015	861	786	83.06	86.0	87.3	89.15	93.65
90	7.25	15.09	18.8	25.04	33.56	1761	1521	1023	863	791	83.21	86.1	87.4	89.21	94.16
100	7.29	15.47	19.1	26.17	34.78	1765	1524	1028	865	799	83.26	86.2	87.4	89.23	95.31

Table 5. Measurements of end-to-end latency, packet loss rate, and overhead performance

No of Nodes	RUAM-IoD	RAMP-IoD	SLAP-IoD	BDTC-IoD	DLARO-IoD	RUAM-IoD	RAMP-IoD	SLAP-IoD	BDTC-IoD	DLARO-IoD	RUAM-IoD	RAMP-IoD	SLAP-IoD	BDTC-IoD	DLARO-IoD
	End-to-End Delay (ms)					Data Loss Ratio (%)					Overhead (Packets)				
10	85.13	71.46	64.28	28.17	15.34	7.36	6.84	4.39	1.25	1.06	76	61	54	21	8
20	188.4	144.0	112.3	75.38	55.66	15.06	11.3	8.02	3.47	2.77	155	121	98	45	11
30	233.5	189.3	166.3	106.3	84.16	21.05	15.3	10.2	6.35	4.33	201	165	123	66	16
40	258.1	211.4	188.4	111.3	99.37	24.31	18.3	12.3	9.11	5.66	259	201	158	89	21
50	287.1	233.5	201.3	121.0	111.5	26.31	20.7	16.3	10.25	8.12	289	235	189	96	44
60	297.3	249.3	226.3	129.0	114.4	28.58	22.4	18.3	11.31	9.99	344	268	214	111	56
70	308.6	258.3	236.5	135.4	116.3	30.07	24.5	20.4	12.03	10.87	359	301	238	116	68
80	315.4	269.3	244.2	139.8	119.3	32.57	25.8	22.0	12.87	11.65	389	326	249	119	76
90	319.3	274.3	251.0	142.0	124.3	33.25	26.8	24.5	13.66	12.04	411	343	267	121	88
100	325.1	286.1	256.1	143.2	125.8	34.13	28.1	25.4	14.23	12.68	415	351	296	124	91

The Malicious detection ratio of the DLARO-IOD approach is 34.78% while RUAM-IOD, RAMP-IOD, SLAP-IOD, and BDTC-IOD reach up to 7.29%, 15.47%, 19.14%, and 26.17% respectively. The DLARO-IOD method has a malicious detection rate that is 7% better than BDTC-IoD, 14% better than SLAP-IOD, 19% better than RAMP-IOD, and 26% better than RUAM-IOD. The Communication Cost is received 799 Bits, whereas for the earlier methods as such as RUAM-IOD, RAMP-IOD, SLAP-IOD, and BDTC-IoD, it arrived at 1765 Bits, 1524 Bits, 1028 Bits, and 865 Bits, respectively. For this reason, the Communication Cost is 60 Bits lower than BDTC-IoD, 220 Bits lower than SLAP-IOD, 700 Bits lower than RAMP-IOD, and 950 Bits lower than RUAM-IOD. The DLARO-IOD method has a Data Success Ratio of 95.31%. In comparison, previous methods like RUAM-IOD, RAMP-IOD, SLAP-IOD, and BDTC-IoD achieved success ratios of 83.26%, 86.28%, 87.49%, and 89.23%. So, the Data Success Ratio is reached at 6 % better than BDTC-IoD, 7% better than SLAP-IOD, 8 % better than RAMP-IOD, and 12% better than RUAM-IO.

DLARO-IOD approach in terms of End-to-End Delay is reached to 7125.84 ms, whereas for the earlier methods as such as RUAM-IOD, RAMP-IOD, SLAP-IOD, and BDTC-IoD, it reaches up to 325.17 ms, 286.17 ms, 256.19 ms, and 143.26 ms, respectively, as shown in Table 5. The DLARO-IOD strategy has an end-to-end delay that is 18 milliseconds less than BDTC-IoD, 120 milliseconds less than SLAP-IOD, 150 milliseconds less than RAMP-IOD, and 200 milliseconds less than RUAM-IOD. The Data Loss Ratio is arrived at 12.68 % whereas for the earlier methods as such as RUAM-IOD,

RAMP-IOD, SLAP-IOD, and BDTC-IoD, it reaches up to 34.13 %, 28.17 %, 25.46 %, and 14.23 % respectively.

