LBTrace: A LoRa and Blockchain Based Contact Tracing Method for COVID-19 and Future Pandemics

Jian Fang#, Wenbo Zhao#, Lei Wang*, Zhenquan Qin, and Bingxian Lu

Abstract—COVID-19 has caused hundreds of millions of infections and hundreds of deaths, and even though vaccinations are increasing, the mutation of the virus makes the pandemic even difficult to control. Existing manual, operator and Bluetooth-based technologies for epidemiological investigation and close contact tracing suffer from high cost, low accuracy, and difficulty in scaling up. Viruses such as Delta variants have a greater ability to survive and spread, making many of the existing human-human close contacts tracing less effective. Also, it is easy to overlook the fact that there is still a large segment of the world's population that does not have access to the Internet and is proficient in using smartphones, which makes the performance of smart device-based tracing much less effective. Inspired by Health Code and Tracetogether, which have been widely accepted in China and Singapore, we propose a LoRa and blockchain-based contact tracing method LBTrace, which is low-power, lightweight, and operation-free. The experimental results demonstrate the high stability and accuracy of our proposed method, which can be used as a complement to existing methods to help some governments effectively control COVID-19 and future outbreaks under certain emergency conditions.

Index Terms—COVID-19, Contact Tracing, LoRa, Blockchain.

1 Introduction

The COVID-19 caused the pneumonia epidemic in the world from 2020, causing the infection of hundreds of millions of people and the death of millions of innocent lives [1]. The World Health Organization (WHO) and governments around the world have taken various measures to contain the epidemic, but a year on, only a handful of countries have actually brought it under control, and the number of infected cases and deaths rising daily is alarming. Because COVID-19 is far more contagious than SARS and MERS and has an incubation period of up to 14 days or more [2], [3], the virus spreads unchecked among unprotected populations. A single infected patient can infect an entire cabin passenger in just a few hours on a flight. Those passengers, known as close contacts, then carried the virus off the plane, then it continued to spread in the workplace and the community. More worrying is the presence of asymptomatic infections, people who are infected with the virus but show no symptoms and continue to act as healthy people. They would not have been detected until some accidents, during which time they had come into contact with a large number of people and could have spread the virus on to others. While a recent sign of danger is that the virus can live on frozen surfaces for a long time and infect people, which is very hard to detect.

- *Jian Fang, Wenbo Zhao, Lei Wang, Zhenquan Qin, and Bingxian Lu are with the School of Software Technology, Dalian University of Technology.*
- *# contribute equally.*
- **Lei Wang is the corresponding author: lei.wang@dlut.edu.cn.*
- *The work was supported by "National Natural Science Foundation of China" with No. 61902052, "National Key Research and Development Plan" with No. 2017YFC0821003-2, "Dalian Science and Technology Innovation Fund" with No. 2019J11CY004 and 2020JJ26GX037, and "the Fundamental Research Funds for the Central Universities" with No. DUT19RC(3)003 and DUT20ZD210.*

An important task in infectious disease prevention and control is epidemiological investigation [4], [5], which traces the movements of an infected patient over some time (14 days in the case of COVID-19, or even longer in some countries) to identify his/her close contacts at multiple levels, and is an important means to determine the target of nucleic acid tests and quarantine. The traditional epidemiological investigation mainly relies on patients' self-report. In June 2020, A localized outbreak occurred in a market in Beijing, China, and was quickly controlled thanks to the good memory of the first patient diagnosed. He accurately recalled his whereabouts over the past 14 days and provided crucial information about the Xinfadi, a very important market in Beijing, which has brought some convenience to the investigation of contacts. But in fact, such lucky events do not always happen, and no government should allow epidemic prevention efforts to be based on individual luck.

Therefore, many places use smartphone sensors and APPs such as transaction records to conduct an investigation. However, the effect is still not ideal, and some people will inevitably be omitted [6]. From the perspective of the medium, existing methods can be roughly divided into location-specific and people-specific. Location-specific methods treat all those who intersect with the patient's itinerary as close contacts and conduct extensive testing and quarantine, it rarely misses positive cases, but it perhaps perplexes some people who have very little risk of infection. Besides, it takes about $3 \sim 5$ steps on QR codes every time we use it and requires strong human supervision. On the other hand, the locations of visits recorded by such methods are not encrypted and are published in epidemiological surveys, resulting in privacy breaches. While Bluetooth technology is generally used in people-specific methods to record people who have been in very close contact. The

coverage is relatively small due to the characteristics of Bluetooth, and the tracing results are targeted, but some secondary contacts are often missed since we know that in addition to direct transmission from person to person through droplets, the virus can also spread through aerosols, surfaces (especially frozen surfaces), etc. Spread through the air or object, especially the new Delta variant [7], is difficult to detect by a human-to-human contact tracing like Google/Apple Exposure Notification [8], [9].

The two methods are widely used around the world, however, with the gradual expansion of the application, a very important problem emerged. Both of them are based on smartphones and the Internet. However, it is not simple. According to Wikipedia [10], about half the population does not skilled or even completely unable to use smartphones, including the elderly, children, and other off-internet people in China, which are happen to be susceptible of infectious diseases. In the United States, the largest developed country, about 20 million people have never used the Internet. It will not be easy to quickly popularize smartphones and the Internet and teach these people how to use them. In addition, the use of smartphones and high-power technology is not suitable for tracing objects. The effectiveness of epidemic tracing systems will be significantly reduced when large numbers of potential targets are unable to participate.

In this paper, we put aside the cultural concepts and try to propose a new method of tracing close contacts just from the perspective of rapid tracing close contacts of COVID-19 during daily life and the emergency lockdown implemented by the government in some countries, or even the more serious infectious diseases that may occur in the future. We believe that a good solution should include the following characteristics:

1) Ease of use: it requires as few and simple actions as possible, without overburdening the user.
2) Low power consumption: it can work long hours with high energy efficiency and without additional cost to the user's device.
3) Reliable: information about patients and close contacts is important and private, so its security must be guaranteed.
4) Universal: it can be used by different people, objects, and places without additional configuration.
5) "Have to" use: combined with the above advantages, the new method can attract as many people as possible to use it for themselves and their families, just like wearing a mask.

Therefore, we propose a LoRa-based Blockchain-enabled privacy-preserving contact tracing method LBTrace, which can meet all the above requirements. It can be used as a supplement to the methods currently in use. It is user-friendly to all, especially the off-internet people, and can even be placed on objects to prevent human infections that often occur when frozen imports are shipped. The usage scenario of LBTrace is shown in the Fig. 1.

First, LBTrace only requires one registration during the initialization phase, and the personal ID and contact information are can only be accessed by the government and medical institution. No other operations are needed and the disclosure of Personally Identifiable Information (PII) information is avoided. Secondly, for end-users, due to the ultra-low power consumption of LoRa, a device can work for years, not only can supply the use of COVID-19, even for new outbreaks that may emerge in the future. And the cost of a single device is low, the volume is small enough, and could be made as wearable devices for mass distribution. We adopt the design of the China Health Code and set indicator lights of the same three colors for the device as an option in some regions. Our method eliminates the inconvenience in the use of current widely used methods: take out the phone - the phone is difficult to identify the face wearing a mask - manually enter the password to unlock - call the APP to scan the code - poor network - repeat. We just need to show the device to the staff and walk into the building if necessary. There is no need to worry that the elderly or children can not use it so that everyone's participation is ensured. In LBTrace, only the necessary contact information is recorded, and because it does not rely on any other smart devices, the possibility of information theft is avoided. Besides, since there is no possibility to modify the operation, users' indoor visit records will be saved whenever we bring the device to participate in the indoor social activity. We adopted Blockchain to prevent data tampering and to say no to anyone who wants to break the law to undermine our efforts. Moreover, the user information is presented anonymously through a hybrid method, which can ensure that the user's PII is not leaked, thus protecting the user's privacy. Finally, LBTrace has good versatility, and users can travel unblocked to the region where the system is deployed without any action. In some scenarios, it can also be used on objects to record their contact with people.

