GaRuDa: A Blockchain-based Delivery Scheme Using Drones for Healthcare 5.0 Applications

Journal:	*IEEE Communications Magazine*
Manuscript ID	COMMAG-20-00520.R2
Topic or Series:	February 2021/Cybersecurity for Critical Infrastructure Systems
Date Submitted by the Author:	29-Oct-2020
Complete List of Authors:	Gupta , Rajesh ; Nirma University, CSED Bhattacharya , Pronaya; Nirma University, CSED Tanwar, Sudeep ; Nirma University of Science and Technology Institute of Technology, Computer Engineering Kumar, Neeraj; Thapar University Patiala , CSED Guizani, Mohsen; University of Idaho, ECE; University of Idaho
Key Words:	Critical infrastructure, Cyber-security, Blockchain

GaRuDa: A Blockchain-based Delivery Scheme Using Drones for Healthcare 5.0 Applications

Rajesh Gupta, *Student Member, IEEE*, Pronaya Bhattacharya, Sudeep Tanwar, *Member, IEEE*, Neeraj Kumar, *Senior Member, IEEE*, Mohsen Guizani, *Fellow of IEEE*

***Abstract*—Over the years, the healthcare industry has transformed from being hospital-centric to patient-centric. The shift is due to the conflux of emergent technologies like Internet-of-Things (IoT)-based healthcare, Fifth-Generation (5G) assisted networking, and data-driven analytics through Artificial Intelligence (AI). The convergence, termed as Healthcare *5.0*, has improved healthcare services to support real-time analytics, user mobility, remote monitoring, and user personalized experience through decentralized applications. However, the medical supply chain systems or delivery operations among healthcare stakeholders suffer from limitations of harsh environmental conditions due to restricted zones, terrains, war-prone areas, poor-road conditions, congested traffic, and remote locations. Thus, Internet-of-Drones (IoDs) are deployed in healthcare *5.0* supply chains to streamline and expedite the medical delivery process through open channels, i.e, the Internet. But, the Internet is an open channel, which opens the doors for the intruders to perform malicious activities so the privacy and confidentiality of patient data can be sacrificed. Blockchain has emerged as a technology to handle the security and reliability of drone delivery among untrusted open channels. Motivated from the aforementioned facts, in this article, we propose, *GaRuDa*, a blockchain-based drone delivery scheme for Healthcare *5.0* applications. The proposed scheme addresses the amalgamation of IoD and blockchain through Fifth Generation (5G)-enabled Tactile Internet (TI) to facilitate low-latency responsive delivery of medical supplies that can be chronologically monitored and tracked among different stakeholders. The proposed scheme is compared with the traditional medical delivery scheme with payment gateways to indicate its effectiveness in terms of computation and communication costs.**

***Index Terms*—Internet of drones, Blockchain, Security, 5G, Unmanned Aerial Vehicle, Tactile Internet.**

I. Introduction

The healthcare industry has experienced a paradigm shift of technology-driven solutions with a transition from Healthcare *1.0* to Healthcare *5.0*. In healthcare *1.0*, medical records are manual and doctor-centric. With digitization, manual records are converted to electronic form in healthcare *2.0*, which is termed as Electronic Health Records (EHRs). As the storage was centralized, Healthcare *3.0* saw the decentralization of EHRs through mobile applications to form a patient-centric ecosystem. These records were subject to security attacks by malicious entities and lacked real-time decision analytics. Healthcare *4.0* introduced convergence of AI and big-data analytics to improve decision models on stored EHRs. The convergence brought interoperability issues among medical stakeholders and with the increase in data, the AI models became complex and inefficient, which makes the applications less responsive. Healthcare *5.0* proposes an umbrella solution to converge light-weight IoT protocols, 5G/Sixth-Generation (6G) communication, and security-based solutions to form a patient-centric responsive business model. The evolution of healthcare industry from Healthcare *1.0* to *5.0* is shown in Fig. 1.

In Healthcare *5.0*, the main concern is to keep the patient at the center of the healthcare ecosystem. To achieve this, medical deliveries are supported by healthcare stakeholders like patients, doctors, clinics, and warehouses. Currently, the health supply-chain streamline delivery operations among drug manufacturers to end-consumers, which suffers from long processing cycles due to the dependency of stakeholders, manual delivery, and traditional payment models. In Healthcare *5.0*, the delivery time can be reduced with the adoption of IoDs in the delivery systems. IoDs are robotic Unmanned Aerial Vehicles (UAVs), or Flying Robots (FR) that are remotely administered through Ground Stations (GS) with wireless communication channels [1]. The demand for UAVs adoption has been increasing in the manufacturing, defense, and healthcare sectors from $0.25 billion in 2013 to approximately $3.3 billion in 2020 [2]. Moreover, UAVs are equipped with directional sensors, processors, and communication cards. Due to dynamic configuration, easy deployment, and faster response, UAVs usage in the healthcare sector increases many folds. However, the usage of a single UAV, due to limited energy and visual computations, can service a limited geographical range. To address the aforementioned issue, multi-UAV systems are proposed to increase spatial coverage. It also increases the robustness of delivery mechanisms to ensure the guaranteed delivery of medical supplies to end-customers in the healthcare *5.0* ecosystem.

