РАДІОЕЛЕКТРОНІКА ТА ТЕЛЕКОМУНІКАЦІЇ

RADIO ELECTRONICS AND TELECOMMUNICATIONS

UDC 621.396.946

IDENTIFICATION OF MOBILE DEVICES BY CORRELATION FEATURES OF THEIR SIGNAL SPECTRA

Antipov I. – Dr. Sc., Professor, Associate Professor of the Department of Computer Radio Engineering and Technical Information Protection Systems, Kharkiv National University of Radio Electronics, Kharkiv, Ukraine.

Vasylenko T. – PhD, Senior Lecturer of the Department of Computer Radio Engineering and Technical Information Protection Systems, Kharkiv National University of Radio Electronics, Kharkiv, Ukraine.

ABSTRACT

Context. The mass spread of Wi-Fi networks is facilitated by the simplicity of their deployment, high speed, universality, and convenience of use. The development and dissemination of these networks continue despite a number of shortcomings. One of the shortcomings is their vulnerability to various types of attacks, including those based on the forgery (imitation) of identification data. At the same time, there are physical layer characteristics, knowledge of which expands the understanding of the network's state, can contribute to increasing the reliability of network subscriber identification, and thus prevent a number of attacks. This research is aimed at the theoretical and practical substantiation of the possibility of their application.

Objective. The aim of the study is to assess the application of detailed analysis of signal spectra emitted by devices connected to wireless Wi-Fi networks for their identification. To achieve this goal, it is necessary to analyze the experimentally measured spectra of wireless devices connected to the Wi-Fi network and evaluate the possibility of using the spectrum for the identification of mobile devices.

Method. This work proposes a method for processing the results of measuring the spectra of Wi-Fi device emissions by evaluating the asymmetry coefficient of the Wi-Fi device spectrum's cross-correlation function. Mathematical modeling was used to assess the effectiveness of the method.

Results. The research results show that the minimum value of the asymmetry coefficient when comparing the template with different positions of one's own device, and large values of the asymmetry coefficient when comparing templates with foreign spectra. Therefore, this characteristic can also be used for the identification of Wi-Fi devices.

Conclusions. The research results suggest the possibility of applying the proposed method for the identification of mobile devices, which will qualitatively complement existing security models with another feature for detecting unauthorized access.

KEYWORDS: security, Wi-Fi, identification, spectrum, asymmetry coefficient, mobile device.

ABBREVIATIONS

A is a smartphone Redmi note 4X;
ACF is an autocorrelation function;
B is a smartphone Redmi note 4X, similar to "A", but the second copy;
C is a smartphone MeizuM5 Note;
CCF is a cross-correlation function;
D is a smartphone Honor 09 Lite;
E is a smartphone MeizuM6 Note;
IDS is an intrusion Detection System;
IoT is an Internet of Things;
MSD is a mean squared deviation;
OSI is a open system interconnection;
Wi-Fi is a wireless fidelity;
WPA is a Wi-Fi Protected Access.

NOMENCLATURE

A is a coefficient of asymmetry;
$B(\tau)$ is a degree of signal difference;
$B(j)$ is a correlation function;
B_{cp} is an average value of the correlation function;
i is a spectral component number;
j is a difference in spectral components;
K is a number of mobile users;
m_3 is a central empirical moment of the third order;
N is a number of spectral components;
$P_{L1}(f_i)$ is a power of each spectral component;
$P_{L2}(f_i)$ is a power of each spectral component of the connecting subscriber;
$P_{L2}(f_{i+j})$ is a power of each spectral component displaced spectral components;
$S(t)$ is a harmonic signal;
$S(t-\tau)$ is a harmonic signal is shifted in time;
σ is a mean squared deviation;
Δ is a spectrum width at the level of 0.5.

INTRODUCTION

The rapid development of Wi-Fi networks covers all spheres of human activity. The principle of building wireless networks carries not only advantages in the form of free movement in the coverage area, sufficient data

DOI 10.15588/1607-3274-2024-4-1

transmission speed and low deployment cost, but also a lot of vulnerabilities and threats.

The main advantage of a Wi-Fi network is the transmission of information over radio waves without using wires, but at the same time it is the greatest threat to transmitted information, because controlling information transmitted through the air is not an easy task. Analysis of threats and attacks on wireless networks [1, 2] shows that most often for the removal or modification of information transmitted or stored in the network is the use of foreign equipment, which is very often disguised as network subscribers. In almost every type of attack there is an element that is disguised as a network subscriber.

