SciencePG
Science Publishing Group

Bluetooth Text Messages Integrity Security (BTMIS) Based on Blockchain

Raed Rasheed, Raed Bulbul, Mohammad Mikki

Faculty of Engineering, Islamic University of Gaza, Gaza, Palestine

Email address:
rrasheed@iugaza.edu.ps (R. Rasheed), rbolbol@iugaza.edu.ps (R. Bulbul), mmikki@iugaza.edu.ps (M. Mikki)

Abstract: Bluetooth is one of the wireless technologies that users connect with one another through at a higher rate than with any other method when they are in close proximity to one another. This type of communication channel is susceptible to a variety of attacks, including Man-In-The-Middle (MITM) attacks and others of their ilk. On the other hand, live chatting has swiftly emerged as the most well-liked mode of text-based communication all over the world. As a consequence of this reality, one of the most significant challenges presented by wireless networks is preserving the authenticity of the data. It is not feasible to determine with absolute certainty whether or not malicious applications are capable of modifying older text that is preserved in a mobile database. This article presents a solution to the challenge of assuring the authenticity of Bluetooth text messages that is based on a distributed ledger technology (blockchain). The problem-solving strategy can be partitioned into two distinct parts. The first possibility involves sending and receiving text messages in real time using the Bluetooth channel of communication. The second type of distributed ledger is a hashing messages distributed ledger, which is based on blockchain technology and saves a hash of each and every message that is stored in the device database. This form of distributed ledger is a sort of distributed ledger for hashing messages.

Keywords: Bluetooth, Blockchain, Text Messaging, Live Chatting

1. Introduction

Bluetooth technology is short-range radio link technology allows neighbor users to exchange data between each other. It is the most wireless technology used in proximity range for digital contact tracing apps [1]. This reflected in the low price, low of power [2] and ease of control and invisible distance limitations. Bluetooth is integrated into mobile devices platforms such as Android and iOS. Meanwhile live chatting is used to connect people it helps to communicate with each other. If those people are beside each other they can exchange text messages without accessing internet, all they want to do use Bluetooth for that purpose. No license needed to Bluetooth operating frequency band simply when Bluetooth turned on it search for another Bluetooth devices then sends signals [3]. Finally, blockchain is a list of blocks holds a data list of transaction records in public database called ledger [4].

We will describe all terms used for this research in the next sub sections:

A. Bluetooth Technology

Bluetooth is the alternative choice to data cables for exchanging data with radio waves. It is designed for connecting portable or fixed electronic devices. The rage it can coverage is about ten to twenty meters length. Mainly Bluetooth connection used for Personal Area Networks (PANs) [5]. In 1994 Bluetooth originated when Ericsson began replacing the cables that connect accessories to mobile phones with wireless connections [2]. There are several forms of Bluetooth connection Point-to-Point, Piconet Network, and Ad-hoc or Scatternet Network [5]. The Point-to-Point Bluetooth connection enable two devices to connect each other. While in the Piconet Network Bluetooth connection forms a small personal area network called Piconet which consists of a master and at most seven active slaves [5]. As shown in Figure 1 it is illustrates Bluetooth Piconet Network connection in manner of one master device with several slave devices. The last form of the Bluetooth connection is Ad-hoc or Scatternet Network in which two or more Piconet Network connected to each other using one of the bridge slaves.
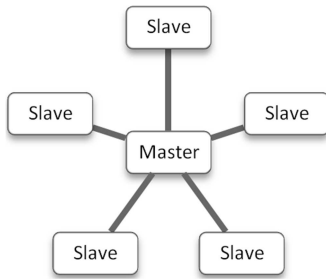
Figure 1. *Bluetooth piconet network.*

Figure 2 depicts how two Piconet Network connected to form new network called Scatternet Network.
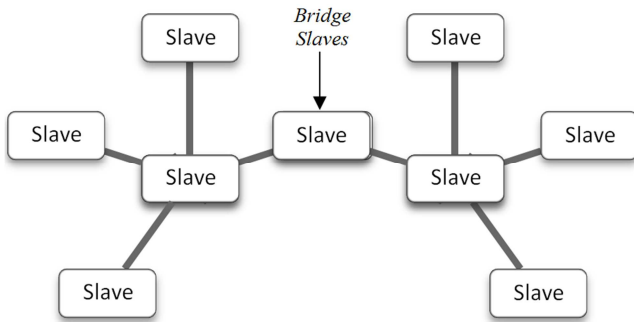