The main contributions of this paper are as follows:

1) We propose and implement a new COVID-19 contact tracing method based on LoRa's stability, anti-interference, and long-distance transmission. It does not rely on smartphones or NSPs and does not require active user participation. It can remotely record the location and time of a user and even an object's visit for the rapid tracing of close contacts.
2) We utilize the Blockchain to ensure the security and reliability of users' private information. To our best knowledge, it is the first work to combine LoRa and Blockchain for COVID-19 contact tracing.
3) We design and conduct a series of experiments to evaluate the accuracy of records, the ability to trace close contacts, and the system response speed on our campus. The experimental results show that LBTrace has a very high accuracy to rapidly trace the potential close contacts with very low energy consumption.

2 Background and Motivation

2.1 Why LoRa

Because the Delta strain has a high load, its exhaled air is highly toxic and infectious. Therefore, the definition of close contacts needs to change from those who were in the same office with the patient and his family two days before the onset of the disease, or shared meals and meetings within one meter, to those who were in the same space, the same

unit, the same building four days before the onset of the disease [11]. However, the most popular Bluetooth-based methods are not able to meet the latest requirements.

Although Wi-Fi and Bluetooth are more prevalent at the moment, IoT devices such as LoRa are also very popular, and due to their smaller size and lower cost, the cost of a single device is around tens of dollars, and the deployment speed is faster, it will catch up with the deployment scale of Wi-Fi and other devices in a short time.

The method of using existing Wi-Fi facilities is limited to indoor. There are also many outdoor possible infections, such as football games, vocal concerts, etc. Since LoRa is outdoor communication technology, the tracking system based on it is ideal for outdoor deployment. LoRa can transmit over very long distances. Unlike Wi-Fi, which requires a large number of deployments, a LoRa-based tracing system only needs one device to cover a building and can be extended based on existing network infrastructure, which is not expensive to build.

IoT technology has developed by leaps and bounds in recent years. The number of IoT applications continues to grow from 2019 to 2020, with the number of companies using IoT technology surging from 85% to 91%. 83% of the applicators have at least one project that has reached the usage stage, compared to 74% in 2019. As a result of COVID-19, one in three companies will increase their investment in IoT. For enterprises in the learning stage, investment in the IoT will be increased after successful application. Companies around the world are increasingly incorporating IoT applications as part of their core technological changes, and businesses across the board are using IoT to improve production and operational efficiency [12]. LoRa is also becoming more and more popular and has become the best choice for many IoT applications, with great potential. On current trends, LoRa could be the next Wi-Fi, with large-scale, full-scale applications in the IoT field. Therefore, devices using LoRa can be easily integrated with IoT applications and have great potential.

And through our actual experiments, we found that LoRa signals can easily penetrate the walls inside the building, but it is difficult to penetrate the thicker outer walls of the building. This feature can also greatly reduce the mutual interference of LoRa signals between various buildings. It is helpful for our design.

We didn't choose LoRaWAN, because LoRaWAN cannot support large-scale concurrent LoRa devices. The experiments in [13] showed that a typical smart city deployment can support 120 nodes per 3.8 ha, which is not sufficient for future IoT deployments.

2.2 User acceptance

We fully understand that there are still a lot of people who would find it difficult to equip an additional tracking device, even if it is for their health and to maintain normal social interaction. Therefore, we need to emphasize our method is only is a complement to existing approaches in the period of the epidemic, and is a choice for the government to effectively curb the spread of the virus during special events like COVID-19, compared with the millions of people who died because of illness, we think that this is an acceptable compromise.

In addition, we do not ask all the people to use our device. For young people, they can continue to use the method based on smartphones. Our main service targets are those who can not use smartphones well or can not always carry their phone, such as the elderly, primary school students, workers in special industries, etc. IoT-based methods can even be used to track objects because of their small size, low power consumption, and no need for operation, These are advantages that other methods do not have.

3 Related Work

Our work is mainly related to the research in the following domains.

3.1 Contact Tracing

Since 2020, various countries and companies around the world have successively launched their own contact tracing methods and applications [14], [15], [16], [17], [18], which can be generally divided into three categories: centralized, decentralized and hybrid [19], [20]. The technologies used are focused on Bluetooth, WiFi, QR code, operator network, etc. In a centralized architecture, a central server plays a key role in performing core functions, such as storing encrypted PII, generating anonymous TempIDs, risk analysis, and close contact notifications. Furthermore, excessive permissions on the server can lead to privacy issues [21], [22]. Among the well-known contact tracing APPs of centralized architecture, there are TraceTogether from Singapore [23], CovidSafe [24] from Australia, and various Health Codes [25] from China. However, in a decentralized architecture, the tracing process is performed locally by application users on their devices. It can alleviate some privacy issues, but it puts higher demands on the user device to complete more calculations. Another significant drawback is that it relies on the user to voluntarily report the diagnosis information, which is very unreliable in practice. Examples of contact tracing APPs of decentralized architectures are Google/Apple Exposure Notification APIs [8], [9], PACT [26]. Hybrid architectures seek to strike a balance between centralized and decentralized architectures. However, only a handful of hybrid architectures have been proposed, such as DESIRE [27] and EpiOne [28]. Moreover, the existing APPs with hybrid architecture require more data communication between the smartphones and the server, which will also lead to an increase in the power consumption of the smartphones.

WiFiTrace [29] records users' trail information through Wi-Fi that has been widely used nowadays and takes the geographic location of each AP as the trail records. However, it puts high requirements on the user's mobile device, that is, the user's device (usually a mobile phone) must be connected to Wi-Fi and switch between various Wi-Fi signals flexibly. Otherwise, a situation can occur where a device is in a certain location but is connected to a distant Wi-Fi AP, causing an error in the geolocation information for the trail record. Besides this, WiFiTrace also has a very high requirement for the coverage of Wi-Fi signals and can only be used in some special places like offices and educational institutions. However, in these places, many Wi-Fi signals can be found in a single room. Therefore, without

the user's inspection, It can be difficult to connect the phone directly to the right Wi-Fi AP for close contact tracing. In addition, few users set their phones to automatically connect to an unknown Wi-Fi signal, which can lead to unstable and costly network switching. So even in an ideal school environment, WiFiTrace is still difficult to be popularized.

All above methods are relying on smartphones, which is very unfriendly to the off-internet people [30]. Even with stand-alone devices like the TraceTogether token, the problems of short-range and high power consumption still exist and degrade the performance. So far, there is no effective way to trace the transmission of the virus from objects to people. With the emergence of new variants of the virus, cases of infection by air and objects are gradually increasing [31]. Therefore, we believe that tracking based on absolute location will be more effective than direct person-to-person tracking.

We have listed a comparison of the methods that are widely used in Table 1 and tried to find a way to address their disadvantages.

3.2 LoRa

In recent years, the LPWAN technologies have gradually attracted more and more scientific attention, and are expected to become an important part of the future scalable IoT. Among them, LoRa/LoRaWAN [32], [33] is notable for its open specification and gateway infrastructure which are completely different from the closed design and managed gateway infrastructure of other LPWAN technologies.

Chirp Spread Spectrum (CSS) enables LoRa to transmit data over distances up to tens of kilometers with very low power consumption, so it is replacing traditional wireless sensor networks in many new IoT applications such as meteorology, transportation, intelligent agriculture, intelligent factory [34], [35]. Although LoRa is generally used in the outdoor environment, combining the above characteristics and the propagation model of wireless signals in the indoor environment provides a new idea for its indoor application [36], such as smart home, new human-computer interaction, and wearable devices.

Inspired by this, we would like to make use of its signal and network characteristics and apply it to the process of visit information transmission in the tracing of close contacts.

3.3 Blockchain

Blockchain is suitable for almost any field that lacks a trust mechanism, and may soon become the foundation of human civilization to build trust [37]. For example, the new generation of Blockchain technology represented by Ethereum is trying to build a new decentralized Internet architecture [38], [39].

