

MODEL DEVELOPMENT WITH SAVING SMARTPHONE BATTERY DUE TO THE ACTIVITY OF DIGITAL BLUETOOTH AND WIFI DEVICES TO INCREASE THE RELIABILITY OF THE DIGITAL WIRELESS REMOTE CONTROL SYSTEM

Kodir Aslonov¹, Anvar Akhmedov², Ramziddin Pirimov², Maktuba Rakhmatova³

¹Bukhara Engineering Technological Institute, doctoral student of the Department of Information and Communication Technologies, Bukhara, 200100, Uzbekistan

²Bukhara Engineering Technological Institute, Department of Energy, Bukhara, 200100, Uzbekistan

³Bukhara Engineering Technological Institute, Department of Electromechanics and technology, Bukhara, 200100, Uzbekistan

Abstract. The article analyzes the advantages of devices for receiving and transmitting information smartphone, Bluetooth and WiFi technologies. In addition, an algorithm for a digital wireless remote control system based on the Arduino UNO microcontroller with Bluetooth and WiFi technologies is presented. In order to increase the reliability of the digital wireless remote control system, a model has been developed to save battery power on a smartphone.

Introduction

Modern telecommunication systems are complex complexes, the so-called complex telecommunication networks, consisting of a large number of interconnected elements, blocks and devices. One of the requirements for telecommunication networks is the reliability of their operation. In this regard, the development of principles and reliable methods for calculating, increasing and ensuring the reliability of telecommunication networks and their constituent elements is one of the urgent and demanded tasks.

Research on the impact of Bluetooth and WiFi wireless digital devices on smartphone battery charge

Bluetooth is a radio frequency technology using the unlicensed 2.5 GHz industrial, scientific and medical (ISM) band [1]. It is an open standard for wireless connectivity, mostly found in mobile devices (smartphones, tablet computers, laptops) to enable short-range communications and replaces proprietary cables. The aim and purpose of Bluetooth technology is to offer universal low cost and user friendly communication. Since the earlier developments of Bluetooth technology, vulnerability exploits have plagued this technology [1]. Well-known vulnerabilities include eavesdropping and impersonation, both which led to various attacks such as Denial of Service (DoS), relay attacks and the creation of Backdoors [1]. These vulnerabilities led to the need to improve Bluetooth security by including techniques such as authorisation, authentication and encryption [1].

Besides the security improvements, Bluetooth technology is still being exploited [1].

Bluetooth technology was invented in 1994 by L.M. Ericsson. During the winter of 1998 Ericsson, Nokia, Intel, IBM and Toshiba further evolved the Bluetooth standard by establishing the Bluetooth Special Industry Group (SIG) [1]. The last few years saw 3COM, Microsoft, Lucent and Motorola also started participating in SIG. The goal behind SIG is to further improve Bluetooth technology as short-range, low cost and user-friendly connection among portable devices, allowing for ad-hoc connectivity [1]. These capabilities are possible due to the architectural design of the Bluetooth technology [1].

The Bluetooth architecture consists of a protocol stack that is divided, by the Bluetooth specification, into three distinct groups: transport protocol group, middleware protocol group and the application group [1]. The transport protocol group consists of the following layers: radio, baseband, link manager and the Logical Link Control and Adaptation Protocol (L2CAP). These layers allow Bluetooth devices to locate each other while managing the physical and logical links [1]. The middleware protocol group includes thirdparty, industry-standard and Bluetooth-SIG protocols, allowing existing and new applications to operate over Bluetooth links [1]. Some of the protocols found in the middleware protocol group are the Internet Protocol (IP), Transmission Control Protocol (TCP) and serial port emulator (RFCOMM). The application group consists of the actual applications that use the Bluetooth links [1]. The architecture of the Bluetooth technology leads to several advantages: publicly available, royalty free, replaces the use of cables, supports both voice and data,

and uses an unregulated frequency band which is available around the world [1].