Figure 2. *Bluetooth scatternet network.*

B. Bluetooth Security Threats

In wireless networks security the main concerns are about preventing attacks and the protection of the main three security services confidentiality, integrity and authentication. Several attacks can be performed in Bluetooth communication such as Man-in-the-Middle (MITH), PIN cracking Attack, Blue jacking Attack, Blue snarfing Attack, and Denial of service Attack [5].

Man-in-the-Middle (MITM): when two devices exchange messages each other a third unauthorized person can read and rewrite their messages.

PIN cracking Attack: attacker sniffing the address of the targeted device. Then try to guess PIN to get the access of another device.

Blue jacking Attack: by sending unsolicited messages trick user into using an access code then enabled to access victim files.

Blue snarfing Attack: stealing the data stored in mobile memory and the attacker can use Bluetooth tool to transfer files.

Denial of service Attack: sending flood of requests to the victim trying to restrict networks accessibility.

C. Blockchain

In 2008, Satoshi Nakamoto shows the first use of blockchain by presenting a peer-to-peer cash system with cryptography-based distributed ledger [6, 7]. This ledger contains all transactions that done by the system users [8]. Blockchain have many different types according to its consensus mechanism such as Public, Private and Consortium blockchain. Public blockchains are open source, and it permits anybody to join as clients or network individuals. Private blockchain or permissioned blockchains which membership approval is required to join in the network [9]. Consortium blockchain is a hybrid blockchain in which two or more organizations govern the blockchain. It's not a public blockchain rather a permissioned blockchain.

Blockchain used the cryptography to create the sequence of blocks each related to the previous one building the blockchain ledger. This ledger contains all transactions that done by the system users [10]. The structure of blockchain is constructed of blocks that linked each other by storing the hash of the previous block. Each block contains four parts [11] the first part is the block size with four bytes used for storing the size of the block. The second part is the block header which consists of several field: version, previous block hash, merkle root hash, timestamp, difficulty target, and nonce. The third part is the transaction counter, and finally the transactions recorded in this block Figure 3 depicts the block structure.

Blocks of blockchain connected to each other using the hash of the previous block hash. Initially, the blockchain creates the genesis block with zero value of previous block hash field. For each block created the hash of the previous block stored in the new block header as previous block hash. This leads to create a chain of blocks each new block point to its previous block. Figure 4 depicts the basic structure of blockchain where there no previous hash for the block_0 (genesis block) and how the block_1 store the hash of whole block_0 in the previous hash field and so forth.
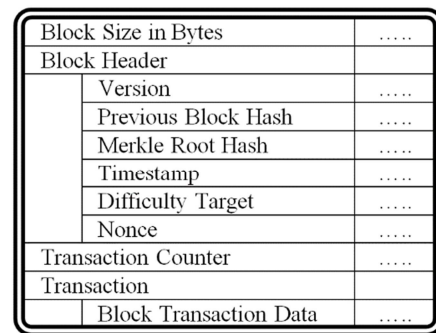
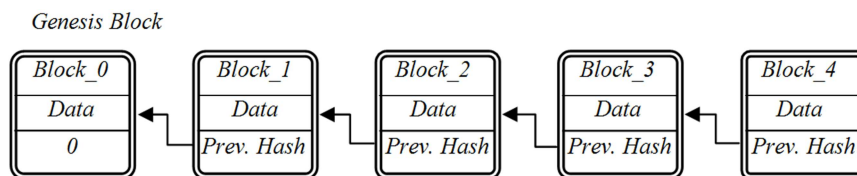| Block Size in Bytes	…..
Block Header	
Version	…..
Previous Block Hash	…..
Merkle Root Hash	…..
Timestamp	…..
Difficulty Target	…..
Nonce	…..
Transaction Counter	…..
Transaction	
Block Transaction Data	…..