In a multi-UAV system, different UAVs form an on-demand ad-hoc vehicular network for location updates, planning of path trajectories, and to increase the lifetime of the entire ecosystem. The UAVs pass information to each other inside a spatial coverage range. As UAVs operate in terrain and tough environmental conditions, so the communication network faces severe bandwidth limitations. This hinders the propagation of real-time updates, precision, and accuracy of the information

R. Gupta, P. Bhattacharya, and S. Tanwar are with the Department of Computer Science and Engineering, Institute of Technology, Nirma University, Ahmedabad, 382481, Gujarat, India. (Emails: 18ftvphde31@nirmauni.ac.in, pronoya.bhattacharya@nirmauni.ac.in, sudeep.tanwar@nirmauni.ac.in)

N. Kumar is with Thapar Institute of Engineering and Technology, Deemed to be University, Patiala, Punjab, India. (E-mail: neeraj.kumar@thapar.edu)

M. Guizani is with the Department of Computer Science and Engineering, Qatar University, Qatar, e-mail: (mguizani@ieee.org).

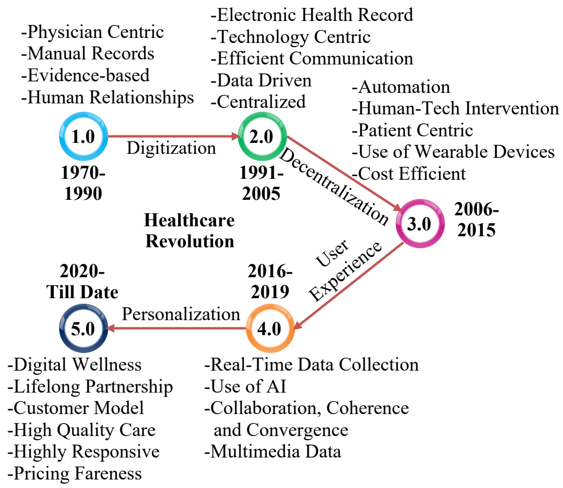

Fig. 1: Revolution in Healthcare Industry from Healthcare *1.0* to *5.0* [3].

being exchanged. Also, UAVs need to communicate with GS to plan their route, which is termed as Line-of-Sight (LOS) of UAVs. In case of poor network connections, information loss leads to incorrect LOS updates and UAVs can divert from their planned trajectories, which leads to unauthorized UAV sightings at restricted zones. To address the aforementioned limitations, 5G communication networks are applicable to ensure low-latency, responsiveness, and higher reliability of the data being exchanged. Also, 5G-enabled TI can reduce UAVs' communication latency and increase responsiveness [4]. However, responsive TI communication suffers from security attacks due to a variety of attack vectors like- channel switching to Fourth Generation (4G)/Third Generation (3G) networks due to poor connectivity, frequent hand-offs, and induced non-linear noises through backhaul optical planes [5]. Various attacks like impersonation, side-channel, channel hijacking, and distributed denial-of-service are possible. Thus, a trust-based framework is required in TI-based drone communication to allow transparency and consensus among multi-UAV entities.

Blockchain technology can be a viable solution to address the aforementioned security concerns of drone communications. It is a distributed ledger that stores hashes of previous blocks in an immutable ledger [6]. The stored blocks are accessible to all stakeholders in the chain. A new block is added through a mining procedure, which ensures consensus among all stakeholders in the chain. The new block is added to the existing chain and a copy is propagated to all nodes. Thus, a chain structure cannot be altered by a malicious user. In the healthcare sector, blockchain is widely adopted by market competitors and healthcare research organizations [7]. In the blockchain, automated payments are facilitated via smart contracts, which are executed as programmable codes when specified conditions are met. They solved the interoperability issues of supply-chains and reduce delays by automating payments. Moreover, they eliminate dependencies among stakeholders and ensure transparency in operations.

Motivated from the aforementioned facts, in this article, we integrate blockchain, 5G-TI communication, and UAVs for healthcare *5.0* ecosystems. The proposed scheme *GaRuDa* facilitates secure drone delivery with a real-time response over the TI channel. This allows higher fault-tolerance and guarantees delivery to end-clients even in terrain and tough environments. In *GaRuDa*, smart contracts are executed in blockchain among different stakeholders in the supply-chain to ensure trust in operations. To ensure security via cryptographic primitives, public/private key pairs of different users executing the smart contract is fetched from InterPlanetary File System (IPFS) to allow a global name-space for all entities. Only transactional meta-data is stored in blocks, thereby addressing the scalability of mined transactions in the blockchain.