The DLARO-IOD method has a data loss ratio that is lower than several other methods: 2% less than BDTC-IoD, 12% less than SLAP-IOD, 15% less than RAMP-IOD, and 22% less than RUAM-IOD. It has an overhead of 91 packets, while recent methods like RUAM-IOD, RAMP-IOD, SLAP-IOD, and BDTC-IoD reach up to.

As a result of this, the Overhead of the proposed DLARO-IOD approach is 30 Packets lower than BDTC-IoD, 100 Packets lower than SLAP-IOD, 250 Packets lower than RAMP-IOD, and 310 Packets lower than RUAM-IOD.

5.3 Performance analysis under varying speeds

The section presents simulation results for various methods: RUAM-IoD, RAMP-IoD, SLAP-IoD, BDTC-IoD, and the new DLARO-IoD. These results are analyzed based on different speeds ranging from 50 km/h to 250 km/h. Key parameters measured include data success rate, malicious detection rate, packet loss rate, energy efficiency, throughput, overhead, communication cost, and end-to-end delay.

5.3.1 Calculation of malicious detection ratio

Figure 13 shows different speeds, which range from 50 km/h to 250 km/h. The DLARO-IoD method outperforms other techniques like RUAM-IOD, RAMP-IOD, SLAP-IOD, and BDTC-IoD in detecting harmful behavior during communication between sensor nodes and UAVs. As a result, the majority of malicious activity occurs in that position specifically. The suggested DLARO-IoD successfully achieves high sensor reliability with the aid of LA.

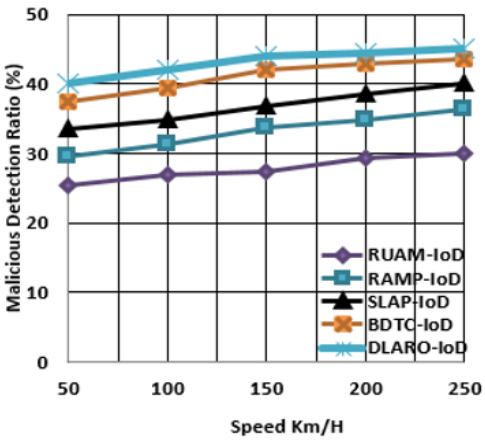

Figure 13. Malicious detection ratio

5.3.2 Calculation of network communication cost

Figure 14 suggests the communication cost design of the approaches such as RUAM-IOD, RAMP-IOD, SLAP-IOD, and BDTC-IoD and as well as it is compared with the proposed DLARO-IoD. Improved LA generates the secret keys using a highly secure one-way hash key. The sensor nodes and UAVs use a secret key to communicate. This reduces latency and overhead, leading to cheaper communication compared to past methods.

5.3.3 Data success ratio calculation

It is the proportion of successful data packets that are successfully sent from the source to the destination at varied speeds between 50 and 250 km/h. The data success ratio calculation is graphically illustrated in Figure 15, and it can be seen from this that the suggested DLARO-IoD performs better than the previous methods, like RUAM-IOD, RAMP-IOD, SLAP-IOD, and BDTC-IoD. The proposed model utilizes a hybrid MAC architecture in conjunction with LA. This integration guarantees that data packets are sent securely and without congestion, which greatly reduces the chances of data loss and consequently enhances the transmission success rate.