The term WiFi is not technical, but is actively used by modern users. The abbreviation WiFi (from the English word combination Wireless Fidelity, which can be literally translated as high fidelity of wireless data transmission) is currently understood as a whole family of standards for transmitting digital data streams over radio channels [4]. In other words, by the term WiFi, users mean the technology of wireless local networks - Wireless Local Area Network (WLAN, Wireless LAN). These technologies allow computers to be connected to local networks wirelessly (that is, using radio waves) and connect them to the Internet [4].

The most correct definition of the term WiFi is a trademark of the WiFi Alliance consortium - an association of the largest manufacturers of computer hardware and WiFi wireless devices [4]. This organization oversees the commercial development of WiFi technology based on standards developed and ratified by the IEEE (802.11 standards group) [4]. One of the tasks of the consortium is to test equipment from different manufacturers for compatibility and correct operation of devices with each other [4].

Wireless technologies are developing more and more every year. No one is surprised by the presence of WiFi networks in transport, recreation areas, cafes and train stations [4]. Wireless networks are especially effective in enterprises where employees actively move around the territory during the working day in order to serve customers or collect information [4].

Bluetooth and WiFi wireless devices, like any other electronic component, consume battery power from a smartphone [1]. Research has shown that if Bluetooth and WiFi are left indefinitely, it will consume the battery of a mobile device almost 51% faster [1, 3]. To minimize smartphone battery consumption due to the activity of digital Bluetooth or WiFi devices, these devices will only be active during certain periods of the day, and also only for a limited period of time. These active periods are based on patterns of human mobility.

Models of human mobility, as a rule, have two useful properties: regularity and randomness [1, 2, 3]. There are patterns that tend to be regular, as people visit the same places over and over again [1, 2, 3]. These patterns can become chaotic in the sense that a random act can change a regular pattern, causing a particular person to associate with different people over a period of time or visit different places. The patterns that tend to be regular are divided into three periods of mobility: no mobility, low mobility, and high mobility [1, 2, 3].

In addition to consuming smartphone battery power, Bluetooth or WiFi technology requires user interaction to pair between a mobile device and a digital wireless remote control unit based on an Arduino UNO microcontroller with Bluetooth or WiFi technology (Fig. 1).

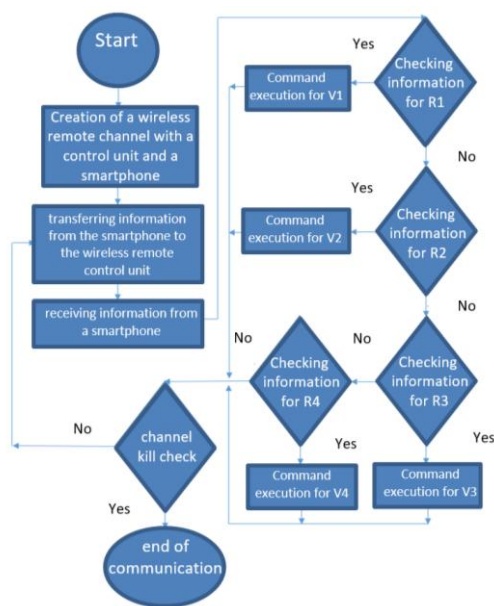


Fig. 1. Algorithm of the wireless remote control system [3]

The digital wireless remote control unit reproduces the information received from the smartphone, and accordingly provides the consumer (V1, V2, V3, V4) with electricity. Electricity consumers are connected to electricity through relays R1, R2, R3 and R4. Each consumer is provided with electric power with voltage from 220V to 250V [3].

The user needs to turn on Bluetooth or WiFi, authorize the connection, and authenticate the connected device. For the successful operation of the Bluetooth or WiFi channel, the channel does not require user participation. Therefore, in order to exclude any user involvement, the Bluetooth or WiFi channel performs the above actions on behalf of the user. After pairing a mobile device and a digital wireless remote control unit, communication can continue via Bluetooth or WiFi without user intervention [1-7].