The structure of this article is as follows. Section II describes the background of key technologies used in healthcare *5.0* applications. Section III describes the proposed *GaRuDa* scheme and Section IV highlights open issues and research challenges. Section V discusses the case study of the traditional drone-delivery scheme and finally, Section VI concludes the article.

II. Background

This section highlights the deployment of drones in the Healthcare *5.0* industry to facilitate the delivery cycle of medical supplies. As the drones communicate through decentralized open networks, trust, interoperability, and automated payments are done via the blockchain.

A. Drones in Healthcare 5.0

Historically, IoDs are developed to support military surveillance to combat German U-Boats during World-War-II in 1942 [8]. Later, as communication networks matured, industries started using UAVs in surveillance operations for the detection of biological and chemical hazards in disaster sites. They acquired real-time high-resolution images of affected sites to provide spatial coverage of affected sites [9]. In the medical industry, IoDs are deployed to support medical tracking and delivery systems. In 2014, *Medecins Sans Frontieres* (MSF) developed a drone-delivery mechanism to deliver tuberculosis samples to hospitals at 25% lower-cost than human delivery [10]. With the increased usage of the intelligent device in multi-user haptic communications with TI, remote telesurgery procedures are performed by robotic arms, which are controlled by surgeons [11]. Healthcare *5.0* focuses on building robust drone delivery chains to provide personalized and affordable medical supplies to remote patients with high availability in cases of any emergencies and terrain/tough environmental conditions. They deliver medics like-vaccines, blood samples, and drugs to medical stakeholders to reduce human effort at a faster speed. A comparison of existing healthcare drones deployed in medical organizations is shown in Table I.

B. Responsive-communication: Tactile Internet

In smart healthcare *5.0* applications, there is a humongous exchange of data content among medical devices. Although

TABLE I: Comparison of existing healthcare drones.

Drone	Year	Description	Company	Services Targeted	Benefits
Ambulance Drone	2014	Deliver the Defibrillator in case of cardiac arrest with high-speed ambulance drone	TU Delft	cardiac arrest, defibrillator delivery	High Speed
Flirtey Eagle	2015	It is a Nevada-based startup which delivers the first aid kits and emergency medication	Flirtey	first aid kit, defibrillator delivery	Highly reliable, safely and precisely delivery
DJI S900 UAV	2016	Speedy transport of blood samples with coolers attached in it to maintain blood integrity	Johns Hopkins University	Blood products	Temperature maintenance, and high speed
Google Drone	2016	It will bring emergency medical aids to people in pain before the arrival of the ambulance	Google	Medical aid delivery, cardiac arrest, anaphylactic shock	App available with Estimated Time of Arrival (ETA)
Ziplines Drone	2016	It is California based company that designed drones for medical supplies in Rwanda	Zipline	Blood, platelets, plasma, vaccines, and medicines	On-demand delivery
HQ-40 UAV	2017	Transport of Blood Samples over Long Distances, i.e, 161 miles by maintaining temperature conditions in Arizona desert	Johns Hopkins University	human blood samples, ability to land in a small area	Cover long distances
Vayu Drone	2018	It is used to transport blood samples and vaccines from emergency location to nearest lab for testing purpose	Vayu Inc.	blood samples and vaccines	Trackable with Iridium satellite network

wireless communications evolved due to the increased capacity of storage devices, Round Trip-Time (RTT) latency between distant host stations in a network is a critical issue. To design real-time responsive applications such as telesurgery, traffic-control, and vehicular networks, RTT latency needs to be reduced to allow responsiveness and interactions through the Internet, which is termed as TI. TI renders interaction latency among communication objects as non-observable to the human eye, to allow visual interactions known as haptics [12]. Thus, it can support virtual reality systems with audio and visual feedback at a low-latency of 1 ms. To address the challenges of low-latency, each frame duration in TI needs to be 33 μs for proper decoding and detection at receiver-transmitter. Currently, advanced Long Term Evolution-Advanced (LTE-A) systems achieve a data rate of 1 Gbps, which is not viable to support such short duration frames. So, the Orthogonal Frequency Multiplexing (OFDM) technique is embedded with LTE supported via optical back-planes to achieve LTE-OFDM rate of 10 Gbps, with a frame-duration close to 70 μs. To fully realize the capability of TI, 5G communication channels are required. Another challenge of TI is the high-availability of 99.99999 % up-time and a failure rate as low as 10^{-7}. 5G Massive-Multiple-in-Multiple-out (m-MIMO) channels with wide-band carrier aggregation are employed to reduce outage of uncorrelated links.

