Exploiting 5G and Blockchain for Medical Applications of Drones

Junxin Chen, Wei Wang, Yicong Zhou, Syed Hassan Ahmed, and Wei Wei

Abstract

In recent years, there has been growing popularity of applying drones for medical services. Such applications always involve flying safety, data transmission, and personal privacy; therefore, reliable communication and enhanced information security should be addressed first. The 5G cellular network and blockchain technology emerge as promising candidates for solving these problems. This article first categorizes the medical applications of drones, and then presents some key challenges in these applications. Then we give preliminaries of 5G and blockchain, and explore their intrinsic characteristics to provide reliable communication and enhanced information security. In the scenario of disaster relief, an illustrative example is presented and discussed. Analytical results demonstrate the great potential of using 5G and blockchain for promoting the medical applications of drones.

Introduction

A drone, also known as an unmanned aerial vehicle (UAV), always refers to an aerial vehicle without a human pilot. It is controlled by a remote end through a wireless link. Such a technology was originally developed for military purpose 100 years ago, dating back to the first World War [1]. In comparison with ground transportation or manned aerial devices, drones own distinct advantages when used for dangerous, high-altitude, traffic-inconvenient, and quick-response tasks. Nowadays, drones have been comprehensively exploited for goods transportation, remote sensing, agricultural monitoring, disaster relief, and so on.

The advances in drones are also revolutionizing the medical field and enriching healthcare delivery modes. Drones enable fast and quick-response medical services to patients who suffer from long distance and traffic inconvenience. A famous project is the blood delivery service in Rwanda, which is launched for conveying blood packets from a distribution center to 21 hospitals that are within 75 km [2]. This project has been saving lives since 2016, and will be extended to more countries worldwide. In addition, drones are also being explored for telemedicine [3], public health monitoring [4], and emergency rescue [5]. Nowadays, the medical use of drones is booming. It is estimated by Global Market Insights that the medical drones market will grow from $88 million in 2018 to over $399 million by 2025 [6].

Reliable communication and enhanced information security are key issues for promoting the medical applications of drones. The communication link should have advantages in terms of high data rate, low latency, high scalability, and low energy cost. These properties are basic requirements for medical applications, especially for those with strict latency requirements such as tele-surgery. In addition, since medical applications always involve patients' private information, the communication link as well as the data records are required to be highly immune against malicious attacks. The security indicators, including confidentiality, integrity, availability, authentication, and so on, are also urgent challenges.

The emerging 5G and blockchain technologies are promising fits to address these problems. 5G enables reliable wireless communication, while blockchain can address the security and privacy concerns. Compared with its predecessors, 5G has distinct advantages in terms of higher data rate (10 Gb/s), low latency (1 ms), and so on. The flying command, with strict latency requirement as well as high-resolution images needing a higher data rate, can be reliably transmitted in the 5G age [7]. Nevertheless, current cellular networks including 4G and 5G are vulnerable against various malicious attacks, and consequently incapable of providing satisfactory information security to drone applications. In this scenario, blockchain technology shows great capabilities. The intrinsic features of blockchain such as immutability, decentralization, and anonymity can be exploited to ensure that the information sent and received is secured and trusted [8].

Although there are individual discussions about applying drones in the medical field or integrating blockchain for security enhancement, there are few articles combining them. This is the primary motivation of this article, which aims to comprehensively exploit 5G and blockchain for promoting medical applications of drones. The next section first reviews the drones' applications in the medical field; then the technical challenges in terms of reliable communication and information security are summarized. Following that, we introduce preliminaries of 5G and blockchain, whose characteristics are subsequently exploited for addressing the communication and security concerns. Finally, an example in the scenario of disaster relief is demonstrated and discussed.

Medical Applications of Drones

Currently, there is increasing popularity of using drones for medical missions, some of which are depicted in Fig. 1. Throughout the literature, med-

Junxin Chen is with the College of Medicine and Biological Information Engineering, Northeastern University; China; Wei Wang (corresponding author) is with the School of Intelligent Systems Engineering, Sun Yat-sen University; Yicong Zhou is with the University of Macau; Syed Hassan Ahmed was with Georgia Southern University; Wei Wei is with Xi'an University of Technology.

Digital Object Identifier:
10.1109/MNET.011.2000144

0890-8044/21/$25.00 © 2021 IEEE

ical applications of drones can be divided into three broad categories.