To protect wireless networks from attacks, IDS is used. They are able to detect and prevent attacks by restricting access to the network or changing the configuration of communication equipment. Signs of attacks in existing IDS are the parameters of network traffic (node network activity, node network settings, data on files and processes) that is, the signs of channel, network and higher levels of the OSI model. This approach is fully justified in leading or fiber-optic networks, where physical connection to the network for intruders is difficult, and therefore the identification of equipment as such is absent (only user authentication is carried out). However, connecting to a Wi-Fi network at the physical level is not a problem for intruders through a torn radio interface.

Therefore, standard protection measures do not provide adequate security [3, 4]. According to Kaspersky Lab [5], any WPA-WPA3 encrypted Wi-Fi network is unprotected and can be attacked by reinstalling the key.

Since it is not possible to control the transmission space of information of a wireless network, then you need to focus on the control (identification) of users of such networks. Each device has its own unique features as a person fingerprints, retina, stroke or handwriting. The equipment of the device included in the Wi-Fi (frequency generator, modulator, radio transmitter, filter, antenna-feeder system) can have their own characteristics [6, 7, 8, 9].

Given the many shortcomings and vulnerabilities that allow malicious influences to successfully overcome the system of information protection, it is important to consider research aimed at comprehensive security, using additional parameters to detect unauthorized access and detection of intruders, namely the search for new methods of comparing spectra, that will allow their use in real protection systems wireless Wi-Fi networks.

The object of study is the process of recognizing similar spectra from different mobile devices from each other. This process is influenced by many factors: technical features of devices, position, distance, signal level and many others.

The subject of study is the evaluation of methods of comparing similar spectra by correlation analysis of the frequency dependence of the signal amplitude.

The purpose of the work is to recognize and identify similar spectrums of mobile devices of wireless Wi-Fi networks to increase the security indicators of the network.

1 PROBLEM STATEMENT

For the input parameters, which are: energy spectra $P_{L1}(f_i)$ (i = 0, 1 ,…, N) (obtained experimentally [10], two of them are presented in Figure 1) K legal network users, together with their MAC-addresses stored in the database in the form of a matrix with dimensions [N×K]; energy spectrum of signals of subscribers connected $P_{L2}(f_i)$ and subject to the identification procedure; the correlation function $B(j)$, is calculated, which is a function of the difference in frequency readings j = –N+1… .N–1.

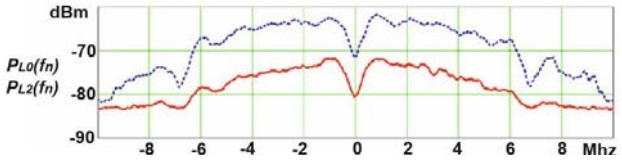

Figure 1 – Spectra of devices

The initial data are parameters $B(j)$ such as σ, Δ, A.

The task of the work consists in choosing such a parameter $B(j)$ (σ, Δ, A) that would allow in the future to quickly and with minimal error determine whether the subscriber who joined the wireless network is the one he claims to be (whose MAC address he uses). For the possibility of identification, the condition must be fulfilled: ACF (σ, Δ, A) → min, and for CCF (σ, Δ, A) → max.

2 REVIEW OF THE LITERATURE

The literature review showed that a fairly developed theory of calculating spectra by incomplete time series, using various window functions, various methods of averaging and smoothing them. In particular, the methods of Bartlett, Welch, Blackman-Tewkey, modified periodogramm and others. They can be used to detect weak frequency components in the signal, or bands where its maximum energy is concentrated, as well as for other similar tasks.

Many studies are conducted to identify by spectra, they use a variety of technologies and methods of comparison. From the calculation of the average amplitude value to neural networks [11, 12]. But all of them are aimed at distinguishing technologies according to frequency and modulation. In our case, we need already existing spectra, and almost identical ones that work at the same frequency, use the same modulation, accurately distinguish as fingerprints in humans.

The biometric identity perspective can be found in [13, 14].

In [15] the authors conduct research on the passive radiometric identification system of the PARADIS devices. This system is its own development of authors. The authors claim that PARADIS identifies unauthorized devices by comparing the radiometric signature of the device with known sanctioned signatures. PARADIS performs identification using two classifiers. One uses the support vector machine algorithm, while the other uses the k-nearest neighbor algorithm. Before a new network

DOI 10.15588/1607-3274-2024-4-1

card is allowed to access the network, the administrator measures and records its radiometric signature. The calculated signature is sent to the PARADIS server for identification. The system then compares the signature obtained with the known radiometric signatures of authorized network cards. If the radiometric signature does not match the network card that is allowed to use the secret key, PARADIS notifies the administrator of a possible security breach.