C. Blockchain Technology

In Healthcare *5.0*, patient wellness is of prime concern to sustain a lifelong partnership among medical stakeholders. According to the Health Insurance Portability and Accountability Act (HIPPA) [13] guidelines, a patient can view, update, and verify EHRs through decentralized applications. To ensure common records, trust, and interoperability among medical stakeholders, blockchain is a preferred choice, which was coined by Nakamoto cryptocurrency to leverage Healthcare *5.0* to secure patient-centric ecosystems. Blockchain is a distributed ledger that can structure EHRs as an immutable, chronological, and timestamped ledger with historical transactions easily accessible by every stakeholder in the chain. The transactions are visible to everyone in the case of a public blockchain, or a group of collaborating organizations in the case of a consortium chain. Nobody can control and operate the chain structure to modify block entries. Thus, blockchain facilitates a multi-party consensus ecosystem where all stakeholders agreed on the committed records making EHRs verifiable and authentic over open untrusted communication channels. To automate financial transactions, smart contracts are executed among participants, which are programmed codes executed automatically when a specified set of financial negotiations among medical stakeholders are met. The contracts execute without the involvement of third-party intermediaries like payment gateways. They are deterministic, accurate, and transparent to all users and their execution time is finitely bounded, hence they exhibit Turing-completeness property. The contracts can be developed using programming languages like Solidity, Go, and Node.js. When programmed on consortium chains, as in the case of permissioned blockchain, they are isolated in docker containers as chain-codes.

D. Integration of Blockchain, TI, and Drone Delivery

UAVs communicate through low-powered open channels to support dynamic responsive healthcare *5.0* applications with high-mobility. UAVs are self-programmed and remotely administered through GS. Moreover, they operate at the terrain and tough environments and are generally susceptible to security attacks such as hijacking, jamming, and side-channel attacks by malicious entities [14]. These entities can drain energy, or change the routing paths of UAVs. Blockchain can secure unauthorized access to UAVs through security measures in block additions and smart contracts. Integrating blockchain in drone delivery systems can induce trust in payment mechanisms, but to address the responsiveness of applications supported by healthcare *5.0*, a 5G-enabled TI channel can be used to ensure low-latency and high up-time

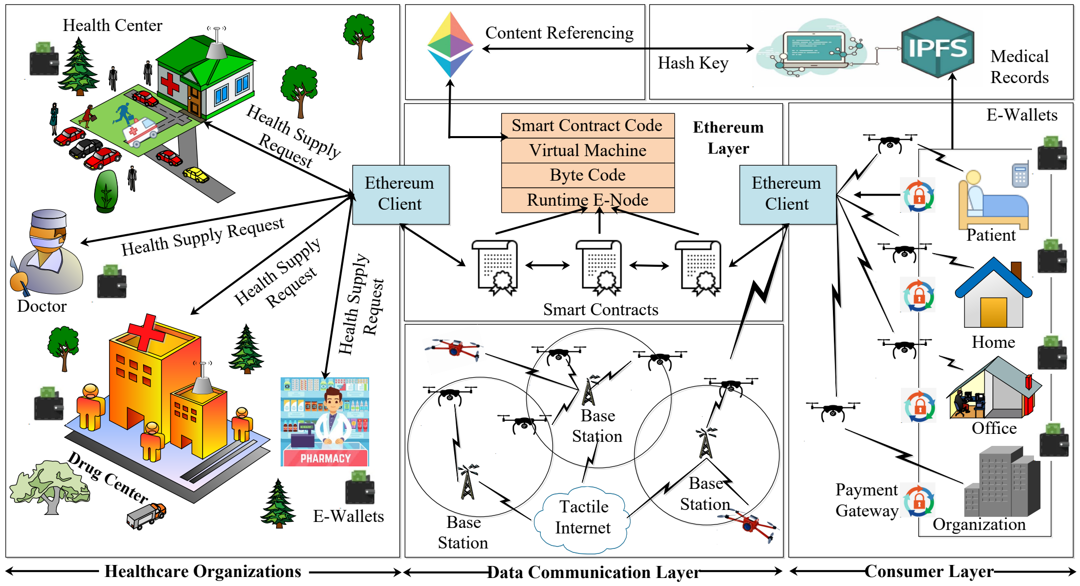

Fig. 2: *GaRuDa*: The proposed blockchain-based delivery scheme for healthcare 5.0 applications.

for applications. It also helps applications to form simpler AI models for analyzing generated data by applications. This facilitates effective business models to form informed decisions on patient critical illness and suggests timely intervention and possible remedial actions.

III. *GaRuDa*: The Proposed Scheme

In this section, we describe the working of *GaRuDa*, blockchain-based drone delivery for healthcare applications shown in Fig. 2 , which is divided into three layers: (i) data dissemination, (ii) data communication, and (iii) consumer layer. The details of these layers are as follows.

