IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 9 October 2023, accepted 22 October 2023, date of publication 1 November 2023, date of current version 7 November 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3329083

RESEARCH ARTICLE

Secured Reliable Communication Through Authentication and Optimal Relay Selection in Blockchain Enabled Cellular IoT Networks

SAMIA ALLAOUA CHELLOUG[1], REEM ALKANHEL[1], (Member, IEEE), AHMED AZIZ[2,3], (Member, IEEE), MOHAMMED SALEH ALI MUTHANNA[4], AND AMMAR MUTHANNA[5], (Member, IEEE)

[1]Department of Information Technology, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, Riyadh 11671, Saudi Arabia
[2]Department of Computer Science, Faculty of Computer and Artificial Intelligence, Benha University, Banha 13511, Egypt
[3]Department of International Business Management, Tashkent State University of Economics, Tashkent 100066, Uzbekistan
[4]Institute of Computer Technologies and Information Security, Southern Federal University, 344006 Taganrog, Russia
[5]Peoples' Friendship University of Russia (RUDN University), 117198 Moscow, Russia

Corresponding author: Samia Allaoua Chelloug (sachelloug@pnu.edu.sa)

This work was supported by Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2023R239), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia, in part the research is supported by postdoc fellowship granted by the Institute of Computer Technologies and Information Security, Southern Federal University, project № P.D./22-01-KT.

ABSTRACT The security and reliability of cellular-based wireless IoT networks are often hindered by eavesdropping attacks. Existing approaches have limitations such as ineffective relay selection, untrusted relay nodes, and improper UAV positioning. This article discusses secure and reliable communication in blockchain-enabled cellular-based IoT networks. In this article, we propose a novel approach that ensures the initial level of security to the UAV relays by enrolling the UAV relay nodes to the edge-assisted base stations for initial security and enhances the optimal UAV relay selection using dual-phase optimal relay selection mechanisms. This article performs authentication of UAV relay nodes to enhance security against active eavesdroppers and mitigates the effects of passive eavesdroppers by jointly optimizing power and position based on their actions. This enables eavesdropping to resist secure communication. The proposed approach beats the state-of-the-art algorithm in terms of decreased deployment time and gradually rising efficiency with increasing UEs. The deployment time for the previously presented algorithm is fast expanding, while the proposed integrated deployment algorithm is progressively increasing. The proposed eavesdropping resisted integration technique harvests an overlay complexity tendency due to its hybrid solution, enhancing system stability and minimizing system complexity. We further integrate the blockchain with UAVs in the system and perform authentication and appropriate relay selection in the networks. We will also demonstrate secure and reliable communication in healthcare, transportation, and industry. This paper emphasizes the significance of safe and dependable IoT connectivity and how blockchain technology and appropriate relay selection techniques might be helpful. The results show that the recommended algorithm is superior in terms of both reliability and complexity. When iteration count is minimal, the proposed method and the completely distributed have a comparable but lowest complexity as they outperform one another in different scenarios. Our proposed approach provides a possible solution to existing issues and contributes to the progress of secure and reliable communication in cellular-based wireless IoT networks.

INDEX TERMS Cellular-based wireless IoT networks, UAV relay nodes, active eavesdroppers, optimizing power, integrated deployment technique, secure and reliable communication.

The associate editor coordinating the review of this manuscript and approving it for publication was Miguel López-Benítez.

I. INTRODUCTION

The Internet of Things (IoT) has become an increasingly important part of our daily lives, with billions of devices connected to the internet and exchanging data with each other. As more devices become connected, the need for secure and reliable communication in IoT networks becomes critical. Blockchain technology and optimal relay selection mechanisms are two important components that can help to ensure the security and reliability of communication in these networks. Blockchain technology provides a distributed and tamper-proof ledger that can be used to maintain a record of all transactions on the network. This ensures the integrity of the data and provides an additional layer of security. Optimal relay selection mechanisms, on the other hand, help to select the best communication path between the sender and receiver, taking into consideration factors such as the quality of the signal, the distance between the devices, and the available bandwidth. The emergence of Internet of Things enables communication of several low powered devices and gateways for various applications such as smart city, smart home, smart transportation etc [1], [2]. The wireless means of communication between the entities is found to be efficient and cost effective than wired networks. The wireless communication between the entities is carried out in two ways such as direct communication and relay-based communication. In former the communication exists between the source and destination nodes whereas in latter the relay nodes between source and destination assist the communication [3]. The increased energy consumption and cost in direct communication caused due to distance between the entities is mitigated by relay-based communication.

The security of communication has become a major threat due to the presence of eavesdroppers in the network. Eavesdropping refers to the illegitimate access to the communication between two devices to steal or modify data. Based on the presence and absence of channel information, the eavesdroppers can be categorized into two namely active eavesdroppers and passive eavesdroppers. The cryptographic based approaches were utilized to mitigate the eavesdropping attacks but were found to increase computational complexity of low power devices and further the computationally capable eavesdropper was able to compromise its security. In order to mitigate these challenges physical layer security was focused. The physical layer security considers physical layer attributes such as CSI, RSSI, SNR etc. of the devices to ensure the secure communication. Several existing approaches concentrated on physical layer attributes-based selection of relay nodes to mitigate the eavesdropping attacks however they considered the presence of single eavesdropper in the network. Few researches proposed attack mitigation techniques under the presence of multiple eavesdroppers it was limited to either active or passive eavesdroppers [4], [5]. The UAV based relaying approach was incorporated to overcome the eavesdropping attacks as the UAVs possessing multiple antennas could achieve secure communication than the eavesdropper with single antenna. This paves way for introduction of UAV eavesdropper in which the UAVs act as eavesdropper nodes to reduce the secrecy rate of the communication. The optimization of source transmit power and positioning of UAVs was performed to mitigate the attacks however the optimal positioning of UAVs was not achieved due to lack of consideration of altitude. Moreover, there is still a demand for effective approach to mitigate both active and passive eavesdropping caused by UAVs [6].

The concept of secure and reliable communication through authentication and optimal relay selection in blockchain-enabled cellular-based IoT networks involves the use of blockchain technology to ensure the security and reliability of communication in IoT networks. The IoT devices are connected to the cellular network, and the blockchain is used to authenticate these devices and ensure that only authorized devices can communicate on the network. The blockchain also maintains a secure and tamper-proof record of all communications that take place on the network, which can be used to verify the integrity of the data. In a blockchain-enabled cellular-based IoT network, secured communication through authentication is a critical component to ensure the privacy and integrity of data exchanged between devices [7]. The authentication process involves verifying the identity of each device that is attempting to communicate on the network. This ensures that only authorized devices can access the network and prevents unauthorized access and data breaches. In this setup, each IoT device has a unique identity that is verified using cryptographic techniques such as digital signatures or public-key encryption. Once the identity is verified, the device can access the network and start communicating with other authorized devices. The use of blockchain technology in this context provides additional security benefits. The blockchain acts as a distributed ledger, recording all transactions that take place on the network. This ensures that every communication is recorded, and any attempt to tamper with the data can be detected. Moreover, blockchain-enabled IoT networks are decentralized, meaning that there is no central authority that can be compromised, making it more difficult for attackers to launch a successful attack [8]. Further, the secure communication through authentication in blockchain-enabled cellular-based IoT networks is critical to ensure the privacy and integrity of data and prevent unauthorized access and data breaches.

In this article, we will explore the concept of secure and reliable communication in blockchain-enabled cellular-based IoT networks. We will explain the importance of authentication and optimal relay selection mechanisms in these networks, as well as the security benefits of using blockchain technology. We will also provide some examples of how secure and reliable communication can be applied in various industries, such as healthcare, transportation, and manufacturing. Ultimately, the goal of this article is to emphasize the importance of secure and reliable communication in IoT networks and how blockchain technology and optimal relay selection mechanisms can help to achieve this goal.

A. PROBLEM STATEMENT

The secure communication in the cellular based wireless network is mainly hindered by eavesdropping attack. Most existing approaches considered either the presence of active eavesdroppers or passive eavesdroppers. However, they possess several problems which are mentioned as follows,

- Ineffective relay selection – The existing approaches performed selection of relay nodes for secure communication from source to destination however the relay selection was performed based on single attribute resulting in ineffective selection when there is a large number of relay nodes.
- Untrusted relay – Most of the existing approaches assumed that the relay nodes are trusted, however in practical scenario the relay node might be a helper node for the eavesdropper resulting in degradation of security.
- Presence of UAV eavesdropper – The existing approaches on UAV-relay based secure communication considered only the eavesdroppers present in ground however, the presence of UAV eavesdropper also affects secrecy rate of communication.
- Improper UAV positioning – The UAV-relay based approaches performed positioning of UAV to mitigate the passive eavesdropper present in ground however the lack of optimization of uncertainties and altitude associated with UAV positioning results in collisions.

B. RESEARCH CONTRIBUTION

The core objective of this work is to ensure security and reliability to the cellular based wireless IoT networks. Given the recent progress in the domain, our investigation presents a series of pioneering contributions pertaining to the domain of secure and dependable communication within cellular-based wireless Internet of Things (IoT) networks.

- The study advances UAV relay node enrollment, which is a topic of contemporary research. These works have examined offloading compute tasks to UAVs while addressing incentive mechanisms and privacy. However, our study focuses on integrating UAV relay nodes with edge-assisted Base Stations to ensure basic security. This phase is crucial to building a robust architecture for smooth IoT network connection.
- New Mobility-Aware Network Model extends optimum UAV relay selection paradigm. In this revolutionary study, we suggest adding mobility-awareness to the network model to improve performance and efficiency. Our approach optimizes relay selection by taking into consideration UAVs' dynamic locations and trajectories. This novel technique might revolutionize network design and operation, enabling more resilient and adaptive communication systems in UAV-enabled networks.
- The suggested approach considers the intrinsic dynamic of unmanned aerial vehicles (UAVs) in their motions to improve UAV relay selection. This novelty efficiently addresses the mobility difficulties of unmanned aerial vehicles (UAVs), a crucial aspect of modern IoT networks.
- Research has focused on authentication and eavesdropping security. Recent investigations have used blockchain technology and privacy-preserving authentication mechanisms. However, our study on UAV relay node authentication pushes this area forward.
- Additionally, appropriate UAV relays are chosen from a pool of authenticated UAVs to improve system security and dependability. Our study focuses on reducing passive eavesdropping's effects. The synergistic optimization of power and location depends on the eavesdroppers' behavior.
- Blockchain technology is used to strengthen data integrity and confidentiality in our study. We work hard to address data transmission and storage issues. This robust framework protects sensitive IoT data.
- Our novel study introduces secrecy rate maximization as a key optimization goal. The score above quantifies the network's ability to maintain communication secrecy despite eavesdroppers, improving IoT communication security.
- Our approach acknowledges trust and untrust in the network to handle rogue nodes. This adaptive technique adds another layer of security, strengthening the network's resilience.

Thus, our investigation expands upon the existing cutting-edge knowledge by tackling the distinctive security and dependability obstacles encountered in cellular-based wireless Internet of Things (IoT) networks. We present innovative resolutions pertaining to enrollment, authentication, and optimal relay selection, all the while emphasizing the utmost importance of data integrity and confidentiality in the face of potential eavesdropping threats. The amalgamation of these contributions effectively augments the security and dependability of Internet of Things (IoT) communications within dynamic and unbounded settings.