The accuracy of the studied systems is simply impressive – 99%. But the material in [15] does not provide detailed technical information on how radiometric signatures are calculated, it is not specified what exactly is understood by the concept of "radiometric signature" and on what it is based. And the nodes of the network are identified by the last four digits of the MAC address, which is the most vulnerable.

The non-standard identification approach for IoT is presented in [16]. This method is based on the use of not the entire spectrum, but the duration of the transition process, which is achieved in the obtained smooth version of the instantaneous amplitude characteristics of the signals of the transmitter using the method of averaging the sliding window.

The classification characteristics of the spectral prints proposed by the authors are evaluated using experimental data and described by a matrix of confusion. The efficiency of spectral prints is quantitatively determined by the criterion of class resolution. The effectiveness of the proposed method in the influence of noise through Monte Carlo simulation is shown.

In the article of the authors of this work [10] experimentally obtained spectra in visual analysis (with simple consideration of drawings) have something in common, and in some ways differ. The similarity of the spectra of Wi-Fi signals of the same device in different positions and differences in the spectra of radiation in different devices are established, which can be used to identify them. For comparison, the method of calculating the mean square of the difference between the corresponding spectral samples was used, taking into account the difference in the average power of different signals, which allows comparing the spectra obtained in different conditions with the patterns. The study [10] shows that each device has its own individual signal spectrum, which can be seen even visually and the results of analysis of spectra based on the calculation of the mean square of the difference indicate their difference. But the method under consideration gives in some cases similarity of results, so you need to look for other methods that can reduce the probability of a first kind error.

For signal analysis has a great practical application correlation statistical analysis of experimental data. The essence of correlation analysis is reduced to the establishment of the equation of regression (algebraic equation), that is, the type of rectilinear or curved relationship between the values, the estimation of the tightness (force) of the relations and the reliability of the measurement results [17]. Similar solutions have been found in the field of voice identification [18].

Therefore, the actual task is to find new methods for comparing the spectra of mobile devices, which will allow their use in real protection systems wireless Wi-Fi networks.

3 MATERIALS AND METHODS

To quantify the degree of difference between the $S(t)$ signal and its offset copy $S(t–\tau)$, the operation uses the $S(t)$ signal's ACF, which is equal to the dot product of the signal and its copy:

$$B(\tau) = \int_{-\infty}^{\infty} S(t)S(t-\tau)dt\,. \tag{1}$$

We apply the expression (1) to compare the spectra:

$$B(j) = \frac{1}{N}\sum_{i=0}^{N-1} P_{L1}(f_i)P_{L2}(f_{i+j})\,. \tag{2}$$

The specified expression (2) is used to calculate the correlation of the template (ACF) and the spectrum of the template with the spectra of "alien" devices (CCF).

The calculation of the MSD for the functions obtained is calculated by the formula:

$$\sigma = \sqrt{\frac{1}{2N\cdot B_{cp}}\sum_{j=-N+1}^{N-1}\left([(j)]^2\cdot B(j)\right)}, \tag{3}$$

$$B_{cp} = \frac{1}{2N}\sum_{j=-N+1}^{N-1} B(j)\,. \tag{4}$$

An important indicator of correlation processing is the asymmetry coefficient. The calculation of the asymmetry coefficient in the work is realized as the ratio of the central empirical moment of the third order to the cube of the mean squared deviation:

$$A = \frac{m_2}{\sigma^2}\,, \tag{5}$$

where, the central empirical moment of the third order was calculated by the formula:

$$m_2 = \frac{1}{2N\cdot B_{cp}}\sum_{j=-N+1}^{N-1}(j-j_{cp})^2 B(j)\,. \tag{6}$$

In relation to our case, asymmetry was calculated:

$$A = \frac{\frac{1}{2N\cdot B_{cp}}\sum_{j=-N+1}^{N-1}(j-j_{cp})^2 B(j)}{\sqrt{\frac{1}{2N\cdot B_{cp}}\sum_{j=-N+1}^{N-1}\left([(j)]^2\cdot B(j)\right)}}\,. \tag{7}$$

DOI 10.15588/1607-3274-2024-4-1

4 EXPERIMENTS

In accordance with the task, the spectra of mobile devices were calculated and modeled in the Mathcad environment. The simulation was conducted sequentially in accordance with (1)–(7).

The results of the simulation are displayed in the form of tables, graphs of dependence on the drug of ACF and CCF for the studied spectra and in the form of drawings.

