UDC 621.391

NOISE RESISTANCE OF REMOTE AUTHENTICATION VIA LTE NETWORK

[1]Andrii A. Astrakhantsev, [2]Galyna E. Liashenko, [2]Anna O. Shcherbak

[1]Igor Sikorsky Kyiv Polytechnic Institute, Kyiv, Ukraine
[2]Kharkiv National University of Radio Electronics, Ukraine

Background. LTE networks support a wide range of applications and services. These networks provide high-quality mobile services and have increased transmission rates and often used for remote biometric authentication, but the influence of noise and fading in wireless channels on quality and stability of biometric authentication is not analyzed yet.

Objective. The aim of the paper is to study the model of the physical layer of the LTE network, which transmits biometric templates for authentication.

Methods. We use computer simulation of biometric authentication system for preparing biometric template and Matlab models of wireless communication channel using the LTE technology for analysis of influence of noise and fading on channel.

Results. The paper presents the results of the evaluation of the authentication system under the influence of interference in communication channels. The impact of the use of MIMO technology on the dependence of the number of bit errors is evaluated. The obtained results show that in order to improve the quality of remote biometric authentication systems, it is advisable to use additional means of noise immunity and the use of adaptive settings on the transmitter side.

Conclusions. The system of remote biometric authentication with data transmission via LTE network was modeled. Influence of AWGS and Doppler shifts in wireless communication channels was analyzed. For noise resistance different error correction codes are implemented.

Keywords: remote authentication; LTE; noise resistance; biometric template; stegosystem.

Introduction

With the growing demand for mobile services and applications, such as streaming music, videos, using banking applications, there is a need to develop the next generation of wireless standards. LTE (Long Term Evolution) and LTE-Advanced have been developed to provide the required data rates, network bandwidth, which are needed to support the operation of mobile applications [1]. In various applications, such as banking networks, smart homes and others, it is very important to properly authenticate to avoid access by third parties. Recently, remote biometric authentication has become increasingly popular. Everyone has their unique biometric features, such as the iris, fingerprint, voice, facial geometry [2]. Also, to increase the security of biometric data, it is possible to use network steganography methods, which hide the fact of this information using network protocols [3].

All these data in remote authentication are transmitted in this case by mobile networks and must be protected, so it is important to study the external effects of mobile networks in LTE.

Description of the remote authentication model via the LTE network

For remote authentication, methods using biometrics were considered. Biometric authentication methods can be divided into static and dynamic.

Static methods use unique and inherent biometric characteristics of a person, such as fingerprint, facial geometry, iris. Dynamic methods use human behavioral characteristics such as dynamic signature, voice recognition. For biometric authentication, the presence of a person is necessary, and this type of authentication also makes it possible not to remember passwords or have special electronic keys.

For biometric authentication, a system that uses one or more biometric characteristics of a person (multimodal biometrics) can be used. The use of characteristics such as fingerprints, iris, face geometry, hands, dynamic signature, voice recognition was considered. Based on the multi-criteria analysis [2,4], the best authentication methods for research were selected (Fig. 1).

Based on the fact that the authentication is considered in the payment systems, smart home systems which are increasingly used with the

smartphone have appropriate use of these authentication methods, such as fingerprint, facial geometry, iris.

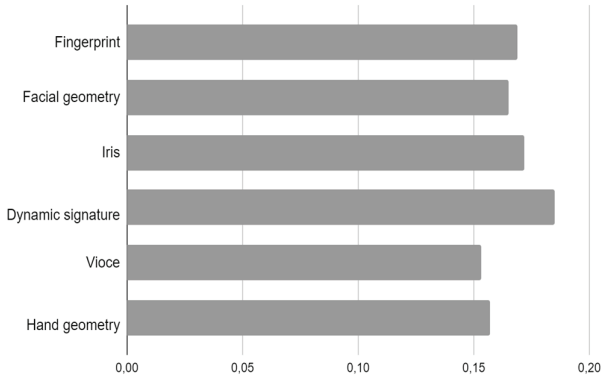

Fig.1 Comparison of biometric authentication methods based on multi-criteria analysis

During remote authentication, the user's biometric features on the first stage (this can be a fingerprint, facial geometry, iris) via biometric sensor and biometric template were prepared.