Since the beginning of 2020, some researchers have proposed using Blockchain technology in contact tracing systems, which could solve many of the existing privacy and security issues, such as it can be technologically designed to provide a solution that protects privacy, rather than relying on compliance with regulations or laws in a centralized system. Blockchain technology, combined with the use of encryption and anonymity, can further protect the identity

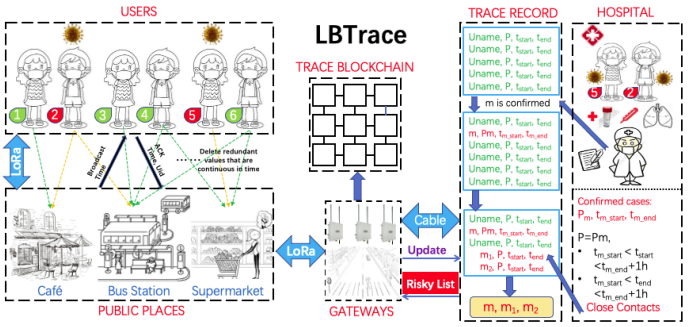

Fig. 1. The usage scenario of LBTrace.

of users, Blockchain is non-regional in nature and thus provides an appropriate global access platform for COVID-19 pandemic tracking and control. The transparent nature of Blockchain can prevent the public from being intentionally misled by authorities or other third parties [40], [41], [42].

Compared with the traditional cryptographic methods, such as Hash and MD5, using Blockchain and pseudonyms together can avoid a lot of risky and cumbersome work, such as requiring users to provide their keys, requiring users to provide registration information, or repeatedly verifying the keys. Moreover, in our scheme, using Blockchain can dramatically reduce the amount of data in the LoRa part and the energy consumption of devices, and improve the reliability and speed of communication.

4 LoRa-based Blockchain-enabled Privacy-preserving Contact Tracing

In this section, we describe the workflow of LBTrace in detail and explain the key concepts. We will begin by describing the entities involved in the system, their roles, and how they work. Then we will describe the workflow of the contact tracing framework.

4.1 Entities, Functions, and Interfaces

4.1.1 *Trace Blockchain*

The Trace Blockchain is maintained by many gateways (GWs), which are used to save the activity track information of users in various public places. It accepts registration of new GWs, making it easier for LBTrace to expand. It only keeps blocks generated in the past fortnight. One Trace Record (TraceRecord) is stored in one block, including trace generation time (TraTime), user's string-formed pseudonym (UName), trace generation location (TraLoc), LoRa GW signature, the hash value of the previous block, the hash of this block. The TraTime is recorded in the form of a timestamp, accurate to minutes. And UName is a 16-character string, in which the characters are randomly selected in the $A \sim Z, a \sim z$ and $0 \sim 9$, so there can be 62^{16} different available strings in total, far more than the number of users. Therefore, UNames have an extremely low probability of repetition and can be ignored. LBTrace is a lightweight application that doesn't store much personal information. Therefore, privacy-preserving only needs to protect the key identity information, and pseudonym is enough. The TraLoc is a string type, which is an officially

Method	Health Code	Itinerary Card	TraceTogether	Exposure Notification
Developer	China Gov	China Gov	Singapore Gov	Google/APPLE Inc.
Technology	QR code	5G, Bluetooth	Bluetooth	Bluetooth
Energy	mid	high	mid	high
Cover	large	large	short	short
Accuracy	mid-high	low	high	high
Target	building	city	close contacts	close contacts
Privacy	low	low	mid	high
Usability	mid	low	high	mid
Reliability	need strong manual supervision	high false alarm rate	depends on user's consciousness	depends on user's consciousness

* Close contacts here means 1st-level close contacts directly to the infected cases, not include close contacts of close contacts.

TABLE 1
A list of currently widely used methods

designated identification code. The signature can be used to verify the validity of the newly uploaded records.

Estimates of maximum processing power for Bitcoin transactions using average or median transaction sizes range from 3.3 to 7 transactions per second [43]. It is sufficient for LBTrace as a complement to the existing contact tracing applications.

4.1.2 Risky Names Server

The Risky Names Server is used to maintain and present the Risky Pseudonym List (RiskyList). It provides a website that can be queried and read by users and GWs. RiskyList is used to record UName and notify the users and is stored in set type, which ensures that each UName is not duplicated, making it easier for low-power Fixed Devices (FDs) and Mobile Devices (MDs).

4.1.3 Fixed Device

The FD is allocated by the government to various indoor public places, like shopping malls and office buildings. The FD is cable powered and located in the center of the building or at the entrance so that every visitor can be covered.

For the LoRa transmission, the larger the SF, the higher the power consumption, the less encoded data per second, the longer the airtime, and the higher the delay. We did serveral simulations with LoRaSim [13] and practical tests [44], the result shows that LoRa with SF7 communicates best at a distance within 90 meters. This coverage is sufficient for indoor use, and the advantage of low SF is conducive to high-frequency data transmission between multiple MDs and an FD. While the communication between FD and GW needs to penetrate the building walls and transmit over a long transmission distance. Therefore, we found that SF9 could just meet the requirement that LoRa signal can penetrate 1 to 4 layers of walls of the building and communicate with the outdoor GW at a distance of about 500m which can support about $7 \sim 8$ devices on the same channel while maintaining a higher data transmission rate.

FDs will broadcast WakeMessage to wake up the MDs from sleeping mode by $SF = 7$, and receive NameMessages with a UName from each MD every 5s. Then, FDs add TraTime and TraLoc information to the UName, generate and send TraceRecords to the GW via LoRa of $SF = 9$. The FD also sends the RiskyList downloaded from the GW along with WakeMessages to each MD and informs each user. Due to the size limitation of the LoRa packet, the FD sends TraceMessages one at a time and waits for an ACK message from the GW along with the RiskyList. The FD will wait for an ACK or resend for $10 \times 10s$, or it reports an error after 10 failures. When the FD receives the ACK message and the RiskyList from the GW, the device will delete the first record in the local TraceRecord list.

4.1.4 Mobile Device

The MD is assigned to users by the government and carried by users. It has an indicator light for the option indicating the user's health status with three colors: red, yellow, and green. The MD periodically updates and saves the UNames used in the past fortnight. LBTrace ensures that a user's personal ID information can't be compromised by others looking at his or her trail records by changing the user's anonymous information randomly. The MD receives and recognizes the WakeMessage sent by the FD and saves the RiskyList accompanying the WakeMessage. The MD then sends the present UName as a reply to the FD, and at the same time pulls all the UNames used in the past fortnight to match them with UNames in the RiskyList. If the match is successful, the infection risk level will be changed to risky (yellow light). Yellow light users need to go to the Diagnostician for a checkup according to the local law, and the Diagnostician can access all the UNames stored in the user's MD in the past fortnight. If a user is confirmed as a patient, the Diagnostician can change the risk level of infection of the user to infected (red light). If the user is determined to have no virus detected after examination, the Diagnostician can change the risk level of the user to no risk (green light).

4.1.5 LoRa Gateway

The GW is a device with strong computing ability in a fixed geographical location. It has a large receiving radius with the range of $7 \sim 9$ public buildings and can receive TraceMessages based on LoRa of $SF = 9$ and frequency band $CN470$ from FDs, and caches these records locally. The GW then signs each TraceRecord, processes it into a block, and uploads it to the Trace Blockchain.

4.1.6 Diagnostician

The Diagnostician diagnoses close contacts to determine if they are infected and has the right to change the color of the indicator light on users' MDs. The Diagnostician uses the patient's record to look up the UName information of the close contacts, and append these newly found UNames to the RiskyList. The RiskyList then will be downloaded by GWs and sent to FDs. The Diagnostician can manipulate

RiskyList in other ways, for example, they can remove UNames of the cured users from RiskyList as well.

At Diagnostician, the criteria for determining whether a user is risky can be adjusted, and this characteristic can be used to deal with different epidemic situations. And it doesn't require any modifications on the massive MDs side.