5 RESULTS

Figure 2 shows that the peaks of correlation functions are at different levels, which makes it impossible to compare them. This is due to the fact that the signal level when removing the patterns of spectra of different mobile devices differ. In practice, the signal level from the devices may be quite insignificant. Therefore, for the convenience of comparing the correlation functions, they were normalized according to the maximum signal strength level when the peaks of the correlation functions are in 1, as shown in Figure 3.

There was no significant difference in the dependencies shown in Figure 3. The results of the calculation σ for one of the templates (A) in relation to the different provisions of the devices are shown in Table 1, showing similar results. Thus, this indicator can not be used to identify mobile devices.

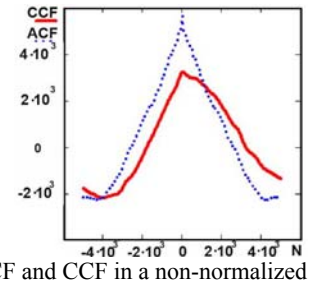

Figure 2 – ACF and CCF in a non-normalized form (ACF smartphone D with a smartphone D template)

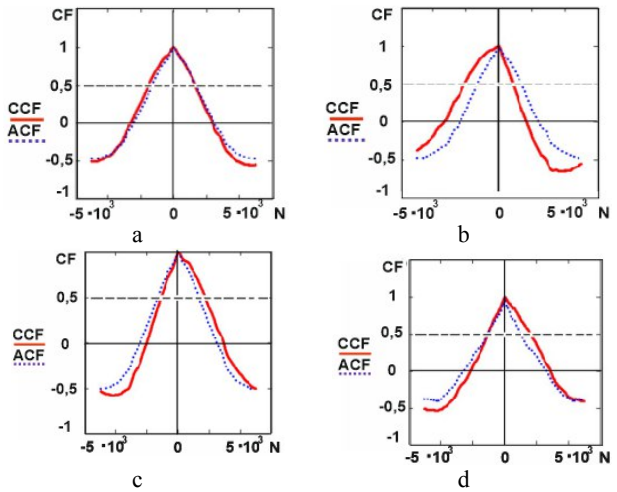

Figure 3 – ACF and CCF in the normalized form
A – ACF smartphone A with a smartphone A template;
B – ACF smartphone D with a smartphone template C;
B – ACF smartphone C with A smartphone A template;
G – ACF smartphone with a smartphone pattern D

Table 1 – σ calculations for pattern A

template	A1	A1	A3	A4	B1	B2	B3	B4
σ	945	943	940	937	937	949	952	952
template	C1	C2	C3	C4	D1	D2	D3	D4
σ	955	953	942	943	944	954	940	932

The study of the width (in the amount of reprint) of the ACF for templates and CCF for all devices with respect to the template at level 0.5 are shown in Table 2.

Table 2 – the results of measuring the width of the ACF and CCF by level 0.5

Position	The width of the ACF (CCF) on level 0.5					
	Pattern A	A	B	C	D	E
1	2650	2655	2715	2864	2701	2929
2	2650	2688	2726	2879	2833	2937
3	2650	2675	2796	2817	2588	2844
4	2650	2635	2796	2785	2459	2807
Middle	2650	2663	2758	2836	2645	2879

From Table 2 it is clear that the width of the CCF of other devices can be narrower than the ACF.

On the basis of the completed calculations, we can say that:

– There is no significant difference in the mean squared deviation of the CCF for the template with its own device and other people's ones;

– The difference in the width of CCF by level 0.5 is also not detected. When normalizing, all functions are almost identical;

– A significant shift in the central frequency in the CCF is also not observed.

Thus, parameters up to the second order inclusive do not allow to detect the difference between the two spectra. But from Figure 3 it is clear that the CCF have a certain "bias", which can be characterized by an estimation of asymmetry for the empirical distribution.

Table 3 shows the results obtained for (7) the asymmetry coefficients. The average value of the asymmetry coefficient was calculated by summing each element by the value of the module. The number near the letter means the number of position of the mobile device, and the index "sr. average for four positions.