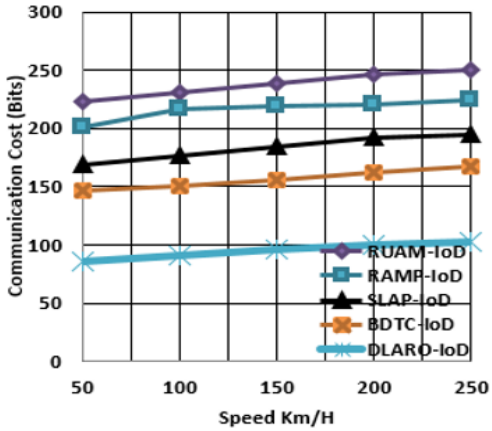

Figure 14. Communication cost

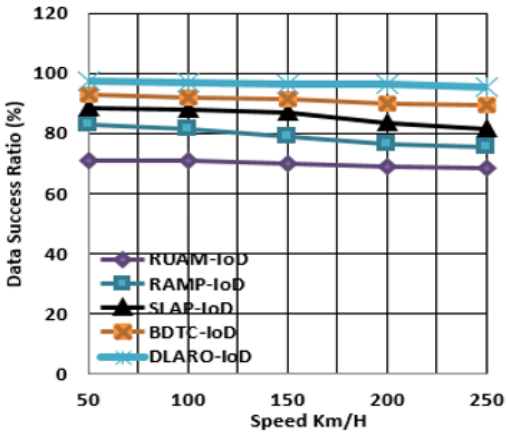

Figure 15. Data success ratio

5.3.4 Packet loss ratio calculation

The data packet loss measurements between the sensor nodes and the UAVs, which range in speed from 50 km/h to 250 km/h, are the focus of this study. When compared to the previous approaches, such as RUAM-IOD, RAMP-IOD, SLAP-IOD, and BDTC-IoD, it was demonstrated that the suggested DLARO-IoD produced minimal packet loss. Figure 16 illustrates the calculation of packet loss for the methods considered in this study. The hybrid MAC model divides data packets according to the degree of congestion between the UAVs and sensor nodes. As a result, the packet loss through congestion is reduced. On the other hand, the LA method protects the data packets using one-way hash keys. So that packet loss is greatly reduced when in a high-speed network.

5.3.5 Computation of end-to-end delay

In comparison to earlier techniques like RUAM-IOD, RAMP-IOD, SLAP-IOD, and BDTC-IoD, it has been demonstrated that the proposed DLARO-IoD results in a reduced end-to-end delay. The end-to-end delay computation

of the approaches taken into consideration in this study is displayed in Figure 17 at different speeds ranging from 50 km/h to 250 km/h. The hybrid MAC approach reduces the latency and energy consumption of high-speed UAVs and sensor nodes by detecting network congestion before initiating data transmission.

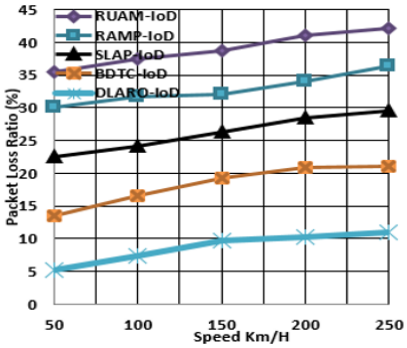

Figure 16. Packet loss ratio

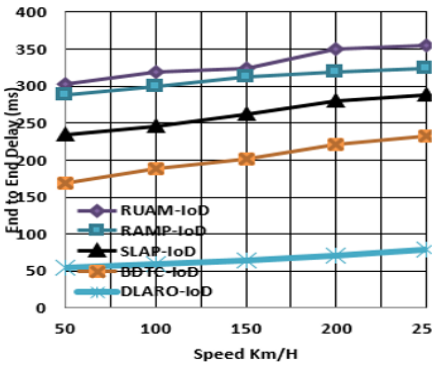

Figure 17. End-to-end delay

5.3.6 Computation of routing overhead

The process entails determining the overall quantity of data packets produced by the source, as well as the aggregate number of data packets transmitted to all sensor nodes and UAVs, while varying speeds range from 50 to 250 km/h. The graphical representation of the routing overhead computation in Figure 18 shows that the proposed DLARO-IoD produced low routing overhead in comparison to the previous approaches, such as RUAM-IOD, RAMP-IOD, SLAP-IOD, and BDTC-IoD. Utilizing the hybrid MAC model, the proposed DLARO-IoD demonstrates effective performance in reducing overhead, particularly at elevated speeds, when there is a significant volume of data being forwarded during the transmission between sensor nodes and UAVs.