When using authentication based on iris biometric template as the fabric used «trabecular meshwork», which makes visible to divide the iris radial sectors. The recognition process on the iris of the eye combines several stages: the eye image processing, filtering, iris code generation [5].

Fingerprint authentication is one of the most common. Existing methods of fingerprint comparison can be divided into three types: comparison based on correlation, comparison of minutia and comparison based on the ridges of papillary lines [6].

In face geometry authentication systems, an image or video stream is input to the recognition system. And the solution is to identify or verify the person in the image or video. Recognition accuracy depends on image quality.

The transmission of the resulting biometric template is unsafe. In the case of interception of these data, an attacker can gain unauthorized access to information. To increase the security of biometric data, in addition to encryption, it is possible to use steganography.

Steganography is a way of transmitting information while hiding the fact of transmitting this information.

There are various ways to hide data using steganography. Data can be hidden in images, video, audio, as well as using data transfer protocols over the network.

In this paper, we considered data hiding using network steganography. The classification of existing methods of network steganography is given in [7]. Methods can be divided into methods that modify packets (packet headers, payload fields), methods that modify the structure of packet transmission (changing the transmission sequence, introducing delays), and hybrid methods.

Packet-modified network steganography methods include methods for modifying unused IP and TCP header fields [8], SCTP protocols [9], and methods that modify packet payloads, such as Transcoding steganography [10].

The work investigated the methods of network steganography, which are based on hiding data transmitted in headers. Efficiency evaluations were carried out for methods that use network data units (PDUs) of the Transmission Control Protocol (TCP), Hypertext Transfer Protocol (HTTP), and Internet Control Message Protocol (ICMP).

To hide the data in the TCP segment, the Window Size field [3] was used. After embedding data in this field, the TCP segment was transmitted to the recipient's side and the data was restored there.

The second method implements hiding data in HTTP headers. In this method, various characteristics of HTTP messages can be used for covert communication. These include modifications to the order of headers, their structure and content.

The third method of fancy steganography is based on capturing data from ICMP headers, using fields such as Identifier, Sequence number and data field.

After performing hashing and error correction encoding, the data is embedded to the stegocontainer and transmitted via model of LTE network. The model of LTE network includes transmitter side, wireless channel and receiver side. The scheme of data processing before transmission is shown on Fig. 2.

The requirements for LTE networks cover the achievement of the following objectives. These networks should have increased bandwidth, high transmission speeds, low latency at the user and management levels, reduced operating costs, support for multiple antennas, and flexible bandwidth operations. The use of MIMO (Multiple Input Multiple Output), turbo coding, OFDM (Orthogonal frequency-division multiplexing), and dynamic channel adaptation methods helps to meet these requirements.

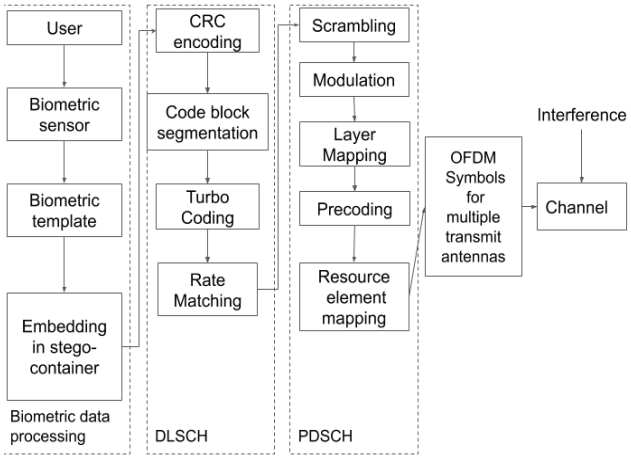

Fig.2 Preparing biometric data for transmission

OFDM is a multi-carrier transmission scheme. The main purpose of this is to separate the information transmitted over the broadband channel in the frequency domain and to match these symbols with a plurality of narrowband orthogonal subchannels.