C. ARTICLE ORGANIZATION

D. The rest of this article is organised as literature review presented in section II, followed by proposed methodology in section III explaining the importance of authentication in blockchain-enabled cellular-based IoT networks, optimal relay selection mechanism and security benefits of blockchain-enabled cellular IOT network which in turn ensures security benefits of blockchain technology in IoT networks. Section IV addresses the comprehensive results and experimental analyses, while Section V discusses applications and future recommendations. Section VI contains the conclusion of this article.

II. LITERATURE REVIEW

Blockchain-enabled IoT networks have recently emerged as a promising solution to provide secure and reliable communication in IoT systems. The integration of blockchain technology with cellular networks has the potential to enhance the security and privacy of IoT devices. Moreover, the use of optimal relay selection can further improve the reliability and efficiency of these networks. Secured reliable communication through authentication and optimal relay selection is a critical issue in blockchain-enabled cellular-based IoT networks. In this section, we present a literature review of the recent studies addressing these issues in such networks.

In a recent study by Zhang et al. [9], the authors proposed a blockchain-based scheme incorporating a blockchain-based authentication mechanism and an optimal relay selection algorithm to improve the security and reliability of the network. The results of their simulation experiments showed that the proposed scheme outperformed existing solutions in terms of communication delay, throughput, and packet delivery ratio.

Another study by Kumar et al. [10] proposed a blockchain-based framework for secure and reliable communication in cellular-based IoT networks. The framework includes a blockchain-based authentication mechanism and an optimal relay selection algorithm to ensure the security and reliability of the network. The authors also conducted a performance evaluation of the proposed framework, and the results showed that it achieved better communication delay, throughput, and packet delivery ratio compared to existing solutions.

In a study by Jan et al. [11], the authors proposed an optimal relay selection algorithm based on a multi-objective optimization approach to improve the reliability and efficiency of IoT networks. The algorithm takes into account factors such as the distance between the nodes, the available bandwidth, and the reliability of the nodes to select the best relay for a specific communication task. The authors evaluated the performance of the proposed algorithm through simulation experimentations, and the outcomes showed that it outperformed existing solutions in terms of communication delay, packet loss, and throughput.

In a study by Karami et al. [12], the authors proposed a solution incorporating a consensus algorithm and an optimal relay selection algorithm to improve the security and reliability of the network. The authors evaluated the performance of the proposed solution through simulation experiments, and the results showed that it achieved better communication delay, packet delivery ratio, and throughput compared to existing solutions.

The studies reviewed above demonstrate the potential of blockchain-enabled cellular-based IoT networks to provide secure and reliable communication. The integration of blockchain technology with optimal relay selection algorithms and authentication mechanisms can enhance the efficiency, reliability, and security of such networks. However, further research is required to address scalability and performance issues in large-scale IoT deployments.

It might be difficult to decide where to position UAVs in a specific region to increase coverage or provide the optimum degree of service to ground UEs. The ideal UAV height for optimising the coverage area was determined by Al-Hourani et al. [13]. By examining the effect of altitude on gearbox power and taking into consideration their mutual interference, Mozaffari et al. [14] expanded their analysis to the case involving two UAVs. In order to maximize the coverage, Wang et al. [15], Alzenad et al. [16], and Bor-Yaliniz et al. [17] studied the effective position of one UAV in 3-D space. The UAV in the cell centre changed its displacement, orientation, and length in accordance with the Poisson distributed mobile consumers inside the targeted cell, as per Wang et al.'s [18] traffic-aware adaptive UAV installation technique. While the works discussed above might readily answer the challenge of putting a single UAV ideally, deploying several organising UAVs is more challenging. According to the authors of [19], UAVs should be used in a way that maximises range while consuming the least amount of power for transmission. Its theoretical underpinning is the circular packing principle. A particle swarm optimization-based heuristic approach was created by Kalantari et al. [20]. In a region with a range of user densities, the algorithm determined the bare minimum number of UAVs and the best locations to deploy them in order to serve all of the users' demands. A novel polynomial-time successful UAV deployment method for UAV-UE communications was proposed by Lyu et al. [21] in order to thinly distribute the wireless coverage of a collection of dispersed ground terminals. However, these works do not account for the ability to communicate between the UAVs when deploying multiple UAVs. The compromise between UAV communication and coverage maximisation was resolved by Orfanus et al. [22] by deploying numerous UAVs as wireless relays to support terrestrial sensors.

Wang et al. [23] examines the essential problem of offloading compute workloads from UAVs to ground infrastructure, notably cars. They proposed strategy-proofness to encourage automobiles to share computing resources with UAVs. Strategy-proofing prevents strategic vehicles from manipulating participation costs, increasing resource fairness. The work prioritizes fairness mechanisms to prevent cars from aborting assignments without penalties and UAVs from not being paid. To prevent releasing sensitive information during transparent payment/task outcomes communication, privacy protection is crucial. However, the approach emphasizes strategy-proofness and fairness, but lacks integration with blockchain technology, a prominent alternative for trust and security in UAV networks. Feng, et al. [24] studies 5G-enabled Internet of Drone security and privacy. They offers a blockchain-based cross-domain authentication mechanism for 5G-enabled Smart Internet of Drones. This method creates a collaborative domain identity federation using threshold-shared signatures. The method prioritizes cross-domain communication security and privacy. Smart contracts authenticate and negotiate session keys to safeguard device connectivity while showing the scheme's resilience to common assaults and secure communication among drones across domains. The study focuses on cross-domain authentication but does not cover other areas of UAV network security and dependability. Wang, et al. [25] studied UAV-based emergency networks for flexibility and reliability. The introduced RescueChain framework, integrates lightweight blockchain-based data sharing, reputation-based consensus protocol, and VFC-based off-chain methods. The architecture protects data sharing during catastrophes and identifies rogue organizations. The reputation-based consensus mechanism encourages UAV honesty. To improve network efficiency, they suggest offloading heavy data processing and storage activities from UAVs to ground vehicles with idle computer capabilities. The study focuses on emergency situations and offloading high data processing workloads, providing potential for UAV network security and dependability studies. Son, et al. [26] discusses the issues of real-time UAV-roadside unit communication in intelligent transportation systems (ITS). Its key feature is a safe and lightweight blockchain-based authentication mechanism for UAVs and RSUs. This approach protects real-time communication between these entities. The proposed scheme is analyzed using various methods, including informal methods like Burrows-Abadi-Nikoogadam logic, formal methods like AVISPA simulation tool, and real-or-random (RoR) model. The scheme's efficiency against security risks is confirmed by this study. The study covers authentication and security in UAV-enabled ITS, however its scope is limited to this application area. Blockchain-based authentication in UAV networks beyond ITS may be possible. Rashid and Khan [27] focuses on the Internet of Battlefield Things (IoBT) and secure authentication and integrity in battlefield message exchange. Blockchain-based Autonomous Authentication and Integrity for the Internet of Battlefield Things (BIoBT) method uses blockchain for entity authentication when receiving data without a separate channel guaranteeing data integrity and non-repudiation, vital in a wartime setting, in addition to authentication. The findings prove BIoBT's efficiency, cost-effectiveness, and security in distributed IoBT. The study focuses on the unique and distinctive context of the Internet of Battlefield Things. UAV network issues in civilian applications and commercial drone services may not be addressed immediately. Gorski [7] integrates messaging systems into software programs and gives an architectural perspective and modelling methodologies for service and business messaging flows. The study offers the Integrated Services Architectural View, a comprehensive approach to integrating messaging systems into software applications. This comprises business and service flows. The article examines extension techniques in the UML Profile for Messaging Patterns as a realistic way to improve modeling capabilities for messaging situations. The study seems to be focused on integrating messaging technologies in a brokerage firm and stock exchange situation. The methodologies and architectural perspectives are useful in this context, but they should be tested in other software integration contexts. Beyond the case study, the article recommends a framework and methodologies with little discussion or proof of their efficacy and application.

Several alternate studies have proposed different approaches to achieve secured reliable communication in blockchain-enabled IoT networks. For instance, one approach is to use a blockchain-based authentication mechanism to ensure the secure exchange of data between IoT devices. Another approach is to use a decentralized consensus algorithm, such as Proof-of-Work (PoW) or Proof-of-Stake (PoS), to secure the transactions in the network. Deploying unmanned aerial vehicles (UAVs) in a target region to provide optimal coverage and service quality for ground users is a challenging task. Previous studies have focused on determining the ideal altitude and placement of a single UAV to maximize coverage, as well as examining the interference between multiple UAVs. However, determining the effective placement of multiple coordinating UAVs remains a challenge. Several approaches have been proposed to address this issue, including a strategy and a heuristic approach using particle swarm optimization to determine the smallest quantity of UAVs needed to serve users in a specific region. Other studies have focused on minimizing wireless coverage overlap and maximizing connectivity between UAVs. Overall, these approaches provide valuable insights into optimizing UAV deployment for wireless communication in various scenarios.

In terms of relay selection, several algorithms have been proposed to select the optimal relay nodes in the network. These algorithms take into consideration factors such as the distance between the nodes, the available bandwidth, and the reliability of the nodes to select the best relay for a specific communication task.

IoT devices may benefit from a secure and dependable communication environment that is made possible by the combination of blockchain technology with cellular networks. Additionally, the network's effectiveness and dependability may be improved by using appropriate relay selection algorithms. To solve the scalability and performance challenges of these networks, particularly in large-scale IoT installations, additional research is necessary.

III. PROPOSED METHODOLOGY

Existing methods for secure communication in Blockchain-Enabled Cellular-Based IoT Networks involve selecting relay nodes to facilitate communication between the source and destination. However, these approaches typically rely on a single attribute for relay selection, leading to ineffective choices, particularly when dealing with a large number of relay nodes. Many conventional approaches assume that all relay nodes can be trusted. However, in practical scenarios, some relay nodes may act as helpers for eavesdroppers, compromising the security of the communication. This highlights the need to consider the presence of untrusted relays when designing secure and reliable communication systems. These existing methods for secure communication in UAV-relay-based systems primarily focus on addressing eavesdroppers on the ground. However, the introduction of UAV eavesdroppers can significantly impact the secrecy rate of the communication. Hence, it is crucial to account for the presence of both ground and UAV eavesdroppers to ensure secure and reliable communication. UAV-relay-based approaches commonly involve positioning UAVs strategically to mitigate the threat of passive eavesdroppers on the ground. However, the lack of optimization regarding uncertainties associated with UAV positioning and the choice of altitude can result in collisions and other issues. Therefore, it is essential to optimize UAV positioning, considering uncertainties and altitude, to achieve secure and reliable communication in Blockchain-Enabled Cellular-Based IoT Networks.

The security model authenticates devices to prevent unauthorized access to the network and data transmission. This authentication prevents data breaches and unwanted access. Blockchain technology provides a tamper-proof record of authenticated devices, improving security. It protects data sent between devices from manipulation. The security model uses optimal relay selection algorithms to choose relay nodes with the highest communication quality and the lowest eavesdropping risk. This ensures safe and dependable communication. The model handles terrestrial and UAV eavesdroppers. It resists eavesdropping and protects conversations. The security model establishes a secure source-to-destination communication channel. To secure data transmission, it analyzes node location, connection quality, and encryption. The approach further secures relay node enrollment in the blockchain network. This keeps communication relay nodes reliable. In addition to authentication, blockchain technology ensures data integrity. Data is stored and verified securely and tamper-proof. The model's optimization goal is to maximize the secrecy rate, which assesses the capacity to keep communication private even with eavesdroppers. The model acknowledges that not all relay nodes may be trusted by including trustworthy and untrusted nodes. Accounting for hostile nodes enhances security. Eavesdroppers and untrusted nodes might pose security risks in IoT networks, therefore the security model attempts to establish a strong foundation for safe and dependable communication. This security approach addresses these difficulties using blockchain technology, optimum relay selection, and authentication.

