Blockchain-Envisioned Softwarized Multi-Swarming UAVs to Tackle COVID-I9 Situations

Rajesh Gupta, Aparna Kumari, Sudeep Tanwar, and Neeraj Kumar

Abstract

With the spread of novel coronavirus, global health concerns have increased as it has flattened the curve of mortality worldwide. To handle such a containment of disease, multi-swarm Unmanned Aerial Vehicles (UAVs) with 5G can be used to reduce human intervention with major benefits of high bandwidth, ultra-low-latency, and reliability. Multi-swarm UAVs sends a huge amount of data to ground stations with real-time connection density of 107/km^2, which is a bottleneck on 5G networks; data security is another issue in sharing sensitive data. Motivated by these issues, in this article, we propose a blockchain-envisioned softwarized multi-swarming UAV communication scheme based on a 6G network with intelligent connectivity, Terahertz (THz) frequency bands, and virtualization of link and physical-level protocols. Softwarization makes the communication infrastructure flexible, agile, and easily configurable, and the potential of blockchain supports data security. Results show that the proposed scheme performs better in terms of processing delay, packet loss reduction, and throughput compared to exiting 4G/5G-based systems.

Introduction

COVID-19, often known as coronavirus, attacks the human respiratory system generally with an age older than 65 years or younger than 10 years and was initially identified in Wuhan, China in December 2019. It has infected approximately 7.01 million people with approximately 402.7K deaths worldwide as of June 7, 2020. It is a global pandemic and affects the daily lives of almost all people [1]. As per the report presented by the World Health Organization (WHO), the symptoms are fatigue, cough, fever, headaches, and diarrhea, and around 70 percent of the population (worldwide) need to protect themselves against the COVID-19 pandemic by 2021. The virus affects exponentially from human to human through touch, cough, sneezing, and exhaling. Anyone can protect themselves from this pandemic by following the WHO guidelines which mention social distancing, regular hand washing, wearing masks, and boosting immunity. The governments of various countries have enforced full lockdowns, so that people cannot come in close contact with others, that is, *stay home stay safe*.

Various departments such as healthcare, municipal, and police are working 24/7 to protect and guide people about COVID-19's seriousness and consequences, so that they can follow the WHO guidelines, which helps to break the COVID-19 chain. The healthcare department monitors the symptoms of coronavirus, the municipal department takes care of sanitization to disinfect the infected area, and the police department resists public movement and monitors social distancing. Initially, manual procedures were followed by all departments to ensure their duties, but many concerned people were infected due to direct contact with COVID-19-infected people. Then, the world started looking for an air medium, which helps the organizations to perform their duties with minimal risk. UAVs can be used as a potential solution to perform day-to-day COVID-19 tasks such as monitoring social distancing, inspecting symptoms, making announcements, and sanitizing the infected areas.

Many countries across the globe have initiated the use of UAVs in a new way with strict guidelines such as maximum altitude and geographic location. The University of South Australia developed the *pandemic drone* to identify COVID-19 infectious people; Spain is using *agricultural* drones to sanitize the infected areas; Virginia is using UAVs to deliver food and medical samples; Spain is also using UAVs to enforce social distancing [2]. UAVs operate over the wireless communication channel and their efficiencies in terms of latency and throughput mainly depend upon the communication technology used, that is, 1G to 6G. Figure 1 shows the comparison of various wireless communication technologies used to operate UAVs. In this article, we considered the communication medium as 6G, which has a massive ultra-low latency (mURLLC, i.e., <100 μ s), user experienced data rate of 1 Gb/s, peak data rate of 1 Tb/s, connection density of 10^7 devices/Km^2, and mobility of 1000 Km/h.

This pandemic spreads all over the world and to keep track of all measures as mentioned above, a single UAV is not sufficient, so there is a need to use swarms of UAVs that can share information among themselves over the 6G communication channel. A single UAV swarming network can cover only one single geographic location. But to monitor multiple geographic locations simultaneously, there is a need for a multi-swarming UAV network. The network management of such a complex multi-swarming UAV network is tedious because of the complexity of the network infrastructure. To handle this, the softwarization technology called Software Defined Network (SDN) plays an important role. SDN aims to decouple the network control plane from the forwarding

Digital Object Identifier:
10.1109/MNET.011.2000439

Rajesh Gupta, Aparna Kumari, and Sudeep Tanwar are with Nirma University; Neeraj Kumar is with Thapar Institute of Engineering and Technology, Asia University, and King Abdul Aziz University.