Development of a model to improve the reliability of the wireless remote control system

Based on the human mobility model, a model has been developed to improve the reliability of the wireless control system, which saves the smartphone battery due to the activity of Bluetooth or WiFi devices. To create a model, the following activities have been developed:

1. A database has been created with the following tables:

Table 1. Register data when creating a wireless control channel and disable the wireless control channel.

id	Devices	Status	Time to create a Bluetooth or WiFi channel	
			Time	Date

id – data log number (1, 2, 3 ...);
 Devices - device name (Bluetooth or WiFi);

Status - pairing status (there is a connection - true, disconnection of devices - false);
 Time - time of device pairing;
 Date - date of pairing devices.

Table 2.

Status - true for pairing smartphones and wireless control units.

id	Devices	Status	Time

id – data log number (1, 2, 3 ...);
 Devices - device name (Bluetooth or WiFi);
 Status - pairing status (there is a connection - true, disconnection of devices - false);
 Time - time of device pairing.

Table 3.

Status - false to disable the wireless control channel.

id	Devices	Status	Time

id – data log number (1, 2, 3 ...);
 Devices - device name (Bluetooth or WiFi);
 Status - disconnection status (disabled - false);
 Time - the time the Bluetooth or WiFi channel was disconnected.

2. Sort tables 2 and 3 in ascending order based on device pairing time and channel disconnection time, respectively;
 3. Establish a connection between the smartphone and the digital wireless remote control unit with respect to the data sorted in Table 2. Create a Bluetooth or WiFi wireless channel without user intervention.

3.1. if the devices (smartphone and digital wireless remote control unit) do not form a pair, organize an attempt to pair soon based on the data in Table 2;

3.2. if it is possible to pair with smartphones and digital wireless remote control units, then create a Bluetooth or WiFi channel and wait for the user's command;

3.3. if a Bluetooth or WiFi channel is created, then organize the disconnection of the connection between the smartphone and the digital wireless remote control unit in the near future based on the data in Table 3;

3.4. if the time interval between the creation of the channel and the disconnection of the channel (Table 3 - disconnecting the Bluetooth or WiFi channel) is more than two hours, then it is necessary to organize the disconnection of the connection between the smartphone and the digital wireless remote control unit after two hours.

4. Disconnect the channel between the smartphone and the digital wireless remote control unit for the data sorted in Table 3. Disconnect the Bluetooth or WiFi wireless channel without user intervention.

4.1. if a Bluetooth or WiFi channel exists, then arrange the channel disconnection as soon as possible based on the data in Table 3;

4.2. when the Bluetooth or WiFi channel is disconnected, organize, without user intervention, the next connection between the smartphone and the digital

wireless remote control unit for the data sorted in Table 2.

Testing the proposed model on an Android smartphone

Based on the developed model, a smartphone application was created. For the experiment, the application is installed on a Samsung J6 + smartphone with Android 9.0 specification and 3 GB of RAM. The results of this experiment are as follows:

Table 4.

Register data when creating a wireless control channel and disable the wireless control channel.

id	Devices	Status	Time to create a Bluetooth or WiFi channel	
			Time	Date
1	Bluetooth	true	08:19	27:03:2020
2	Bluetooth	false	08:34	27:03:2020
3	Bluetooth	true	17:14	27:03:2020
4	Bluetooth	true	19:23	27:03:2020
5	Bluetooth	false	19:48	27:03:2020
6	Bluetooth	true	21:38	27:03:2020
7	Bluetooth	false	22:04	27:03:2020
8	Bluetooth	true	06:17	28:03:2020
9	Bluetooth	false	08:23	28:03:2020
10	Bluetooth	true	17:24	28:03:2020
11	Bluetooth	false	17:51	28:03:2020
12	Bluetooth	true	06:15	29:03:2020
13	Bluetooth	false	07:44	29:03:2020
14	Bluetooth	true	16:58	29:03:2020
15	Bluetooth	false	17:45	29:03:2020
16	Bluetooth	false	22:00	29:03:2020
17	Bluetooth	true	06:12	30:03:2020

Table 5.