Moreover, the medical record system and LBTrace are separate and unrelated. In LBTrace, Diagnostician cannot obtain any identifying information of any undiagnosed user. It protects the users' privacy well.

4.2 Workflow of LBTrace

The workflow of LBTrace is shown in the Fig. 2, and we will introduce how each step works in details:

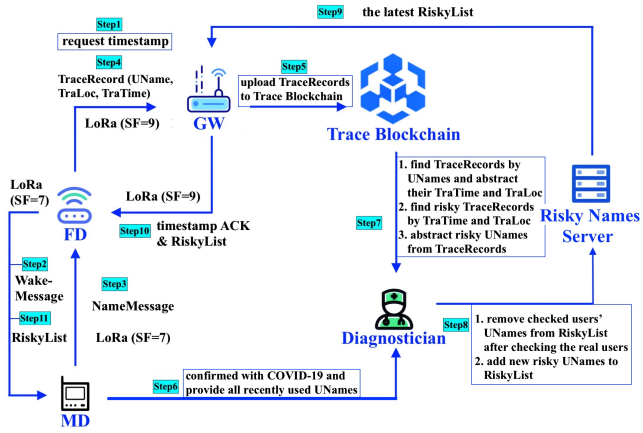

Fig. 2. Workflow of LBTrace

STEP 1: The FD runs a total of two processes: a process that receives and processes messages, and a process that sends messages. First, the FD sends a timestamp request periodically and continuously to the GW via the LoRa signal of $SF = 9$ and in the frequency band $CN470$ until it receives an ACK containing the current timestamp from the GW. Then it saves the received timestamp locally.

During the LBTrace deployment phase, a staff member in charge of the public place needs to carry an MD and send several special data packets to the FD at various locations in the interior, edge, and exterior of the building to quickly determine the acceptance range by Received Signal Strength Indication (RSSI) through logistic regression. This process only needs to be done once, so the cost is not significant.

STEP 2: The FD will broadcast WakeMessage based on LoRa signal of SF=7 and frequency band of CN470 periodically every $5s$ to wake up MDs. The period is set short to minimize omissions, and because the FD is cable-powered, there is no need to worry about its power consumption.

STEP 3: The MD runs four processes: a process that maintains pseudonyms, a process that sends messages, a process that receives and processes messages, and a process that controls its indicator light. The MDs automatically update the present pseudonym periodically in a random period of $2 \sim 4h$ and save the previous present pseudonym. The MD stores all UNames used in the past fortnight in the device, while others will be deleted.

When an MD enters the broadcast range of an FD, it will receive the WakeMessages sent by the FD and replies to a NameMessage. The NameMessage contains the user's 16-character UName string and a code identifying the type of sending device. MDs do not need to wait or receive ACK messages and will switches to the sleeping mode for $10min$ to minimize their energy consumption.

When the MD does not receive the WakeMessage, it will enter the listening mode for 5s every time it enters to finish the sleeping mode for 55s. The 5s listening mode time is to ensure that there is an opportunity for the MD to be detected because the FD broadcasts a WakeMessage every 5s.

STEP 4: The FD combines the time of receiving the NameMessage as TraTime, the UName, and the FD's geographic location as TraLoc, to form a new TraceRecord. It periodically sends unreported TraceRecords to the GW every $5s$ during the uploading period.

The TraceMessage includes a TraceRecord, the type code identifying the sending device, the code of the GW, and a 10-digit message sequence number. The FD uses the message sequence number to ensure the ACK message has been received, or it will resend the TraceMessage every $5s$.

STEP 5: The GW immediately returns an ACK message with the corresponding sequence number and stores the sequence number in its temporary blacklist for duplicate checking after receive TraceMessages based on LoRa of $SF = 9$ and band $CN470$ from FDs in a wider area.

The GW runs three processes: a process that maintains the Trace Blockchain, a process that receives and processes messages, and a process that sends messages. The GW connects LoRa communication and the Internet part of LBTrace, which also has the functions of verifying signatures and maintaining Trace Blockchain. The GW receives a TraceMessage from an FD, signs the TraceRecord with its private key, uploads it to the Trace Blockchain, and informs other GW devices. Eventually, in the Trace Blockchain, every block contains a TraceRecord, a GW code, a signature, the hash value of this block, the hash value of the previous block. Each GW stores and updates the public keys of all other networked GWs. Other GWs will verify the validity of new blocks notified and add them to the Trace Blockchain they maintain, otherwise discarding the invalid blocks. Blockchain technology can improve the reliability of contact tracing and avoid being tampered with or exploited by criminals.

STEP 6: When the user is diagnosed as an infected case, the Diagnostician has the permission to obtain all UNames that the user has used in the past fortnight and change the patient's MD indicator light to red.

STEP 7: The Diagnostician uses these patient's UNames to find all the TraceRecords of this patient in the Trace Blockchain. We regard a user who has the same TraLoc as the TraLoc of an infected patient and is generated within $1h$ after the TraTime of the infected patient's as close contacts (See Sec 5.2). These TraceRecordes are seen as risky TraceRecords.

STEP 8: The Diagnostician extracts the UNames of the risky TraceRecords and uploads them to the Risky Names Server to update the RiskyList.

STEP 9: The GW periodically updates its local RiskyList by accessing the Risky Names Server and getting the latest RiskyList by accessing the specific IP address and port, then

sends the latest RiskyList along with the ACK message to FDs.

STEP 10: The FD receives the RiskyList from GW by receiving ACK messages and sends it to MDs by broadcasting WakeMessages. FDs make no changes to the RiskyList.

STEP 11: The FD will send the RiskyList to MDs along with the WakeMessages, and the MDs will then match the RiskyList with all the UNames they have used in the past fortnight. If the match is successful, the indicator light color changes to yellow, which means this user is probably a close contact and need to be tested. Close contact means high risky rather than being infected, and it is up to the medical establishment to decide whether a user is infected in different countries. Additionally, when a patient is cured, the Diagnostician can change the user's MD's indicator light from red to green.

5 Experiment and Evaluation

5.1 Settings

To demonstrate the feasibility and practicability of LBTrace, we implemented a prototype system. As shown in Fig. 3(a), we use Pycom LoPy4 and Pycom ExpansionBoard 3.1 as both MD and FD, each is powered by a LiPo battery of 5000mAh. In practical application, the FDs are usually cable-powered. The antennas are Pycom 900MHz Antenna Kit. The size of our MD and FD device is 65*50*10mm, with an antenna of 15cm. But these are just our laboratory devices, which have a lot of other functions that have nothing to do with LoRa. If only the LoRa function and simple computing power are realized on the device, its size and cost will be much smaller. As shown in Fig. 3(b), we use Pycom LoPy4 and Pycom PyGate connected to a MacBook Pro 2018 A1989 as the GW. In the GW, the Pycom devices are wired to the MacBook. The communication between MDs/FDs and FDs/GWs is through the raw LoRa signal of frequency band CN470, and the communication between GWs is through the Internet. The PC part of GW is installed with the program related to the operation of the Blockchain, which plays the role of maintaining the Trace Blockchain.

The PC part of the GW can display the block addition information of the Trace Blockchain. We run the Risky Names Server on Tencent Cloud Server, and set up a special IP address and port for each GW to access and obtain the RiskyList, and a special port for Diagnosticians to modify the RiskyList. We use a laptop as a Diagnostician that can add and remove UNames to the RiskyList.

(a) Mobile Device and Fixed Device (b) Gateway

Fig. 3. Devices used in LBTrace

As shown in Fig. 4, our experiment was conducted in the teaching buildings on our campus. There are three buildings A, B, and C, all of which are concrete buildings with an average wall thickness of about $0.5m$. In the experiment, MDs were all held by volunteers, and each volunteer walked randomly within the designated area of the building, as shown in Fig. 5.

Fig. 4. The buildings and surroundings in which we conduct our experiments

Fig. 5. Volunteers held MDs and walked randomly in designated areas

To save the test time and increase the number of tests, we speeded up the working frequency of the devices in proportion, which does not affect the accuracy of the experiment. While Experiment 5 is configured according to the actual working frequency of our designation. We increased the frequency at which FDs send WakeMessages, the frequency at which FDs upload TraceRecords, and the rate at which GW uploads TraceRecords to the Trace Blockchain, and reduced the sleeping mode time of MDs.