MIMO is one of the key technologies used in LTE standards. MIMO methods allow you to take advantage of multiple antennas to meet the requirements of the LTE standard for peak data rates and bandwidth.

Physical layer modeling includes processing the transmitted data bits that are transmitted to the physical layer, signal processing and delivering the data to an antenna for transmission.

LTE downlink transmission occurs in several stages. The data is multiplexed and encoded in a downlink common channel processing step. The step includes attaching a code to detect errors, segmenting the data into subblocks, performing channel coding, turbo coding operations on the user data, performing rate matching operations that select the number of output bits to reflect the desired coding rate, and reconstructs the code blocks into codewords. At the next stage, the codewords are scrambled to form a modulated symbol stream. Next, multi-antenna (MIMO) processing occurs, in which the modulated symbol stream is divided into multiple substreams for transmission over multiple antennas. In MIMO operations, precoding is first performed, which scales and orders the symbols that are assigned to each substream. Layer mapping selects and routes data to each substream to implement one of the MIMO modes defined for downlink transmission.

Available radio spectra in different frequency bands define LTE standards. LTE networks are being integrated with previous mobile systems. Frequency bands identified for previous 3GPP standards are available for LTE deployment. Like previous 3GPP standards, LTE supports Frequency Division Duplex (FDD) and Time Division Duplex (TDD) modes. FDD provides simultaneous transmission on two frequencies: one for the downlink and one for the uplink. The paired bands are also indicated with sufficient spacing to improve receiver performance [11].

Modeling and obtained results

The physical LTE level was simulated with such parameters as two transmitting antennas, two receive antennas, channel bandwidth 20MHz, 16QAM, two symbols for DCI, target coding rate: ⅓, frequency-selective fading channel model, Frequency Division Duplex (FDD).

On the receiver side, templates are compared and a decision is made to grant access. In the communication channel, the effect of Additive White Gaussian Noise (AWGN) noise is simulated, it has a uniform power spectral density at all frequencies, is distributed normally by time values and has an additive way of affecting the signal. Doppler fading has also been set, which affects the wireless communication by creating signal fading. This occurs when the signal transmitter moves in relation to the receiver. Relative movement shifts the frequency of the signal, making it different in relation to the transmitter. Fading also occurs when the Doppler shift between two signals is different due to multipath [12].

At the given parameters of the signal-to-noise ratio and Doppler fading, the biometric templates obtained on the receiving side were compared and compared with the original.

Fig. 3 shows the effect of the Doppler fading and SNR on the bit error rate. The results of this study showed that as the signal-to-noise ratio (SNR) increases, the BER value decreases. The presence of the Doppler shift leads to an increase in the bit error rate. To eliminate this, it is necessary to increase the transmitter power, to use noise-tolerant codes and modulation algorithms.

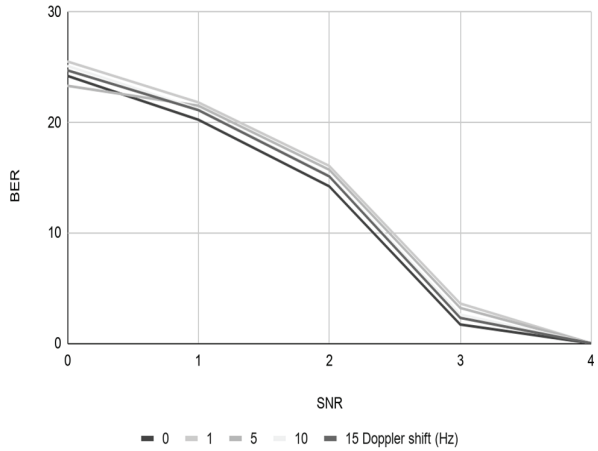

Fig.3 Dependence of BER on the SNR value at different values of Doppler shift

The SNR thresholds at which the correct comparison of the original biometric template with the template after interference ceases to occur were also evaluated. In the absence of Doppler fading, correct authentication occurs at SNR > 3.4, and the presence of fading has little effect on the trigger threshold (Fig. 4).

The code rate was also investigated, which shows the ratio of the number of characters at the input of the error-correcting encoder to the number of characters at the output. Reducing code speed usually improves noise immunity, but reduces the effective data rate. Studies have shown that reducing the code speed to increase noise immunity can almost double the trigger thresholds for the authentication system.