Figure 3. *Blockchain block structure.*

Figure 4. *Basic Blockchain structure.*

The main advantage of blockchain use is the protecting of the data integrity in which any tiny change on the block data will cause change of the block hash. That leads to detect the difference between the new hash with new data and the original hash with the original data. For example, when we use the hash function SHA256 to hash the string "*welcome to hash*" the hash string will be:

0x64cd83296fc1f99834862abf8c99a89157b72f7227ee376 94245211ca83d8793

Then if we capitalize the first character of the same string "Welcome to hash" the hash string will be different as:

0x33251f4dd195323f3bfaeb2b6377c7419e5b9309d3807f0 6cc392bd8c0922b4b

That mean if any byte of the original data changed the hash must be different and the hash of the block will be different then all the hashes in the blockchain after the changed block will be different. Another feature of the blockchain is the decentralization of the blockchain ledger that means the blockchain network must vote for the correct ledger in all nodes. The voting will check all of the blockchain ledgers in the network then choose the 51% winner.

2. Related Works

M. Idrees et al presented a Blockchain-based digital tracing app supported challenges, issues, solutions, and future directions for the COVID-19 pandemic. The authors involve a cloud app for the protection and privacy of the proposed network. Bluetooth is that the foremost generally used wireless technology in digital contact tracing apps and its proximity range is relatively high [1]. D. Han et al. work for smart home security system and use the blockchain for that. Using the blockchain, it could access several places around the house supported data sent from the sensor [12]. A. Takale et al. developed a text messaging application using blockchain connected by peer-to-peer network [13]. Sourabh et al. presented a chatting application using Ethereum smart contract. They used end-to-end encryption for messages are being sent over insecure channels. When the message block is added to the blockchain then, it'll never be changed [14].

3. Description of the Problem

Bluetooth is one of the most widely used wireless technology for proximity range users connecting [1]. This kind of communication channel can be sniffed by attackers. On the other hand, live chatting is the most popular texting communication tool used worldwide. In that manner data integrity is one of the concerns for Bluetooth communications. Man in the middle (MITM) and it's like attacks can change messages contents during the dialogue used by Bluetooth connection. The main issue we concerns is to protect data integrity during the Bluetooth text messaging connection.

4. Attack Scenario

As we mentioned before there are several Bluetooth networks attacks. We focus on data integrity in attacks like Man-in-the-Middle when a third person (intruder) can receive and send messages traveled between two other devices. In this attack the intruder enabled to insert itself into two paired devices [15]. Jackobsson et al. shows that attack can be performed using Bluetooth version 2.0+EDR [16].

