ACADEMICIA

ISSN: 2249-7137 Vol. 11, Issue 3, March 2021 Impact Factor: SJIF 2021 = 7.492

ACADEMICIA

An International Multidisciplinary Research Journal

(Double Blind Refereed & Peer Reviewed Journal)

DOI: 10.5958/2249-7137.2021.00709.6

ANALYSIS OF THE GSM COMMUNICATION CHANNEL IN SECURITY SYSTEMS

Abdullajon Odiljon ogli Komilov*; Sherali Muhamadaliyevich Toshpulatov; Murod Makhamadalimovich Dadabaev***; Dilyorjon Baxtiyorovich Alimdjanov******

[1,2]Assistant,
[3,4]Master Student,
Fergana Branch of Tashkent University of Information,
Technologies Named after Muhammad al-Khwarizmi Fergana City
UZBEKISTAN

ABSTRACT

The article outlines the basic principles initially; wireless systems were not widely used due to low reliability. But now there is a wide range of various additional devices, and new generations of wireless communication systems are actively used. The capabilities provided by mobile operators are increasingly used in security systems. The capabilities provided by mobile operators are increasingly used in security systems. To date, wireless security systems based on the base have become widespread due to their relatively low cost and ease of installation and operation. The GSM-900/1800 cellular network provides good communication quality and is already deployed in most cities.

KEYWORDS: *GSM operators, GPRS channel, 3G, SMS messages, mode, DTMF, GSM/GPRS communication.*

INTRODUCTION

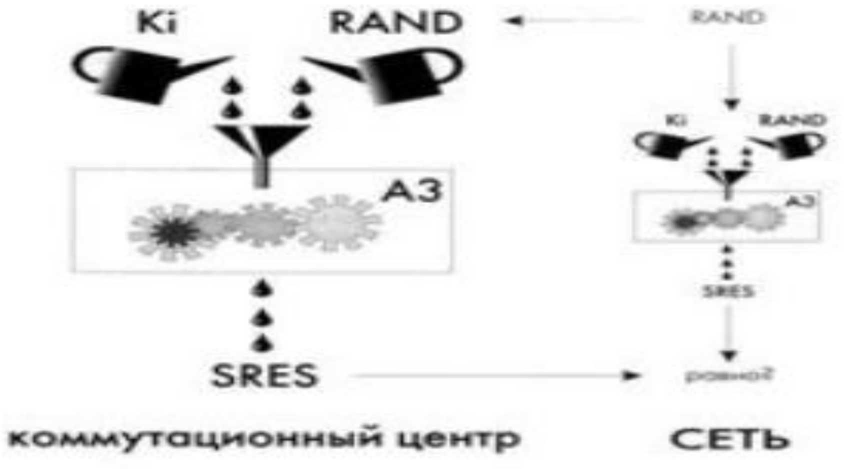
Initially, wireless systems were not widely used due to low reliability. But now there is a wide range of various additional devices, and new generations of wireless communication systems are actively used. The capabilities provided by mobile operators are increasingly used in security systems. To date, wireless security systems based on the base have become widespread due to their relatively low cost and ease of installation and operation. The GSM-900/1800 cellular network provides good communication quality and is already deployed in most cities.

MAIN PART

The use of GSM eliminates the need to deploy your own network of repeaters-the repeaters of GSM operators are used. As a result, it is possible to protect objects wherever the GSM operator's network works confidently. The use of new 3G protocols and networks specifically designed for corporate clients - virtual corporate data transmission networks with information protection-is promising. However, a significant disadvantage of such systems is low noise immunity. GSM systems use SMS messages, modem connection (CSD), tone transmission (DTMF mode), and GPRS packet message transmission as a method of transmitting information. The appearance of the GPRS mode has significantly reduced the cost of operating radio protection systems. To date, wireless security systems based on GSM have become quite widespread due to their relatively low cost and ease of installation and operation. However, a significant disadvantage of such systems is low noise immunity; the operation of the GSM network is not always very stable and can fail at the most inopportune moment.

A typical GPS monitoring system consists of three parts: terminals installed on cars, servers, and client workstations. The terminals are specialized GPS trackers containing the GPS module itself and the cellular communication module (GSM or CDMA). The server functions can be performed by a regular PC with server software installed. Unlike workstations, the server must always be turned on, since it is on it that route data is accumulated. In rare cases, the client software can be combined into a single program with the server part, but as a rule, it is allowed to connect several workstations to the same server at the same time.