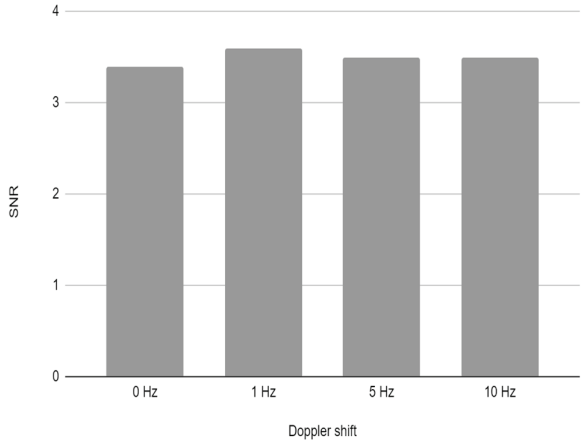

Fig.4 Influence of SNR and Doppler shift on the quality of pattern comparison

Table 1 shows the comparison results of the original biometric template and the resulting transmission over a channel with AWGN noise and a given SNR in the LTE model.

TABLE 1 Comparison results

Maximum Doppler shift	0	1	5	10	40	80
SNR						
3,3	-	-	-	-	-	-
3,4	1	-	-	-	-	-
3,5	1	1	1	1	-	-
3,6	1	1	1	1	-	-
3,7	1	1	1	1	-	-
3,8	1	1	1	1	1	-
3,9	1	1	1	1	1	-
4	1	1	1	1	1	-
4,1	1	1	1	1	1	-
4,2	1	1	1	1	1	1

Table 1 shows at which values of the Doppler shift and SNR the templates match, when comparing, and at which, due to the number of errors and distortion of certain bits, the templates comparison program does not accept a template that was transmitted over a noisy channel.

Conclusions

The system of remote biometric authentication with data transmission via LTE network was modeled in the work. During authentication correct matching is very important to obtain a decision to grant access to the resource. In wireless communication channels, the signal is affected by AWGS and Doppler shifts occur. The study of the model showed that the Doppler shifts have little effect on the accuracy of the comparison of patterns, and with increasing SNR, the quality of the obtained signal is better. To avoid fading, it is necessary to adjust the signals by the forecast.

In the future, it is planned to study the impact of interference in wireless communication channels on the quality of authentication systems in the operation of various methods of network steganography and the use

of multimodal biometric systems. This will allow you to evaluate and select methods to improve the quality and reliability of authentication systems.

References

1. Ivanenko S.A., Bezruk V.M. Planning and optimization of networks 4G // 23 Int. Crimean Conference “Microwave & Telecommunication Technology” (CriMiCo’2013) John Wiley & Sons, Inc. – 2014. – pp.500-501.
2. Liashenko G., Astrakhantsev A. Analysis of biometric authentication techniques // Information processing systems, Kharkov – 2017. Vol.2, No. 147. – pp.111-114.
3. Shcherbak A., Astrakhantsev A., Shcherbak O., Liashenko G. Analysis of stealth and noise resistance of network steganography methods (Ukrainian) // scientific journal Problems of Telecommunications. – 2020. Vol.2, No.23. – pp.89-98.
4. Saaty T., Decision making with the analytic hierarchy process // International Journal of Services Sciences, vol. 1, no. 1, pp. 83-98, 2008.
5. Liashenko G., Astrakhantsev A. and Chernikova V., Network steganography application for remote biometrie user authentication // 2018 IEEE 9th International Conference on Dependable Systems Services and Technologies (DESSERT), pp. 326-330, 2018.
6. Maltoni D., Cappelli R. Fingerprint Recognition // Handbook of Biometrics. Springer, Boston, MA, 2008 –pp. 23-42.– DOI:10.1007/978-0-387-71041-9_2.
7. Mazurczyk W., Smolarczyk M. and Szczypiorski K. Retransmission steganography and its detection // Soft Computing Journal, Springer, no. 500, November 2009.
8. Cauich E., Gómez R. and Watanabe R. Data Hiding in Identification and Offset IP Fields // Proceedings of 5th International School and Symposium of Advanced Distributed Systems (ISSADS) 2005, pp. 118-125, 2005.
9. Frączek W., Mazurczyk W. and Szczypiorski K. Hiding information in a Stream Control Transmission Protocol // Computer Communications, vol. 35, no. 2, pp. 159-169, 2012.
10. Mazurczyk W., Szaga P. and Szczypiorski K. Using transcoding for hidden communication in IP telephony // Multimedia Tools and Applications, vol. 70, no. 3, pp. 2139-2165, June 2014.
11. Budigere Karthik, Panchakarla Nagasai, Chemmagate Binoy, Roy Shourov LTE: Long Term Evolution of 3GPP 2010.
12. Riyadh Khlf Ahmed, Doppler fading communication channel performance simulation // International journal of physical sciences. – 2017. – Vol.12, No. 7. – pp.89-94.