A. Data Dissemination Layer

It consists of healthcare product supply entities (E_{hs}) such as healthcare organizations, healthcare officials, drug delivery centers, and pharmacies, which receives the health supply requests from patients at the consumer layer (E_c). E_{hs} can use a patient's hash key to access their previous medical records/prescriptions, which are stored in the IPFS. Based on the medical history, E_{hs} can validate the E_c request for a particular healthcare product. The requests are being arranged or classified as an Emergency (E) or Non-Emergency (NE) based on the criticality of the patient and generate their Criticality Score (CS) accordingly. The value of CS ranges from 0 to 1, where 1 represents emergency (*priority delivery*) and 0 represents non-emergency.

One of the simplest classification algorithms is Naive Bayes classifier because its output is the probability value, i.e., 0 to 1. We also set the threshold value as 0.7 to identify the emergency requests, i.e., CS $\geq$ 0.7. The payment settlement between the communicating parties (i.e., E_{hs} and E_c) can be well-taken care of by the smart contracts. It also ensures the consistency and reliability of the delivery system, i.e., the next stage of the process will only be initiated once the payment has been received by the E_{hs}. After receiving the payment, communication is established with the data communication layer via an Ethereum client for further processing.

B. Data Communication Layer

This layer is responsible for delivering a package (i.e., healthcare supplies) from source to destination via drones using the 5G-enabled TI channel. Drones can initiate the delivery only if they satisfy the smart contract conditions (i.e., payment settlement status, destination distance, environmental conditions, and package mass). If they satisfy the conditions, then a particular delivery entry can be stored into the blockchain as a transaction and a drone initiates the delivery. An entry contains the information like sender's address, consumer's address, package mass, distance covered, and location tracing).

To store the data on a blockchain is quite costly (not affordable) due to its limited storage capacity. To overcome such a costly data storage operation, *GaRuDa* used IPFS, which is a distributed and immutable data storage system. The distributed feature of IPFS increases the throughput and reduces the latency in data access. Instead of storing the data into the blockchain, *GaRuDa* stores the entire data into the IPFS storage and generates a fixed-length hash value. So, this generated hash value can be stored in the blockchain as a transaction. If any E_{hs} wants to view the E_c data for the classification of health supply requests, then they must know the hash key of the E_c.

Once everything is verified, the shipping has been initiated via drones and the communication path it follows during their flight is 5G-enabled TI, which is having features like ultra-low end-to-end latency (*<1ms*) and ultra-high reliability (*99.999%*). 5G-TI ensures fast delivery as well as the reliability of the communication channel. The drones are continuously sharing information like location, distance covered, and delivery status (delivered: yes and not delivered: no). Drones are bounded with the flight time to cover a round trip. If it goes beyond the maximum stipulated time, then there is a possibility of mishappening, but in *GaRuDa*, both the data and hashes are kept in the immutable storage, i.e., IPFS and blockchain which cannot be modified. *GaRuDa* allows the tracing of drones activity to identify the origin of mishappening.

C. Consumer Layer

It consists of E_c who needs healthcare supplies. An entity E_c can be either patient or a normal person who can put their request for medical aids from the E_{hs} via blockchain. The E_c records are stored into the IPFS system (connected to Ethereum), which is directly accessible to E_{hs} using the E_c's hash key value. This layer also gives the location where the required supplies get delivered by drones and must be in the range of E_{hs}.

IV. Open Issues and Research Challenges

This section discusses the future research challenges for combining blockchain and IPFS with UAVs. The brief description of these open issues and future research challenges is as follows.

A. Infrastructure maintenance cost

UAVs are used in various applications such as defence, healthcare, agriculture, and package delivery. UAVs are driven by infrastructures (drone centers, base stations) installed at remote locations. There is always a heavy maintenance cost associated with the drone centers, communication channels, and drones itself.

B. Limited Flying Time

Drones are light-weight battery-powered devices with limited processing capabilities and battery time. It is not suitable to deliver the packages over long distances, which restricts its flying time. This issue can be resolved by installing more drone centers for battery replacement/charging, which is quite costly.

C. Energy Efficiency

UAVs are energy powered, so, their efficiency depends upon various parameters like design parameters (drone mass, max. speed, no. of circuits used, and no. motors used), area parameters (area distance and density), package characteristics (weight and distance covered), delivery type (critical or non-critical) and environmental conditions (rain and snowfall). So, it can be difficult to consider all the aforementioned parameters to make UAV energy efficient.

D. Processing Capability

Autonomous drones in the movement need to process a large amount of data captured from their surroundings to take quick decisions. Drones are small devices, which are not having complex processing capabilities. Researchers around the world are working on solving the aforementioned issue.