Man in the middle attack is a type of attacks in which an intruder stealth between two interlocutors in a network without the knowledge of either of them. Suppose Alice wishes to communicate with Bob via a conversation. Meanwhile, Eve wants to intercept the conversation, eavesdrop, and possibly deliver a bogus message to Bob. Using this method of Eve can achieve her goals [15]. The attack scenario will start with Alice search Bob device to connect. First, Alice start Secure Simple Pairing (SSP) mode with Out-Of-Band (OOB) authentication method but Eve (MITM) acts first to impersonate Bob using Avoiding Just Works (JW) association with important data [15]. Then Eve establishes connection with Alice at the same time Eve start connect to Bob impersonate Alice and establish the connection as shown in Figure 5.
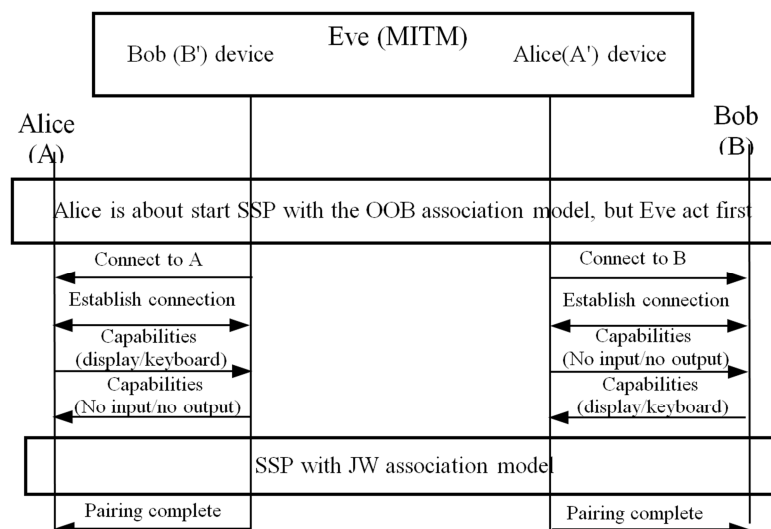
Figure 5. *The main idea of BT-SSP-OOB-MITM attack [8].*
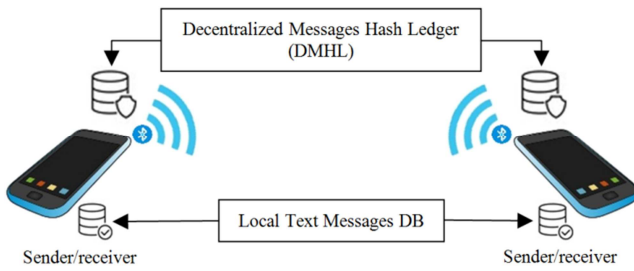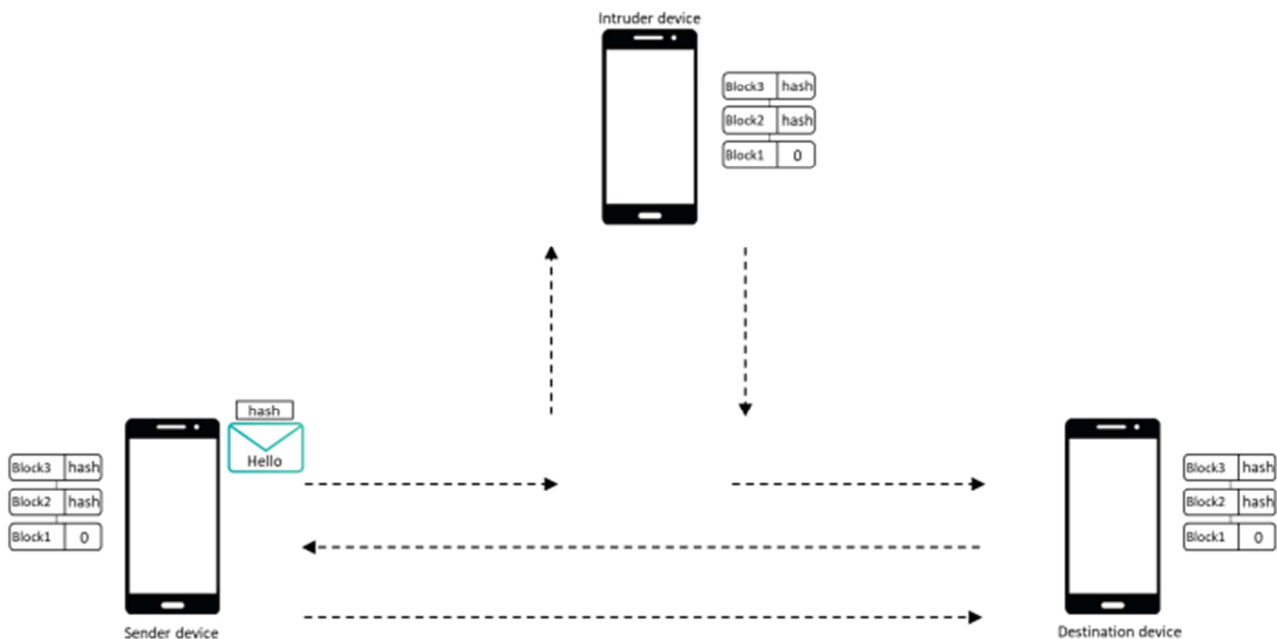
5. (BTMIS) Solution Approach