0890-8044/21/$25.00 © 2021 IEEE

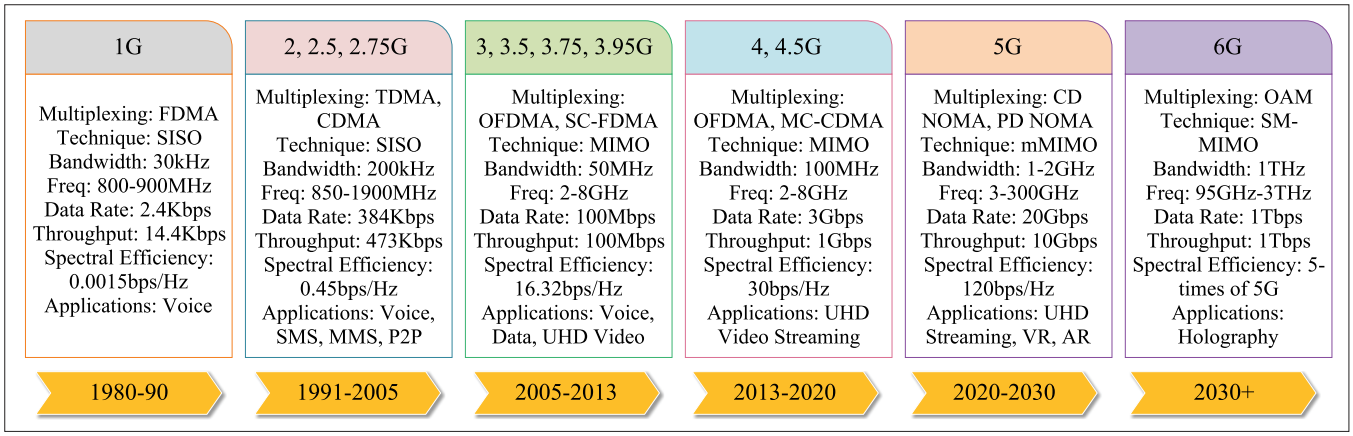


FIGURE 1. Evolution of communication systems to handle the COVID-19 pandemic.

function (data plane) by using open interfaces such as *OpenFlow* and *OpenDaylight*. SDN-based UAV communication improves the network flexibility and dynamism in UAV deployment for diverse applications. Despite the many benefits offered by SDN, a multi-swarming UAV network is vulnerable to various security threats, which is due to the open nature of communication channels, that is, 6G. The attacks would be spoofing, man-in-the-middle, data modification, denial-of-service, and distributed denial-of-service attacks.

To overcome the issues mentioned above, blockchain (BC) is a prominent solution, which is a distributed and immutable ledger that stores transactions in the blocks. Smart contracts (SC) eliminate the need for trusted third-party systems to perpetuate trust among the participating members. In this article, we present BC-envisioned softwarized multi-swarming UAVs to tackle COVID-19 pandemic situations and protection against various security threats.

Motivation

The motivation of the article is as follows:

- The importance of softwarization in multi-swarming UAV network in the COVID-19 pandemic is one of the prime criterias to enhance the security of various stakeholders such as governing bodies and patients. When the multi-swarming UAV network becomes softwarized, then its administration becomes effortless, flexible, agile, and dynamically configurable.
- Current research work is mostly dedicated to UAVs in COVID-19. Multi-swarming UAVs and security and management aspects of UAVs have not been explored to its full potential. Hence, there is a need to write an article with the integration of all aspects mentioned above.
- The proposed work benefits society by restraining the COVID-19 pandemic in real-time.

Research Contributions

Following are the major contributions of this article.

- We highlight the purpose of multi-swarming UAVs in the COVID-19 pandemic by highlighting its security, privacy, and management issues.
- A blockchain-enabled secure and softwarized multi-swarming UAV architecture is proposed to tackle the COVID-19 situations.
- The performance of proposed 6G-based scheme is evaluated over latency, throughput, and packet loss parameters.

Organization

The rest of the article is arranged as follows. The following sections describes the important concepts related to the theme of the article. We then describe the proposed architecture. Following that we highlight the various research challenges in the integration of softwarized UAVs and 6G through the proposed scheme. Then we present a case study on managing the lockdown implementation. Finally, we conclude the article.

Important Concepts: Benefits and Issues

This section describes the concepts related to the theme of the article.

COVID-19 Pandemic Awareness

The governing body spread awareness of the COVID-19 pandemic using UAVs, that is, monitoring social distancing, sanitizing affected areas, and monitoring people's health. UAVs can communicate with each other over the wireless communication channel for data exchange. UAVs mostly target those areas which are labeled as orange or red zones (the highly affected areas). UAVs monitor people's health and social distancing and also send a report to the ground stations, where it informs the sanitization UAV about the affected area for disinfection.

Monitoring Social Distancing: Social distancing is the prevention and control mechanism to avoid contact between people, which slows down COVID-19 transmission. Implementation of UAVs aims to ensure that people are maintaining a specified distance from each other. Here, the UAVs are equipped with an infrared/thermal image camera that locates humans and calculates the distance (Manhattan or Euclidean) between them and compare it with the threshold value. If distance is less than the threshold, then an automatic announcement can be made by the UAVs in regard to maintain social distancing.