Medical Transportation Service

Similar to conveying commercial things by Amazon, drones are straightforwardly applicable for delivering medical supplies, especially suitable for emergency scenarios and geographically challenging situations. Such an application can be first traced in 2007, and has been frequently adopted in some serious disasters such as the 2010 earthquake in Haiti and the 2015 earthquake in Nepal. A more famous case is the blood delivering service in Rwanda, which has been provided by Zipline since 2016 [2]. Using a fixed-wing drone, called Zips, blood packs are flown from a distribution center to 21 hospitals located within 75 km. Generally, the blood packs can reach the destination within 30 minutes. Such efficiency cannot be achieved by other carriers due to the weather conditions and traffic infrastructure in Rwanda. Currently, Zipline's medical transportation service has covered all of Rwanda, and is being extended to Ghana, India, and Tanzania.

In critical scenarios, timely accessing emergency medicine is fatally important for sustaining life. Medical drones can facilitate the delivery process [3], benefiting from their intrinsic high flexibility and maneuverability. Delft University in the Netherlands has investigated delivering automated external defibrillators (AEDs) to individuals who are in cardiac arrest. Within a 1.2 mi^2 radius, drones were found to be able to complete an AED delivery task in less than 2 minutes [3], thus improving survival possibility. In addition, uses of drones for delivering vaccines, human organs, microbiology, resuscitation equipment, and injured soldiers have also been reported [1–3].

Drone-Aided Telemedicine Service

Different from delivering medical things, the telemedicine discussed always refers to scenarios where drones are armed with certain indispensable equipment/capability in addition to medical kits. Multimedia guidance or online instruction may be integrated into such applications. Telemedicine has been considered as one of the most promising drone applications [3]. The Health Integrated Rescue Operations project [9] is a typical case, where a drone-based working prototype was configured for emergency response in rural areas. Drones equipped with diagnostic devices and easy-to-use lifesaving treatments quickly arrived at the emergency site and then called a remote physician for instructions and medical treatment [9].

Another type of telemedicine application uses drones as part of a wireless infrastructure. For the first time, Harnett *et al.* employed a drone as a wireless communication provider for remote tele-surgery [10]. With the wireless link established by a drone, two surgeons, located remotely from the patient, were able to perform surgical procedures using a robot. This indicated that drones were suitable for providing highly portable, quickly deployable, and low-latency wireless link for remote diagnosis.

Public Healthcare Surveillance and Rescue

Applying drones for surveillance historically existed in the military field, and currently, it is being popularly extended for a wide range of public healthcare services. In 2013, typhoon Haiyon struck the Philippines and brought about serious damage. The Huginn X1 drone, equipped with two cameras, provided significant aerial surveillance, assisting effective disaster relief and response. For eliminating malaria, drones have been exploited to identify mosquito habitats through video/photo surveillance. Compared to the ground teams, Hardy *et al.* showed that drones provided a high-efficiency, flexible, and low-cost solution for mapping water bodies and further helping to eradicate mosquito vector-borne disease [4].

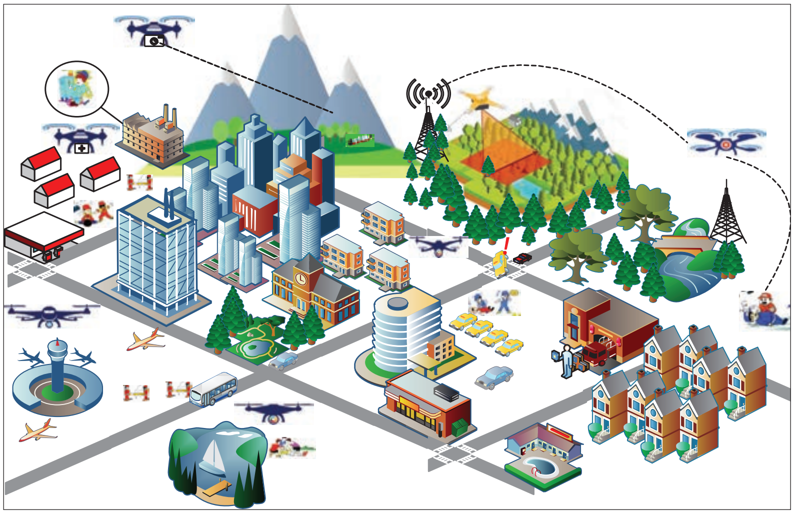

FIGURE 1. Medical applications of drones.

In rescue applications, some Swedish researchers have studied using drones for identifying drowning victims [5]. From the start to locating the simulated manikin, the drone spent a medium time of 0.47 min. On the other hand, 4.34 min were taken by the ground search party. An average of 3.37 min has been saved in the positioning process, which is clinically important for the subsequent rescue treatment such as cardiopulmonary resuscitation. In wider area search and secure missions, drones can obviously locate the victim faster and then arrive earlier with rescue equipment or medicine.