A. SIMULATION SCENARIO

The simulation scenario represents a real-world IoT network where devices communicate through blockchain-enabled cellular connectivity. The IoT devices considered for this research environment are 400. For setting the parameters, a simulated scenario with 50 UAVs and 200 land vehicles in a 1000 m × 1000 m catastrophe zone. UAVs fly above the two-lane road at a set altitude of 50 meters while following the predetermined straight-line route [6]. Vehicles are first randomly positioned on each lane of the road with a minimum safe distance of 15 meters and UAVs are initially placed alongside the road every 100 meters. Ground vehicles on the road are only permitted to go at speeds between 25 km/h and 75 km/h. The number of jobs offloaded by UAVs is distributed uniformly between 10 and 20. The simulation of the experimental implementation is done using MATLAB environment and Go 1.13 × 64 compiler for simulation of IOT environment, in order to evaluate the computation as well as communication cost of the entire deployment process.

B. PROBLEM FORMULATION

Let us consider a mathematical problem formulation that incorporates the mentioned challenges in secure communication. The object is to find an optimal relay node selection and UAV positioning strategy that maximizes the secrecy rate while considering the presence of untrusted relay nodes, UAV eavesdroppers, and uncertainties associated with UAV positioning.

Given: A set of relay nodes $R = \{R_1, R_2, \ldots, R_n\}$ with n relay nodes.

- A set of trusted relay nodes $TR \subseteq R$.
- A set of untrusted relay nodes $UR = R \setminus TR$.
- A set of ground eavesdroppers $E = \{E_1, E_2, \ldots, E_m\}$ with m eavesdroppers.
- A set of UAV eavesdroppers $UE = \{UE_1, UE_2, \ldots, UE_k\}$ with k eavesdroppers.
- A source node S and a destination node D.
- Uncertainties associated with UAV positioning, denoted by $U = \{U_1, U_2, \ldots, U_o\}$.
- Altitude options for UAV positioning, denoted by $A = \{A_1, A_2, \ldots, A_p\}$.

Let x_i be a binary decision variable that indicates whether relay node R_i is selected for communication, where $x_i = 1$ if R_i is selected and $x_i = 0$ otherwise.

Let y_j be a binary decision variable that indicates whether UAV eavesdropper UE_j is present during communication, where $y_j = 1$ if UE_j is present and $y_j = 0$ otherwise.

Let z_u be a binary decision variable that indicates whether UAV is positioned at altitude A_u, where $z_u = 1$ if UAV is positioned at A_u and $z_u = 0$ otherwise.

Objective Function: Maximize the Secrecy Rate, denoted as Secrecy_Rate, which is a function of the binary decision variables x, y, and z, representing relay node selection, presence of UAV eavesdroppers, and UAV positioning.

Maximize: $\text{Secrecy\_Rate} = f(x, y, z)$

Constraints:

➢ Exactly one relay node should be selected for communication:

Subject to: $\sum(x_i) = 1$, for i in $\{1, 2, \ldots, n\}$

This constraint ensures that exactly one relay node is selected for communication.

➢ At most k UAV eavesdroppers should be present during communication:

Subject to: $\sum(y_j) \leq k$, for j in $\{1, 2, \ldots, m\}$

This constraint limits the number of UAV eavesdroppers present during communication to at most k.

- ➢ Exactly one altitude option should be selected for UAV positioning:
  Subject to: $\sum(zu) = 1$, for u in $\{1, 2, \ldots, p\}$
  This constraint ensures that exactly one altitude option is selected for UAV positioning.
- ➢ Additional constraints based on the specific scenario and system model, such as communication range, power constraints, channel conditions, etc., can be added as needed.

1) SECRECY RATE CALCULATION

The Secrecy_Rate is computed based on relay node selection (x), presence of UAV eavesdroppers (y), and UAV positioning (z). The exact formulation of the Secrecy_Rate depends on the specific system model and objectives of the problem. It should account for the challenges mentioned in the problem description, such as ineffective relay selection, presence of untrusted relay nodes, presence of UAV eavesdroppers, and improper UAV positioning.

$$\text{Secrecy\_Rate} = g(x, y, z)$$

The methodology proposed in this article utilizes the major aspects of blockchain-enabled IOT network like blockchain based relay enrolment, construction of mobility aware network model, dual phase relay selection and eavesdropping resisted secure communication as shown in Figure 1. This article addresses several complications of blockchain-enabled cellular-based IOT networks, which further aids the eavesdropping resisted integrated deployment process of the proposed scheme for blockchain-enabled cellular-based IOT networks [28], [29]. These aspects specifically cover blockchain based relay enrolment, construction of mobility aware network model, dual phase relay selection and eavesdropping resisted secure communication followed by integrated deployment process which is discussed in the further subsections.

C. BLOCKCHAIN BASED RELAY ENROLMENT USING AUTHENTICATION IN CELLULAR-BASED IOT NETWORKS

Authentication is a critical component of secure and reliable communication in blockchain-enabled cellular-based IoT networks. Authentication helps to confirm that only authorized devices are able to access the network and exchange data with other devices. In this section, we will explain the importance of authentication in IoT networks and how it can be achieved using blockchain technology. Authentication in IoT networks involves verifying the identity of each device that connects to the network. This is typically done using cryptographic techniques such as digital signatures or public-key encryption. These techniques allow each device to generate a unique digital signature that can be used to authenticate its identity. One of the main challenges of authentication in IoT networks is the large number of devices that need to be authenticated [30]. This can be particularly challenging in cellular-based IoT networks, where devices are often located in remote or hard-to-reach areas. To address this challenge, blockchain technology can be used to provide a distributed and tamper-proof ledger of all authenticated devices on the network. The mechanism of authentication in Blockchain-Enabled Cellular-Based IoT Networks is depicted in Figure 9.

When a new UE device wants to connect to the network, it can submit a request to the blockchain to be authenticated. The blockchain will then verify the device's identity using its unique digital signature and add it to the list of authenticated devices on the network. Once a device is authenticated, it can then securely exchange data with other devices on the network. Another benefit of using blockchain technology for authentication in IoT networks is that it provides a supplementary layer of security. The distributed nature of the blockchain makes it tough for attackers to tamper with the data or disrupt the communication on the network. This ensures the integrity of the data and provides an added level of protection against cyber-attacks. The authentication is a critical component of secure and reliable communication in blockchain-enabled cellular-based IoT networks. Blockchain technology can be used to provide a distributed and tamper-proof ledger of all authenticated devices on the network, which helps to confirm the security and integrity of the data exchanged between devices.

The mathematical formulation of Blockchain-based Relay Enrolment using Authentication in Cellular-Based IoT Network for establishing a secure and reliable relay enrolment process through the utilization of blockchain technology is given as follows.

Given: A set of relay nodes $R = \{R_1, R_2, \ldots, R_n\}$ with n relay nodes.

A set of IoT devices $D = \{D_1, D_2, \ldots, D_m\}$ with m IoT devices.

A blockchain network B to store relay enrolment information and authentication details.

Authentication keys for relay nodes and IoT devices, denoted by K_R and K_D respectively.

Let x_i be a binary decision variable indicating whether relay node R_i is enrolled, where $x_i = 1$ if R_i is enrolled and $x_i = 0$ otherwise. Also let y_j be a binary decision variable indicating whether IoT device D_j is authenticated, where $y_j = 1$ if D_j is authenticated and $y_j = 0$ otherwise.

The problem can be formulated as an optimization problem to maximize: Enrolment_Reliability = f(x, y)

Subject to: $\sum(x\_i) = k$, for i in $\{1, 2, \ldots, n\}$ (Enrol exactly k relay nodes into the blockchain network).

$\sum(y\_j) = m$, for j in $\{1, 2, \ldots, m\}$ (Authenticate all m IoT devices in the network).

Enrolment_Reliability = g(x, y), in order to compute the reliability of the relay enrolment and authentication process.

Additional constraints based on the specific scenario and system model, such as communication range, power constraints, processing capability, etc. Also, the functions f(x, y) and g(x, y) depends on the specific formulation and system

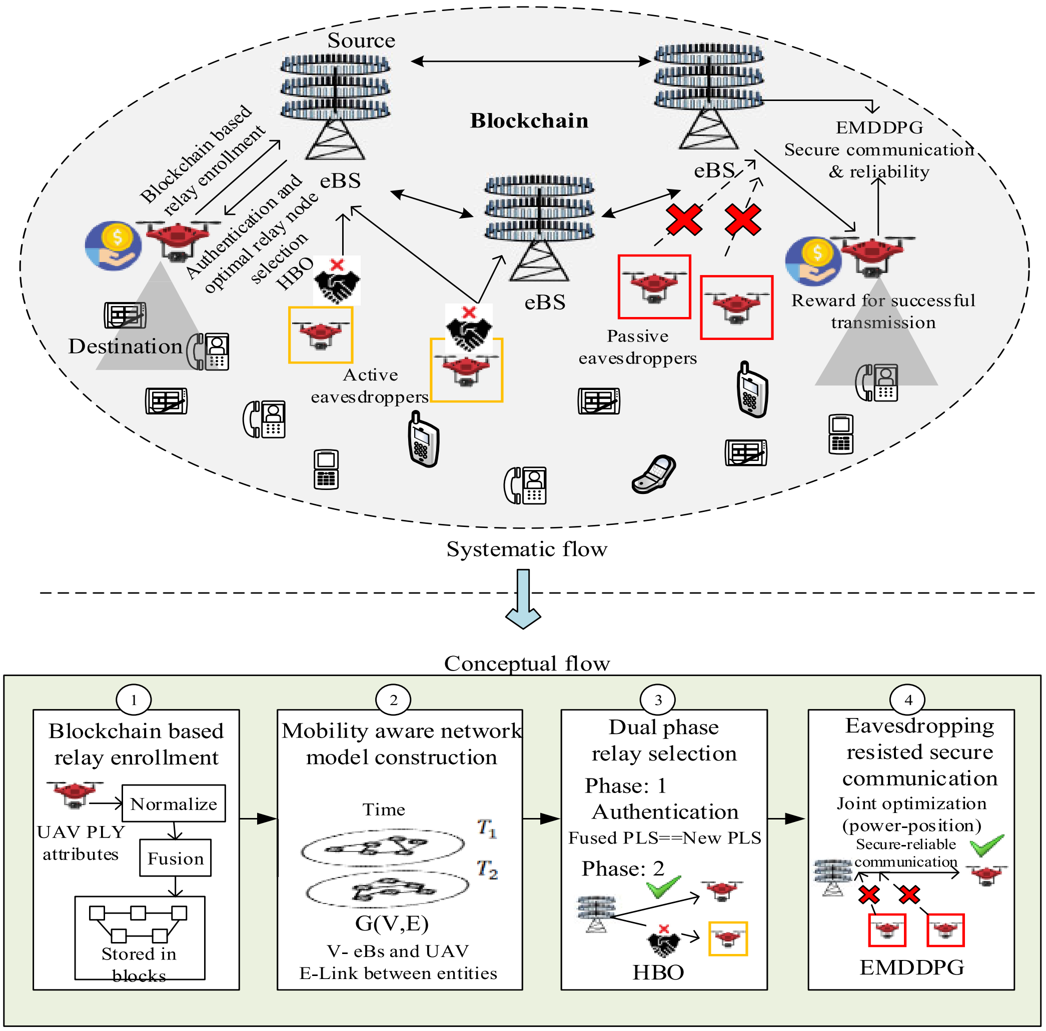


FIGURE 1. Blockchain-Enabled IoT network.

model used to calculate the enrolment reliability and achieve the optimization objective.