E. Bandwidth Requirement

The inclusion of IPFS saves the data storage cost but requires an excessive bandwidth (increased network cost), which restricts their adoption in real applications. The possible solution to overcome such an issue is to offer financial rewards to the content publishers, which covers the cost and encourage its adoption.

F. Legislation

Many countries have policies regarding the deployment of UAVs. As per the guidelines of the Federal Aviation Administration (FAA), drones cannot go beyond the line-of-sight. Until there are no regulations for UAVs, it can be difficult for a researcher to explore their full potential.

G. Data Availability

IPFS storage in the proposed scheme does not guarantee data availability each time it is requested. However, it can be guaranteed by using *content pinning*, which continually saves the transactional data copies on the IPFS storage node. IPFS retains only the pinned contents for a longer duration. If the complete transactional data is important, then it requires content pinning for every transaction, which is quite storage and time expensive.

H. Data Privacy

The proposed scheme uses IPFS for data storage, but it is public. If anyone knows the content hash, they can access the complete sequence of data. So, there exists no in-built solution in IPFS that ensure the security of data. *Cryptographic techniques* can be used to protect the data or by creating a list of private members who can access the IPFS data.

V. Performance Evaluation: A Case Study

In this section, a use-case of a traditional drone delivery scheme for the healthcare sector is presented. The traditional medical delivery company deals with the delivery of blood, platelets, frozen plasma, and cryoprecipitate to distribution centers around the world [15].

A. Traditional Scheme

In traditional medical drone-delivery ecosystems, there are distribution centers that support healthcare supply units with distributed healthcare facilities. The current annual-turnover of the healthcare industries assisting drone delivery services is estimated at $190 million and is expected to rise to $1.2 billion by 2020. Fig. 3 shows the healthcare ecosystem in which medical orders are collected via a common OFDM multiplexed channel that operates at 10Gbps. Once an order is collected, at the data communication layer, GS updates the location coordinates of the recipient through the 4G-LTE communication channel. The drone is launched with support cargo of a maximum of 1.3kgs (or 3.9 lbs) and launches GPS to ensure precision in flight at a range of 1,600 ft. The drones are capable to deliver medical supplies at a range of 80 km

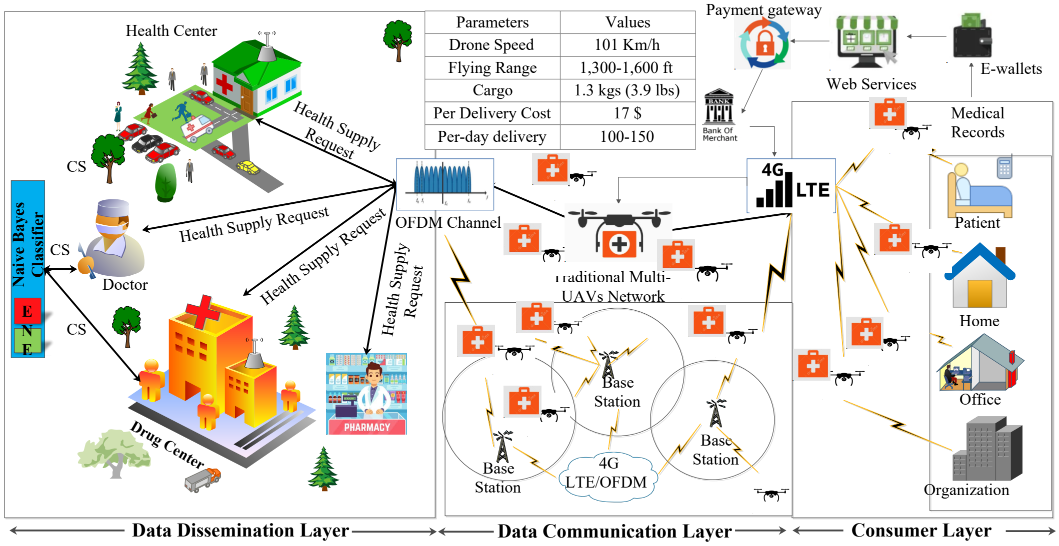

Fig. 3: Case Study: Traditional drone-delivery through third-party payment gateways

.

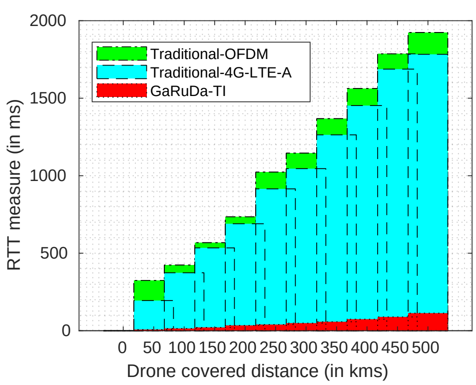

Fig. 4: *GaRuDa*: Computation cost.