Астраханцев А.А., Ляшенко Г. Є., Щербак А.О.

Дослідження моделі віддаленої автентифікації при передачі даних через мережу LTE

Проблематика. Мережі LTE підтримують широкий спектр програм та послуг. Ці системи високоякісних мобільних послуг мають підвищену швидкість передачі і часто використовуються для віддаленої біометричної автентифікації, але вплив шуму і завмирання в бездротових каналах на якість і стабільність біометричної автентифікації ще не проаналізовано.

Мета досліджень. Метою роботи є вивчення моделі фізичного рівня мережі LTE, що передає біометричні шаблони для автентифікації.

Методика реалізації. Було проведено комп'ютерне моделювання системи біометричної автентифікації для підготовки біометричного шаблону і Matlab моделі каналу бездротового зв'язку за технологією LTE для аналізу впливу шуму і завмирання на канал.

Результати досліджень. У статті представлені результати оцінки системи автентифікації при впливі завад в каналах зв'язку, оцінено вплив використання технології MIMO на залежність кількості бітових помилок. Отримані результати показують, що для підвищення якості віддалених систем біометричної автентифікації доцільно використовувати додаткові методи завадозахищеності та використання адаптивних налаштувань на стороні передавача.

Висновки. Змодельована система віддаленої біометричної автентифікації з передачею даних по мережі LTE. Проаналізовано вплив AWGS і доплеровских зсувів в каналах бездротового зв'язку. Для стійкості до завад реалізовані різні коди корекції помилок.

Ключові слова: віддалена автентифікація; LTE; стійкість перед перешкодами; біометричний шаблон; стегосистеми.

Астраханцев А.А., Ляшенко Г.Е., Щербак А.О.

Исследование модели удаленной аутентификации при передаче данных через сеть LTE

Проблематика. Сети LTE поддерживают широкий спектр приложений и услуг. Эти сети предоставляют высококачественные мобильные услуги и имеют повышенную скорость передачи и часто используются для удаленной биометрической аутентификации, но влияние шума и замирания в беспроводных каналах на качество и стабильность биометрической аутентификации еще не проанализировано.

Цель исследований. Целью работы является изучение модели физического уровня сети LTE, передающей биометрические шаблоны для аутентификации.

Методика реализации. Было проведено компьютерное моделирование системы биометрической аутентификации для подготовки биометрического шаблона и Matlab модели канала беспроводной связи по технологии LTE для анализа влияния шума и замирания на канал.

Результаты исследований. В статье представлены результаты оценки системы аутентификации при воздействии помех в каналах связи, оценено влияние использования технологии MIMO на зависимость количества битовых ошибок. Полученные результаты показывают, что для повышения качества удаленных систем биометрической аутентификации целесообразно использовать дополнительные средства помехозащищенности и использование адаптивных настроек на стороне передатчика.

Выводы. Смоделирована система удаленной биометрической аутентификации с передачей данных по сети LTE. Проанализировано влияние AWGS и доплеровских сдвигов в каналах беспроводной связи. Для устойчивости к помехам реализованы различные коды коррекции ошибок.

Ключевые слова: удаленная аутентификация; LTE; помехоустойчивость; биометрический шаблон; стегосистема.