Sanitizing Infected Areas: The sanitizing UAVs aim to disinfect the COVID-19 affected areas at regular intervals to minimize its spread. Sanitizing

UAVs receive the geographic location of infected areas from the other UAVs over the wireless communication channel. Therefore, the sanitization UAV locates and disinfects the area with accuracy and less depletion of disinfectant.

Health Monitoring: To monitor the people's health, specialized healthcare UAVs can be used to measure COVID-19 symptoms, that is, heart rate, blood pressure, and body temperature. If anyone is having any of the symptoms, then the related information can be forwarded to the healthcare department. Based on that, a person can be tracked and quarantined for a specific period of time.

COVID-19 Pandemic Related Announcements: To handle the outbreak of COVID-19, the government makes various announcements related to lockdowns, wearing a face mask, and closing of schools, colleges, and public facilities.

Multi-Swarming UAVs and Security Issues

A swarm of UAVs is a group of aerial vehicles that work together to achieve a particular goal. Each UAV in a swarm is driven by a precise number of rotors and has the capability of vertical take-off and landing. The swarms of drones can be categorized as fully and semi-autonomous swarms. It can also be envisioned as single-layered (UAV itself is the leader) and multi-layered swarms having a dedicated leader UAV at each layer [3]. It comprises heterogeneous UAVs moving in a self-governing as well as coordinated way. It relies on local decisions from heterogeneous and distributed entities embryonic in different swarms. The highly dynamic network of multi-swarm UAV systems requires efficient mobility behaviors and optimized ad-hoc communications among the swarms.

Security Issues in Multi-Swarming UAVs: Multi-swarm UAVs are self-governing, which makes it compulsory to preserve its wireless communication channel against various types of security attacks. The communication channel has many security issues due to highly mobile multi-swarm UAVs engaged in a dynamic environment [4]. The probable security attacks are as follows.

Hijacking Attack: Aims to take complete control of UAVs and modify the stored instructions. For example, during suspicious activity by the attacker, the UAV camera is turned off.

GPS Spoofing Attack: The attackers aim to bind the multi-swarm UAVs with false time and location data. Here, a malicious node transmits the counterfeit GPS signals to the victim node, not interfering with the current operation [5].

DDoS/DoS and Jamming Attack: Aims to interrupt the communication channel through interference, data packet flooding, extensive external noise, or collision of data. This is one of the most accessible attacks as it does not need any in-depth knowledge of the victim's system.

Man-in-the-Middle Attack: In this attack, an attacker overhears the UAV communication and manipulates it by generating false commands to the ground control station.

Traffic Analysis: Here, the attacker passively listens to the communication between the UAVs over the susceptible communication channels.

Hence, UAV communication needs to be secure against various security attacks, which can be done using softwarization technique like SDN, which is discussed in the next subsection. Nevertheless, softwarization techniques are compute extensive that requires powerful UAVs with long battery power. To handle such issues, BC is a feasible solution to be incorporated with softwarized multi-swarm UAVs that we will discuss in a subsequent section.

Softwarization: Techniques and Concepts

There are several softwarization technologies such as SDN and NFV for effective network management, which makes the network agile, flexible, and easily configurable in a multi-swarm UAV platform [6]. It centralizes the intelligence, management, and configuration of network devices such as switches and routers in a software-defined controller to make dynamic decisions. In a traditional network, the packet flow is destination-based, whereas in SDN, the packet movement from source to destination is flow-based. It is well-equipped for adaptive, error-free, cost-effective, and high-bandwidth applications [7]. The SDN architecture is fully programmable, responsive, agile, vendor-neutral, and centrally managed, which consists of three abstraction planes: application, control, and data planes. A brief discussion of these layers follows.

Data Plane: This layer comprises physical hardware devices such as access points, switches, and routers to transmit user data packets from source to destination based on the flow table (stores the route information). If the route entry is not found in the flow table, then the request is sent back to the controller for further directions. The policies executed on the data plane are dependent on the network devices, which can be either dislocated or collocated [8]. The functionalities of dislocated devices are controlled by the central entity, whereas the collocated devices can self-manage the functions without the involvement of any external entity.

Control Plane: This layer manages the entire network infrastructure and creates the data packet forwarding rules. It makes all decisions such as switching, routing, access control, and load balancing intelligently. Here, each control entity is an abstract view of the entire network, which streamlines its control logic implementation [9].

Application Plane: This layer associates the SDN controller through the northbound interface. The global abstract view of the entire network infrastructure can be retrieved by means of the SDN/business/network applications at this layer for decision-making [9]. It leverages several SDN applications, for instance, rescue operations, military operations, healthcare 4.0, and many more with available network resources.