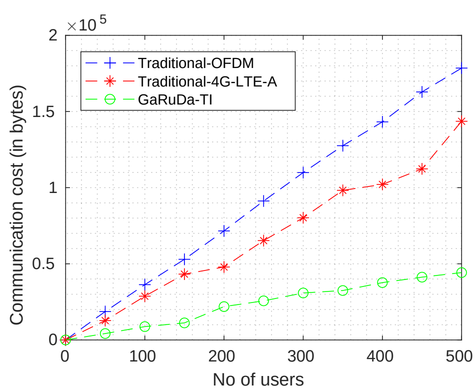

Fig. 5: *GaRuDa*: Communication cost.

at distribution centers clocking at a speed of 63 mph. The acceleration rate is from 0-70 mph in 0.33 seconds. Each drone can make 100-150 deliveries in a day depending on the environmental conditions. At the consumer layer, the drone drops the delivery packet at an accuracy of 16ft diameter of the recipient location zone. The per-delivery cost is estimated to be \$17, which the end-customer pays through payment wallets through third-party payment gateways.

B. Efficiency of GaRuDa

In this section, we evaluate the performance of the traditional scheme against the proposed scheme by considering communication and computation costs. We consider the computation cost in terms of distance covered by drones and the measured RTT value. In traditional schemes, 4G-LTE and 4G- channel multiplexing via OFDM are used. The maximum achievable throughput in 4G channels is *18Mbps* with *1.4 Mbps* of packet overheads consisting of channel and control information. In *GaRuDa*, we propose a TI-channel with optical backhauls to support a data-rate of *10Gbps*. Thus, the measured RTT value of traditional delivery scheme using LTE and OFDM is $\approx 18.3ms$ for OFDM and $\approx 17.51ms$ for LTE-advanced (LTE-A) [12]. Compared to this, TI has a measured RTT of $\approx 0.051ms$ as shown in Fig. 4. To evaluate the communication cost as shown in Fig. 5, we consider processing overheads against a number of users. Moreover, we consider the payload size of normal packets serviced through payment gateways. To secure electronic payments, the merchant provides *X.509* signed certificates, which ensures secured web-transactions. The encoding overheads of certificate generation are 831 bytes. Compared to this, in *GaRuDa*, we propose smart contracts for automating payments. An Ethereum transaction stores Tx.beneficiary, hash, and nonce as meta-information, which can be encoded in 92 bytes [14]. Thus, with more users, the proposed scheme, *GaRuDa*, has a lower communication cost. Thus, from extensive simulations, it is evident that integrating blockchain in 5G-enabled TI-channel for medical drones reduces the overall computation, communication, and operational costs to provide responsive support in healthcare *5.0* ecosystems.

VI. Conclusion

In this article, we propose a secure delivery scheme, *GaRuDa*, to expedite the delivery process of medical supply chains in Healthcare *5.0* using a 5G- enabled TI communication channel. The article is divided into four sections. In the first section, we discussed the impact and background of integrating blockchain and IoD to secure drone delivery over open untrusted channels. To address latency in communication a TI channel is assumed to allow low-latency in operations. The second part of the article discusses the proposed blockchain-based drone delivery scheme *GaRuDa* through operations of three layers, namely, the data dissemination layer, data communication layer, and the consumer layer. The third part discusses the open issues and challenges of deploying the proposed scheme in Healthcare *5.0* applications. Then, a recent case study of the traditional drone-delivery scheme over 4G communication is explored against the proposed 5G-enabled TI scheme. The experimental results demonstrate the efficacy of the proposed scheme compared to existing services in terms of computation, communication, and operational costs. In the future, to address the issues of low-latency and reliability of TI channels, successive interference cancellation (SIC) of non-orthogonal multiple access channels of communicating drones in a spatial coverage range will be explored in detail as well as blockchain's privacy and interoperability issues.

Acknowledgment

This publication is an outcome of the R&D work undertaken project under the Visvesvaraya PhD Scheme of Ministry of Electronics & Information Technology, Government of India, being implemented by Digital India Corporation (MEITY-PHD-2828).

References

[1] M. Gharibi, R. Boutaba, and S. L. Waslander, "Internet of Drones," *IEEE Access*, vol. 4, pp. 1148–1162, 2016.

[2] G. Choudhary, V. Sharma, and I. You, "Sustainable and secure trajectories for the military internet of drones (iod) through an efficient medium access control (mac) protocol," *Computers & Electrical Engineering*, vol. 74, pp. 59 – 73, 2019.

[3] M. Kowalkiewicz, "Health 5.0: the emergence of digital wellness." https://medium.com/qut-cde/health-5-0-the-emergence-of-digital-wellness-b21fdff635b9. Last Accessed: 2017.