For greater observation, the results of this study are presented in graphic form in Figure 4, which shows the

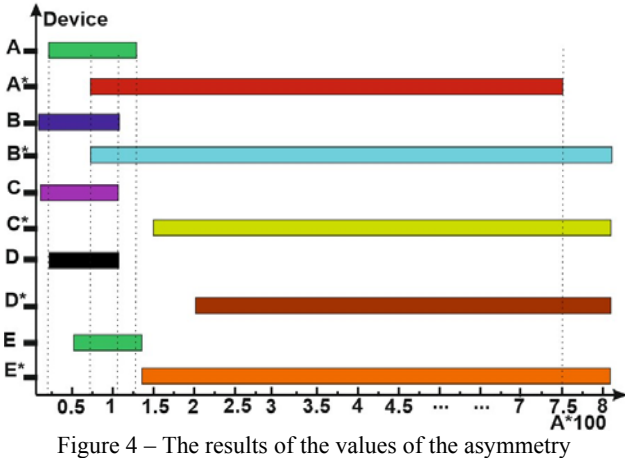

Figure 4 – The results of the values of the asymmetry coefficients in the graphic form

DOI 10.15588/1607-3274-2024-4-1

Table 3 – results of the value of the assymmetry coefficients

		Device patterns									
		A	$A_{ср}$	B	$B_{ср}$	C	$C_{ср}$	Д	$Д_{ср}$	E	$E_{ср}$
Devices in different positions	A1	0.013	0.0057	0.008	0.007	–0.07	0.07	0.075	0.06	0.038	0.03
	A2	0.002		–0.005		–0.07		0.06		0.03	
	A3	0.004		–0.007		–0.07		0.06		0.029	
	A4	0.004		–0.008		–0.066		0.059		0.017	
	B1	0.005	0.008	–0.007	0.0048	–0.066	0.074	0.049	0.07	0.026	0.04
	B2	0.003		–0.0004		–0.076		0.074		0.038	
	B3	0.016		0.011		–0.075		0.087		0.046	
	B4	0.006		0.0007		–0.079		0.077		0.036	
	C1	0.077	0.07	0.079	0.07	–0.008	0.0055	0.057	0.025	0.093	0.09
	C2	0.077		0.08		0.011		–0.002		0.065	
	C3	0.063		0.067		–0.002		0.022		0.093	
	C4	0.064		0.069		0.001		0.017		0.094	
	D1	–0.077	0.06	–0.083	0.07	0.038	0.04	–0.023	0.01	–0.08	0.06
	D2	–0.07		–0.075		–0.039		0.016		–0.05	
	D3	–0.051		–0.057		–0.056		0.012		–0.049	
	D4	–0.048		–0.022		–0.022		0.002		–0.068	
	E1	–0.012	0.024	–0.022	0.03	–0,098	0.09	0.08	0.07	0.016	0.016
	E2	–0.012		–0.019		–0.114		0.08		0.022	
	E3	–0.038		–0.044		–0.078		0.052		–0.014	
	E4	–0.038		–0.045		–0.078		0.051		–0.012	

ranges of the obtained values of ACF and CCF. The letters in the figure show the ranges of values for the template and its device, and the letter with an asterisk shows the ranges of values for the template with other devices.

As can be seen from Figure 4, the values of the asymmetry coefficients for a template with its own device are in the range from 0 to 1.5. And the value for templates with other devices can be from 0.7 to 8. In most cases, the values of templates and other devices do not overlap. But still for some mobile tristroi (A and B) we see that there is a small range of values. In this range, additional research of the spectrum should be carried out (visually they differ significantly from each other) in order to prevent errors of the first kind.

6 DISCUSSION

The considered method of identification of devices in wireless networks Wi-Fi uses the sign of the state of the network at the physical level, which allows to detect and together with intrusion detection systems to prevent a number of attacks and thereby increase the security of Wi-Fi networks.

The obtained results showed the minimum value of the asymmetry coefficient when comparing the template with different positions of your own device.

Therefore, this feature can also be used to identify Wi-Fi devices in a model to detect abnormal network states [19]. Previous studies [10] which were based on the calculation of the mean square of the difference due to different signal levels can give a large error in the results, in contrast to the proposed method where the obtained values of the correlation functions were normalized.

Further research is advisable to develop in the direction of finding additional methods of analysis in ranges that do not give an unambiguous answer to the belonging of the mobile spectrum to the template. It is also necessary to confirm the effectiveness of this method in the presence of noise and experimental studies of the decision-making model on the abnormal state of the network [19] taking into account the parameter under consideration.

CONCLUSIONS

1. The method of processing the results of measuring the radiation spectra of Wi-Fi devices by assessing the asymmetry coefficient of the intercorrelation function of the spectrum of Wi-Fi devices is proposed.

2. It is shown that the asymmetry coefficient of the CCF for the template and the corresponding device is significantly less than for the template and other device, which can serve as an identifying sign.