Nevertheless, SDN empowers many benefits related to the network management, data flow, and device discovery, but raises many security vulnerabilities, such as DDoS, replay, duplicacy, and authentication attacks. Several research works have been done in this direction, such as Lam *et al.*, [10] offered an identity-based cryptography approach for secure data plane communication of SDN. Varadharajan *et al.* [11] presented an access control approach for policy-based SDN architecture. This approach imple-

Blockchain characteristics	Description	Potential applications in the COVID-19 pandemic
Decentralization	It is a distributed ledger and shared among all participants of the BC network.	Eliminates the need for trusted third-party systems in a BC-enabled multi-swarming UAV network as well as the complex encryption-decryption primitives to secure monitoring, inspection, and sanitization data. It is not having a single point failure, which ensures the availability of UAV networks in the COVID-19 pandemic.
Immutability	It does not allow any modification of data once it is stored in the BC.	In the Covid-19 pandemic, this BC characteristic does not allow any participant (doctors or COVID-19 affected patients) to modify the recorded health information, i.e., fever, heart rate, and cough.
Transparency	Transactional data is publicly available among all BC network participants.	COVID-19 data can be viewed by all concerned bodies such as police, doctors, municipal corporations, and government bodies instantly without fail, so they can make appropriate decisions to control the COVID-19 pandemic.
Security and privacy	BC uses cryptographic techniques and access control mechanisms to ensure BC data security and privacy.	BC offers high security for COVID-19 data captured through a multi-swarming UAV network. Due to its distributed property, the same data is encrypted and distributed among all the participants, so it is difficult for a malicious user to update all instances of the data.
Trust	BC ensures the trust of data which is distributed among the participants.	BC ensures the trust among the participants of COVID-19 BC for the data captured using UAVs.
Traceability	BC stores the transaction without allowing any kind of modification in it along with the timestamp and hash of the transaction.	In the COVID-19 pandemic, traceability plays an important role in identifying people who come in contact with a corona-positive patient.

TABLE 1. Characteristics of blockchain and their potential to COVID-19 pandemic [14].

ments the flow-based and path-based security policies to secure SDN architecture compare to the OpenSec framework. Later, Guerber *et al*. in [12] proposed to handle the wormhole, DDoS, and blackhole attacks. Despite the benefits of SDN, multi-swarm UAV communication security is a big challenge, and BC technology is a feasible solution to handle the above-mentioned issues. The next section presents an in-depth discussion of BC technology.

Blockchain: Security and Privacy Aspects

The emergent technology BC is a secure distributed ledger that shares any information in real time between significant participating nodes, that is, it shares the copy of the ledger with each participating node [13]. It has various characteristics such as transparency, trust, security, privacy, and immutability. The BC safeguards data security and privacy using cryptography primitives, where every single participant uses their digital signature to validate the transaction. Thus, the cryptographic primitives secure the participant's identity and data immutability as well using SC. The digital agreement established between two parties in the BC network is known as a SC, which is self-executed and enforceable.

In the COVID-19 pandemic, BC could connect the WHO, the health ministry of every country worldwide, and nodal hospitals to share real-time data and information related to new communicable diseases. This might have alerted the world much earlier and might have led to travel restrictions, social distancing, and quarantining policies much earlier to resist the spread of COVID-19. The BC has major benefits with regard to the COVID-19 pandemic as shown in Table 1. The COVID-19 pandemic has never been seen before, so the reporting infrastructure for this needs to be improved to handle similar pandemics in the future. Here, the BC is an enabler to ensure the efficiency and security of sensitive data. But again, it depends on the goodwill of governments and people working in the pandemic.

The Proposed Architecture

This section describes the working of the proposed scheme, that is, a BC-envisioned softwarized multi-swarming UAV scheme to tackle COVID-19 pandemic situations. Many authors across the globe are working to eliminate the COVID-19 pandemic using UAVs to save the lives of their human observers. The authors in [15] proposed to overcome the pandemic situation using different technologies, but they presented only a review article without any performance analysis. Companies are also contributing, but they are using traditional communication channels, that is, 4G, LTE-A, and 5G, which are having latency and connection density issues. To overcome such issues, the proposed system uses 6G as a communication medium. The proposed system is conceptually bifurcated into five connected layers, i.e., data (COVID-19), virtualization, network control plane, application layer, and BC layer, as shown in Fig. 2. A detailed description of these layers follows.

Application Layer

This layer initiates and forwards the network function requirements to the SDN controller over the northbound interface. It consists of physical entities such as police stations, healthcare, and municipal offices, which control the application-specific (monitoring, inspecting, and sanitizing) UAVs at the COVID-19 layer using software programs. The police department controls the monitoring UAV, whereas healthcare and municipal departments control the inspection and sanitization UAVs, respectively. This layer collects the multi-swarming UAV network statistics from the network control layer for optimized and efficient decision making via ethereum BC.