D. CONSTRUCTION OF MOBILITY AWARE NETWORK MODEL

For the construction of a mobility-aware network model, we can use mathematical expressions and explanations to represent the various components and factors involved.

Let G(V, E) denote the network topology, where V represents the set of network nodes (including both stationary and mobile nodes) and E represents the set of edges connecting the nodes. Each node v ∈ V can be represented by its coordinates, v = (x, y), where x and y denote the node's position in the network.

Consider a set of mobile nodes $M = \{M_1, M_2, \ldots, M_n\}$, where n is the total number of mobile nodes in the network. Each mobile node M_i can have its own mobility pattern, which can be represented by a mathematical function or model specific to the scenario. For example, M_i's mobility pattern can be described by Brownian motion model. The mobility pattern of each mobile node can be represented by parameters such as speed, direction, acceleration, or other relevant factors.

To quantify the mobility of the network, various metrics can be defined, such as node speed, node displacement, node connectivity, or other relevant measures.

One of such metric is average speed of mobile nodes which can be calculated as:

$$Speed = \frac{\sum Speed\ of\ all\ mobile\ nodes}{number\ of\ mobile\ nodes}$$

Node displacement is calculated as the Euclidean distance between a node's current position and its initial position:

$$Displacement = \sqrt{(x - x_{initial})^2 + (y - y_{initial})^2}$$

Consider a set of source nodes $S = \{S_1, S_2, \ldots, S_m\}$, where m is the total number of source nodes.

Each source node Si wants to send data packets to a destination node D.

The routing algorithm should consider the mobility of nodes and select the most appropriate path from S_i to D. The selection of the path can be based on factors such as node connectivity, link quality, node stability, or any other mobility-related parameters.

The objective of the mobility-aware network model can vary depending on the specific scenario and requirements. It could be to maximize network connectivity, minimize packet loss, minimize end-to-end delay, or optimize energy consumption, among other objectives. The optimization objective can be formulated as an objective function that incorporates mobility-related metrics and other relevant factors. To optimize the mobility-aware network model, mathematical optimization techniques can be applied. This may involve formulating the problem as an optimization problem with constraints and objectives, and then using optimization algorithms to find optimal solutions. Techniques such as linear programming, integer programming, or heuristic algorithms can be employed depending on the complexity of the problem and available resources. By utilizing mathematical expressions and explanations, we can develop a mobility-aware network model that takes into account node mobility, connectivity, routing, and optimization objectives. This is used to analyse and optimize the network's performance under varying mobility patterns and scenarios.

E. DUAL-PHASE OPTIMAL RELAY SELECTION MECHANISMS IN BLOCKCHAIN-ENABLED CELLULAR-BASED IOT NETWORKS

Dual-phase optimal relay selection mechanisms are another important component of secure and reliable communication in blockchain-enabled cellular-based IoT networks [31]. Dual-Phase Optimal Relay Selection Mechanisms in Blockchain-Enabled Cellular-Based IoT Networks can be formulated and optimized. This approach ensures efficient selection of relay nodes based on both primary and secondary criteria, resulting in improved performance, reliability, and security in the network. This mechanism help to select the best communication path between the sender and receiver, taking into consideration factors such as the quality of the signal, the distance between the devices, and the available bandwidth. The optimality scheme utilized in this article shown in Figure 3, exploits the concept of optimal relay selection mechanisms and gives an idea of how they can be used in IoT networks.

Optimal relay selection mechanisms involve selecting the best relay node for each communication on the network. A relay node is an intermediate node that helps to transmit data between the sender and receiver. The goal of optimal relay selection mechanisms is to select the relay node that provides the best communication quality, while minimizing the delay and maximizing the throughput. Machine learning algorithms are used to analyze network conditions and select the best relay node for each communication, while dropping the unwanted connections during optimal selection [32]. These algorithms can take into consideration factors such as the distance between the devices, the quality of the signal, and the available bandwidth. Based on this analysis, the algorithm can select the relay node that provides the best communication quality for each communication. One of the benefits of optimal relay selection mechanisms is that they can help to advance the performance of the networking system. By selecting the best relay node for each communication, the mechanisms can help to reduce the delay and maximize the throughput, which can improve the overall efficiency of the network.

Let $R = \{R_1, R_2, \ldots, R_n\}$ represent the set of available relay nodes in the network.

Each relay node R_i has associated attributes or characteristics, such as location, connectivity, energy level, or reliability. To perform optimal relay node selection, we need to define a set of metrics or criteria based on the specific objectives and requirements of the network.

Let $R_{selected} = \{R_i | x_i = 1\}$ be the subset of relay nodes selected for the current phase, where x_i is a binary decision variable indicating whether relay node R_i is selected.

The Dual-Phase Optimal Relay Selection Mechanism consists of two distinct phases: an Initial Phase and a Final Phase. In the Initial Phase, a subset of relay nodes is selected based on a primary set of criteria or metrics, such as proximity to the source node, signal strength, or connectivity.

Let $R_{initial} = \{R_i \mid y_i = 1\}$ be the subset of relay nodes selected during the Initial Phase, where y_i is a binary decision variable indicating whether relay node Ri is selected in the Initial Phase.

Further, in the final phase, the relay nodes selected in the Initial Phase are further evaluated using additional criteria or metrics. These criteria may include security factors, reliability, available resources, energy consumption, or other relevant considerations. A mathematical evaluation function, denoted as $E(R_i)$, can be defined to assess the suitability of each relay node R_i in the Final Phase. The evaluation function considers a combination of attributes and assigns a score or rank to each relay node. To determine the optimal relay node selection, we need to optimize an objective function that considers both the Initial Phase and the Final Phase.

The objective function can be defined as: Maximize $f(R_{selected}) = g(R_{initial}) + h(R_{final})$, where $g(R_{initial})$ represents the performance or suitability score of relay nodes in the Initial Phase, and $h(R_{final})$ represents the performance or suitability score of relay nodes in the Final Phase.

The objective function can incorporate weightings to balance the importance of different phases or criteria based on their relative significance. In addition to improving performance, optimal relay selection mechanisms can also help to enhance the security of the network. By selecting the best relay node for each communication, the mechanisms can help to ensure that data is transmitted securely and that there are no vulnerabilities in the communication path. Optimal relay selection mechanisms are an important component of secure and reliable communication in blockchain-enabled

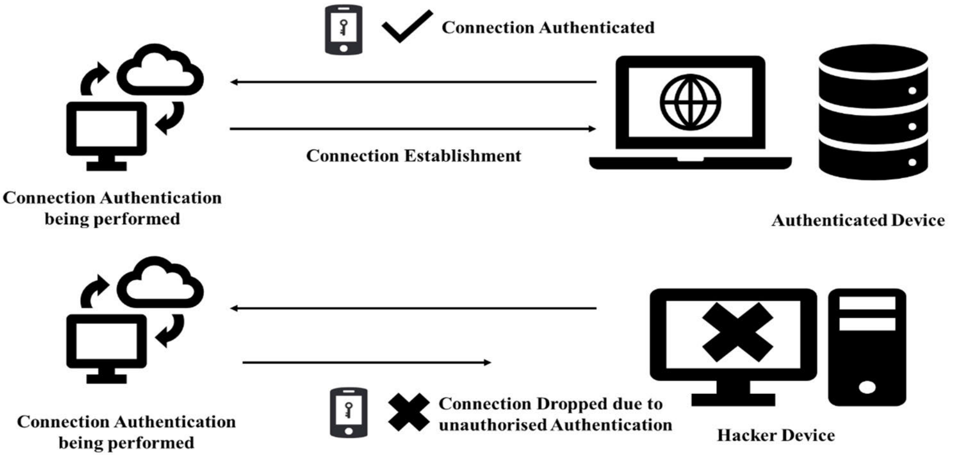

Connection Authenticated
Connection Establishment
Connection Authentication being performed
Authenticated Device
Connection Authentication being performed
Connection Dropped due to unauthorised Authentication
Hacker Device

FIGURE 2. Mechanism of authentication in blockchain-enabled cellular-based IoT networks.

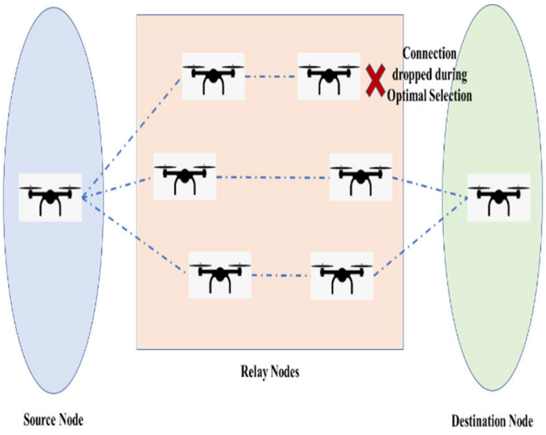


FIGURE 3. Mechanism of optimality scheme in blockchain-enabled cellular-based IoT networks.

cellular-based IoT networks. These mechanisms can help to improve the overall performance and security of the network, ensuring that data is transmitted securely and efficiently between devices.

F. DUAL-PHASE OPTIMAL RELAY SELECTION MECHANISMS IN BLOCKCHAIN-ENABLED CELLULAR-BASED IOT NETWORKS

In order to formulate an algorithm for eavesdropping-resistant secure communication, we can outline the steps and considerations involved by utilizing a secure communication path from S to D.

This article incorporates the requirements for authentication, blockchain-based enrolment, and other relevant factors specific to the cellular-based IoT network scenario. The solution to this optimization problem will provide an optimal relay enrolment strategy, authentication process, and the corresponding enrolment reliability, ensuring secure and reliable relay enrolment using authentication in Blockchain-Based Cellular-Based IoT Networks.