Communication and Security Challenges

It is undisputed that drones will have wider applications in medicine. Nevertheless, there are many challenges to be addressed. These factors can be identified in the communication and security aspects.

Communication Issues

Some communication challenges in the medical applications of drones are listed in Table 1 and described as follows.

Data Rate: In many of the drone-aided medical applications, real-time and large-volume data transmission is required. Taking tele-surgery as an example, the remote surgeon has to clearly watch the operating room; hence, real-time and high-resolution video transmission should be guaranteed. When this surgery connects several remote physicians (i.e., teleconsulting exists), the data rate needs to be doubled or redoubled. Similarly, real-time wireless transmission is also required

Challenges	Applications	Negtive effects
Data rate	Tele-surgery	The remote surgeon may lose the surgery scene, and the surgery may be suspended
	Emergency rescue	Few pictures are transmitted, and the efficiency is thus decreased
Latency	Every drone flying applications	Control of the drones could be lost, causing crashes and further damage to other assets and human lives
	Tele-surgery	Incorrect surgical operation may be caused and further threaten the patient's life
	Surveillance applications	Choppy animation of the monitor
Scalability	Emergency remote diagnosis	Extra time is required for the drone to access the patient's monitoring devices, thereby delaying timely treatment
Energy cost	Applications including self-sustainable sensors	Reduce the sensors' lifespan and hence decrease the healthy monitoring duration

TABLE 1. Some communication challenges when applying drones for medical applications.

in other drone-based surveillance applications. The rescue drone has to transmit high-resolution pictures of the shallow [5] to remote analysts; insufficient data rate will severely decrease the rescue efficiency. Speeding up data transmission is a fundamental factor for promoting the medical applications of drones.

Latency: Roughly speaking, latency refers to the information (e.g., camera data or flying command for drones) delivery time from the sender to the destination. Medical applications of drones generally have rigorous latency requirements. Latency is critical for operating drones in a safe and controlled mode; high latency of piloting command may bring about a series of casualties. It is also a basic requirement for interactive applications such as drone-aided remote surgery [11], where the remote surgeon's operation accuracy and thus the patient's safety are weak against the wireless link's delay. For surveillance applications, the captured pictures of flying drones should be transmitted within a delay of 3 ms [12], which cannot be ensured by current cellular networks whose latency is about 10 ms.

Scalability, Power Consumption, and So On: In recent years, progress of wearable devices and the Internet of Things (IoT) has significantly facilitated the monitoring of healthcare parameters. These devices and their gathered data records are also required during drone-aided medical applications. The network infrastructure is thus required to be scalable to seamlessly integrate a massive number of devices without interfering with ongoing operation. In addition, it has been proven that wireless communication is the primary energy consumer of self-sustainable sensors. Therefore, reducing the communication energy cost can prolong the sensor's lifespan and provide more support to the applications. In the literature, impacts of the networking capacity, massive devices support, and other issues are also discussed [13].

Security Issues

In addition to the requirement of reliable communication, a massive amount of security issues also need to be addressed prior to the deployment of medical applications of drones. They are important requirements in medical applications as strictly required by the Health Insurance Portability and Accountability Act (HIPAA). HIPAA was established by the U.S. Department of Health and Human Services to develop regulations for protecting the security and privacy of medical information.

Confidentiality: Confidentiality refers to the property that sensitive information is prevented from being exposed to unauthorized entities. It is a basic requirement of HIPAA. The data records produced in medical applications always involve patients' privacy, and leakage or misuse of these records may cause severe interference to the owners and may even threaten their lives. From both the legal and moral perspectives, any information in medical applications should be securely used, transmitted, and stored. Generally, data encryption methods such as Data Encryption Standard (DES) and Advanced Encryption Standard (AES) can be applied.

Availability: As the name suggests, the data has to be available to the users and applications anytime they need it. This property is a basic requirement of any information system to serve its duty. Reliability, accessibility, and timeliness are often adopted to depict the primary features of availability. Ensuring data availability requests the systems being secure against distributed denial of service (DDoS) attack, which is typically performed by flooding the target machine. In addition, a highly available system also has to prevent other service loss in terms of power supply, hardware failure, and so on. Obviously, medical applications require strict availability due to the intrinsic emergency property.

Integrity: Together with the aforementioned confidentiality and availability, integrity is the third fundamental component of information security. Different from availability, data integrity refers to the trustworthiness of the received data, since any unauthorized modification should be assumed malicious. It refers to the overall accuracy, reliability, and completeness of data. Specifically, the data can only be accessed, modified, and deleted by authorized users. Error checking techniques should be employed to ensure information integrity, in other words, to prevent malicious entities modifying the sending data.