Network Control Plane

This layer is called the brain of the multi-swarming UAV network, where all network control decisions can be taken. It is logically decoupled from

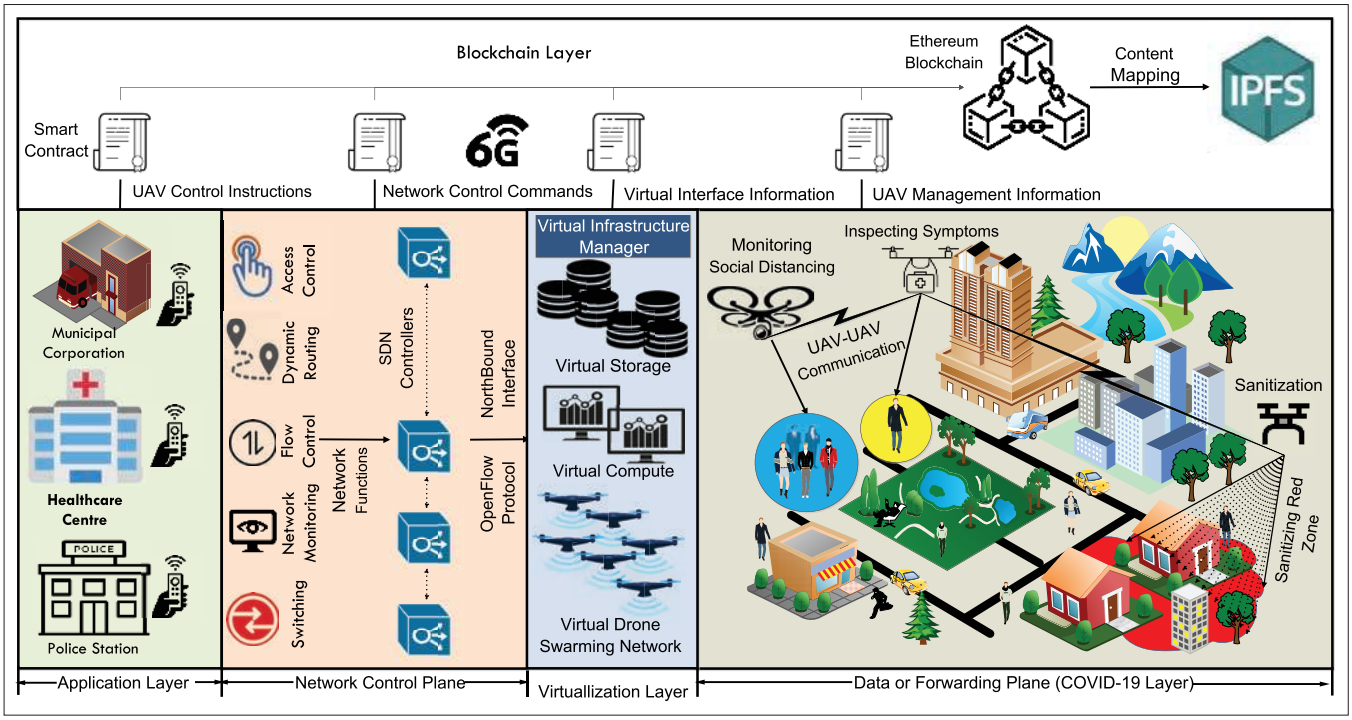


FIGURE 2. Blockchain-envisioned softwarized multi-swarming UAV scheme to manage the COVID-19 pandemic.

the data plane with the benefit of providing an abstract prospect of the entire multi-swarming UAV network to the software applications at the application layer and the efficient management of the UAV network. This layer comprises the various network functions (such as access control, dynamic routing, flow control, network monitoring, and switching) and the SDN controllers. The controller captures the network statistics and prepares a flow table for the data traveling from source to destination and passes it to the data plane via the open source southbound and OpenFlow protocol. Each SDN controller manages the application-specific UAV-swarming network. The number of SDN controllers increases the scalability of the applications of a multi-swarming UAV network. All control related information is passed to the application layer and data plane via the BC network.

Virtualization Layer

This layer virtualizes the network control functions as well as the network devices through NFV. Based on that, it is bifurcated into function virtualization and device virtualization. Function virtualization is the virtualization of all network node functions, whereas device virtualization is the virtualization of network nodes such as switches and routers in the COVID-19 layer using logical abstraction. The virtual infrastructure manager at the virtualization layer takes care of the resource and network virtualization.

Forwarding Plane or COVID-19 Layer

This layer is also known as the infrastructure layer, which comprises physical network hardware devices such as network switches, routers, and multi-swarming UAVs. In reality, there are *m*-number of UAVs operating in the sky to tackle COVID-19 operated by different organizations in the form of multi-swarming, as shown in Fig. 3. UAVs can do the following tasks:

- Monitor social distancing norms that people follow to break the corona chain.
- Inspect COVID-19 symptoms such as fever, heart-rate, and cough of people while on the go.
- Sanitize COVID-19 infected area efficiently.
- Make regular announcements related to the policies, rules, and regulations of COVID-19.

UAVs are under the control of operating bodies at the application layer of the proposed scheme. All UAVs are communicating with each other and pass the information to the relevant UAV. For example, when monitoring UAVs identify that people are not following social distancing norms, the information is passed to the announcement UAV for announcements related to the same.