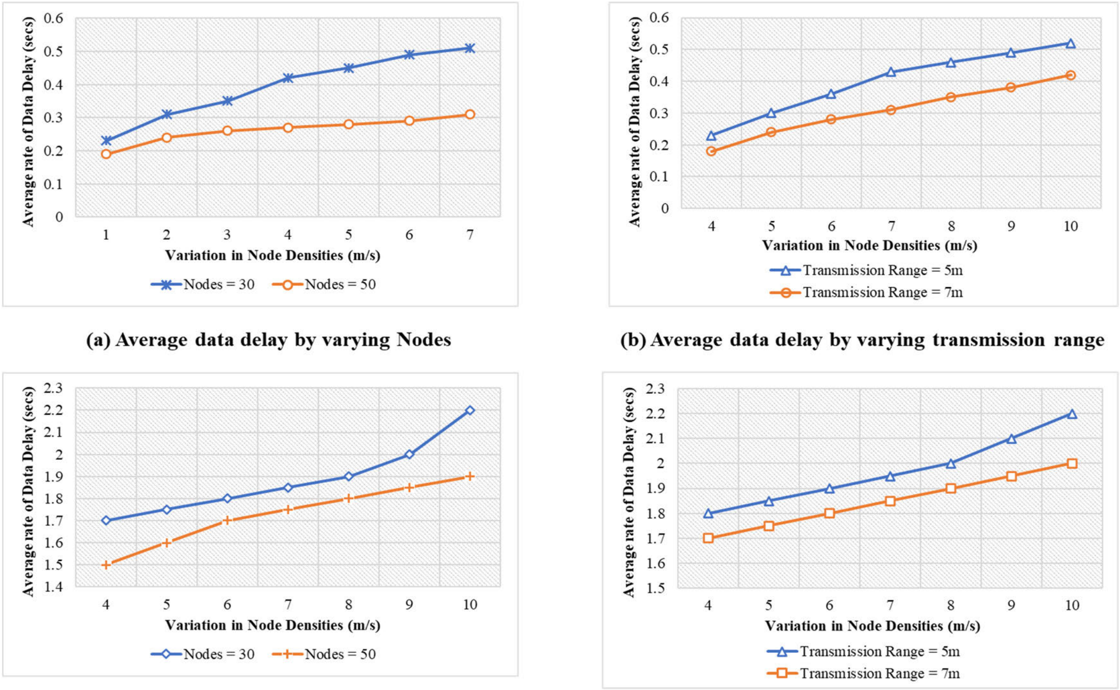
IV. RESULTS AND EXPERIMENTAL ANALYSIS

The simulation of the experimental implementation is done using MATLAB environment and Go 1.13 × 64 compiler for simulation of IoT environment, to evaluate the computation as well as communication cost of the entire deployment process.

A. ANALYSIS OF BLOCKCHAIN-BASED RELAY ENROLMENT BASED ON THE AUTHENTICATION PROCESS

To analyze the blockchain-based relay enrolment based on authentication in blockchain-enables cellular-based IOT networks, system initialization is evaluated setting the user varying from 100 to 1000 users. The authentication evaluation is presented in Figure 4 (a), which clearly i the linear graphical presentation between the average execution time and the number of users during the initialization process. However, when the number of nodes is increased, the execution time also gradually (as indicated in Figure 4 (b)) improves as more authentication inquiries are needed to be built during this process. For the execution of further optimization, the average execution time further increases with increasing the number of authentication inquiries, while keeping the number of nodes constant (in a case indicated in Figure 4 (c)). A comparative study, of authentication analysis, is indicated in Figure 4 (d) which shows the graph between authentication and the number of node inquiries considered for no optimization case and other cases when the recently used capacity of the optimized authentication mechanism is kept 100, 300 and 500 at respectively.

According to the graphical representation in Figure 4, the optimization method has nearly 32% fewer inquiries than the non-optimized technique when the recently used capacity is equal to 300. This results in nearly 25% lower computation & communication expenses for the full nodes, which further



(a) Average data delay by varying Nodes

(b) Average data delay by varying transmission range

(c) Link reliability by varying Nodes

(d) Link reliability by varying transmission range

FIGURE 4. **Blockchain based relay enrolment based on authentication evaluation in blockchain-enabled cellular-based IoT networks.**

improves the effectiveness of the suggested authentication approach.

B. ANALYSIS OF DUAL PHASE OPTIMAL RELAY SELECTION IN BLOCKCHAIN-ENABLED CELLULAR-BASED IOT NETWORKS

For the analysis of node density and transmission range, average data delay in networks with various node densities is analyzed and presented in Figure 5 (a) and Figure 5 (b). Moreover, an analysis of link reliability of the network is also done for varying node densities which is presented in Figure 5 (c) and Figure 5 (d).

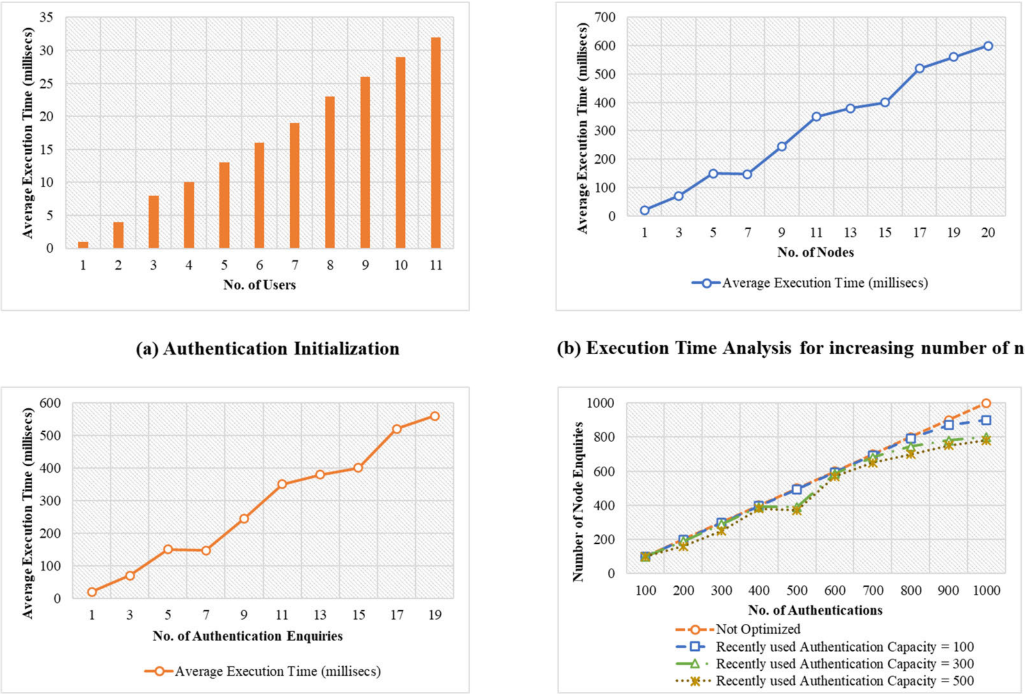
Figure 5 (a) depicts the average data delay of a network of nodes with various node densities. The average data latency is reduced as node density increases. In Figure 5(a), 40% of all linkages are presumptively assumed. All of the sensor nodes' transmission range is thought to be 10 meters. Figure 5(b) illustrates the average data delay of the suggested optimal relay node selection approach for a network with various node transmission ranges. For this network configuration, 50 nodes are utilized. More links are introduced into a network as nodes' transmission ranges increase. It has been experimentally detected that the average data latency decreases as the sensor node transmission range increases.

Figure 5(c) depicts the average link reliability of a given network with various node densities. Link dependability increases with a node density increase. 30% of the links in Figure 5(c) are presumed to be known a priori. In a network with varying node transmission ranges, the proposed optimum relaying node selection method's average link unreliability is depicted in Figure 5(d). It has been found that when the sensor node transmission range increases, average data latency gets better.

Figure 6 compares the proposed method's packet replication costs to those of the state-of-the-art routing techniques [33], [34]. Because the Epidemic routing protocol discussed in [34] sends a packet to each of its neighbors, the cost of packet replication is very high. It rises when a network's nodes grow in number. As opposed to the other two methods, the proposed method does not flood the network with packets. As a result, implementing the suggested strategy results in lower packet replication costs. Comparing the suggested method to the state-of-the-art Spray and Wait routing method [33], the cost of packet replication is almost 2.5 times lower. When averaged across many networks, the suggested method has a nearly 4.5 times lower packet replication cost than the Epidemic routing method [34].

C. ANALYSIS OF EAVESDROPPING RESISTED SECURE COMMUNICATION-BASED INTEGRATED DEPLOYMENT PROCESS

For simulation purposes, the UEs are distributed in an area of interest AOII) of 1000 m × 1000 m. To evaluate the reliability of the proposed algorithm, various scenarios of deployment are considered as follows:



(a) Authentication Initialization

(b) Execution Time Analysis for increasing number of nodes

(c) Execution Time Analysis for increasing Authentication Enquiries

(d) Comparison between authentication and number of node enquiries

FIGURE 5. Dual phase optimal relay selection analysis in blockchain-enabled cellular-based IoT networks.

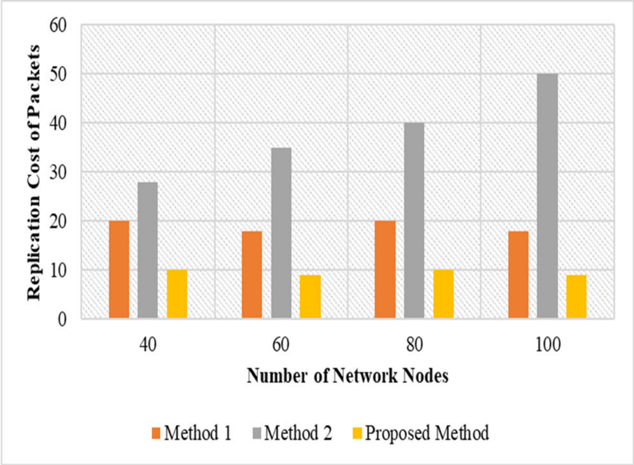


FIGURE 6. Comparison of proposed method's packet replication costs to state-of-the-art routing method 1 [33] and method 2 [34] techniques.

i **Fixed BSs:** The two possibilities with and without fixed BSs are taken into consideration. In the first scenario, UAVs are deployed to service every UE, but they also serve in the second scenario to assist the stationary BSs in servicing the unrevealed UEs.

ii **UEs Distribution:** UEs are distributed according to two different patterns: randomly (where they are spread out randomly over the AoI) and clustered (where they are grouped into several clusters).

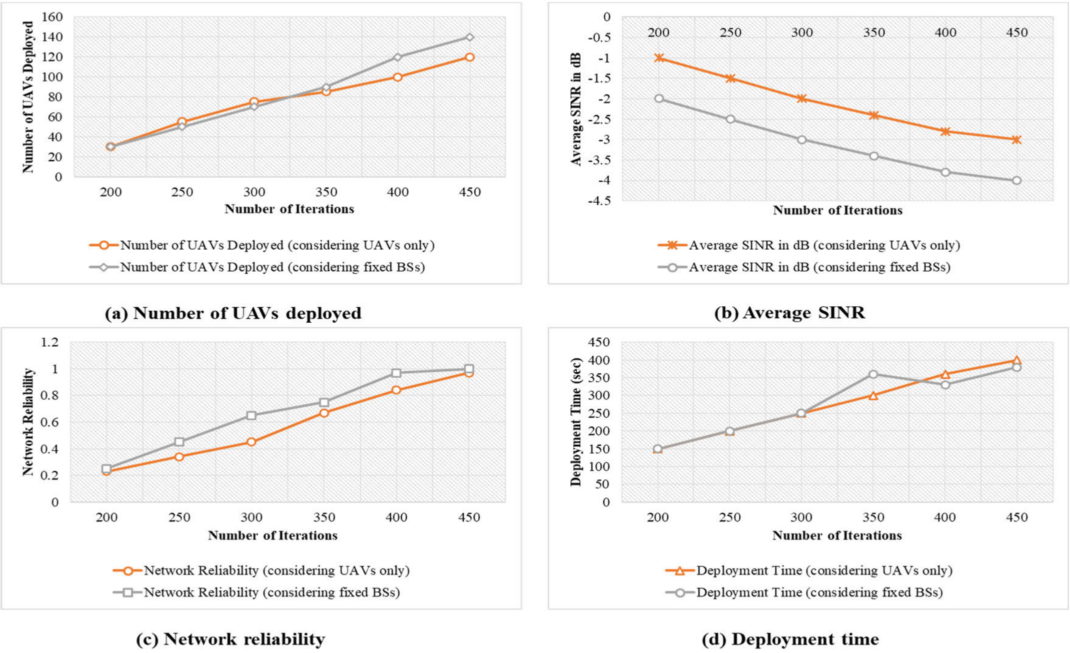
iii **UE number and UAV candidates:** We chose several types of UE and potential UAV numbers for the third point. Naturally, more UEs call for more UAVs to be deployed.