Moreover, in these experiments, we added a prefix that can be used to identify MDs in the randomly generated UName to distinguish the MDs corresponding to each TraceRecord. In this way, we can calculate the packet loss rate (PLR) of different MDs and figure out the relationship between the PLR of MDs and the distance, location, obstacles, and the number of concurrent devices. In practice, however, prefixes are not used to ensure that the users are completely anonymous. Working frequency configuration for each experiment as well as practical application is shown in Table 2.

No.	A	B	C	D	E
c(FD_wakeup)	5s	5s	2s	2s	5s
c(FD_upload)	5s	5s	2s	2s	5s
c(MD_sleep)	5s	5s	4min	4min	10min
♯ of packets	300	50∼200 (interval: 25)	400	360	-

TABLE 2
Working frequency configuration for each experiment and practical application

We determine the effectiveness of LBTrace by evaluating packet loss rate and response time. LBTrace highly depends on the data interaction between MDs and FDs to determine the situation of personnel visits, so the performance of LBTrace is closely dependent on the reception rate of packet transmission.

Therefore, in Experiment A to Experiment D, we calculated the packet loss rate under different circumstances. In Experiment E, we measured the reaction speed.

5.2 How to Define the Close Contacts in LBTrace

As mentioned above, the definition of close contact is changing [45] as the virus continues to mutate, from the early days

of very close direct human contact to the present day when being present in the same space across several days, or have used the same object may be defined as a close contact. The definition of it may vary in different regions, at different periods, and under different conditions, so it is a parameter that can be flexibly adjusted considering the reliability of prevention and the scope of impact on the population. It should be noted that the definition of close contacts does not affect the use of the method proposed in this paper, but will only produce different results depending on the expectations of the managers. In this paper, we only provide what we believe to be a more balanced calculation.

We fisrt define a visit record of a user is $R(P, t_{start}, t_{end})$. For any P_i, the first and last continuously recorded time stamps are $t_{i\_start'}$ and $t_{i\_end'}$, continuous record means that there is no other P_j record in the time period $t_{i\_start'}$ and $t_{i\_end'}$, where $t_{i\_start} = t_{i\_start'} - \Delta t$ and $t_{i\_end} = t_{i\_end'} + \Delta t$ are with the consideration of that the patient may enter and exit P between the two exchange of information windows Δt between MD and FD. We assume that all public places visited by a diagnosed patient m in the past fortnight is $P_m = \{P_1, P_2, \cdots\}$. When tracing the close contacts of the patient m, all R satisfying $P \in P_m, t_{m\_start} < t_{start} < t_{m\_end} + 1h$ or $P \in P_m, t_{m\_start} < t_{end} < t_{m\_end} + 1h$ will be regarded a risky record and added into the RiskyList.

In this subsection, we have only introduced time and location-related close contact determination rules, in fact, a TraceRecord in LBTrace also contains changing Unames which has been discussed earlier in Sec. 4.1.

5.3 Experiment

5.3.1 Experiment A

In experiment A, we used a single MD and a single FD. This experiment is designed to test whether the basic communication function between MDs and FDs in LBTrace can be persistent and stable. The GW and FD are located in the center on the 2nd floor of building A. We ask a volunteer to carry the MD and walk around the building at will on the 1st, 2nd, and 3rd floors. Every time, the FD sends one WakeMessage every 5s for a total of 300 WakeMessages. The frequency of uploading TraceRecord from FDs is every 5s one record. The sleeping period of MDs should be 10min, but we are using a limited number of MDs to simulate a large number of MDs, so we set the sleeping period of MDs to be equal to the wakeup interval of FDs, which is 5s. And each MD can be woken up an unlimited number of times.

Ideally, the Trace Blockchain should end up with 300 blocks. The experiment was repeated 30 times, and the experimental results showed that there were 283 blocks on average in the Trace Blockchain, and the average PLR is 5.7%. The PLR is relatively high, but normally a person stays in a building for average 30 minutes so that the MD will upload information repeatedly within each duration of stay. The repetition can greatly reduce the probability of omission. This will be explained in detail later.

5.3.2 Experiment B

Before this experiment, we used LoRaSim to simulate multiple LoRa APs working concurrently to get the relationship between the packet loss rate and the number of LoRa APs. We simulated 100 to 500 LoRa APs working concurrently with the step size of 20, and get each data extraction rate (DER). DER means the percentage of LoRa packets that are successfully received. The result is shown in Fig. 6. As we can see from the resulting line chart, as the number of concurrently working LoRa APs increases, DER decreases approximately linearly. But when the number of concurrently working LoRa APs reaches 500, the DER is still over 97%, which means a very low PLR. For LBTrace, 500 MDs working concurrently on a single site is quite sufficient. Therefore, the result of the LoRaSim simulation supports our Experiment B to obtain the relationship between the number of concurrent MDs and the PLR.

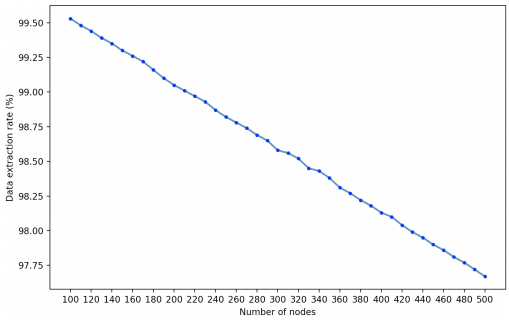

Fig. 6. Relationship between DER and number of concurrent LoRa APs

We used multiple MDs and a single FD. This experiment is designed to obtain the relationship between the number of concurrent MDs and the PLR, to obtain the number of concurrent MDs that can be supported by a single FD when the PLR is low. We did it 10 times with 7 groups, using 2, 3, 4, 5, 6, 7, and 8 MDs, respectively. The GW and FDs are also located in the center of the $2nd$ floor of building A. Then all MDs were started within $2s$, and the areas of movement of all MDs in each experiment was in area 1 as shown in Fig. 7. The FD sends a WakeMessage every 5s, and the number of times of broadcasting WakeMessages is unlimited. FDs upload TraceRecords every 5s. The sleeping period of MDs should be 10min, but we are using a limited number of MDs to simulate a large number of MDs, so we set the sleeping period of MDs to be equal to the wakeup interval of FDs, which is 5s. And each MD can be awakened 25 times. The volunteers walked randomly in the designated area. Ideally, the Trace Blockchain should end up with 50, 75, 100, 125, 150, 175, 200 blocks, respectively. The experimental results are shown in Fig 8. As can be seen from the line chart, the PLR increases with the increase of the number of MDs working concurrently, showing an 'S' shape on the whole. When the number of concurrent MDs exceeds 5, the PLR increases slowly.