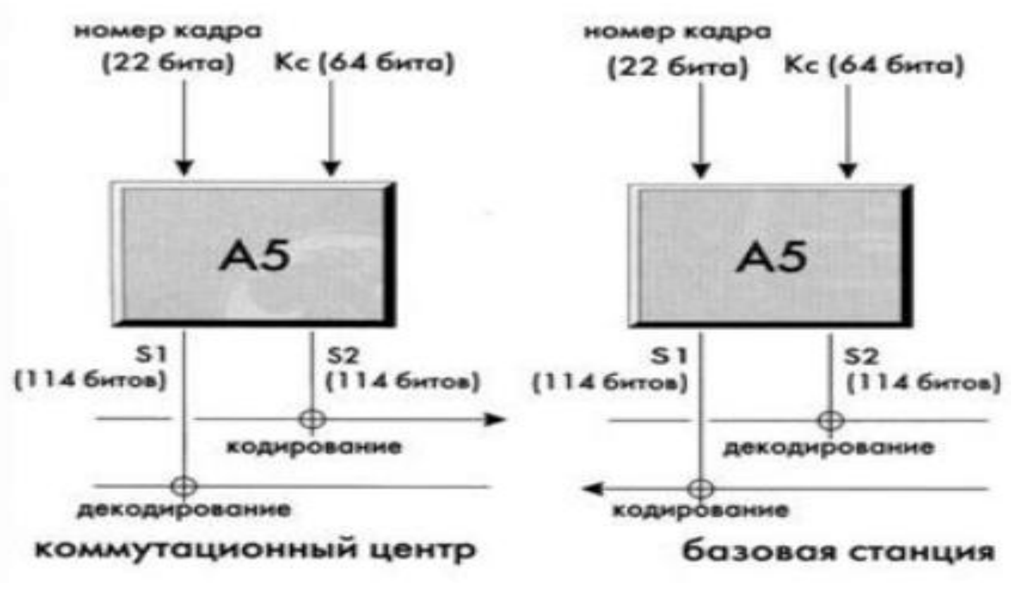
When building security systems in GSM channels, a password (or PIN code - a personal identification digital code) is used - one of the simplest authentication methods. It provides a very low level of protection in the conditions of radio communication use. It is enough to hear this personal code just once to bypass the security measures. In reality, GSM uses a PIN CODE in combination with a SIM (Subscriber Identity Module): this PIN CODE is checked on the spot by the SIM itself without being broadcast.



Pic. 1. Calculating Authentication

GSM uses a more complex method, which consists of using a random number that can only be answered by the corresponding subscriber equipment (in this case, the SIM). The essence of this method is that there are a huge number of similar numbers and therefore it is unlikely that it will be used twice.

Authentication is performed by requiring a correct answer to the following: the subscriber can deduce the SRES response from the incoming RAND by applying an algorithm with the private (secret) key Ki. The response, which is called SRES (Signed Result), is obtained in the form of a calculation result that includes a secret parameter belonging to this user, which is called Ki. The secrecy of the Ki is the cornerstone of all security mechanisms - even the subscriber cannot know his own Ki. The algorithm that describes the order of calculation is called the A3 algorithm. As a rule, such an algorithm is kept secret. In order to achieve the required level of security, the algorithm must be a unidirectional function, as it is called by cryptographic experts. This means that calculating SRES for known Ki and RAND should be simple, and the reverse action-calculating Ki for known RAND and SRES-should be as difficult as possible. Of course, this is what ultimately determines the level of security. The value calculated by the algorithm must be 32 bits long. Ki can have any format and length. Cryptographic methods make it possible to achieve a high level of security using relatively simple means. GSM uses uniform methods to protect all data, whether it is user information, transmission of user-related signals, and transmission of system signals. For example, messages that contains the numbers of the called phones or the transmission of system signals of messages containing the results of radio measurements to prepare for transmission. It is necessary to distinguish only between two cases: the communication is secure, or the communication is unsecured, then all information is sent as an unencrypted digital sequence.



Pic.2. Encryption and Decryption

The algorithm outputs an encryption sequence of 114 bits for each packet separately, taking into account the frame number and the encryption key of the Cs.