The two scenarios—UAV independently and with static BSs, by randomized and unrandomized patterns of traffic—are first explained using deployment examples. To validate the approach of the penetration motion algorithm and create a new virtual connection line, a second simulation is performed. We chose an identical number and distribution of candidate UAVs (i.e., N = 50 consistently dispersed candidate UAVs) that are sufficiently enough to accommodate all the UEs (i.e., M = 200 UEs) under various conditions [35]. This was done to show the applicability of the centralized candidate UAVs.

The statistics considered for performance evaluation are the number of UAVs deployed, average SINR, network reliability and deployment time. The number of UAVs depleted are defined by the number of active UAVs after deletion of redundant and idle UAVs is presented in Figure 7 (a), average SINR depicted in Figure 7 (b) is reflected based on QOS of UEs, network reliability shown in Figure 7 (c) is evaluated in terms of neighbourhood UAVs and deployment time depicted in Figure 7 (d) reflects the time complexity of the proposed system.

A comparison is done of the proposed integrated system with the completed centralized [36] and one completely distributed system [37], in terms of the number of UEs and deployment time, which is indicated in Figure 8.

By comparing the deployment time of the recommended eavesdropping resisted integrated algorithm with that of the



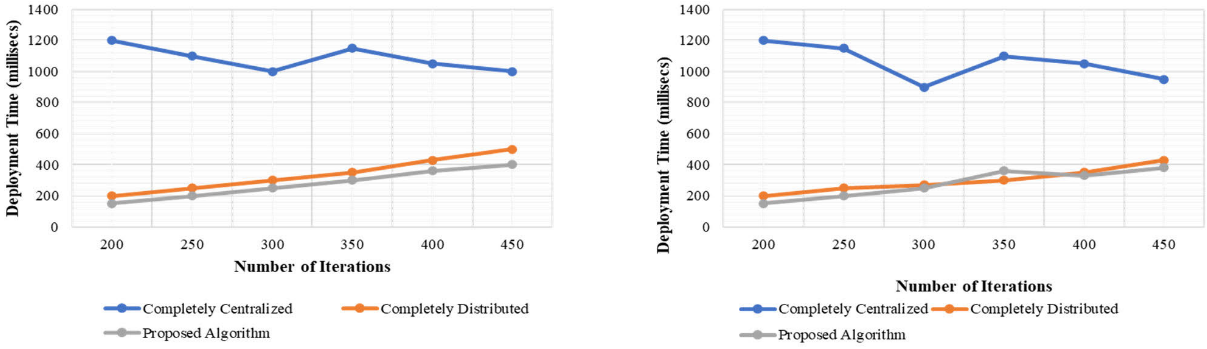
(a) Number of UAVs deployed

(b) Average SINR

(c) Network reliability

(d) Deployment time

FIGURE 7. (a) Number of UAVs deployed, (b)Average SINR (dB), (c) Network reliability, and (d) Deployment time millisecondss).



(a) Comparative Analysis considering UAV only

(a) Comparative Analysis considering Fixed BSs

FIGURE 8. Comparison of proposed eavesdropping resisted integrated system with the completed centralized [36] and one completely distributed [37] system.

other two algorithms in [36] and [37], namely the completely centralized and the completely distributed, we may assess the suggested hybrid algorithm's complexity. The amount of time used in this instance is an average of the random and clustered patterns. Figure 8 plots the deployment times for the three contrasting strategies against the number of UEs. The figures show that the pure centralized algorithm is significantly more time-complex than the other two. This is because it takes a long time to iterate since a large amount of candidate UAVs must be configured to function similarly to the suggested approach. However, the distributed algorithm finds it to be simpler.

The suggested technique and the entirely distributed method both outperform one another in various circumstances where the iteration count is low (i.e., when UAVs are deployed using fixed BSs and when UAVs are dispersed alone). However, when iteration count is low, as it is when these two scenarios are. However, the suggested approach outperforms purely distributed algorithm in the following areas: 1) The former's deployment time is lower than the latter's when M is large, and 2) The former's deployment time increases much more gradually than the latter's as UEs rise. The graphical representations further demonstrate that the deployment time for the completely distributed algorithm is growing quickly, the deployment time for the suggested hybrid method is increasing gradually, and the deployment time for the completely centralized algorithm is consistently reducing. This is understandable given that as UE increases: 1) For the completely distributed algorithm, more UAVs are going to investigate to cover more UEs, which results in an

Algorithm Dual-Phase Optimal Relay Selection in Blockchain-Enabled Cellular-Based IoT Networks

```
Input:
  - Source node S
  - Destination node D
  - Set of relay nodes $R = \{R_1, R_2, \ldots, R_n\}$
  - Set of eavesdroppers $E = \{E_1, E_2, \ldots, E_m\}$
  - Threshold for channel capacity
Output:
- Secure communication path from S to D
Procedure:
1. Calculate Secrecy Rates:
  For each relay potential node $R_i$ in R:
  a. Calculate the channel capacity between S and $R_i$ using secure communication techniques.
  b. Calculate the channel capacity between $R_i$ and D using secure communication techniques.
  c. For each eavesdropper $E_j$ in E, calculate the channel capacity between $R_i$ and $E_j$.
  d. Calculate the secrecy rate for the link between S and $R_i$:
  SecrecyRate(S-$R_i$) = min(Capacity(S-$R_i$), Capacity($R_i$-D)) - max(Capacity($R_i$-$E_j$)) for all $E_j$ in E.
2. Relay Selection:
  a. Sort relay nodes in descending order based on their secrecy rates.
  b. Initialize an empty set $R_{selected}$ to store selected relay nodes.
  c. While $R_{selected}$ is not empty or there are remaining relay nodes:
  i. Select the relay node with the highest secrecy rate from the sorted list.
  ii. Add the selected relay node to $R_{selected}$.
3. Secure Communication Path Construction:
  a. Construct the secure communication path starting with source node S.
  b. Set the current node as S.
  c. For each relay node $R_i$ in $R_{selected}$:
  i. Calculate the channel capacity between the current node and $R_i$.
  ii. If the channel capacity is above the threshold and the link is secure, proceed to the next relay node.
  iii. Otherwise, remove $R_i$ from $R_{selected}$ and update the previous node as the new current node.
4. Connect the last relay node in $R_{selected}$ to the destination node D.
5. Return the secure communication path from S to D.
```

extended convergence time; 2) In the centralized approach, fewer candidate UAVs will be eliminated, which reduces the number of iterations required; 3) in the proposed algorithm, the hybrid solution results in both a lowered complexity and an overlay complexity tendency that is rather stable. The findings in the part before show that the proposed technique is preferable in terms of complexity.

Further, certain applications of secure and reliable communication in blockchain-enabled cellular-based IOT networks and future scope and recommendations are provided in this section.

D. ANALYSIS OF TASK COMPLETION TIME, LATENCY RATE, AND ENERGY CONSUMPTION DURING DATA UPLOADING TO THE BLOCKCHAIN

The detailed blockchain-based UAV system setup includes the decentralized blockchain which includes multiple members collectively contributing to maintaining the blockchain. This setup allows for a distributed and collaborative approach to blockchain management. The UAV environment in the simulation is the scenario where UAVs are used to perform various tasks, possibly related to data collection, monitoring, or other missions. The environment is characterized by the use of 50 UAVs for performing these tasks, and the simulation aims to evaluate the performance and efficiency of the UAV system. Key parameters being assessed include task completion time, latency rate, and energy consumption, which are critical factors in UAV operations. A UAV simulation environment with 50 UAVs and 200 ground vehicles in a 1000 m x 1000 m catastrophe zone was used to define parameters. UAVs take a straight-line route above the two-lane road at 50 meters. First, vehicles are randomly put on each lane of the road with a minimum safe distance of 15 meters and UAVs are placed every 100 meters. Ground vehicles can only travel 25–75 km/h on roads. The number of jobs offloaded by UAVs is distributed evenly between 10 and 20.

To analyse the process of data uploading to the blockchain, certain parameters like completion time, latency and energy consumption are evaluated. These parameters are analyzed for two different cases of blockchain: decentralized and distributed datasets. In the case of a decentralized blockchain, the members collectively contribute to the upkeep of the blockchain, which is not overseen by a single entity. However, in a distributed blockchain dataset, the full database history is accessible to every node in the blockchain, making it impossible for any node to modify the database. Considering, these two blockchain categories, the analysis of task completion time, latency rate, and energy consumption during data uploading to a blockchain is done. Figure 9 depicts the task completion time and energy consumption for a different number of tasks.

As in Figure 9, the task completion time and energy consumption are evaluated for different numbers of tasks considering decentralized and distributed blockchain mechanisms. With the increase in the number of tasks, completion time as well as energy consumption also increase. This is because rise in the number of tasks increases the delay in task processing and UAV transfer. The decentralized blockchain approach achieves the least task processing latency and the distributed blockchain-based approach performs similarly to that. Both incur considerable energy costs and go beyond the UAV's battery capacity. Additionally, the decentralized blockchain-based approach outperforms distributed when the

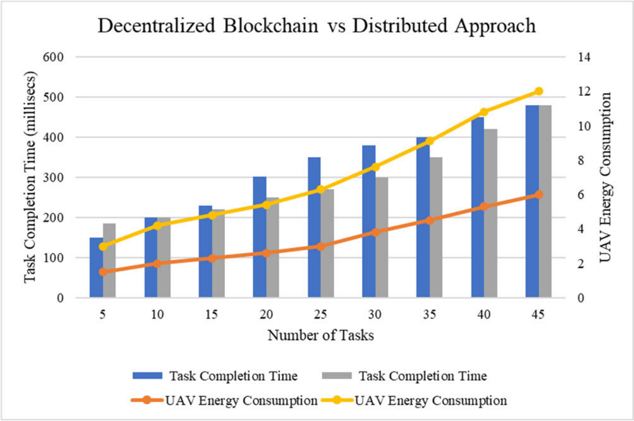


FIGURE 9. **Comparison of the number of tasks Vs. task completion time and UAV energy consumption.**

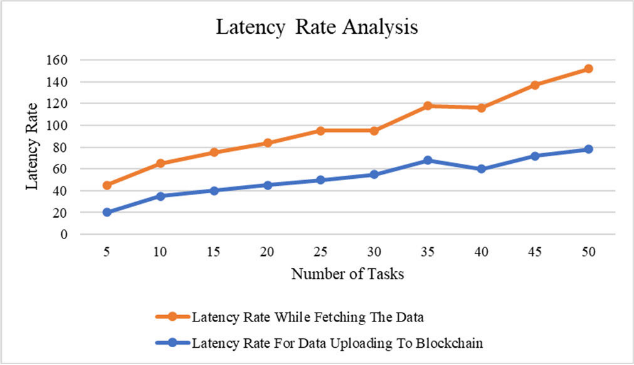


FIGURE 10. **Comparison of proposed method's latency rate for data uploading to blockchain and while fetching the data.**

number of tasks is small, but distributed blockchain outperforms decentralized blockchain and even violates the battery limitation when number of tasks is large. The rationale is that while traveling between sites requires more propulsion energy at high speeds, lifting against gravity requires less energy at lower flight speeds. When the number of tasks is big, the distributed blockchain violates the battery restriction since UAVs fly at random, maximum, and lowest speeds, increasing the energy cost in transitions.