In Experiment 2, the FD sends a WakeMessage every 5s, and the sleeping period of MDs is reduced to 5s. The reduced sleeping period of MDs can simulate a large number of MDs working concurrently. Due to the performance limitation of the MDs, the PLR of the experimental results should be higher than that of the actual application. Assuming that everyone stays in a building for $30min$, in Experiment 2, taking 8 MDs send messages concurrently working as an example, the experimental result is that the PLR is 14.5%, the FD woke up 8 MDs every 5s, and the

Fig. 7. Active areas on the 2nd floor of Building A

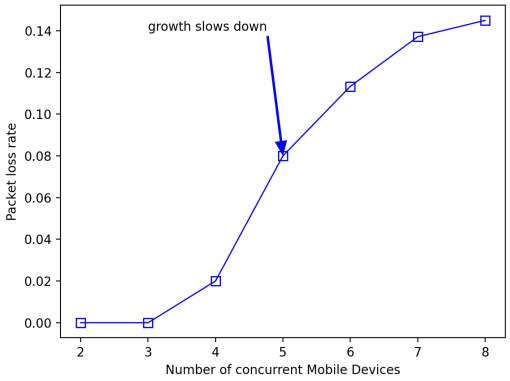

Fig. 8. Relationship between PLR and number of concurrent MDs

sleeping period of MDs should be 10min which is much longer than 5s. Since each person will stay for 30min, each MD will be woken up at least three times. That is, among the 8 MDs each time they are awakened, there are three situations, the first awakening, the second awakening, and the third awakening. It can be assumed that there are 2.7 MDs in each situation, that is, after each wake-up cycle of FD, 2.7 new MDs join, and 2.7 MDs will exit after this wake-up. Since the MD sleeps for 10min each time, the FD can wake up 120 times in each MD sleeping period, which means 324 (2.7*120) new MDs can join. With each MD staying for an average of three sleeping periods, an FD can support 972 (324*3) MDs on-site at the same time. We define that an MD is ignored as all three NameMessages sent by this MD are lost during these three wake-up cycles. The probability that all the three NameMessages sent by one MD will be lost at all within this 30min is $(14.5\%)^3 \approx 0.3048\%$. That is to say, in Experiment 2, an FD can support at most about 972 users in the building, with the probability of ignoring a user equals 0.3048%. Moreover, in practical applications, the working frequency of all MDs is lower, so, an FD can support more users present at the same time. It can be concluded that the relationship between the number of concurrent MDs N and the maximum number of users supported in the building M is $M = \frac{N}{3} * 120 * 3 = 120N$. According to this formula and the results of Experiment 2, we can calculate the number of users present at the same time that an FD can support under the conditions of other lower PLR as shown in Table 3, where P are the probability that a mobile device will not be detected at all within 30 minutes. The relationship between PLR and P is $P = (PLR)^3$. We define that when the FD is at full load, the number of users who may not be detected at all

N	2	3	4	5	6	7	8
$PLR(\%)$	0	0	2	8	11.3	13.7	14.5
M	240	360	480	600	720	840	960
$P(\%)^*$	0	0	0.0008	0.0512	0.1443	0.2571	0.3048
R	0	0	0.0038	0.3072	1.0390	2.1596	2.9260

TABLE 3
Several key parameters to measure LBTrace performance

within $30min$ as R. The relationship between R and M is $R = M * P$ and is shown in Fig. 9. With the increase of the number of users in the building, the number of users who are not detected will increase and the growth rate will increase as well. But when the number of users inside a building is less than 600, the minimum rate of omission can be less than 0.06%. The 8 MDs in our experiment simulated 972 devices by reducing the sleep period, not 8. Moreover, the disadvantage of the high average packet loss rate in a single packet transmission can be made up by multiple packet transmissions, for example, each MD sends once every 10min within 30min in the experiment. As long as any packet sent by an MD is received within 30 minutes or longer, it is successful.

As mentioned earlier, LBTrace is a way to complement existing methods. Based on our experiments and the cheap devices we used, LBTrace can support around 600 people at a time. Therefore, if combined with other existing contact tracing methods, contact tracing coverage can be improved to a greater extent, and omissions can be reduced to improve efficiency. Also because it is a complementary way, high concurrency and collision occur only in rare cases, and the capacity of 600 people is enough for detecting the vulnerable groups (such as the elderly and children). In addition, we can also make up for the shortcoming of the higher packet loss rate of single high concurrent detection by multiple detections.

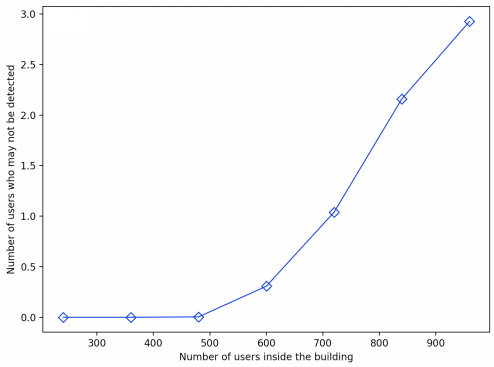

Fig. 9. Relationship between the number of users R who may not be detected when the FD is fully loaded and the number of users inside the building M.

5.3.3 Experiment C

In experiment C, we used 8 MDs and a single FD. This experiment is designed to obtain the relationship between the environmental conditions and LBTrace's performance, and obtain the ideal layout environment. The GW and FD are both located in the center on the 2nd floor of building A. Then we started all MDs one after another at

an interval of 10s, and the areas' distribution of each MD is shown in Fig. 7. Areas 1, 2, and 3 are corridor areas without any obstacles, while areas 4, 5, 6, 7, and 8 are indoor areas with concrete walls and stairs. The FD sends one WakeMessage every 2s, and the number of times of broadcasting WakeMessages is unlimited. The FD uploads TraceRecords every 2s one record. The sleeping period of MDs is 4min, and each MD can be awakened 50 times. Eight volunteers walked randomly in their designated areas. Ideally, the Trace Blockchain should end up with 400 blocks. The experimental results are shown in Fig. 10 as a 3D scatter plot. The meaning of the distance coordinate axis is the distance between the FD and area centers in meters. As can be seen from Fig. 10: in areas 1, 2, and 3, in the case of no obstacles, the PLR is close to 0, while in areas 4, 5, 6, 7, and 8, the PLR increases with the increase of the distance and obstacles but is more affected by obstacles. The maximum value is in area 7, which is 14%, but it is still a low value according to the conclusion of experiment C. Therefore, FD is more suitable to be placed in the empty hall or corridor.

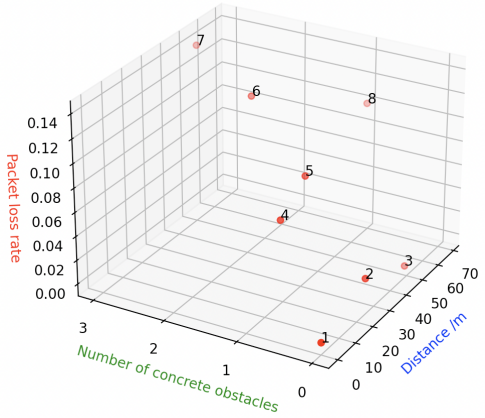

Fig. 10. Relationship between PLR and regional location

5.3.4 Experiment D

In experiment D, we used multiple MDs and multiple FDs. This experiment is designed to simulate the work of LBTrace in the real environment and test its performance. First, we started up and configured the GW and 3 FDs. The GW is placed in the center of these three buildings. The 3 FDs are located respectively in the center of the 2nd floor of building A, B, and C. Then, we started 2 MDs in building A, B, and C at an interval of 10s. In each building, there are 2 volunteers moving randomly on the 1st and 2nd floor. The FDs send one WakeMessage every 2s, and the number of times of broadcasting WakeMessages is unlimited. FDs upload TraceRecords every 2s one record. The sleeping period of MDs is 4min, and each MD can be awakened 60 times. Ideally, the Trace Blockchain will end up with 360 blocks. The experimental results show that there is an average of 314 blocks in the Trace Blockchain, so the PLR is 12.8%. Assuming that every person stays in a building for 30min, the omission probability is 0.2097%. So, the system has a very low omission probability, which means our prototype system implemented on Pycom devices has achieved a very reliable performance.

5.3.5 Experiment E

This experiment is to measure the average time interval between the Diagnostician inputting a UName to the RiskyList and the corresponding MD changing its indicator light color. Based on the geographical distribution in experiment D, we configured each experimental device according to the working frequency in the practical application. Each time, we randomly selected a UName in one of the TraceRecords in the Trace Blockchain and added the UName to the RiskyList through the Diagnostician's program. This experiment was repeated 40 times and the average time interval was calculated. The results show that the average response time was 22.0min, meaning the MD was able to respond to the updated RiskyList after a second or third wake-up.