Many areas/locations are infected by the COVID-19 pandemic, so operating and controlling organizations need to disinfect, make announcements, monitor, and inspect all those areas. It requires extensive hardware purchases and installation, which is quite costly and time-consuming. To overcome this, the virtualization layer helps to create virtual instances of the network resources and devices that save cost and time. This makes a multi-swarming UAV swarming network feasible and cost-effective.

Blockchain Layer

BC is a distributed, decentralized, and immutable ledger, which acts as a security layer between all four layers of the proposed scheme. Here, we have considered ethereum (public) BC to store the data and information of all the layers. Data is stored in a BC only if it satisfies the smart contract conditions. To maintain the integrity and reliability of data stored in the BC network, the proposed system uses the proof-of-work (PoW) consensus mechanism, where a transaction is added to the block only if all stakeholders agree. The PoW consensus mechanism resolves the conflicts among

the various stakeholders of the system. The application layer stores the UAV control information, that is, UAV movement through remote control in the BC network. The network control layer keeps the network devices and functions control commands in the BC network. The virtualization layer stores the information about the available virtual instances for the network, storage, and compute in the BC network, whereas the COVID-19 layer stores the information like a person's inspection details (i.e., fever, heart-rate, and cough), sanitization details (area to sanitize), and UAV swarming communication. All layers communicate with the BC via an ethereum client. The benefits of using BC in a softwarized multi-swarming UAV network are data immutability, traceability, transparency, data reliability, security, and privacy.

The data storage cost in ethereum is extremely high, that is, approximately $530 for 1MB of data. To overcome the data storage cost issues, the proposed system has used the Interplanetary File System (IPFS) data storage, which is free of cost, distributed, and immutable. IPFS generates a unique hash value (i.e., <<< 1MB), and stores it in the ethereum block, which accommodates more transactions in a single block.

Research Challenges

Figure 4 highlights some of the major open issues and research challenges for future viewpoints on COVID-19. A description of each follows.

Health Hazards: 6G provides remarkably high-speed communication through high data rate (in terabytes) over the THz waves that are hazardous for human skin tissue and eyes, which is a critical task to handle in the COVID-19 scenario.

Energy Management: Multi-Swarm UAVs are lightweight flying devices and battery-operated with limited lifetime. UAVs and 6G infrastructure generate huge amounts of COVID-19 data at specific intervals. Hence, processing of such a huge amount of data in a Multi-Swarm UAV environment requires high computation power.

Security: Multi-Swarm UAVs are capable of over the wireless channel that may be attacked by any malevolent node. A malevolent user can either hijack the UAV or change the entire path of the UAV. Hence, the security aspect of multi-swarm UAVs is of extreme importance in a critical scenario such as the COVID-19 outbreak.

User Data Privacy: In a multi-swarm UAV-based environment, user data privacy is of utmost importance as an attacker can misuse the private data of users collected during the monitoring of COVID-19. This can be accomplished using various cryptographic algorithms (e.g., message digest algorithms and SHA-256).

Ecological Conditions: The existing ecological conditions pose a challenge to change the predetermined path for a destination in which multi-swarm UAV is operating, which causes mission failures during the pandemic.

High Operational and Maintenance cost: The intelligent network of multi-swarm UAVs based on 6G communication channels is equipped with AI algorithms to improve its quality of service (QoS), quality of experience (QoE), and its performance. Here, distinct QoS is mapped to the network intelligently with QoE and results in an increased cost of COVID-19.