Figure 10 provides the latency rate comparison for the two scenarios; one is the data uploading process to the blockchain and the other is fetching data from the blockchain. Data uploading latency is minimal when there are fewer number of tasks, as illustrated in Figure 10, and the latency variation is controlled within a narrow range as the number of uploading operations rises. Additionally, we can see that data uploading latency rises with the number of tasks, which is a result of the lengthening of the time required for consensus among nodes and transaction verification. We can optimize the consensus procedures to reduce data uploading latency. The delay in fetching data from the blockchain is also displayed in Fig. 10. Data may be retrieved from a local backup of the ledger and fetching operation does not require transaction validation and consensus. It is very effective since the expansion of domains does not result in significant changes in latency.

V. DISCUSSION AND LIMITATIONS

A. DISCUSSION

In this study, we have proposed a comprehensive framework for achieving secure and reliable communication in Blockchain-Enabled Cellular-Based IoT Networks. We have introduced methodologies for authentication and optimal relay selection, both of which play crucial roles in enhancing the overall security and performance of IoT networks. Below, we discuss the key findings and implications of our research.

1) AUTHENTICATION IN BLOCKCHAIN-BASED IOT NETWORKS

Authentication is a fundamental component of securing IoT networks. By leveraging blockchain technology, we have demonstrated the potential to create a robust authentication process for IoT devices. Our simulation scenarios have shown that using blockchain for device enrollment and authentication offers several advantages:

2) TAMPER-PROOF RECORDS

The distributed and immutable nature of the blockchain ensures that device enrollment records are tamper-proof, enhancing the integrity and trustworthiness of the network.

3) SCALABILITY

Blockchain provides a scalable solution for managing authentication records, even in large-scale IoT deployments. It effectively addresses the challenge of enrolling a large number of IoT devices securely.

4) SUPPLEMENTARY SECURITY LAYER

Blockchain acts as an additional security layer, making it difficult for attackers to compromise device authentication data. This enhances the overall security posture of the network.

5) AUDITABILITY

Blockchain's transparency allows for easy auditing of authentication processes, enabling network administrators to monitor and verify device enrollments effectively.

6) DUAL-PHASE OPTIMAL RELAY SELECTION

Our research has also introduced dual-phase optimal relay selection mechanisms for improving communication quality in IoT networks. By selecting relay nodes based on both primary and secondary criteria, we aim to enhance network reliability and performance. Key findings include:

7) PERFORMANCE IMPROVEMENT

Dual-phase relay selection significantly improves communication performance in terms of reduced latency, increased throughput, and enhanced reliability. This is especially valuable in scenarios with unreliable or congested communication channels.

8) ENHANCED SECURITY

Optimal relay selection mechanisms contribute to improved security by selecting relay nodes that provide secure communication paths. This helps in mitigating eavesdropping threats and enhancing data confidentiality.

9) EFFICIENCY

Our simulations show that these mechanisms increase the efficiency of communication, reducing resource consumption and, consequently, energy consumption in IoT devices.

B. LIMITATIONS

While our research demonstrates promising results, it is essential to acknowledge the limitations and areas for further investigation:

1) BLOCKCHAIN OVERHEAD

Implementing blockchain technology introduces overhead in terms of computational resources and storage. The practical feasibility of deploying blockchain in resource-constrained IoT devices requires further exploration.

2) REAL-WORLD DEPLOYMENT

Our study is primarily simulation-based, and real-world deployment challenges, such as interoperability, scalability, and hardware constraints, need to be addressed for practical implementation.

3) DYNAMIC ENVIRONMENTS

IoT networks often operate in dynamic environments, where nodes join and leave the network frequently. Adapting blockchain-based authentication and relay selection to dynamic scenarios is an ongoing challenge.

4) SECURITY ENHANCEMENTS

While blockchain offers enhanced security, the network should also consider the security of blockchain itself, including protection against 51% attacks and smart contract vulnerabilities.

5) COMMUNICATION RANGE

Our simulations assume fixed communication ranges. In reality, the communication range may vary, leading to unpredictable connectivity issues.

6) ALGORITHM COMPLEXITY

Implementing optimal relay selection algorithms in resource-constrained IoT devices may require efficient algorithms and careful consideration of computational complexity.

C. FUTURE DIRECTIONS

To address the limitations and further advance secure and reliable communication in Blockchain-Enabled Cellular-Based IoT Networks, future research directions may include:

1) HARDWARE-OPTIMIZED BLOCKCHAIN

Exploring hardware acceleration for blockchain operations to reduce resource overhead in IoT devices.

2) DYNAMIC NETWORKS

Developing adaptive authentication and relay selection mechanisms capable of handling the dynamic nature of IoT networks.

3) BLOCKCHAIN SECURITY

Research on advanced blockchain security mechanisms and consensus algorithms for enhanced resilience.

4) REAL-WORLD TESTING

Conducting real-world experiments and pilots to validate the effectiveness of blockchain-based solutions.

5) INTEROPERABILITY

Investigating interoperability standards to ensure compatibility between diverse IoT devices and blockchain networks.

Our research lays the foundation for securing IoT communications through blockchain-based authentication and optimal relay selection. While promising, practical implementation and addressing associated challenges require further exploration in future studies. These efforts are vital to realizing the full potential of secure and reliable communication in the evolving landscape of cellular-based IoT networks.

VI. CONCLUSION

In this article, we proposed a novel approach to address the limitations of existing approaches and ensure secure and reliable communication in cellular-based wireless IoT networks. By enrolling UAV relay nodes in edge-assisted base stations, we provide an initial level of security to the UAV relays. We enhance optimal UAV relay selection by constructing a time-based graph network model and performing authentication of UAV relay nodes to enhance security against active eavesdroppers. The number of users has a linear connection with the execution time during system initialization. The execution time steadily gets faster as the number of nodes grows since there are more authentication requests. When optimization is used, the quantity of authentication inquiries causes the average execution time to rise. The relay enrollment and authentication optimization approach decreases inquiries by around 32%, which results in a 25% decrease in computation and transmission costs. We also mitigate the effects of passive eavesdroppers by jointly optimizing power and position based on their actions. The suggested approach outperforms the state-of-the-art algorithm in terms of lower deployment time and increasing efficiency much more gradually with increasing UEs. The deployment time for the previously presented algorithm is rapidly increasing, gradually increasing for the proposed eavesdropping resisted integrated deployment algorithm. Because of its hybrid solution, the proposed eavesdropping resisted integrated deployment algorithm harvests an overlay complexity tendency improving stability and lowering the complexity of the system. We further explored the security features of blockchain technology and the importance of authentication and relay selection. This article demonstrates secure and reliable healthcare, transportation, and industry communication emphasizing the importance of secure IoT communication and how blockchain and relay selection might be helpful. The outcomes obtained support the recommended algorithm's superiority in terms of reliability as well as complexity. Data latency is greatly reduced by the suggested relay selection strategy, which also increases network dependability. For eavesdropping-resisted secure communication, the hybrid algorithm performs better than both centralized and fully dispersed methods, especially when there are a lot of UEs involved. With more operations in the future, data uploading latency rises, although this may be improved for faster uploading. Our proposed eavesdropping-resisted integrated approach offers a promising solution to the challenges faced by existing approaches and contributes to the advancement of secure and reliable communication in cellular-based wireless IoT networks.

SYMBOL/ABBREVIATION TABLE

Symbol/Abbreviation	**Description**
R	Set of relay nodes
TR	Set of trusted relay nodes
UR	Set of untrusted relay nodes
E	Set of ground eavesdroppers
UE	Set of UAV eavesdroppers
S	Source node
D	Destination node
U	Uncertainties associated with UAV positioning
A	Altitude options for UAV positioning
xi	Binary variable indicating relay node selection
yj	Binary variable indicating UAV eavesdropper presence
zu	Binary variable indicating UAV positioning
Secrecy_Rate	Secrecy rate achieved in communication
Enrolment_Reliability	Reliability of relay enrolment and authentication process
G(V, E)	Network topology
M	Set of mobile nodes
Si	Source nodes
Speed	The average speed of mobile nodes
Displacement	Node displacement
E(Ri)	Evaluation function for relay node Ri
Rinitial	A subset of relay nodes selected in the Initial Phase
Rselected	A subset of relay nodes selected for communication

ACKNOWLEDGMENT

The authors express their gratitude to Princess Nourah bint Abdulrahman University Researchers Supporting

Project number (PNURSP2023R239), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

REFERENCES

[1] B. Li, Z. Fei, and Y. Zhang, ''UAV communications for 5G and beyond: Recent advances and future trends,'' *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2241–2263, Apr. 2019.

[2] P. K. Singh and A. Sharma, ''An intelligent WSN-UAV-based IoT framework for precision agriculture application,'' *Comput. Elect. Eng.*, vol. 100, May 2022, Art. no. 107912.

[3] H. Wang, H. Zhao, J. Zhang, D. Ma, J. Li, and J. Wei, ''Survey on unmanned aerial vehicle networks: A cyber physical system perspective,'' *IEEE Commun. Surveys Tuts.*, vol. 22, no. 2, pp. 1027–1070, 2nd Quart., 2020.

[4] H. Zeng, G. Dhiman, A. Sharma, A. Sharma, and A. Tselykh, ''An IoT and blockchain-based approach for the smart water management system in agriculture,'' *Expert Syst.*, vol. 40, no. 4, 2023, Art. no. e12892.

[5] C. Bhardwaj, S. Jain, and M. Sood, ''Transfer learning based robust automatic detection system for diabetic retinopathy grading,'' *Neural Comput. Appl.*, vol. 33, no. 20, pp. 13999–14019, Oct. 2021.

[6] J. Yang, A. Sharma, and R. Kumar, ''IoT-based framework for smart agriculture,'' *Int. J. Agricult. Environ. Inf. Syst.*, vol. 12, no. 2, pp. 1–14, Apr. 2021.

[7] T. Górski, ''Integration flows modeling in the context of architectural views,'' *IEEE Access*, vol. 11, pp. 35220–35231, 2023, doi: 10.1109/ACCESS.2023.3265210.

[8] A. Sharma, P. K. Singh, A. Sharma, and R. Kumar, ''An efficient architecture for the accurate detection and monitoring of an event through the sky,'' *Comput. Commun.*, vol. 148, pp. 115–128, Dec. 2019.

[9] C. Zhang, L. Zhu, and C. Xu, ''BPAF: Blockchain-enabled reliable and privacy-preserving authentication for fog-based IoT devices,'' *IEEE Consum. Electron. Mag.*, vol. 11, no. 2, pp. 88–96, Mar. 2022.

[10] R. Kumar, K. Taneja, and H. Taneja, ''Performance evaluation of MANET using multi-channel MAC framework,'' *Proc. Comput. Sci.*, vol. 133, pp. 755–762, Jan. 2018.