[4] S. H. Alsamhi, O. Ma, M. S. Ansari, and F. A. Almalki, "Survey on collaborative smart drones and internet of things for improving smartness of smart cities," *IEEE Access*, vol. 7, pp. 128125–128152, 2019.

[5] I. Budhiraja, S. Tyagi, S. Tanwar, N. Kumar, and J. J. P. C. Rodrigues, "Diya: Tactile internet driven delay assessment noma-based scheme for d2d communication," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 12, pp. 6354–6366, 2019.

[6] N. Kabra, P. Bhattacharya, S. Tanwar, and S. Tyagi, "Mudrachain: Blockchain-based framework for automated cheque clearance in financial institutions," *Future Generation Computer Systems*, vol. 102, pp. 574 – 587, 2020.

[7] "Global blockchain in healthcare market: Focus on industry analysis and opportunity matrix - analysis and forecast, 2018-2025." https://bisresearch.com/industry-report/global-blockchain-in-healthcare-market-2025.html. Accessed: 2018.

[8] H. Ullah, N. Gopalakrishnan Nair, A. Moore, C. Nugent, P. Muschamp, and M. Cuevas, "5g communication: An overview of vehicle-to-everything, drones, and healthcare use-cases," *IEEE Access*, vol. 7, pp. 37251–37268, 2019.

[9] A. V. Savkin and H. Huang, "A method for optimized deployment of a network of surveillance aerial drones," *IEEE Systems Journal*, vol. 13, no. 4, pp. 4474–4477, 2019.

[10] M. S. Frontiers, "Innovating to reach remote tb patients and improve access to treatment." https://www.msf.org/papua-new-guinea-innovating-reach-remote-tb-patients-and-improve-access-treatment. Last Accessed: 2020.

[11] R. Gupta, S. Tanwar, S. Tyagi, and N. Kumar, "Tactile-internet-based telesurgery system for healthcare 4.0: An architecture, research challenges, and future directions," *IEEE Network*, vol. 33, no. 6, pp. 22–29, 2019.

[12] G. P. Fettweis, "The tactile internet: Applications and challenges," *IEEE Vehicular Technology Magazine*, vol. 9, no. 1, pp. 64–70, 2014.

[13] D. Vanderpool, "Hipaa compliance: A common sense approach," *Innovations in Clinical Neuroscience*, vol. 16, no. 1-2, p. 38, 2019.

[14] P. Mehta, R. Gupta, and S. Tanwar, "Blockchain envisioned uav networks: Challenges, solutions, and comparisons," *Computer Communications*, vol. 151, pp. 518 – 538, 2020.

[15] J. E. Scott and C. H. Scott, "Models for drone delivery of medications and other healthcare items," *Int. J. Healthc. Inf. Syst. Inform.*, vol. 13, p. 2034, July 2018.

Rajesh Gupta is a Full-Time Ph.D. Research Scholar in the Computer science and Engineering Department at Nirma University, Ahmedabad, India under the supervision of Dr. Sudeep Tanwar. He has authored/co-authored 21 publications (including 14 papers in SCI Indexed Journals and 07 papers in IEEE ComSoc sponsored International Conferences). His research interests includes blockchain technology and device-to-device communication.

Pronaya Bhattacharya is an Assistant Professor at Nirma University, India. He has authored/co-authored more than 30 publications including SCI Indexed Journals and IEEE ComSoc sponsored International Conferences). His research interests includes blockchain technology, edge computing, and software-defined networking.

Sudeep Tanwar is an Associate Professor at Nirma University, India and was visiting professor at Jan Wyzykowski University in Polkowice, Poland and University of Pitesti in Pitesti, Romania. He received his Ph.D. in computer science and engineering from Mewar University, India. His research interests includes WSN, blockchain technology, fog computing, and smart grid. He has authored/coauthored more than 150 research papers in leading journals and conferences of repute and has edited/authores 10 books published in leading publication houses like IET, Springer. He is an Associate Editor of IJCS and Security and Privacy Journal, Wiley.

Neeraj Kumar is working as a Professor at Thapar Institute of Engineering and Technology, Deemed to be University, India. He received his Ph.D. from SMVD University, India in CSE and was a postdoctoral research fellow at Coventry University, United Kingdom. He has more than 300 research papers in leading journals and conferences of repute. He is an Associate Editor/Technical Editor of IEEE Communication Magazine, IEEE Networks Magazine, IJCS- Wiley, JNCA-Elsevier, ComCom-Elsevier, Security and Privacy, Wiley, IEEE System Journal, and ACM Computing Surveys.

Mohsen Guizani is currently a Professor in the CSE Department at Qatar University. He is a fellow of IEEE and Senior Member of ACM. His research interests include wireless communications and mobile computing, computer networks, mobile cloud computing, security, and smart grid.