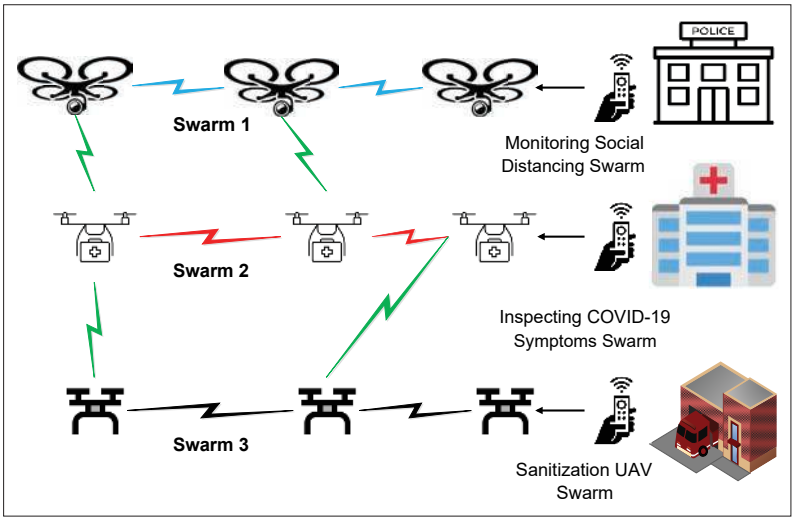


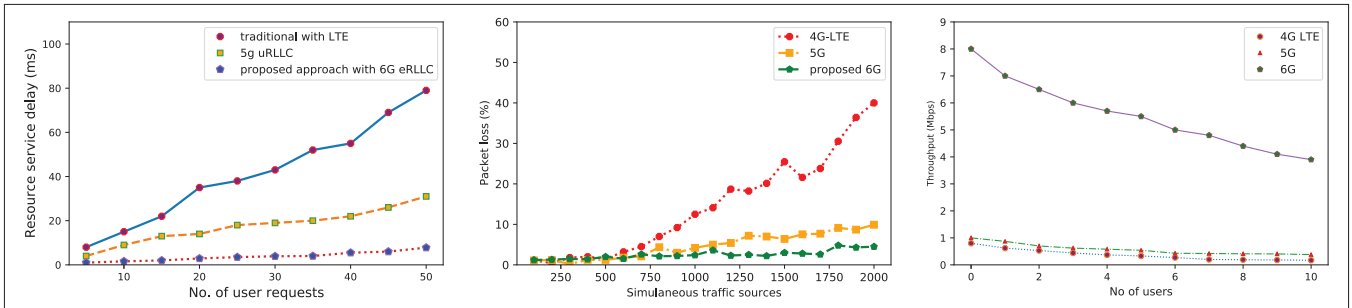
FIGURE 3. Multi-swarming scenario to tackle COVID-19.

FIGURE 4. Research challenges.

Blockchain-Based Spectrum Band Prejudice: 6G operates in a 3.5 GHz spectrum band, which allows users to share the band for their application requirements. Nevertheless, the accessibility of the band can be monopolized by auction-based strategies to benefit a specific group of users, affect other authentic users, and raises concerns in the COVID-19 outbreak.

Managing the Lockdown Implementation: A Case Study

As the world continues to handle the ongoing COVID-19 outbreak, UAVs have the capability to play a major role in fighting the coronavirus. UAV startups in areound the world are working in conjunction with government authorities to provide services such as delivering medical supplies, managing crowds, and disinfecting contaminated regions. Though government personnel have been arranged to check temperatures of each individual personally, the personnel leading the check are at an equal risk of getting infected by the virus. To avoid such a situation, UAVs can be used to measure body temperature, which is loaded with airborne infrared cameras. The results show that the camera can get an accurate reading. The standardized UAV camera can be



(a) Analysis of communication latencies in resource service.

(b) Analysis of packet loss of 6G over 4G and 5G.

(c) Analysis of throughput of 6G over 4G and 5G.

FIGURE 5. Benefits of deploying 6G in multi-swarming UAV network over 4G and 5G communication channels.

used to measure body temperatures, keeping the officer at a safe distance; however, this solution needs to be reverified with manual methods.

Further, to manage the lockdown, the administration uses UAVs to monitor the movements of people. In another application, Delhi police have deployed UAVs to ensure social distancing in Azadpur mandi, Asia's largest fruit and vegetable market, by capturing people's movements. Then, municipal administration authorities are using UAVs to disinfect the infected areas by spraying disinfectants. Lastly, government authorities have found UAVs as a friend in these tough times of a "touch-me-not" environment to manage the COVID-19 outbreak.

Performance Evaluation

Figure 5 shows the performance evaluation of the proposed BC-based softwarized multi-swarm UAV scheme compared to conventional approaches in terms of various parameters such as latency, packet loss, and throughput. Figure 5a shows a plot depicting the latency in the proposed scheme using a 6G communication channel and compares it with the traditional LTE-based approach and 5G uRLLC. With the increasing number of users, service delay (ms) in the allocation of resources is reasonably low in the case of the proposed scheme. Figure 5b shows the graph of packet loss concerning the simultaneous traffic sources. Here, packet loss is quite low in the case of a 6G-based proposed scheme. Figure 5c shows the system throughput when the number of users increases, which is relatively high compared to the other conventional approaches.

Conclusion

In this article, we propose a BC-envisioned softwarized multi-swarming UAV scheme based on a 6G network to discuss the challenges of the COVID-19 outbreak. First, we highlight the challenges of COVID-19, such as social distancing, health monitoring, and sanitization of infected regions. To reduce human intervention, multi-swarm UAVs need to be deployed over a 6G-network. This enabled UAVs to communicate with each other through a directed short-range communication channel in the infected region and share real-time data of resident locations with high precision (i.e., geo-location coordinates). Then, SDN infrastructure makes communication network flexible, agile, and easily configurable, and the collected data is stored on a BC-based IPFS system with high security. The decentralized architecture of BC makes these real-time data accessible from anywhere at any time. Then, research challenges and open issues in the deployment of the proposed scheme are discussed. In the future, the scalability of the proposed scheme along with the contact tracing of potentially affected persons will be explored with immutability, trust, traceability of transactions without compromising the throughput of the system.