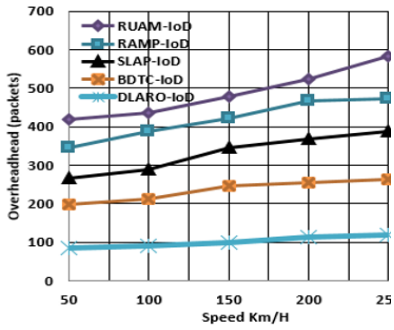

Figure 18. Routing overhead

5.3.7 Estimation of energy utilization efficiency

Figure 19 illustrates a graphical depiction of the energy efficiency calculation at various speeds, spanning from 50 km/h to 250 km/h. It has been shown that the proposed DLARO-IoD surpasses earlier methods, including RUAM-IOD, RAMP-IOD, SLAP-IOD, and BDTC-IoD, regarding efficiency. Each transmission within the proposed network is carried out effectively and with reduced energy consumption, which plays a crucial role in attaining optimal efficiency, even during high-speed data transfers within the network.

5.3.8 Throughput calculation

With changing speeds ranging from 50 km/h to 250 km/h, it calculates the maximum number of data packets that may be transmitted from all sensor nodes and UAVs. The throughput assessment of the methods evaluated in this research is illustrated in Figure 20, which demonstrates that the proposed DLARO-IoD achieved a higher throughput compared to earlier methods, including RUAM-IOD, RAMP-IOD, SLAP-IOD, and BDTC-IoD. The use of LA and the TDMA/CSMA model reduces packet loss and routing overhead during data transmission between sensor nodes and UAVs. This leads to the transmission of large data packets, which increases network throughput during communication.

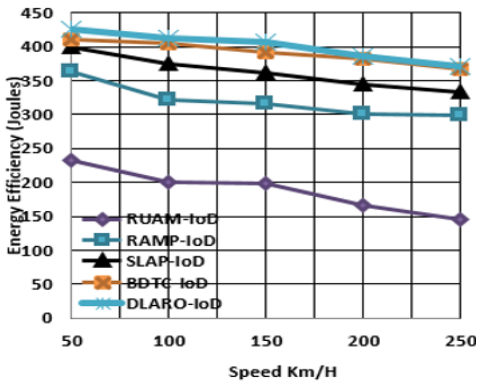

Figure 19. Energy efficiency

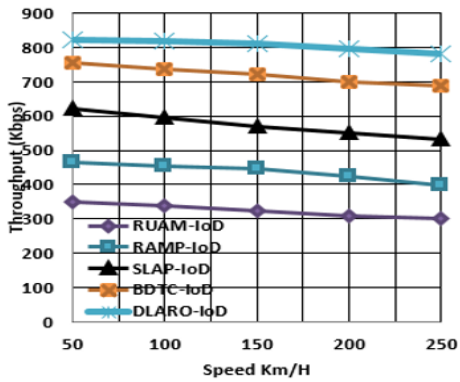

Figure 20. Throughput

5.3.9 P-value calculations

The analysis focuses on p-values across five groups to assess of findings. Group A has a low p-value of 0.01. Group B, with a p-value of 0.15. Group C has a p-value of 0.03. Group D has the highest p-value of 0.20, while Group E is on the edge of a p-value of 0.05. Groups A, C, and E, while B and D are not, is shown in Figure 21, the p-value calculation.

5.4 Performance results and discussion under variable speed conditions

This section analyzes the simulation outcomes of techniques, including RUAM-IoD, RAMP-IoD, SLAP-IoD, and BDTC-IoD, while also evaluating the proposed DLARO-IOD method in relation to varying speeds ranging from 50 km/h to 250 km/h. Malicious detection ratio, communication cost, data success rate, computing time, packet loss rate, overhead, energy efficiency, and throughput are the metrics used to assess performance. Tables 6 and 7 display the measurements of the computed parameters.