Both encryption and decryption are performed by applying the "exclusive or" operation to the 114 "encoded" bits of the radio packet and the 114-bit encryption sequence generated by a special algorithm. In order to get the encryption sequence for each packet, the algorithm performs a calculation using two inputs: one is the frame number, and the other is a key known only to the mobile station and the network (Figure 2). Two different sequences are used in both directions of the connection: in each packet, one sequence is used for encryption in the mobile station and for decryption on the BTS, while the other sequence is used for encryption in the BTS and decryption in the mobile station.

The frame number varies from packet to packet for all types of radio channels. The Cs key is controlled by the means of signal transmission and changes, as a rule, with each message. This key is not made public, but since it changes frequently, it does not need as strong security as the Ki key; for example, the Cs can be freely read in the SIM. The CS key must be agreed upon by the mobile station and the network before encryption begins. The peculiarity of the GSM standard is that the Cs key is calculated before the encryption begins during the authentication process. The CS is then inserted into the non-volatile memory inside the SIM so that it is stored there even after the end of the communication session. This key is also stored on the network and used for encryption.

Interference in the radio channel is created both due to distortion of the signal during its propagation, and as a result of the influence of external sources. The first type of distortion is relatively easy to eliminate, at the same time, interference from external sources is combated by expanding the spectrum of the transmitted signal. Theoretically, increasing the signal base allows you to reduce the interference to an arbitrarily small level.

The main difficulty in building a GSM channel is associated with the inability to ensure the continuity of GSM/GPRS communication with the operator due to network outages, which lead to data transmission interruptions, but also to modem hang-ups. Practice shows that no GSM operator currently provides a guaranteed GPRS communication channel. In attempts to implement continuity of connection, developers are forced to additionally equip traditional GSM modems with additional devices - external controllers, watchdog timers that reset the modem when it freezes. Unfortunately, such solutions, although usually "economical", still do not guarantee a continuous and uninterrupted data transfer process, and also lead to a complication of the system as a whole and, as a result, to a decrease in its reliability.

CONCLUSION

Noise immunity in the field of radio-channel fire and security systems is determined by the number of frequency ranges in which the radio system can operate, the number of frequency channels in each range, the ability to automatically select backup channels, and the presence of automatic adjustment of the radiation power. From time to time, the connection with a particular radio device is lost. Most likely, the reason is not deliberate sabotage of the system, but the operation of other devices and systems on the selected communication channel when installing the system. To reduce signal jamming, you need to have a duplicate channel for exchanging important information, use a periodic test from the object, and use remote antennas.

REFERENCES

1. Fundamentals of telecommunication systems and networks: textbook for universities / VV Krukhmalev, NV Gordienko, AD Mochenov and others; under. Ed. VN Gordienko and VV Krukhmaleva. - M.: Hot line. Telecom, 2004 - 510 p
2. Anin B.Yu. Protection of computer information / B.Yu.Anin. - St. Petersburg: BHV - St. Petersburg, 2000.
3. Kartashevsky VG Motor communication networks / VG Kartashevsky, SN Semenov, TV Firstova. - M .: Eco-Trends, 2001.
4. Mobile communication systems: textbook for universities / V.P. Ipatov, VK Orlov, IM Samoilov, VN Smirnov; under the editorship of VP Ipatova. - M .: Hot line - Telecom, 2003. - 272 p., Ill.
5. Karimov U. et al. USING NEW INFORMATION TECHNOLOGIES IN DISTANCE LEARNING SYSTEM // NEW INDUSTRIAL REVOLUTION IN THE MIRROR OF MODERN SCIENCE. - 2018. - C. 9-11.
6. Karimov A., Muxammadjonov X. INFORMATION TECHNOLOGIES: INFORMATION EDUCATION AND INFORMATICS // Economics and society. – 2020. – №. 8. – C. 40-43.
7. Yahyo, Muhammad Amin. Protection from internet threats. Supporting tutorial. Tashkent, 2016.
8. M.Tojiyev, R.Salaxutdinov. Modern information technologies in the educational process. Tashkent, 2001.
9. http://ru. wikipedia.org/
10. http://pbsecurity.ru/
11. http://tzmagazine.ru/
12. https://smekni.com/a/119758/