References

[1] R. Y. Kim, "The Impact of Covid-19 on Consumers: Preparing for Digital Sales," *IEEE Engineering Management Review*, 2020, pp. 1–1.

[2] T. Mondal and M. Madhur, "Keep an Eye on Covid-19 Drone Use Cases for Future Business Opportunities," https://www.hfsresearch.com/pointsofview/Keep-an-eye-on-COVID- 19-drone-use-cases-for-future-business-opportunities, accessed: May 2020.

[3] A. Tahir *et al.*, "Swarms of Unmanned Aerial Vehicles: A Survey," *J. Industrial Information Integration*, vol. 16, 2019, pp. 100–06.

[4] L. Gupta, R. Jain, and G. Vaszkun, "Survey of Important Issues in UAV Communication Networks," *IEEE Commun. Surveys Tutorials*, vol. 18, no. 2, 2016, pp. 1123–52.

[5] P. Mehta, R. Gupta, and S. Tanwar, "Blockchain Envisioned UAV Networks: Challenges, Solutions, and Comparisons," *Computer Commun.*, vol. 151, 2020, pp. 518–38.

[6] R. Chaudhary and N. Kumar, "LOADS: Load Optimization and Anomaly Detection Scheme for Software-Defined Networks," *IEEE Trans. Vehicular Technology*, vol. 68, no. 12, 2019, pp. 12329–44.

[7] C. Rametta and G. Schembra, "Designing a Softwarized Network Deployed on a Fleet of Drones for Rural Zone Monitoring," *Future Internet*, vol. 9, no. 1, 2017, pp. 1–21.

[8] Cisco, "Software defined networking," https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/DataCenter/VMDC/SDN/SDN.html, accessed: May 2013.

[9] A. H. Shamsan and A. R. Faridi, "Network Softwarization for IoT: A Survey," *Proc. 2019 6th Int'l. Conf. Computing for Sustainable Global Development (INDIACom)*, New Delhi, India, 2019, pp. 1163–68.

[10] J. H. Lam *et al.*, "Securing SDN Southbound and Data Plane Communication with IBC," *Mobile Information Systems*, vol. 2016, 2016, pp. 1–12.

[11] V. Varadharajan *et al.*, "A Policy-Based Security Architecture for Software-Defined Networks," *IEEE Trans. Information Forensics and Security*, vol. 14, no. 4, 2019, pp. 897–912.

[12] C. Guerber, N. Larrieu, and M. ROYER, "Software Defined Network Based Architecture to Improve Security in a Swarm of Drones," *Proc. 2019 Int'l. Conf. Unmanned Aircraft Systems (ICUAS)*, Atlanta, GA, USA, 2019, pp. 51–60.

[13] S. K. Singh *et al.*, "Smart Contract-Based Pool Hopping Attack Prevention for Blockchain Networks," *Symmetry*, vol. 11, no. 7, 2019, pp. 1–19.

[14] D. C. Nguyen *et al.*, "Blockchain for 5G and Beyond Networks: A State of the Art Survey," *J. Network and Computer Applications*, vol. 166, 2020, pp. 1–38.

[15] V. Chamola *et al.*, "A Comprehensive Review of the Covid-19 Pandemic and the Role of IoT, Drones, AI, Blockchain, and 5G in Managing Its Impact," *IEEE Access*, vol. 8, 2020, pp. 90225–65.

Biographies

Rajesh Gupta (18ftvphde31@nirmauni.ac.in) is currently a full-time research scholar with the Department of Computer Science and Engineering, Institute of Technology, Nirma University, Ahmedabad, India, supervised by Sudeep Tanwar. His research interests includes blockchain technology, healthcare, and device-to-device communication for 5G.

Aparna Kumari (17ftphde22@nirmauni.ac.in) is currently a full-time research scholar with the Department of Computer Science and Engineering, Institute of Technology, Nirma University, Ahmedabad, India, supervised by Sudeep Tanwar. Her research interests includes blockchain technology, big data analytics, and smart grid.

Sudeep Tanwar (sudeep.tanwar@nirmauni.ac.in) is an associate professor with the Department of Computer Science and Engineering, Nirma University. He received his Ph.D. in computer science and engineering from Mewar University, India. His research interests include blockchain technology, computational aspects of smart grid, and fog computing. He has authored more than 130 research papers in leading journals and conferences and 10 books. He is an associate editor of IJCS and SPY journals of Wiley.

Neeraj Kumar (neeraj.kumar@thapar.edu) is working as a professor at Thapar Institute of Engineering and Technology, Patiala, India. He received his Ph.D. from SMVD University, India, in computer science and engineering and was a postdoctoral research fellow at Coventry University, United Kingdom. He has more than 400 research papers in leading journals and conferences of repute. He is an associate editor/technical editor of *IEEE Communications Magazine*, *IEEE Transactions on Sustainable Computing*, IJCS (Wiley), JNCA (Elsevier), *Elsevier Computer Communications*, and the *Security and Communications Journal*.