DOI 10.15588/1607-3274-2024-4-1

3. Set the range of the asymmetry coefficients, which can correspond to both the same device in different positions and different devices. To identify devices in this range, it is necessary to carry out a more detailed analysis of the spectrum.

ACKNOWLEDGEMENTS

The authors express their gratitude to the Department of computer Radio Engineering and Systems of Technical Information Protection of Kharkiv National University of Radio Electronics for access to equipment for experimental research, the analysis and processing of which was written publication.

REFERENCES

1. Sahabul A., Debashis D. Analysis of security theats in wireless sensor network, *International Journal of Wireless & Mobile Networks*, 2014, Vol. 6, № 2, pp. 35–46. DOI: 10.5121/ijwmn.2014.6204
2. Gupta A., Jha R. K. Security threats of wireless networks: A survey, *International Conference on Computing, Communication & Automation, Greater Noida, 15–16 May 2015: proceedings*. Greater Noida, IEEE, 2015, pp. 389–395. DOI: 10.1109/CCAA.2015.7148407
3. Catania. C. A., Garino C. G. Automatic network intrusion detection: Current techniques and open issues, *Computers and Electrical Engineering,* 2012, Vol. 38, pp. 1062–1072. DOI: 10.1016/j.compeleceng.2012.05.013
4. Garcıa-Teodoroa P., Dıaz-Verdejoa J., Macia´-Fernandeza G. et al. Anomaly-based network intrusion detection: Techniques, systems and challenges, *Computers & Security*, 2009, Vol. 28, pp. 18–28. DOI: 10.1016/j.cose.2008.08.003
5. “Your Wi-Fi connection is unsecured” warning [Electronic resource]. Access mode: https://support.kaspersky.com/common/macos/14582
6. Agilent 802.11a/g Manufacturing Test Application Note : A Guide toGetting Started. Application note 1308-3 [Electronic resource]. Access mode: https://studylib.net/doc/18797817/agilent-802.11a-g-manufacturing-test-application-note-—-a...
7. Making 802.11g transmitter measurements. Application note 1380-4 [Electronic resource]. Access mode: https://www.testunlimited.com/pdf/an/5988-7813EN.pdf
8. RF Testing of WLAN products. Application note 1380-1 [Electronic resource]. Access mode: https://www.testunlimited.com/pdf/an/5988-3762EN.pdf
9. Agilent Technologies. Testing and Troubleshooting Digital RF Communications Transmitter Designs. Application note 1313 [Electronic resource]. Access mode: https://archive.org/details/manualzilla-id-6880267/page/12/mode/2up
10. Antipov I. Ye., Vasylenko T. O. Ydentyfykatsyia mobylnykh ustroistv po osobennostiam spektrov ykh syhnalov, *Radiotekhnika. Vseukr. mizhvid. nauk.-tekhn. zb.*, 2020, Vyp. 201, pp. 91–97.
11. Perez-Neira A. I., Member S., Lagunas M. A., Rojas M. A., Stoica P. Correlation Matching Approach for Spectrum Sensing in Open Spectrum Communications [Electronic resource]. Access mode: https://www.academia.edu/7471893/Correlation_matching_approach_for_spectrum_sensing_in_open_spectrum_communications
12. Tekbıyık K., Akbunar Ö., Ekti A. R.et al. Correlation matching approach for spectrum sensing in open spectrum communications, *IEEE Transactions on Signal Processing*, 2020, Vol. 57, № 12, pp. 18–28. DOI: 10.1109/TSP.2009.2027778
13. Ross A., Jain A. Information fusion in biometrics, *Pattern Recognition Letters,* 2003, Vol. 24, pp. 2115–2125. DOI: DOI:10.1016/S0167-8655(03)00079-5
14. Tuyls P., Goseling J. Capacity and Examples of Template-Protecting Biometric Authentication Systems, *Biometric Authentication, ECCV International Workshop, Prague, 15 May, 2004: proceedings*. Prague, BioAW, 2004. pp. 1–13. DOI:10.1007/978-3-540-25976-3_15
15. Brik V., Banerjee S., Gruteser M. et al. Wireless device identification with radiometric signatures, *MobiCom ‘08: Proceedings of the 14th ACM international conference on Mobile computing and networking, San Francisco 14–19 September 2008: proceedings*. San Francisco, 2008, pp. 116–127. DOI:10.1145/1409944.1409959
16. Köse M. Taşcioğlu S., Telatar Z. RF Fingerprinting of IoT Devices Based on Transient Energy Spectrum, *IEEE Access*, 2019, Vol. 7, pp. 18715–18726. DOI: 10.1109/ACCESS.2019.2896696
17. Sydenko V. M., Hrushko Y. M. Osnovy nauchnykh yssledovanyi. Kharkov, Vyshcha shkola, 1978, 200 p.
18. Craciun A., Gabrea M. Correlation coefficient-based voice activity detector algorithm, *Canadian Conference on Electrical and Computer Engineering, Canada, 2–5 May, 2004: proceedings*. Niagara Falls, ON, Canada, IEEE, 2004, pp. 1789–1792. DOI: 10.1109/CCECE.2004.1349763
19. Antipov I., Vasilenko T. Improving the model of decision making about abnormal network state using a positioning system, *Eastern-European Journal of Enterprise Technologies*, 2019, Vol. 1, № 9 (97), pp. 6–11. DOI: 10.15587/1729-4061.2019.157001