Authentication: Theoretically, authentication is not a standard component of information security. It is emphasized here because it is regarded as significantly important in drone-aided medical applications. Authentication refers to the process of validating whether someone (something) is who (what) he/she (it) declares him/herself (itself) to be. The validated objective may be a person such as the pilot, and also may be an equipment such as another drone intending to join the application. As observed, drone-aided medical applications always have strict security constraints, so any unauthorized access would cause great risks to not only the patient's privacy but also flying safety. If a malicious pilot is authenticated entering the system, piloting power may be robbed, further causing flying accidents [14]. In [14], Leela *et al.* reported a specific software using this attack to take control of a drone. An actual de-authentication attack of A.R. Drone was presented.

Enhanced authentication techniques have to be employed for drone-aided medical applications.

5G and Blockchain

5G and blockchain are two revolutionary technologies in recent years that have gained worldwide attention from both the academic and industrial communities. Preliminaries of 5G and blockchain are given in this section.

5G Cellular Network

As the name suggests, 5G is the fifth generation of cellular networks that began being widely deployed in 2019. Before 5G, four types of cellular networks had been developed and deployed. Essentially, 5G is a transformative communication ecosystem rather than a simple extension of the previous 3G and 4G technologies. In the 5G era, connectivity between any devices and applications is provided, so the current user-centric world will evolve to one with bulks of machine-type communications.

5G has advantages in terms of data rate, latency, networking scalability, energy consumption, and so on. This technical progress helps to promote drone-aided medical applications in a straightforward way, as seen in the following section.

Blockchain

Blockchain was initially proposed as the foundation technology for Bitcoin, the first decentralized cryptocurrency in the world. Logically, four primary components constitute the concept of blockchain and its operation network. They are asymmetric cryptography and nodes, transactions, consensus protocol, and the distributed ledger [8, 15]. The functionalities of these components are sketched as follows; interested readers can refer to [15] for more details.

Asymmetric Cryptography and Nodes: Participants (nodes) of a blockchain application should be capable of processing application-specific messages and interacting with peer nodes. For secure operation, asymmetric cryptography is adopted in blockchain. In the Bitcoin case, the public key of a participant acts as its cryptographic address (like a bank account) for transactions with others, while a corresponding private key is generally for digital signature. Although the transactions are transparent and broadcasted to each node of the blockchain, the delicate usage of asymmetric cryptography can ensure the security and privacy of the transaction parties.

Transactions: A transaction in a blockchain application refers to information exchange between participants, such as the dealing data of Bitcoin. A file including the transaction details is first generated as per application. Since there is no direct link between the source and destination in the blockchain, the transaction packet is broadcast to the whole network. Thanks to the adopted asymmetric cryptography, only valid users can claim ownership of the transaction. The transaction has to be checked for compliance with the regulations; then the validated transactions are accumulated together into a block, which is finally linked to the blockchain. The aforementioned validation and approval rules depend on the consensus protocol of a specific application.

Blockchain was initially proposed as the foundation technology for Bitcoin, the first decentralized cryptocurrency in the world. Logically, four primary components constitute the concept of blockchain and its operation network. They are asymmetric cryptography and nodes, transactions, consensus protocol, and the distributed ledger.

Consensus Protocol: The consensus protocol is defined as the application's "playing rules" which must ensure that all the blocks have an identical ledger. Basically, it should include rules for confirming the transaction's validity, updating the blocks' ledger, as well as accepting a new block. Proof of work (PoW) was first proposed and adopted for Bitcoin; other variants are also investigated with their own characteristics. The network property (public, consortium, or private) and other requirements (e.g., latency) ask for a specific consensus protocol.

Distributed Ledger: The distributed ledger refers to the data structure maintained on each node of the application. Sometimes, it is the narrower definition of blockchain. The distributed ledger has two distinct features. First, all nodes have an identical distributed ledger, and the maintenance and updating are performed by means of the consensus protocol. Second, a distributed ledger is a chain of blocks wherein the current block is linked with the previous one through a hash identifier.

Opportunities of 5G and Blockchain in Medical Applications of Drones

Exploiting 5G for Promoting Communication Reliability

As summarized above, reliable communication is highly required for promoting the medical applications of drones. Taking advantage in terms of high data rate, low latency, and so on, the evolutionary 5G cellular network is a promising solution.