Status - true for pairing smartphones and wireless control units (sorted table).

id	Devices	Status	Time
17	Bluetooth	true	06:12
12	Bluetooth	true	06:15
8	Bluetooth	true	06:17
1	Bluetooth	true	08:12
14	Bluetooth	true	16:58
3	Bluetooth	true	17:14
10	Bluetooth	true	17:24
4	Bluetooth	true	19:23
6	Bluetooth	true	21:38

Table 6.

Status - false to disable the wireless control channel (sorted table)..

id	Devices	Status	Time
13	Bluetooth	false	07:44
9	Bluetooth	false	08:23
2	Bluetooth	false	08:34
15	Bluetooth	false	17:45
11	Bluetooth	false	17:51
5	Bluetooth	false	19:48
7	Bluetooth	false	22:04
16	Bluetooth	false	22:00
13	Bluetooth	false	07:44

Table 4. shows that the average operating time of the wireless control channel is 649 minutes in 3 days. This means that the average operating time of the wireless control channel per day is 216 minutes, taking into account the time interval between the creation and disconnection of the wireless control channel is 2 hours [8-11].

Result

As described above, for Bluetooth or WiFi devices, the battery of the mobile device will drain 51% faster [1, 3]. Assuming 100% mobile device battery life is sufficient for 24 hours without Bluetooth or WiFi. By current, a smartphone can work 738 minutes without charging the battery when Bluetooth or WiFi devices are active.

$$k = 24 * 60 = 1440 \text{ minutes;}$$

$$z = 0.51k = 738 \text{ minutes}$$

As a result, in the middle of the day, the smartphone comes back to charging. This causes discomfort in the system, that is, when required, the smartphone that performs the system control function can be in a completely discharged state.

Based on the model, the app takes 216 minutes to charge the smartphone battery, which is 15% of the 1440 minutes when the Bluetooth or WiFi devices were active, which means that the smartphone can last 1224 minutes without charging the battery. This results in 36% efficiency compared to 738 minutes.

Forecast

If the application implements the time interval between the creation and disconnection of the wireless control channel is equal to 1 hour, then Table 4 shows that the average operation time of the wireless control channel is 440 minutes in 3 days. This means that the average operating time of the wireless control channel per day is 146 minutes, which is 10% of the 1440 minutes when Bluetooth or WiFi devices are active. As a result, the smartphone can work for 1294 minutes without charging the battery. This results in 41% efficiency compared to 738 minutes. The forecast results are shown in Diagram 1 and Diagram 2.

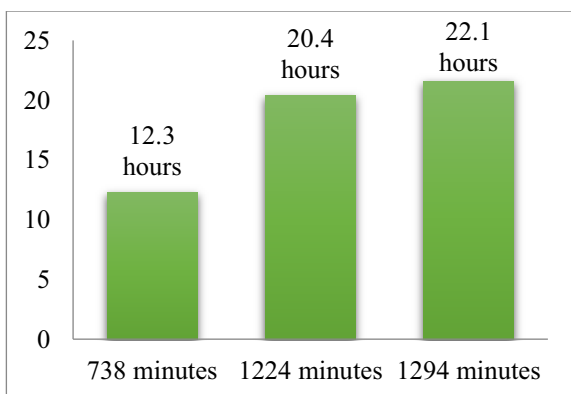


Diagram 1. Smartphone operating time when implementing the proposed model.