Received 06.05.2024.
Accepted 26.09.2024.

DOI 10.15588/1607-3274-2024-4-1

УДК 621.396.946

ІДЕНТИФІКАЦІЯ МОБІЛЬНИХ ПРИСТРОЇВ ЗА КОРЕЛЯЦІЙНИМИ ОСОБЛИВОСТЯМИ ЇХ СИГНАЛІВ

Антіпов І. Є. – д-р техн. наук, професор, завідувач кафедри комп'ютерної радіоінженерії та систем технічного захисту інформації, Харківський національний університет радіоелектроніки, м. Харків, Україна.

Василенко Т. О. – канд. техн. наук, старший викладач кафедри комп'ютерної радіоінженерії та систем технічного захисту інформації, Харківський національний університет радіоелектроніки, м. Харків, Україна.

АНОТАЦІЯ

Актуальність. Масовому поширенню Wi-Fi мереж сприяє простота їх розгортання, висока швидкість, універсальність і зручність використання. Розвиток і поширення цих мереж триває, незважаючи на наявність ряду недоліків. Одним з недоліків є їх вразливість до різних видів атак, у тому числі, основаних на підробці (імітації) ідентифікаційних даних. Разом з тим існують ознаки фізичного рівня, знання яких розширює уявлення про стан мережі, може сприяти підвищенню надійності ідентифікації абонентів мережі і таким чином запобіганню ряду атак. Це дослідження направлене на теоретичне обґрунтування можливості їх застосування.

Мета. Метою дослідження є оцінка застосування детального аналізу спектрів сигналів, випромінюваних пристроями, підключеними до безпровідних мереж Wi-Fi, для їх ідентифікації. Для досягнення поставленої мети необхідно на основі експериментально виміряних спектрів безпровідних пристроїв, підключених до мережі Wi-Fi, провести аналіз отриманих результатів та оцінити можливість використання спектра для ідентифікації мобільних пристроїв.

Метод. В даній роботі запропоновано метод обробки результатів вимірювання спектрів випромінювання Wi-Fi пристроїв шляхом оцінки коефіцієнта асиметрії взаємокореляційної функції спектру Wi-Fi пристроїв. Для оцінки ефективності методу використовувалося математичне моделювання.

Результати. Результати досліджень показують, що мінімальне значення коефіцієнта асиметрії при порівнянні шаблону з різними положеннями власного пристрою, і великі значення коефіцієнта асиметрії при порівнянні шаблонів з чужими спектрами. Отже, ця ознака також може бути використана для ідентифікації Wi-Fi пристроїв.

Висновки. Результати досліджень говорять про можливість застосування запропонованого методу для ідентифікації мобільних пристроїв , що дозволить якісно доповнити існуючі моделі забезпечення безпеки ще однією ознакою виявлення несанкціонованого доступу.

КЛЮЧОВІ СЛОВА: безпека, Wi-Fi, ідентифікація, спектр, коефіцієнт асиметрії, мобільній пристрій.