Figure 6. *The main idea of the proposed solution.*

From the last section we can find that intruder can access the messages exchanged between the two original devices and that enabled him to modify those messages. If we concern the messages integrity the blockchain technology will be good choice for that. As we mentioned before blockchain take into account the data integrity as prime security protection. So, the proposed solution depends on the decentralized ledger of blockchain. As we see in section IV the attack scenario the messages received by the intruder before the destination device that mean we must perform some protection immediately when the message has been sent from the sender device. For doing that we choose to create a new block for the current message hash immediately then insert this block into the local hash ledger and send the new block for each node in the network to modify its own blockchain ledger. After inserting the new message hash into the decentralized ledger, the message can be sent to the destination device. If the intruder tries to manipulates the message as in the MITM attack scenario then send the modified message to the destination device the destination device will check the blockchain ledger for the message hash before accept the message. While the message hash stored in the blockchain ledger does not match

the received message hash it will request the sender device to resend the message again. In Figure 6 we can show the main idea of the proposed solution using Bluetooth communication and the local database for the text messages stored and the Decentralized Messages Hash Ledger (DMHL) where the messages hashes stored.

As shown in Figure 7(a) a three mobile device were connected with Bluetooth network the sender device, the intruder device, and the destination device respectively. Blockchain decentralized ledger with three blocks placed in each device before sending the current message from the sender device. The sender device starts to create a new text message for the live chatting with the destination device. The intruder uses the MITM attack and insert itself between the two devices. When the sender creates the new message, it will immediately hash the message and store the message hash into the local blockchain ledger. The next steps of the proposed solution are described in the Figure 7(b).

Figure 7(b) illustrates the steps of the proposed solution after creation of the new message. Firstly, the new message hash will be stored in the local blockchain ledger as new block at the top of the ledger. Secondly, after the new block stored in the local ledger of the sender device it will distributed to all devices in the network including the intruder device. Thirdly, the new message will be sent through the Bluetooth connection which the intruder will receive it to manipulate in the step 4 and 5. Next, the intruder will send the modified message to the destination device as step 6 and 7. The destination device must check the hash of the received message with the hash in the blockchain ledger as in step 8. If the destination device find that the two hashes are different then it will request a resending message to the sender device as in step 9 and A. Finally, the sender device will resend the original message again as in step B and C.
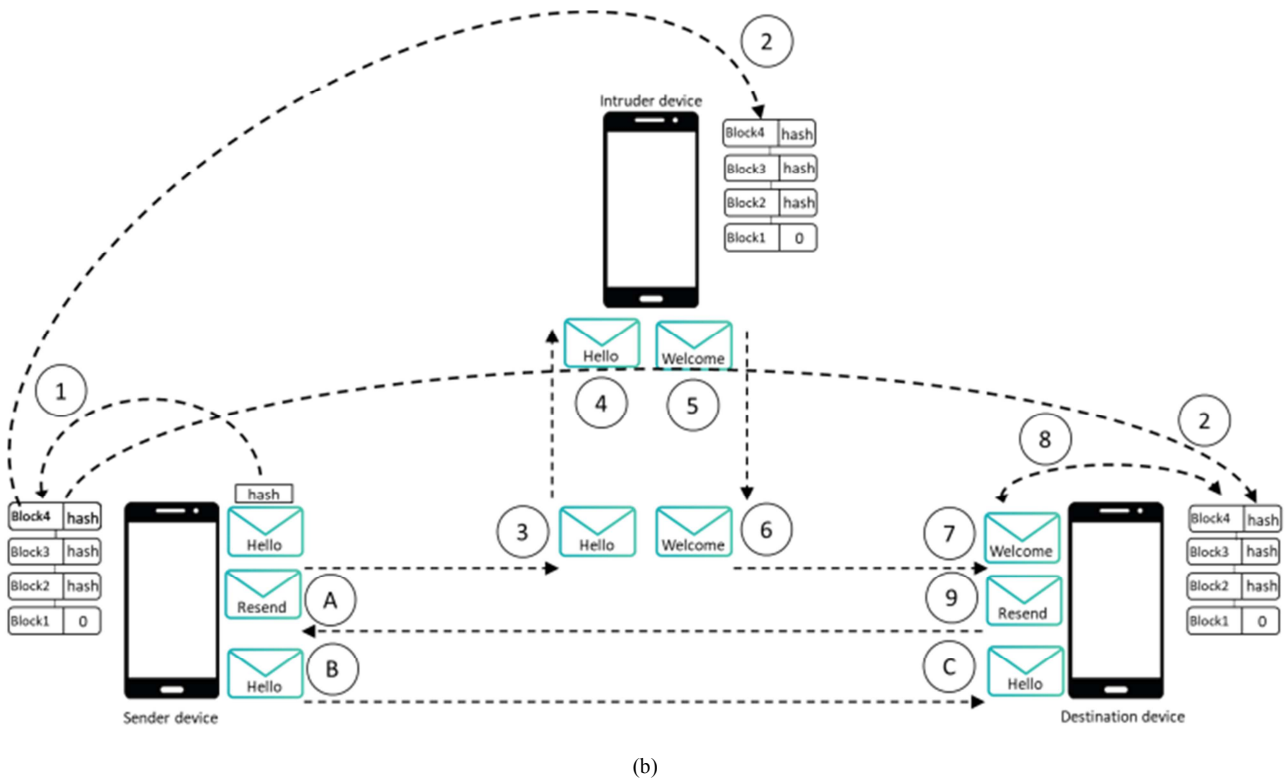