High Data Rate: The data rate of 4G limits the wireless transmission speed, especially block applications integrating remote surveillance or video transmission (e.g., tele-surgery). The peak data rate of 5G is expected to reach 10 Gb/s, and may increase to 20 Gb/s under certain conditions. Such speed is approximately 10 times that in the 4G era. This speed enables remote doctors having high-resolution monitoring pictures of patients, and further facilitates the flexible allocation of the data rate resource in multi-participant scenarios.

Low Latency: Applications of drones always require strict latency, because the remote pilot has to operate the drones in a guaranteed fashion to avoid collision. The 10 ms latency of 4G will be reduced to 1 ms in 5G, which enables accurate piloting of flying drones. In addition, tele-surgery also benefits much from such low latency. In future scenarios, a patient lacking modern medical care or traffic convenience can refer to remote treatment, while the operating physician may be located anywhere in the world.

High Scalability and Low Energy Cost: The 5G cellular network supports machine-to-machine and IoT solutions, so a massive number of devices can be connected via 5G infrastructure. For the concerned applications, drones and wearable devices of a patient can be well integrated by 5G

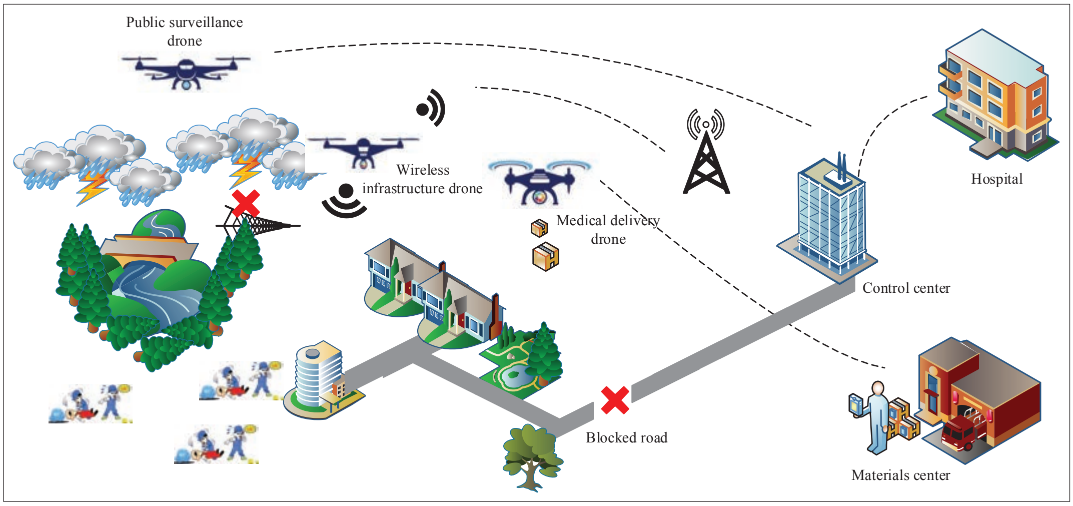

FIGURE 2. Applications of drones in a scenario of disaster relief.

to improve treatment. In addition, energy saving is another distinct feature of 5G. This property remarkably reduces the energy consumption in terms of radio access and wireless data transmission, and further prolongs the sensor's lifespan in medical applications.

Exploiting Blockchain for Security Enhancement

Although there are some security mechanisms in 5G, the security requirements of drone-aided medical applications cannot be fully satisfied by the 5G cellular network. In this scenario, blockchain emerges as a promising solution. Remarkable security enhancements are achievable by exploiting the intrinsic features of blockchain.

Confidentiality: As aforementioned, asymmetric cryptography is used to encrypt the privacy-sensitive information in a blockchain application, as adopted in Bitcoin. Peer nodes can listen to the transactions but are unable to know the participants of these messages. In addition, the data record inside the transactions can also be specifically encrypted for further enhancements. In this case, both the participants and the transaction message are secure against eavesdropping.

Integrity: The immutability property of blockchain perfectly matches the concept of integrity. With per consensus protocol of a blockchain application, a transaction cannot ever be modified once it is accepted. It is stored in a block, together with other transactions of the current billing cycle. This block will be linked into the blockchain, and its hash value acts as a component of the subsequent block. We can observe that modification of one block will cause successive mismatching of all subsequent blocks. That means the alternation will be immediately sensed and thus prevented. Even if an opponent changes all the blocks in one node, since peer nodes have a copy of the ledger, the modification can also be easily found out. Therefore, higher integrity can be obtained.