ЛІТЕРАТУРА

1. Sahabul A. Analysis of security theats in wireless sensor network / A. Sahabul, D. Debashis // International Journal of Wireless & Mobile Networks – 2014. – Vol. 6, № 2. – P. 35–46. DOI: 10.5121/ijwmn.2014.6204
2. Gupta A. Security threats of wireless networks: A survey / A. Gupta, R. K. Jha // International Conference on Computing, Communication & Automation, Greater Noida, 15–16 May 2015: proceedings. – Greater Noida: IEEE, 2015. – P. 389–395. DOI: 10.1109/CCAA.2015.7148407
3. Catania. C. A. Automatic network intrusion detection: Current techniques and open issues / C.A. Catania, C. G. Garino // Computers and Electrical Engineering. – 2012. – Vol. 38. – P. 1062–1072. DOI: 10.1016/j.compeleceng.2012.05.013
4. Anomaly-based network intrusion detection: Techniques, systems and challenges / [P. Garcıa-Teodoroa, J. Dıaz-Verdejoa, G. Macia´-Fernandeza et al.] // Computers & Security. – 2009. – Vol. 28. – P. 18–28. DOI: 10.1016/j.cose.2008.08.003
5. "Your Wi-Fi connection is unsecured" warning [Electronic resource]. – Access mode: https://support.kaspersky.com/common/macos/14582
6. Agilent 802.11a/g Manufacturing Test Application Note : A Guide toGetting Started. Application note 1308-3 [Electronic resource]. – Access mode: https://studylib.net/doc/18797817/agilent-802.11a-g-manufacturing-test-application-note---a...
7. Making 802.11g transmitter measurements. Application note 1380-4 [Electronic resource]. – Access mode: https://www.testunlimited.com/pdf/an/5988-7813EN.pdf
8. RF Testing of WLAN products. Application note 1380-1 [Electronic resource]. – Access mode: https://www.testunlimited.com/pdf/an/5988-3762EN.pdf
9. Agilent Technologies. Testing and Troubleshooting Digital RF Communications Transmitter Designs. Application note 1313 [Electronic resource]. – Access mode: https://archive.org/details/manualzilla-id-6880267/page/12/mode/2up
10. Антіпов І. Є. Идентификация мобильных устройств по особенностям спектров их сигналов / І. Є. Антіпов, Т. О. Василенко // Радіотехніка. Всеукр. міжвід. наук.-техн. зб. – 2020. – Вип. 201. – С. 91–97.
11. Correlation Matching Approach for Spectrum Sensing in Open Spectrum Communications / [A. I. Pérez-Neira, S. Member, M. A. Lagunas et al.] [Electronic resource]. – Access mode: https://www.academia.edu/7471893/Correlation_matching_approach_for_spectrum_sensing_in_open_spectrum_communications
12. Correlation matching approach for spectrum sensing in open spectrum communications [K. Tekbıyık, Ö. Akbunar, A. R. Ekti et al.] // IEEE Transactions on Signal Processing. – 2020. – Vol. 57, № 12. – P. 18–28. DOI: 10.1109/TSP.2009.2027778
13. Ross A. Information fusion in biometrics / A. Ross, A. Jain // Pattern Recognition Letters. – 2003. – Vol. 24. – P. 2115–2125. DOI: DOI:10.1016/S0167-8655(03)00079-5
14. Tuyls P. Capacity and Examples of Template-Protecting Biometric Authentication Systems / P. Tuyls, J. Goseling // Biometric Authentication, ECCV International Workshop, Prague, 15 May, 2004: proceedings. – Prague : BioAW, 2004. – P. 1–13. DOI:10.1007/978-3-540-25976-3_15
15. Wireless device identification with radiometric signatures [V. Brik, S. Banerjee, M. Gruteser et al.] MobiCom '08: Proceedings of the 14th ACM international conference on Mobile computing and networking, San Francisco 14–19 September 2008: proceedings. – San Francisco, 2008. – P. 116–127. DOI:10.1145/1409944.1409959
16. Köse M. RF Fingerprinting of IoT Devices Based on Transient Energy Spectrum / M. Köse, S. Taşcioğlu, Z. Telatar // IEEE Access. – 2019. – Vol. 7. – P. 18715–18726. DOI: 10.1109/ACCESS.2019.2896696
17. Сиденко В. М. Основы научных исследований / В. М. Сиденко, И. М. Грушко. – Харьков : Выща школа, 1978. – 200 с.
18. Craciun A. Correlation coefficient-based voice activity detector algorithm / A. Craciun, M. Gabrea // Canadian Conference on Electrical and Computer Engineering, Canada, 2–5 May, 2004: proceedings. – Niagara Falls, ON, Canada, IEEE, 2004. – P. 1789–1792. DOI: 10.1109/CCECE.2004.1349763
19. Antipov I. Improving the model of decision making about abnormal network state using a positioning system / I. Antipov, T. Vasilenko // Eastern-European Journal of Enterprise Technologies. – 2019. – Vol. 1, № 9 (97). – P. 6–11. DOI: 10.15587/1729-4061.2019.157001

DOI 10.15588/1607-3274-2024-4-1