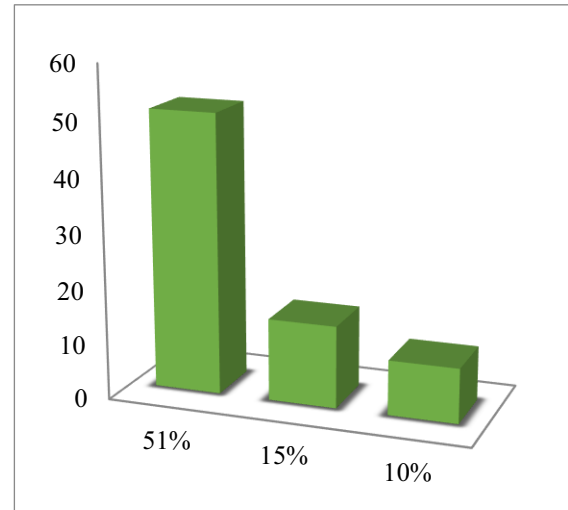


Diagram 2. Energy efficiency of a smartphone battery when implementing the proposed model.

Conclusion

Thus, the operating time of the smartphone from the wireless control channel has increased from 738 minutes to 1294 minutes, which increases the reliability of the digital wireless remote control system by 1.75 times and the smartphone's battery saving is 90%.

References

1. Heloise Pieterse, Martin S. Olivier. Bluetooth Command and Control channel. *Computers & security* 2014; 45:75-83.
2. Aviv AJ, Sherr M, Blaze M, Smith JM. Moving targets: geographically routed human movement networks. Department of Computer & Information Science, University of Pennsylvania; 2010.
3. Kodir Aslonov. Creation of a model of a wireless control system based on the Arduino Uno board with Bluetooth 2.0 technology. *Development of science and technology*. Bukhara 2020; №2: 125-131.
4. E.V. Smirnova, A.V. Proletarsky, E.A. Romashkina, S.A. Balyuk, A.M. Surovov. Technologies of modern wireless networks Wi-Fi. // *Computer systems and networks*. Moscow 2017; 12-45.
5. I U Rakhmonov, L A Nematov, N N Niyozov, K M Reymov and T M Yuldoshev (2020) Power consumption management from the positions of the general system theory. *Journal of Physics: Conference Series* doi:10.1088/1742-6596/1515/2/022054.
6. I U Rakhmonov, A N Tovbaev, L A Nematov and T Sh Alibekova (2020) Development of forecasted values of specific norms for the issues of produced products in industrial enterprises. *Journal of Physics: Conference Series* doi:10.1088/1742-6596/1515/2/022050.
7. [Allayev, K.R.](#), [Fedorenko, G.M.](#), [Postnikov, V.I.](#), [Ostapchuk, L.B.](#) Asynchronous generators as power system's natural dampers. 43rd International Conference on Large High Voltage Electric Systems 2010, CIGRE 20102010, 9p43rd International Conference on Large

High Voltage Electric Systems 2010, CIGRE 2010; Paris; France; 22 August 2010.

8. [Fazylov, Kh.F., Allaev, K.R.](#) Analysis of the operation of an electrical system during simultaneous operation of synchronous and asynchronous generators. Power engineering New York Volume 18, Issue 3, 1980, Pages 81-88.

9. [Fazylov, Kh.F., Allaev, K.R.](#) Asynchronous turbogenerators with stator excitation and the prospects for their utilization. Power engineering New York Volume 23, Issue 2, 1985, Pages 7-13.

10. [Fazylov, Kh.F., Allaev, K.R.](#) Calculation and experimental analysis of conditions of electrical power systems containing induction generators Power Engineering New York Volume 27, Issue 6, 1989, Pages 27-34.

11. Allaev K., Makhmudov T. Prospects of diversification and ensuring energy safety of Uzbekistan. E3S Web Conf., Volume 139, 2019, Rudenko International Conference "Methodological problems in reliability study of large energy systems" (RSES 2019). <https://doi.org/10.1051/e3sconf/201913901002>