Availability: The availability of a traditional information system is weak against jamming or flooding attacks (e.g., DDoS). By flooding the centralized node (e.g., the authentication center), the whole system breaks down. The decentralization feature of a blockchain system brings high security against such attacks, although each blockchain node is vulnerable. Because a copy of the ledger is maintained and kept in all nodes, the attacked/unavailable node can be immediately excluded from the whole network while others can operate as usual.

Authentication: Unauthorized access to the information system and data records is preventable via blockchain. A public blockchain network is free to join; however, consortium and private blockchain networks are born with authentication of users who can participate. In addition, the transactions disseminated to the application nodes are all protected via asymmetric cryptography, so only the valid user who has the correct private key can claim ownership. Such a design, provides high-level authentication to the system.

Illustrative Case in Drone-Aided Disaster Relief

In the scenario of disaster relief, this section gives an illustrative adoption of 5G and blockchain for promoting medical applications of drones. A disaster is assumed in this example, wherein the roads break down and the cellular network is also unavailable; suppose that the base stations have collapsed. Public healthcare surveillance is required for lossy assessment and for designing a rescue plan. In addition, emergency medical materials (blood, medicine, etc.) are also in high demand. In this scenario, the drones are employed for medical delivery, emergency communication establishment, surveillance, and rescue. 5G and blockchain are introduced for providing reliable communication and information security. An example is illustrated in Fig. 2.

Reliable wireless communication is the first issue to be addressed. In this example, a flying drone is required for public surveillance and needs a high data rate to transmit the high-resolution images captured by the cameras. Delivery of medical materials and piloting of massive flying drones both require low-latency and high-scalability wireless networks, as indicated in Table 1. Since the local cellular network is assumed to be damaged, wireless infrastructure drones are employed to extend the network coverage. There are various options for the integration of 5G and drones [7], and a 5G cellular network can be flexibly and quickly established. Thanks to the technical progress of 5G, the established wireless link has advantages in terms of high data rate, low latency, and high scalability. The flying drone as well as the medical equipment can quickly communicate with the surviving devices. Normalizing those of 4G as 1, the performance indicators of a 5G-based wireless link are depicted in Fig. 3.

After establishing wireless communication using drones and 5G, it is blockchain's turn to solve security issues. Exploring intrinsic features of blockchain, information security in terms of confidentiality, integrity, availability, and authentication can be achieved, as illustrated in Fig. 4.

First, public blockchain rather than its consortium or private counterpart is preferred, because this case is a public health emergency. External nodes should be permitted access to the blockchain network, since they can provide more computation resources and thus relax the burden of the nodes in the disaster area. However, access to sensitive information is also restricted due to privacy concerns. Therefore, asymmetric cryptography is adopted, with the public key serving as cryptographic address while the corresponding private key solves the digital signature problem. In addition to ensuring confidentiality, this design also helps to securely confirm who is the valid owner of the medical package (blood, medicine, etc.) delivered by a drone, similar to the case of Bitcoin. Asymmetric cryptography also significantly promotes the authentication, so unauthorized access into the flying link is thus preventable. The transactions (messages) in this application are also stored in blocks that are chained together. Due to the inherent characteristic of blockchain, these messages have immutability and traceability, which are significantly important to facilitate whole rescue procedures. We also do not need to worry about the availability of these data records, since all the nodes hold an identical copy. Even if one or more nodes collapse, the stored data is also available from other nodes. Regarding the consensus problem, Bitcoin's PoW mechanism is not suitable for this emergency scenario due to its high computation load. Thus, a low-cost consensus mechanism should be developed. In summary, information security of the application system has been dramatically enhanced by blockchain.