In contrast to the preceding approaches like RUAM-IOD, RAMP-IOD, SLAP-IOD, and BDTC-IoD, which have malicious detection ratios of up to 30.09 percent, 36.47 percent, 40.08 percent, and 43.59 percent, respectively, the proposed DLARO-IOD methodology has a malicious detection ratio of 45.22 percent. Therefore, the suggested DLARO-IOD approach's malicious detection ratio is 1% higher than BDTC-IoD, 5% higher than SLAP-IOD, 9% higher than RAMP-IOD, and 15% higher than RUAM-IOD.

The suggested DLARO-IOD strategy has a communication cost of 102.49 bits, while the previous approaches, including RUAM-IOD, RAMP-IOD, SLAP-IOD, and BDTC-IoD, have communication costs of up to 250.45 bits, 224.37 bits, 194.31 bits, and 167.24 bits. The Communication Cost associated with the proposed DLARO-IOD method is 60 Bits less than that of BDTC-IoD, 90 Bits less than SLAP-IOD, 120 Bits less than RAMP-IOD, and 150 Bits less than RUAM-IOD. The Data Success Ratio for the proposed DLARO-IOD method stands at 95.34 %, in contrast to the earlier methods such as RUAM-IOD, RAMP-IOD, SLAP-IOD, and BDTC-IoD, which achieve ratios of 68.57 %, 75.46 %, 81.61 %, and 89.66 % respectively. Thus, the Data Success Ratio of the proposed DLARO-IOD method is 6 % superior to that of BDTC-IoD, 14 % superior to SLAP-IOD, 20 % superior to RAMP-IOD, and 27 % superior to RUAM-IOD.

The Packet Loss Ratio for the proposed DLARO-IOD method is 10.98%, in contrast to the earlier techniques such as RUAM-IOD, RAMP-IOD, SLAP-IOD, and BDTC-IoD, which exhibit ratios of 42.16%, 36.44%, 29.45%, and 21.03%. So, the Packet Loss Ratio of the proposed DLARO-IOD approach is 10 % lower than BDTC-IoD, 19 % lower than SLAP-IOD, 26 % lower than RAMP-IOD, and 32 % lower than RUAM-IOD.

The End-to-End Delay for the proposed DLARO-IOD method is 78.55 ms, in contrast to the previous methods, such as RUAM-IOD, RAMP-IOD, SLAP-IOD, and BDTC-IoD, which have delays of 355.45 ms, 324.19 ms, 287.94 ms, and 233.14 ms, respectively. Consequently, the End-to-End Delay of the proposed DLARO-IOD method is 150 ms less than that of BDTC-IoD, 200 ms less than SLAP-IOD, 230 ms less than RAMP-IOD, and 270 ms less than RUAM-IOD. The Overhead for the proposed DLARO-IOD method is 120 Packets, whereas the earlier methods, such as RUAM-IOD, RAMP-IOD, SLAP-IOD, and BDTC-IOD, have overheads of 583 Packets, 474 Packets, 389 Packets, and 264 Packets, respectively.

The Energy Efficiency of the proposed DLARO-IOD method is 370 Joules, while the previous techniques, such as RUAM-IOD, RAMP-IOD, SLAP-IOD, and BDTC-IoD, achieve efficiencies of 145 Joules, 298 Joules, 333 Joules, and 367 Joules, respectively. Thus, the Energy Efficiency of the proposed DLARO-IOD method surpasses that of BDTC-IoD by 3 Joules, exceeds SLAP-IOD by 35 Joules, outperforms RAMP-IOD by 70 Joules, and is 220 Joules better than RUAM-IOD. In terms of Throughput, the proposed DLARO-IOD method achieves 780 Kbps, whereas the earlier methods, such as RUAM-IOD, RAMP-IOD, SLAP-IOD, and BDTC-IoD, reach Throughput levels of 301 Kbps, 399 Kbps, 531 Kbps, and 687 Kbps, respectively. Thus, the throughput of the suggested DLARO-IOD method surpasses that of BDTC-IoD by 90 Kbps, exceeds SLAP-IOD by 250 Kbps, outperforms RAMP-IOD by 380 Kbps, and is 480 Kbps greater than RUAM-IOD.