(a)

(b)

Figure 7. *(a). Creates new message and its hash; (b). All steps of the proposed solution.*
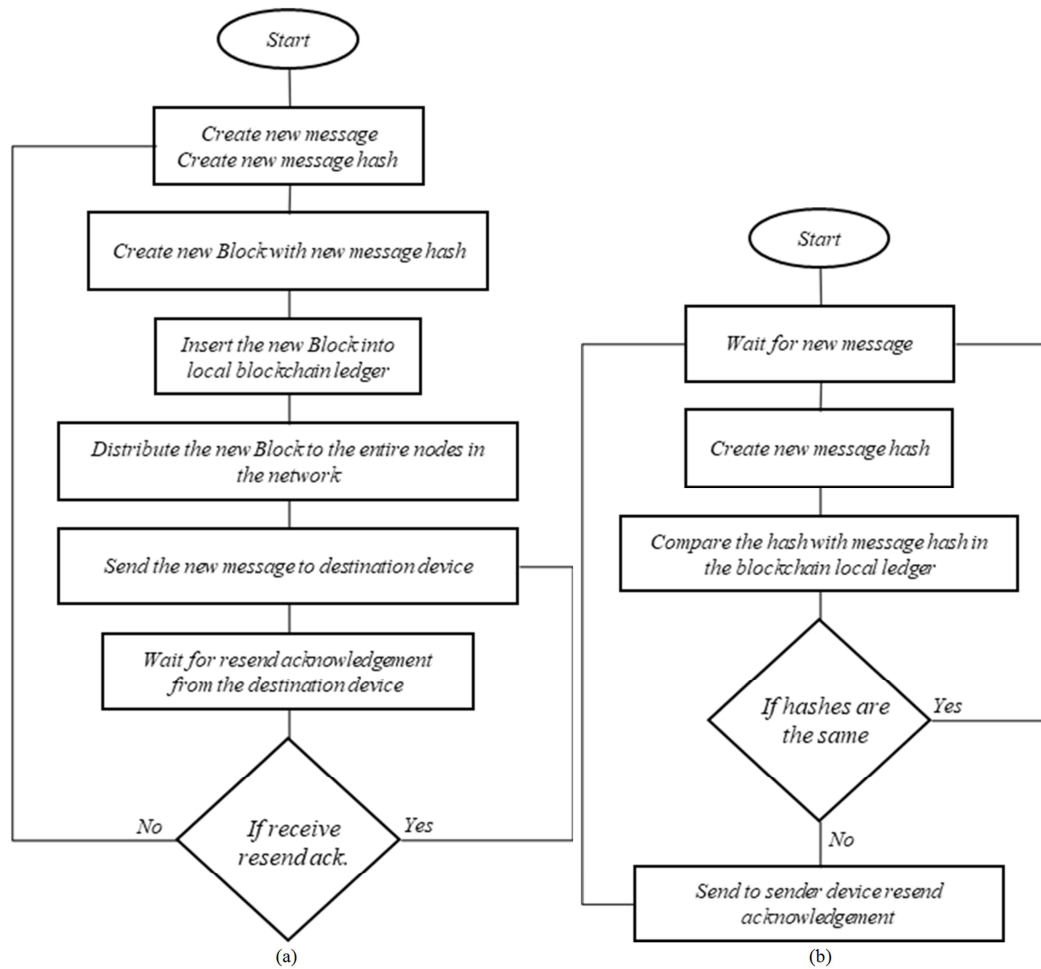