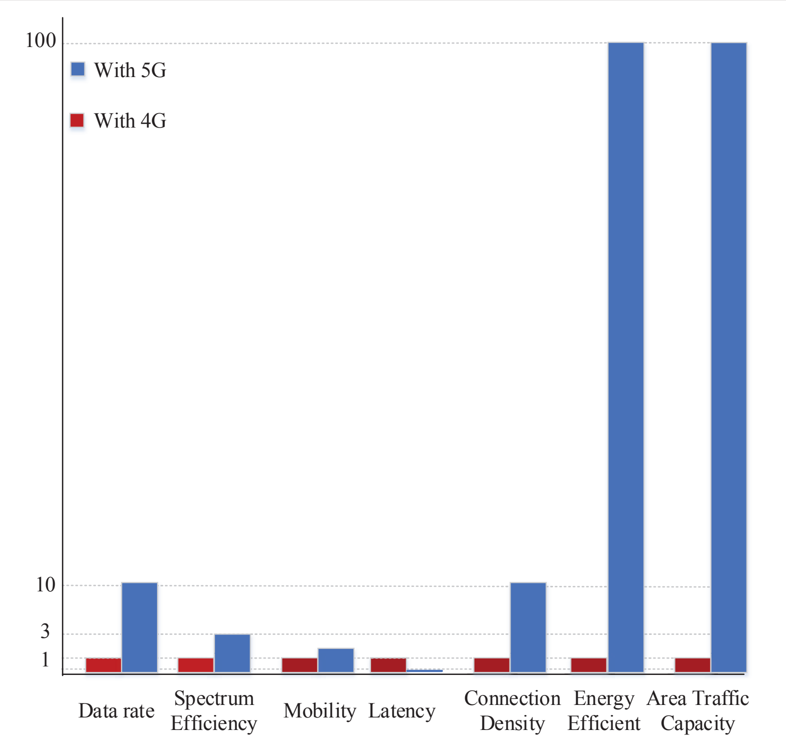

FIGURE 3. Performance comparison of the wireless links of 5G and 4G.

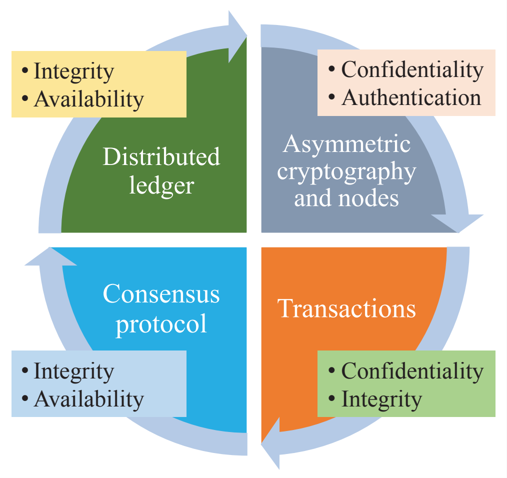

FIGURE 4. Exploiting blockchain for security enhancement.

Conclusions

This article exploits 5G and blockchain to address the communication and security issues in the application of drones for medical services. Theoretical discussions are first presented, and an example in the scenario of disaster relief is given for illustration. The results reveal the capabilities of 5G and blockchain in providing reliable communication and enhanced information security. Nowadays, drones are popularly employed for medical treatment. We hope this article is beneficial for motivating deeper research in academia, and also for promoting reliable and secure drone-aided medical services in practice.

Acknowledgments

This work is funded by the National Natural Science Foundation of China (Nos. 61802055, 61771121), the Fundamental Research Funds for the Central Universities (No. N2019001), the China Postdoctoral Science Foundation (2019M651115), the Science and Technology Development Fund, Macau SAR (File no. 189/2017/A3), and the University of Macau (File no. MYRG2018-00136-FST).

References

[1] K. Bhatt, A. Pourmand, and N. Sikka, "Targeted Applications of Unmanned Aerial Vehicles (Drones) in Telemedicine," *Telemedicine J. and E-health*, vol. 24, no. 11, 2018, pp. 833–38.

[2] E. Ackerman and E. Strickland, "Medical Delivery Drones Take Flight in East Africa," *IEEE Spectrum*, vol. 55, no. 1, 2018, pp. 34–35.

[3] J. C. Rosser Jr. *et al.*, "Surgical and Medical Applications of Drones: A Comprehensive Review," *JSLS: J. Society of Laparoendoscopic Surgeons*, vol. 22, no. 3, 2018.

[4] A. Hardy *et al.*, "Using Low-Cost Drones to Map Malaria Vector Habitats," *Parasites & Vectors*, vol. 10, no. 1, 2017, pp. 29–29.

[5] A. Claesson *et al.*, "Drones May Be Used to Save Lives in Out of Hospital Cardiac Arrest Due to Drowning," *Resuscitation*, vol. 114, 2017, pp. 152–56.

[6] Global Market Insights, "Medical Drones Market Expects to Reach Almost $400m by 2025," 2019; https://www.gminsights.com/industry-analysis/medical-drones-market, accessed July 2019.

[7] I. Boryaliniz *et al.*, "Is 5G Ready for Drones: A Look into Contemporary and Prospective Wireless Networks from a Standardization Perspective," *IEEE Wireless Commun.*, vol. 26, no. 1, Feb. 2019, pp. 18–27.

[8] I. J. Jensen, D. F. Selvaraj, and P. Ranganathan, "Blockchain Technology for Networked Swarms of Unmanned Aerial Vehicles (UAVs)," *Proc. 2019 IEEE 20th Int'l. Symp. a World of Wireless, Mobile and Multimedia Networks*, 2019, pp. 1–7.