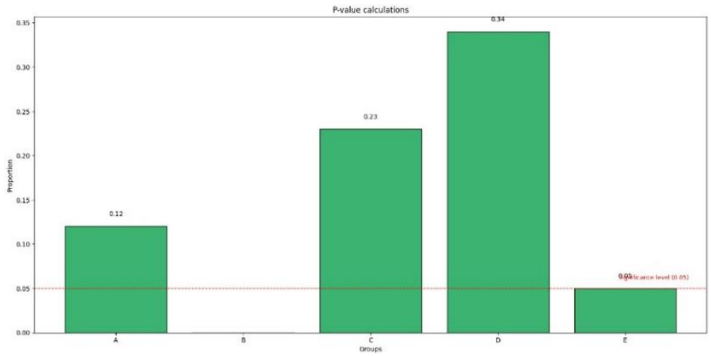

Figure 21. P-value calculation

Table 6. Evaluation metrics for end-to-end latency, packet loss rate, and overhead

Speed Km/H	RUAM-IoD	RAMP-IoD	SLAP-IoD	BDTC-IoD	DLARO-IoD	RUAM-IoD	RAMP-IoD	SLAP-IoD	BDTC-IoD	DLARO-IoD	RUAM-IoD	RAMP-IoD	SLAP-IoD	BDTC-IoD	DLARO-IoD
	Packet Loss Ratio (%)					End-to-End Delay (ms)					Overhead (packets)				
50	35.46	30.14	22.47	13.5	5.23	302.7	287	233	168	55.24	420	346	267	198	85
100	37.41	31.64	24.11	16.4	7.44	318.6	299	245	187	59.64	436	387	289	213	91
150	38.64	32.08	26.37	19.3	9.66	323.3	312	262	201	64.37	478	421	346	246	99
200	41.08	34.09	28.46	20.7	10.26	349.5	319	278	221	71.69	523	466	367	255	114
250	42.16	36.44	29.45	21.0	10.98	355.4	324	287	233	78.55	583	474	389	264	120

Table 7. Assessment of energy efficiency and throughput performance

Speed Km/H	RUAM-IoD	RAMP-IoD	SLAP-IoD	BDTC-IoD	DLARO-IoD	RUAM-IoD	RAMP-IoD	SLAP-IoD	BDTC-IoD	DLARO-IoD
	Energy Efficiency (Joules)					Throughput (Kbps)				
50	233	364	399	410	425	350	465	621	754	824
100	201	321	374	405	413	338	453	597	737	819
150	198	316	361	391	406	324	447	568	721	811
200	167	301	344	382	386	309	423	549	698	798
250	145	298	333	367	370	301	399	531	687	780

6. CONCLUSION

In this paper, the IoD network performance enhancement is concentrated on the purpose of enhancing the LA mechanism with RO. The proposed authentication process greatly helps to protect the network from attack models such as man in a middle attack, a replay attack, a traceability attack, and a denial of service attack. By using of enhanced LA process, the network delay and routing overhead are reduced. Meanwhile, RO is performed mainly to reduce the energy and time consumption in the network. Why, because in the earlier research the apart from security issues, the high utilization of energy and time becomes the major drawback. For that purpose, in our RO, energy and time consumption reduction are highly concentrated. For the process of comparative analysis, the recent researches are considered like RUAM-IoD, RAMP-IoD, SLAP-IoD, and BDTC-IoD.

Two categories—number of nodes and variable speed—are used to classify the performance analysis. When compared to recent research, the proposed DLARO-IOD achieves a higher malicious detection rate of 7% to 19%, a lower communication cost of 150 bits to 900 bits, a higher data success ratio of 2% to 6%, a lower end-to-end delay of 90 ms to 180 ms, a lower packet loss ratio of 9% to 20%, a lower routing overhead of 175 packets to 290 packets, a higher energy efficiency of 70 joules to 170 joules, and a higher throughput of 40Kbps to 200Kbps.