Given the results of Experiments A, B, and C, it can be seen that the LBTrace has a very low PLR when each FD corresponds to a small number of concurrent MDs. As the number of MDs working concurrently corresponding to each FD increases from 2 to 8, the PLR starts to increase, but it is less than 15%. Moreover, as the location of the MD is closer to the edge of the building of the FD, the PLR is higher. The reason is that the RSSI value of the LoRa signal sent by the MD at the edge is close to the critical value detected by the FD, and is sometimes counted as out of range.

5.4 Analysis on Tracing Effectiveness and Energy Consumption

Taking the COVID-19 epidemic model as an example, in countries with strong outbreak preparedness, such as the Chinese mainland at the beginning of 2020, the average infected-suspected ratio is 2.399 [14], namely one person will most likely infect 2.399 other people, and those 2.399 people will each go on to infect 2.399 more people and so forth. Referring to the results of experiment B, assuming that each person stays in a building for 30min and there are about 600 people in the building at the same time, the probability of someone being completely ignored is 0.0512%. If one virus carrier is initially in a building, then the probability of someone being undetected among all the virus carriers after an infection is: $1-(1-0.000512)^{(1+2.399)} \approx 0.1739\%$, which is extremely low.

In this project, we take the Pycom device as an example. As an MD, its battery life is very long. LoPy4's working current is 15mA in active mode and 1μA in standby. As described in Step2 of the workflow of LBTrace, when in the state of undetected, the working cycle of MD can be divided into 5s listening mode and 55s sleeping mode. And when in the state of detected, it can be divided into 5s listening mode, 2s sending a NameMessage, and 10min sleeping mode.

In the state of undetected, the MD only needs to alternate between listening and sleeping modes. In this state, the power consumption per hour is $(15*5+0.001*55)*60/60^2 \approx 1.2509mAh$. So the power consumption per day is about 30.0216mAh. In this state, the MD will work for up to about 166.5 days on a 5000mAh LiPo battery.

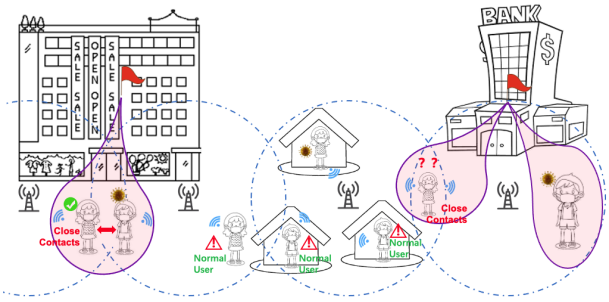

Fig. 11. Some possible misjudgment situations

For the detected state mixed with undetected state, we assume that everyone works 8 hours a day. In other words, the user is always in the public place and the MD is always in the cycle of listening-sending-sleeping during the 8h period. At other times, the user is in a non-public place and the MD is undetected mentioned earlier. The power consumption during the 8h working time is $[(600-2)*0.001+2*15]*6*8/60^2 \approx 0.4080mAh$. In the rest of the time, the power consumption is about 20.0144mAh. So, the power consumption for the whole day is about $0.4080 + 20.0144 = 20.4224mAh$. In this mixed state, the MD will work for up to about 244.8 days on a 5000mAh LiPo battery. This charging frequency is very convenient for users. The device we use is an all-in-one IoT device, and if it is on a more specialized device, the energy consumption becomes even lower.

6 Conclusion and Discussion

This paper proposes LBTrace, a novel contact tracing method based on LoRa and Blockchain, we took contact tracing off the hook of smartphones and enabled off-internet people, even objects, involved. We used LoRa to achieve long-range contactless recording of user visits during the pandemic. We addressed single points of failure, data falsification and tampering, and user privacy issues with distributed Blockchain. We tested our prototype system in the teaching buildings on our campus, and the experimental results proved that LBTrace has the characteristics of low power consumption, low cost, portability, easy popularization, high reliability, good security, and strong traceability. We believe LBTrace could be a good refinement to the current approach and play an important role in daily epidemic control and emergency lockdown.

We are now developing a website for LBTrace to query the trace records of users, with the function of generating a trace report. We also try to provide a website where the entire blockchain data can be accessed and reviewed. We are working to advance its application to practical COVID-19 and future pandemics control on our campus.

During the experiment, we found that although LBTrace solves the problem of contact tracing well, there are still some points that can be improved, such as the battery-free user device (backscatter), how to minimize false positives due to the nature of wireless signal propagation as shown in Fig. 11, and insufficient single-hop transmission distance problem. We will leave them for our future work.

References

[1] "World Health Organization. coronavirus disease (covid-19) pandemic," [EB/OL], https://www.who.int/emergencies/diseases/novel-coronavirus-2019?

[2] D. M. Morens and A. S. Fauci, "Emerging pandemic diseases: How we got to covid-19," *Cell*, 2020.

[3] T. P. Velavan and C. G. Meyer, "The covid-19 epidemic," *Tropical medicine & international health*, vol. 25, no. 3, p. 278, 2020.

[4] "World Health Organization. contact tracing," [EB/OL], https://www.who.int/news-room/q-a-detail/contact-tracing.

[5] L. Ferretti, C. Wymant, M. Kendall, L. Zhao, A. Nurtay, L. Abeler-Dörner, M. Parker, D. Bonsall, and C. Fraser, "Quantifying sars-cov-2 transmission suggests epidemic control with digital contact tracing," *Science*, vol. 368, no. 6491, 2020.

[6] L. Bai, D. Yang, X. Wang, L. Tong, X. Zhu, N. Zhong, C. Bai, C. A. Powell, R. Chen, J. Zhou *et al.*, "Chinese experts' consensus on the internet of things-aided diagnosis and treatment of coronavirus disease 2019 (covid-19)," *Clinical eHealth*, vol. 3, pp. 7–15, 2020.

[7] M. Zhang, J. Xiao, A. Deng, Y. Zhang, Y. Zhuang, T. Hu, J. Li, H. Tu, B. Li, Y. Zhou *et al.*, "Transmission dynamics of an outbreak of the covid-19 delta variant b. 1.617. 2—guangdong province, china, may–june 2021," *China CDC Wkly*, vol. 3, pp. 584–586, 2021.

[8] "Exposure notifications: Using technology to help public health authorities fight covid-19," [EB/OL], https://www.google.com/covid19/exposurenotifications/.

[9] "Privacy-preserving contact tracing," [EB/OL], https://covid19.apple.com/contacttracing.

[10] "Wikipedia. global internet usage," [EB/OL], https://en.wikipedia.org/wiki/Global_Interne_usage.

[11] "World Health Organization. tracking sars-cov-2 variants," [EB/OL], https://www.who.int/en/activities/tracking-SARS-CoV-2-variants/.

[12] "Microsoft Azure. iot signals report," [EB/OL], https://azure.microsoft.com/en-us/resources/iot-signals/.

[13] M. C. Bor, U. Roedig, T. Voigt, and J. M. Alonso, "Do lora low-power wide-area networks scale?" in *Proceedings of the 19th ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems*, 2016, pp. 59–67.

[14] F. B. Hamzah, C. Lau, H. Nazri, D. Ligot, G. Lee, C. Tan, M. Shaib, U. Zaidon, A. Abdullah, M. Chung *et al.*, "Coronatracker: world-wide covid-19 outbreak data analysis and prediction," *Bull World Health Organ*, vol. 1, no. 32, 2020.

[15] H.-Y. Cheng, S.-W. Jian, D.-P. Liu, T.-C. Ng, W.-T. Huang, H.-H. Lin *et al.*, "Contact tracing assessment of covid-19 transmission dynamics in taiwan and risk at different exposure periods before and after symptom onset," *JAMA internal medicine*, vol. 180, no. 9, pp. 1156–1163, 2020.

[16] R. R. Lash, C. V. Donovan, A. T. Fleischauer, Z. S. Moore, G. Harris, S. Hayes, M. Sullivan, A. Wilburn, J. Ong, D. Wright *et al.*, "Covid-19 contact tracing in two counties—north carolina, june–july 2020," *Morbidity and Mortality Weekly Report*, vol. 69, no. 38, p. 1360, 2020.