[11] M. A. Jan, S. R. U. Jan, M. Alam, A. Akhunzada, and I. U. Rahman, ''A comprehensive analysis of congestion control protocols in wireless sensor networks,'' *Mobile Netw. Appl.*, vol. 23, no. 3, pp. 456–468, Jun. 2018.

[12] A. Karami and M. Guerrero-Zapata, ''An ANFIS-based cache replacement method for mitigating cache pollution attacks in named data networking,'' *Comput. Netw.*, vol. 80, pp. 51–65, Apr. 2015.

[13] A. Al-Hourani, S. Kandeepan, and S. Lardner, ''Optimal LAP altitude for maximum coverage,'' *IEEE Wireless Commun. Lett.*, vol. 3, no. 6, pp. 569–572, Dec. 2014.

[14] M. Mozaffari, W. Saad, M. Bennis, and M. Debbah, ''Drone small cells in the clouds: Design, deployment and performance analysis,'' in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2015, pp. 1–6.

[15] R. I. Bor-Yaliniz, A. El-Keyi, and H. Yanikomeroglu, ''Efficient 3-D placement of an aerial base station in next generation cellular networks,'' in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2016, pp. 1–5.

[16] M. Alzenad, A. El-Keyi, F. Lagum, and H. Yanikomeroglu, ''3-D placement of an unmanned aerial vehicle base station (UAV-BS) for energy-efficient maximal coverage,'' *IEEE Wireless Commun. Lett.*, vol. 6, no. 4, pp. 434–437, Aug. 2017.

[17] L. Wang, B. Hu, and S. Chen, ''Energy efficient placement of a drone base station for minimum required transmit power,'' *IEEE Wireless Commun. Lett.*, vol. 9, no. 12, pp. 2010–2014, Dec. 2020.

[18] Z. Wang, L. Duan, and R. Zhang, ''Adaptive deployment for UAV-aided communication networks,'' *IEEE Trans. Wireless Commun.*, vol. 18, no. 9, pp. 4531–4543, Sep. 2019.

[19] M. Mozaffari, W. Saad, M. Bennis, and M. Debbah, ''Efficient deployment of multiple unmanned aerial vehicles for optimal wireless coverage,'' *IEEE Commun. Lett.*, vol. 20, no. 8, pp. 1647–1650, Aug. 2016.

[20] E. Kalantari, H. Yanikomeroglu, and A. Yongacoglu, ''On the number and 3D placement of drone base stations in wireless cellular networks,'' in *Proc. IEEE 84th Veh. Technol. Conf. (VTC-Fall)*, Sep. 2016, pp. 1–6.

[21] J. Lyu, Y. Zeng, R. Zhang, and T. J. Lim, ''Placement optimization of UAV-mounted mobile base stations,'' *IEEE Commun. Lett.*, vol. 21, no. 3, pp. 604–607, Mar. 2017.

[22] D. Orfanus, E. P. de Freitas, and F. Eliassen, ''Self-organization as a supporting paradigm for military UAV relay networks,'' *IEEE Commun. Lett.*, vol. 20, no. 4, pp. 804–807, Apr. 2016.

[23] Y. Wang, Z. Su, T. H. Luan, J. Li, Q. Xu, and R. Li, ''SEAL: A strategy-proof and privacy-preserving UAV computation offloading framework,'' *IEEE Trans. Inf. Forensics Security*, vol. 18, pp. 5213–5228, 2023.

[24] C. Feng, B. Liu, Z. Guo, K. Yu, Z. Qin, and K. R. Choo, ''Blockchain-based cross-domain authentication for intelligent 5G-enabled Internet of Drones,'' *IEEE Internet Things J.*, vol. 9, no. 8, pp. 6224–6238, Apr. 2022.

[25] Y. Wang, Z. Su, Q. Xu, R. Li, T. H. Luan, and P. Wang, ''A secure and intelligent data sharing scheme for UAV-assisted disaster rescue,'' *IEEE/ACM Trans. Netw.*, early access, Apr. 20, 2023, doi: 10.1109/TNET.2022.3226458.

[26] S. Son, D. Kwon, S. Lee, Y. Jeon, A. K. Das, and Y. Park, ''Design of secure and lightweight authentication scheme for UAV-enabled intelligent transportation systems using blockchain and PUF,'' *IEEE Access*, vol. 11, pp. 60240–60253, 2023.

[27] A. Rashid and A. U. R. Khan, ''Blockchain-based autonomous authentication and integrity for Internet of Battlefield Things in C3I system,'' *IEEE Access*, vol. 10, pp. 91572–91587, 2022.

[28] O. I. Khalaf and G. M. Abdulsahib, ''Optimized dynamic storage of data (ODSD) in IoT based on blockchain for wireless sensor networks,'' *Peer-to-Peer Netw. Appl.*, vol. 14, no. 5, pp. 2858–2873, Sep. 2021.

[29] C. Bhardwaj, S. Jain, and M. Sood, ''Deep learning–based diabetic retinopathy severity grading system employing quadrant ensemble model,'' *J. Digit. Imag.*, vol. 34, no. 2, pp. 440–457, Apr. 2021.

[30] W. Jiang, H. Li, G. Xu, M. Wen, G. Dong, and X. Lin, ''PTAS: Privacy-preserving thin-client authentication scheme in blockchain-based PKI,'' *Future Gener. Comput. Syst.*, vol. 96, pp. 185–195, Jul. 2019.

[31] A. Capone, Y. Li, M. Pióro, and D. Yuan, ''Minimizing end-to-end delay in multi-hop wireless networks with optimized transmission scheduling,'' *Ad Hoc Netw.*, vol. 89, pp. 236–248, Jun. 2019.

[32] S. Sharma, Y. Shi, Y. T. Hou, H. D. Sherali, and S. Kompella, ''Joint optimization of session grouping and relay node selection for network-coded cooperative communications,'' *IEEE Trans. Mobile Comput.*, vol. 13, no. 9, pp. 2028–2041, Sep. 2014.

[33] H. Zhao, H. Wang, W. Wu, and J. Wei, ''Deployment algorithms for UAV airborne networks toward on-demand coverage,'' *IEEE J. Sel. Areas Commun.*, vol. 36, no. 9, pp. 2015–2031, Sep. 2018.

[34] T. Spyropoulos, K. Psounis, and C. S. Raghavendra, ''Spray and wait: An efficient routing scheme for intermittently connected mobile networks,'' in *Proc. ACM SIGCOMM Workshop Delay-Tolerant Netw.*, Apr. 2005, pp. 252–259.

[35] M. Zhang and R. S. Wolff, ''A border node based routing protocol for partially connected vehicular ad hoc networks,'' *J. Commun.*, vol. 5, no. 2, pp. 130–143, Feb. 2010.

[36] F. Lagum, I. Bor-Yaliniz, and H. Yanikomeroglu, ''Strategic densification with UAV-BSs in cellular networks,'' *IEEE Wireless Commun. Lett.*, vol. 7, no. 3, pp. 384–387, Jun. 2018.

[37] H. Wu, X. Tao, N. Zhang, and X. Shen, ''Cooperative UAV cluster-assisted terrestrial cellular networks for ubiquitous coverage,'' *IEEE J. Sel. Areas Commun.*, vol. 36, no. 9, pp. 2045–2058, Sep. 2018.

SAMIA ALLAOUA CHELLOUG received the Engineering and master's degrees in computer science and the Ph.D. degree in networking from the University of Constantine, Algeria, in 2003, 2006, and 2013, respectively. From 2006 to 2013, she was an Assistant Professor with the Faculty of Computer Science, University of Constantine. In August 2013, she joined the Department of Networks and Communication Systems, Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia, where she is currently an Assistant Professor. She has published more than 20 papers in journals and conference proceedings and has reviewed some ICCC15 conference papers. Her current research interests include wireless sensor networks, body area networks, cloud computing, cognitive radio, mobile wireless networks, vehicular networks, the Internet of Things, and pervasive computing.

REEM ALKANHEL (Member, IEEE) received the B.S. degree in computer sciences from King Saud University, Riyadh, Saudi Arabia, in 1996, the M.S. degree in information technology (computer networks and information security) from the Queensland University of Technology, Brisbane, Australia, in 2007, and the Ph.D. degree in information technology (networks and communication systems) from Plymouth University, Plymouth, U.K., in 2019. She has been with Princess Nourah bint Abdulrahman University, Riyadh, since 1997, where she is currently a Teacher Assistant with the College of Computer and Information Sciences. Her current research interests include communication systems, networking, the Internet of Things, information security, information technology, quality of service and experience, software-defined networks, and deep reinforcement learning.

AHMED AZIZ (Member, IEEE) received the B.Sc. degree (Hons.) in computer science and the M.S. degree in computer science from the Faculty of Computers and Informatics, Benha University, Benha, Egypt, in June 2007 and October 2014, respectively, and the Ph.D. degree in computer science from the School of Computer and System Science, Jawaharlal Nehru University, New Delhi, India, in 2019. From December 2007 to December 2010, he was a Lecturer Assistant with the Computer Science Department, Faculty of Science, Benha University, where he was also an Assistant Professor with the Faculty of Computer and Artificial Intelligence, from 2014 to 2019. From August 2019 to September 2020, he was an Associate Professor with the Department of Computer Science and Engineering, Sharad University, India (Uzbekistan). Since October 2020, he has been a Professor with the Department of International Business Management, Tashkent State University of Economics (TSUE), Tashkent, Uzbekistan. He has published more than 18 research articles of SCI with high-impact factors, such as IEEE Sensor Journal (IF3.7), IEEE Internet of Things Journal (IF 9.07), *Journal of Network and Computer Applications* (IF 5.9), and IEEE Access (IF 4.05); and quarter one Scopus-index journals. His research interests include sensor networks, compressive sensing, computing, wireless networks, and the IoT.

MOHAMMED SALEH ALI MUTHANNA received the M.S. degree from the Computer Science Department, Saint-Petersburg Electrotechnical University "LETI," Russia, in 2016, and the Ph.D. degree from the Chongqing University of Posts and Telecommunications, Chongqing, China, in 2021. Currently, he is a Postdoctoral Fellow with the Institute of Computer Technologies and Information Security, Southern Federal University, Russia. His main research interests include mobile edge computing, software-defined networks (SDN), the IoT, industrial wireless, and sensor networks.

AMMAR MUTHANNA (Member, IEEE) received the B.Sc., M.Sc., and Ph.D. degrees from the Saint Petersburg State University of Telecommunications, in 2009, 2011, and 2016, respectively. In 2012 and 2013, he took part in the Erasmus Student Program with the Faculty of Electrical Engineering, University of Ljubljana. In 2014, he was a Visitor Researcher with Tampere University, Finland. From 2017 to 2019, he was a Postdoctoral Researcher with the Peoples' Friendship University of Russia (RUDN University). He is currently an Associate Professor with the Department of Telecommunication Networks, the Deputy Head of Science, and the Head of the SDN Laboratory and in part he is an Associate Professor with the Peoples' Friendship University of Russia (RUDN University). His research interests include wireless communications, 5G/6G cellular systems, the IoT applications, edge computing, and software-defined networking. He has been an active member of the technical program committee at many international conferences and journals. He has been an Expert on the Judges Panel and Challenge Management Board at AI-5G-Challenge, ITU, and Russian Host Organizer.