When compared to recent research, the proposed DLARO-IOD has been shown to achieve a higher malicious detection rate of 1% to 15%, a lower communication cost of 60 bits to 150 bits, a higher data success ratio of 6% to 27%, a lower end-to-end delay of 150 ms to 270 ms, a lower packet loss ratio of 10% to 32%, a lower routing overhead of 140 packets to 460 packets, a higher energy efficiency of 10 joules to 220 joules, and a higher throughput of 90 Kbps to 480 Kbps. The UAVs within the network will focus on increasing the density in the future.

REFERENCES

[1] Das, A.K., Bera, B., Wazid, M., Jamal, S.S., Park, Y. (2021). iGCACS-IoD: An improved certificate-enabled generic access control scheme for Internet of Drones deployment. IEEE Access, 9: 87024-87048. https://doi.org/10.1109/ACCESS.2021.3089871

[2] Pu, C., Carpenter, L. (2020). Psched: A priority-based service scheduling scheme for the Internet of Drones. IEEE Systems Journal, 15(3): 4230-4239. https://doi.org/10.1109/JSYST.2020.2998010

[3] Kouroshnezhad, S., Peiravi, A., Haghighi, M.S., Jolfaei, A. (2020). Energy-efficient drone trajectory planning for the localization of 6G-enabled IoT devices. IEEE Internet of Things Journal, 8(7): 5202-5210. https://doi.org/10.1109/JIOT.2020.3032347

[4] Cho, S.M., Hong, E., Seo, S.H. (2020). Random number generator using sensors for drone. IEEE Access, 8: 30343-30354. https://doi.org/10.1109/ACCESS.2020.2972958

[5] Zhang, M.H., Li, X. (2020). Drone-enabled Internet-of-Things relay for environmental monitoring in remote areas without public networks. IEEE Internet of Things Journal, 7(8): 7648-7662. https://doi.org/10.1109/JIOT.2020.2988249

[6] Savkin, A.V., Huang, H.L. (2020). Range-based reactive deployment of autonomous drones for optimal coverage in disaster areas. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 51(7): 4606-4610. https://doi.org/10.1109/TSMC.2019.2944010

[7] Sobouti, M.J., Rahimi, Z., Mohajerzadeh, A.H., Seno, S.A.H., Ghanbari, R., Marquez-Barja, J.M., Ahmadi, H. (2020). Efficient deployment of small cell base stations mounted on unmanned aerial vehicles for the internet of things infrastructure. IEEE Sensors Journal, 20(13): 7460-7471. https://doi.org/10.1109/JSEN.2020.2973320

[8] Ahmed, G.A., Sheltami, T.R., Mahmoud, A.S., Imran, M., Shoaib, M. (2021). A novel collaborative IoD-assisted VANET approach for coverage area maximization. IEEE Access, 9: 61211-61223. https://doi.org/10.1109/ACCESS.2021.3072431

[9] Singh, M., Aujla, G.S., Bali, R.S. (2021). A deep learning-based blockchain mechanism for a secure Internet of Drones environment. IEEE Transactions on Intelligent Transportation Systems, 22(7): 4404-4413. https://doi.org/10.1109/TITS.2020.2997469

[10] Lei, Y., Zeng, L.N., Li, Y.X., Wang, M.X., Qin, H.S. (2021). A lightweight authentication protocol for UAV networks based on security and computational resource optimization. IEEE Access, 9: 53769-53785. https://doi.org/10.1109/ACCESS.2021.3070683

[11] Nguyen, T., Katila, R., Gia, T.N. (2023). An advanced Internet-of-Drones system with blockchain for improving quality of service of search and rescue: A feasibility study. Future Generation Computer Systems, 140: 36-52. https://doi.org/10.1016/j.future.2022.10.002

[12] Chaudhry, S.A., Yahya, K., Karuppiah, M., Kharel, R., Bashir, A.K., Zikria, Y.B. (2021). GCACS-IoD: A certificate-based generic access control scheme for Internet of Drones. Computer Networks, 191: 107999. https://doi.org/10.1016/j.comnet.2021.107999