[9] J. Braun *et al.*, "The Promising Future of Drones in Prehospital Medical Care and Its Application to Battlefield Medicine," *J. Trauma and Acute Care Surgery*, vol. 87, no. 1S, 2019, pp. S28–34.

[10] B. M. Harnett *et al.*, "Evaluation of Unmanned Airborne Vehicles and Mobile Robotic Telesurgery in an Extreme Environment," *Telemedicine J. Ehealth*, vol. 14, no. 6, 2008, pp. 539–44.

[11] N. Mohamed *et al.*, "Unmanned Aerial Vehicles Applications in Future Smart Cities," *Technological Forecasting and Social Change*, 2018, p. 119,293.

[12] H. Ullah *et al.*, "5G Communication: An Overview of Vehicle-to-Everything, Drones, and Healthcare Use-Cases," *IEEE Access*, vol. 7, 2019, pp. 37,251–68.

[13] W. D. De Mattos and P. R. D. L. Gondim, "M-Health Solutions Using 5G Networks and M2M Communications," *IT Professional*, vol. 18, no. 3, 2016, pp. 24–29.

[14] C. G. L. Krishna and R. R. Murphy, "A Review on Cybersecurity Vulnerabilities for Unmanned Aerial Vehicles," *Proc. 2017 IEEE Int'l. Symp. Safety, Security and Rescue Robotics*, 2017, pp. 194–99.

[15] D. Puthal *et al.*, "Everything You Wanted to Know About the Blockchain: Its Promise, Components, Processes, and Problems," *IEEE Consumer Electronics Mag.*, vol. 7, no. 4, 2018, pp. 6–14.

Biographies

Junxin Chen received his B. Sc., M.Sc., and Ph.D. degrees, all in communications engineering, from Northeastern University, Shenyang, China, in 2007, 2009, and 2016, respectively. He is currently an associate professor at the College of Medicine and Biological Information Engineering, Northeastern University; he is also with the Department of Computer and Information Science, University of Macau, China. He has authored/co-authored over 50 scientific papers in peer-reviewed journals and conferences, including *IEEE Transactions of Industrial Informatics*, the *IEEE Internet of Things Journal*, the *IEEE Photonics Journal*, *Information Sciences*, and others. His research interests include biosignal processing, compressive sensing, security, and privacy.

Wei Wang (wangw328@mail.sysu.edu.cn) received his B.Sc. degree in electronic information science and technology from Shenyang University in 2012, and his Ph.D. degree in software engineering from Dalian University of Technology in 2018. He is now an associate professor at the School of Intelligent Systems Engineering, Sun Yat-sen University, Shenzhen, China. He has authored/co-authored over 30 scientific papers in international journals and conferences, including IEEE Transactions on Big Data, *IEEE Transactions on Emerging Topics in Computing*, *IEEE Transactions on Human-Machine Systems*, WWW, and so on. He received the best paper award of the IEEE International Conference on Ubiquitous Intelligence and Computing in 2014. His research interests include computational social science, data mining, and mobile social networks.

Yicong Zhou received his B.S. degree from Hunan University, Changsha, China, and his M.S. and Ph.D. degrees from Tufts University, Massachusetts, all in electrical engineering. He is an associate professor and director of the Vision and Image Processing Laboratory at the University of Macau. His research interests include image processing and understanding, computer vision, machine learning, and multimedia security. He is a Co-Chair of the Technical Committee on Cognitive Computing in the IEEE Systems, Man, and Cybernetics Society. He serves as an Associate Editor for *IEEE Transactions on Neural Networks and Learning Systems*, *IEEE Transactions on Circuits and Systems for Video Technology*, and others.

Syed Hassan Ahmed [S'13, M'17, SM'18] completed his B.S. at KUST, Pakistan, and his M.S./Ph.D. at Kyungpook National University, South Korea, both in computer science, in 2012 and 2017, respectively. Later, he was a postdoctoral researcher with the University of Central Florida, Orlando, and on the faculty of the Computer Science Department of Georgia Southern University at Statesboro, where his research interests included sensor and ad hoc networks, cyber-physical systems, vehicular communications, and Future Internet. Currently, he is with JMA Wireless as a product specialist with a focus on distributed antenna systems and mmWave products.

Wei Wang received his M.S. and Ph.D. degrees from Xi'an Jiaotong University in 2005 and 2011, respectively. He is currently an associate professor with the School of Computer Science and Engineering, Xi'an University of Technology, China. His research interests are wireless networks, wireless sensor network applications, image processing, mobile computing, distributed computing and pervasive computing, the Internet of Things, and sensor data clouds. He is a Senior Member of CCF.