[17] R. A. Kleinman and C. Merkel, "Digital contact tracing for covid-19," *CMAJ*, vol. 192, no. 24, pp. E653–E656, 2020.

[18] J. Morley, J. Cowls, M. Taddeo, and L. Floridi, "Ethical guidelines for covid-19 tracing apps," 2020.

[19] N. Ahmed, R. A. Michelin, W. Xue, S. Ruj, R. Malaney, S. S. Kanhere, A. Seneviratne, W. Hu, H. Janicke, and S. K. Jha, "A survey of covid-19 contact tracing apps," *IEEE Access*, vol. 8, pp. 134 577–134 601, 2020.

[20] J. Li and X. Guo, "Covid-19 contact-tracing apps: A survey on the global deployment and challenges," *arXiv preprint arXiv:2005.03599*, 2020.

[21] L. Reichert, S. Brack, and B. Scheuermann, "Privacy-preserving contact tracing of covid-19 patients." *IACR Cryptol. ePrint Arch.*, vol. 2020, p. 375, 2020.

[22] Y. Bengio, R. Janda, Y. W. Yu, D. Ippolito, M. Jarvie, D. Pilat, B. Struck, S. Krastev, and A. Sharma, "The need for privacy with public digital contact tracing during the covid-19 pandemic," *The Lancet Digital Health*, vol. 2, no. 7, pp. e342–e344, 2020.

[23] H. Stevens and M. B. Haines, "Tracetogether: pandemic response, democracy, and technology," *East Asian Science, Technology and Society: An International Journal*, vol. 14, no. 3, pp. 523–532, 2020.

[24] D. Watts, "Covidsafe, australia's digital contact tracing app: the legal issues," *Australia's Digital Contact Tracing App: The Legal Issues (May 2, 2020)*, 2020.

[25] "General Office of the State Council of China. integrated service for epidemic prevention and health information codes," [EB/OL], http://gjzwfw.www.gov.cn/col/col641/index.html.

[26] J. Chan, S. Gollakota, E. Horvitz, J. Jaeger, S. Kakade, T. Kohno, J. Langford, J. Larson, S. Singanamalla, J. Sunshine *et al.*, "Pact: Privacy sensitive protocols and mechanisms for mobile contact tracing," *arXiv preprint arXiv:2004.03544*, 2020.

[27] C. Castelluccia, N. Bielova, A. Boutet, M. Cunche, C. Lauradoux, D. L. Métayer, and V. Roca, "Desire: A third way for a european exposure notification system leveraging the best of centralized and decentralized systems," *arXiv preprint arXiv:2008.01621*, 2020.

[28] N. Trieu, K. Shehata, P. Saxena, R. Shokri, and D. Song, "Epione: Lightweight contact tracing with strong privacy," *arXiv preprint arXiv:2004.13293*, 2020.

[29] A. Trivedi, C. Zakaria, R. Balan, A. Becker, G. Corey, and P. Shenoy, "Wifitrace: Network-based contact tracing for infectious diseases using passive wifi sensing," *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, vol. 5, no. 1, pp. 1–26, 2021.

[30] "Chloe Kent. covid-19: digital contact tracing for those without smartphones," [EB/OL], https://www.medicaldevice-network.com/features/covid-19-contact-tracing-app/.

[31] G. Kampf, D. Todt, S. Pfaender, and E. Steinmann, "Persistence of coronaviruses on inanimate surfaces and their inactivation with biocidal agents," *Journal of hospital infection*, vol. 104, no. 3, pp. 246–251, 2020.

[32] R. Sanchez-Iborra, J. Sanchez-Gomez, J. Ballesta-Viñas, M.-D. Cano, and A. F. Skarmeta, "Performance evaluation of lora considering scenario conditions," *Sensors*, vol. 18, no. 3, p. 772, 2018.

[33] R. S. Sinha, Y. Wei, and S.-H. Hwang, "A survey on lpwa technology: Lora and nb-iot," *Ict Express*, vol. 3, no. 1, pp. 14–21, 2017.

[34] H. T. Reda, P. T. Daely, J. Kharel, and S. Y. Shin, "On the application of iot: Meteorological information display system based on lora wireless communication," *IETE Technical Review*, vol. 35, no. 3, pp. 256–265, 2018.

[35] R. Salazar-Cabrera, Á. Pachón de la Cruz, and J. M. Madrid Molina, "Proof of concept of an iot-based public vehicle tracking system, using lora (long range) and intelligent transportation system (its) services," *Journal of Computer Networks and Communications*, vol. 2019, 2019.

[36] E. D. Ayele, C. Hakkenberg, J. P. Meijers, K. Zhang, N. Meratnia, and P. J. Havinga, "Performance analysis of lora radio for an indoor iot applications," in *2017 International Conference on Internet of Things for the Global Community (IoTGC)*. IEEE, 2017, pp. 1–8.

[37] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Manubot, Tech. Rep., 2019.

[38] Z. Xiong, Y. Zhang, D. Niyato, P. Wang, and Z. Han, "When mobile blockchain meets edge computing," *IEEE Communications Magazine*, vol. 56, no. 8, pp. 33–39, 2018.

[39] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with iot. challenges and opportunities," *Future generation computer systems*, vol. 88, pp. 173–190, 2018.

[40] H. Xu, L. Zhang, O. Onireti, Y. Fang, W. J. Buchanan, and M. A. Imran, "Beeptrace: blockchain-enabled privacy-preserving contact tracing for covid-19 pandemic and beyond," *IEEE Internet of Things Journal*, 2020.

[41] W. Lv, S. Wu, C. Jiang, Y. Cui, X. Qiu, and Y. Zhang, "Decentralized blockchain for privacy-preserving large-scale contact tracing," *arXiv preprint arXiv:2007.00894*, 2020.

[42] M. M. Arifeen, A. Al Mamun, M. S. Kaiser, and M. Mahmud, "Blockchain-enable contact tracing for preserving user privacy during covid-19 outbreak," 2020.

[43] K. Croman, C. Decker, I. Eyal, A. E. Gencer, A. Juels, A. Kosba, A. Miller, P. Saxena, E. Shi, E. G. Sirer *et al.*, "On scaling decentralized blockchains," in *International conference on financial cryptography and data security*. Springer, 2016, pp. 106–125.

[44] J. Fang, Z. Qin, L. Wang, B. Lu, M. Zhu, and Z. Wang, "Chinese Patent. a low-power ocean sensing data return method," 2021.

[45] "Global Times. expand examination scope, swift identification of transmission route… zhong nanshan talks about china's success in dealing with delta variant," [EB/OL], https://www.globaltimes.cn/page/202106/1227196.shtml.

Jian Fang received the B.S. and M.S. degree in software engineering from Dalian University of Technology in 2015 and 2017, respectively. Now he is Ph.D candidate in the School of Software, Dalian University of Technology. His current research interests include wireless network, mobile computing, LPWAN, and Internet of Things.

Wenbo Zhao received the B.S. degree from Dalian University of Technology in 2021. Now he is a Master of Computer Science candidate in Rice University. His current research interests include wireless network, LPWAN, and Internet of Things.

Lei Wang is currently a full professor of the School of Software, Dalian University of Technology, China. He received his B.S., M.S., and Ph.D. from Tianjin University, China, in 1995, 1998, and 2001, respectively. His research interests involve wireless ad hoc networks, sensor networks, social networks, and network security. He is a member of the IEEE, ACM and a senior member of the China Computer Federation (CCF).

Zhenquan Qin received the B.S. degree and the Ph.D. degree from University of Science and Technology of China in 2002 and 2007, respectively. Now he is an associate professor in the School of Software, Dalian University of Technology. His current research interests include unmanned aerial vehicle communications, cross-layer network optimization, and Internet of Things.

Bingxian Lu is currently an assistant professor of the School of Software, Dalian University of Technology, China. He received his B.S., M.E., and Ph.D. in 2012, 2014, and 2019 both from Dalian University of Technology. His research interests include wireless network, mobile computing, and pervasive computing applications. He is a member of the IEEE and ACM.