Figure 8. *(a). Sender side algorithm; (b). Destination side algorithm.*

(BTMIS) approach divided into two modules the first is the text chatting using Bluetooth connection and the second module is about the use of blockchain to implement the proposed solution. The second module is divided into two sub modules Figure 8 show the main algorithm for the first sub module used in sender side. This sub module starts with creating new message and creating the hash of the current message. Then insert the new block into local blockchain ledger and distribute the new block to the entire nodes in the network. Finally, the sender device will send the new message to destination device and wait for resend acknowledgement from the destination device. If receive resend acknowledgement from the destination it will resend the current message again otherwise it will start to create new message from the start.

The second sub module we start waiting for a new message. If a message received the sub module creates the hash for the current received message, then compare the hash with message hash in the blockchain local ledger. If hashes are not the same it will Send to sender device resend acknowledgement to the sender device. Figure 8(b) depicts the second sub module in the destination device.

6. (BTMIS) Evaluation and Tools

A. Android

The Android is an open-source operating system based on a modified version of the Linux kernel and other open-source software, Android owned and maintained by Google, Android is developed by the Open Handset Alliance, Some Android device manufacturers include Acer, HTC, Samsung, LG, Sony Ericsson and Motorola and others.

Android (API 1) was launched on the 23rd Of September 2008. Android offered included Google Maps, YouTube, an HTML browser, Gmail, camera, Bluetooth, Wi-Fi, and other. Android has Market (now Play Store) from where the users could download and update. Android applications additional to what was already pre-installed. In addition, Android has a large number of app developer Communities (apps) that extend the functionality of the device.

B. Android Studio

Android Studio is a new and fully integrated development environment -Integrated Development Environment IDE (Integrated Development Environment) for Android application development, based on IntelliJ IDEA. It is purpose-built for Android to accelerate your development and it helps to build the highest-quality apps for every Android device.

Android Studio provides extensive tools such as the Android Virtual Device Manager and the Android Device Monitor, also it tests Android apps with JUnit 4 and functional UI test frameworks. With Espresso Test Recorder, it can generate UI test code by recording the interactions with the app on a device or emulator. it can run the tests on a device, an emulator, a continuous integration environment, or in Firebase Test Lab. It also contains Gradle, which helps to configure the Android

application seamlessly; Android Studio offers more features to increase the productivity when creating Android apps, for example, feature-rich Emulator, Flexible Gradle-based build system, test performance on other types of devices, code templates to help you build common app features, full-featured editor with lots of extra tools and other.

Each project such as Messaging in Android Studio contains one or more modules, types of modules include android app Module, library Module, Google App Engine Module.

Each application module contains the following folder manifests which include AndroidManifest file, java which include Java source code files, and res which include XML layout, UI strings, and bitmap images.

C. (BTMIS) Testing

To evaluate (BTMIS) approach we implement it as a mobile App using Java language in Android Studio. The App consist of five main classes, three for Bluetooth communication and two blockchain ledger. We create *SereverClass* for the master Bluetooth node and *ClientClass* for slave Bluetooth nodes. Finally, we create *SendReceive* class to manipulate the message transformation. For blockchain ledger we create the *Block* class which contains the data for each block and *Blockchain* class to store the blocks that works as ledger.

We test the (BTMIS) approach by changing the content of one of the transferred messages then let the approach test if the message ledger is verified or not. Immediately, after the message change the App alert that the message is not the same message were sent and stored in the message's ledger. (BTMIS) can return the original message of the changed message.