[13] Bera, B., Das, A.K., Sutrala, A.K. (2021). Private blockchain-based access control mechanism for unauthorized UAV detection and mitigation in Internet

of Drones environment. Computer Communications, 166: 91-109. https://doi.org/10.1016/j.comcom.2020.12.005

[14] Nikooghadam, M., Amintoosi, H., Islam, S.H., Moghadam, M.F. (2021). A provably secure and lightweight authentication scheme for Internet of Drones for smart city surveillance. Journal of Systems Architecture, 115: 101955. https://doi.org/10.1016/j.sysarc.2020.101955

[15] Qureshi, K.N., Alhudhaif, A., Shah, A.A., Majeed, S., Jeon, G. (2021). Trust and priority-based drone-assisted routing and mobility and service-oriented solution for the internet of vehicles networks. Journal of Information Security and Applications, 59: 102864. https://doi.org/10.1016/j.jisa.2021.102864

[16] Zhang, Y.R., He, D.B., Li, L., Chen, B.W. (2020). A lightweight authentication and key agreement scheme for Internet of Drones. Computer Communications, 154: 455-464. https://doi.org/10.1016/j.comcom.2020.02.067

[17] Bera, B., Chattaraj, D., Das, A.K. (2020). Designing secure blockchain-based access control scheme in IoT-enabled Internet of Drones deployment. Computer Communications, 153: 229-249. https://doi.org/10.1016/j.comcom.2020.02.011

[18] Hussain, S., Mahmood, K., Khan, M.K., Chen, C.M., Alzahrani, B.A., Chaudhry, S.A. (2022). Designing secure and lightweight user access to drones for smart city surveillance. Computer Standards & Interfaces, 80: 103566. https://doi.org/10.1016/j.csi.2021.103566

[19] Bera, B., Vangala, A., Das, A.K., Lorenz, P., Khan, M.K. (2022). Private blockchain-envisioned drones-assisted authentication scheme in IoT-enabled agricultural environment. Computer Standards & Interfaces, 80: 103567. https://doi.org/10.1016/j.csi.2021.103567

[20] Ever, Y.K. (2020). A secure authentication scheme framework for mobile-sinks used in the Internet of Drones applications. Computer Communications, 155: 143-149. https://doi.org/10.1016/j.comcom.2020.03.009

[21] Ch, R., Srivastava, G., Gadekallu, T.R., Maddikunta, P.K.R., Bhattacharya, S. (2020). Security and privacy of UAV data using blockchain technology. Journal of Information Security and Applications, 55: 102670. https://doi.org/10.1016/j.jisa.2020.102670

[22] Hussain, S., Chaudhry, S.A., Alomari, O.A., Alsharif, M.H., Khan, M.K., Kumar, N. (2021). Amassing the security: An ECC-based authentication scheme for Internet of drones. IEEE Systems Journal, 15(3): 4431-4438. https://doi.org/10.1109/JSYST.2021.3057047

[23] Tanveer, M., Alkhayyat, A., Naushad, A., Khan, A.U., Kumar, N., Alharbi, A.G. (2022). RUAM-IoD: A robust user authentication mechanism for the Internet of Drones. IEEE Access, 10: 19836-19851. https://doi.org/10.1109/ACCESS.2022.3149376

[24] Tanveer, M., Khan, A.U., Kumar, N., Hassan, M.M. (2022). RAMP-IoD: A Robust authenticated key management protocol for the Internet of Drones. IEEE Internet of Things Journal, 9(2): 1339-1353. https://doi.org/10.1109/JIOT.2021.3084946

[25] Yu, S.J., Das, A.K., Park, Y., Lorenz, P. (2022). SLAP-IoD: Secure and lightweight authentication protocol using physical unclonable functions for Internet of Drones in smart city environments. IEEE Transactions on Vehicular Technology, 71(10): 10374-10388. https://doi.org/10.1109/TVT.2022.3188769

[26] Jghef, Y.S., Jasim, M.J.M., Ghanimi, H.M.A., Algarni, A.D., et al. (2022). Bio-inspired dynamic trust and congestion-aware zone-based Secured Internet of Drone Things (SIoDT). Drones, 6(11): 337. https://doi.org/10.3390/drones6110337