7. Conclusion

Bluetooth is one of the most widely used wireless technology for proximity range users connecting. This kind of communication channel can be sniffed by attackers. On the other hand, live chatting is the most popular texting communication tool used worldwide. We propose (BTMIS) as a solution approach to detect attack that breaks text messages integrity used by Bluetooth communication. Our (BTMIS) approach based on blockchain where transferred messages stored in decentralized leger. We experimented (BTMIS) approach by implementing it as mobile App using android studio and Java programming language. The experiments results that any change of the transferred messages can be detected by verifying the messages hash ledger where an alter displayed when the ledger is not verified.

References

[1] S. M. Idrees, M. Nowostawski and R. Jameel, "Blockchain-based digital contact tracing apps for COVID-19 pandemic management: issues, challenges, solutions, and future directions." JMIR medical informatics 9.2 2021.

[2] N. Mahajan, G. Verma, G. Erale, S. Bonde and D. Arya, "Design of Chatting Application Based on Android Bluetooth.", International Journal of Computer Science and Mobile Computing, Vol. 3 Issue. 3, 2014.

[3] R. Verma, R. Gupta, M. Gupta and R. Singh, A Complete Study of Chatting Room System based on Android Bluetooth, International Journal of Emerging Technology and Advanced Engineering, 2014.

[4] A. P. Takale and C. V. Vaidya, Decentralized Chat Application using Blockchain Technology, International Journal for Research in Engineering Application & Management (IJREAM), 2018.

[5] A. Bhat and A. Jain, BLUETOOTH NETWORK SECURITY, Journal of Analysis and Computation (JAC), 2020.

[6] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[7] M. M. O. a. M. A. OBAID, "Mobile Payment Using Blockchain Security," 2021.

[8] B. K. S. S. P. a. D. J. Mohanta, "An overview of smart contract and use cases in blockchain technology," 9th international conference on computing, communication and networking technologies (ICCCNT), 2018.

[9] T. A. A. T. H. Q. J. a. Q. Q. Khan, "A Hybrid Blockchain-based Zero Reconciliation Approach for an Effective Mobile Wallet.," 2nd International Conference on Sustainable Technologies for Industry 4.0 (STI), 2020.

[10] B. K. Mohanta, S. S. Panda and D. Jena, An Overview of Smart Contract and Use cases in Blockchain Technology, Bengaluru, India: 9th ICCCNT, 2018.

[11] A. M. Antonopoulos, Mastring Bitcoin, SECOND EDITION, O'Reilly, 2017.

[12] D. Han, H. Kim and J. Jang, Blockchain based Smart Door Lock system, International Conference on Information and Communication Technology Convergence (ICTC), 2017, pp. 1165-1167, doi: 10.1109/ICTC.2017.8190886., 2017.

[13] M. Stearns, A Decentralized Approach to Messaging Using Blockchain Technology, California State University, Northridge, 2019.

[14] Sourabh, D. Rawat, K. Kapkoti, S. Aggarwal and A. Khanna, bChat: A Decentralized Chat Application, International Research Journal of Engineering and Technology (IRJET), 2020.

[15] M. A. Albahar, K. Haataja and P. Toivanen, "Bluetooth Mitm Vulnerabilities: A Literature Review, Novel Attack Scenarios, Novel Countermeasures, And Lessons Learned", International Journal on Information Technologies & Security, № 4, 2016.

[16] Wetzel, M. Jakobsson and Susanne, "Security Weaknesses in Bluetooth,", Springer Berlin Heidelberg, 2002.

Biography

Raed Rasheed is lecturer in software development department, faculty of IT, Islamic University-Gaza. His current interest research includes security, web services, computer vision and multimedia.
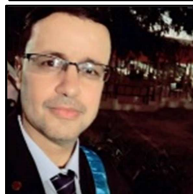
Raed Bulbul is Lecturer of Computer Engineering. Computer Engineering Department the Islamic University of Gaza.

Mohammad Mikki is Professor of Computer Engineering. Computer Engineering Department the Islamic University of Gaza.