ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 6, Issue 7 , July 2019

The method of searching for digital means of illegal reception of information in information systems in the working range of Wi-Fi

Laptev A.A., Barabash O.V., Savchenko V.V., Savchenko V.A., Sobchuk V.V.

P.G.Ph.D., Senior Researcher, Associate Professor of the Department of Information and Cybersecurity Systems, State University of Telecommunications, Kyiv, Ukraine;
Doctor of Technical Sciences, Professor, Head of the Department of Higher Mathematics, State University of Telecommunications, Kyiv, Ukraine;
Masters of Software Development,Department of Informatics and IT, National Polytechnic Institute "KPI";
Doctor of Technical Sciences, ProfessorDepartment of Technical Cybersecurity, State University of Telecommunications, Kyiv, Ukraine;
Candidate of Physical And Mathematical Sciences, Associate Professor, Assistant Professor of The Department of Differential Equations And Mathematical Physics of the Faculty of Information Systems, Physics and Mathematics, Lesya Ukrainka Eastern European National University, Lutsk, Ukraine;

ABSTRACT An analysis of the Wi-Fi digital frequency range with various devices and devices is carried out. The advanced method of searching digital means of secret information acquisition in the digital Wi-Fi range is provided, which allows, in addition to the classic search methods, to further analyze the MAC addresses of the means. The methodical recommendations for the creation of a modern software and hardware complex for the analysis of the search for secret means of receiving information that operate under the cover of Wi-Fi networks are developed.

KEY WORDS: Wi-Fi range, voice recorder, tacit reception, radio frequency spectrum, Wi-Fi-camera, MAC addresses.

I.FORMULATION OF THE PROBLEM

Considering the history of Wi-Fi, it should be noted that the abbreviation Wi-Fi is the abbreviated name of the registered trademark Wi-Fi AUiance. Wi-Fi technology was developed in 1991 by NCR Corporation (which at that time was absorbed by AT & T, and since 1997 became independent again) and was originally intended for use in trading cash registers. [1]. The technology was based on the methodology for transmitting data over a radio channel at a frequency of 2.4 GHz using signal coding with operating frequencies and special applications. Wi-Fi technology is used to organize high-speed wireless LANs operating in the international non-licensed frequency range (ISM) of 2.4 GHz and 5 GHz. [2] The main advantage of Wi-Fi before other technologies is the high speed of transmission (up to 1300 Mbps). The scope of this technology is related to Internet access networks, wireless transmission of audio and video information, industrial telemetry, transport local wireless networks.

Almost all wireless video cameras and speed loggers that are installed on highways use Wi-Fi. Also, this technology is used to organize local networks between buildings and industrial objects. It should be emphasized that the 5 GHz Wi-Fi range is best for the organization of industrial local area networks in the presence of high-level barriers. Thanks to the tight attachment to a specific area within which information is distributed, Wi-Fi is the perfect technology for a paid Internet connection in cafes, restaurants, hotels.

At present, it is difficult to find another active radio frequency spectrum used at 2.4 GHz. This range includes Wi-Fi, Bluetooth, ZigBee, analog and digital video transmitters, remote control and access systems, microwave ovens and more. Naturally, the more used is the area of the radio frequency spectrum, the more difficult it is to control and analyze. This circumstance is often decisive when choosing environment-haters for the option of masking their privately- illegal receiving information (IRI) to intercept restricted information. Based on the above, the search for the IRI in the range of Wi-Fi is especially important, and the development of a search method for such IRI is an urgent task.

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 6, Issue 7 , July 2019

II. ANALYSIS OF RECENT RESEARCH AND PUBLICATIONS.

The task of searching for tacit removal of information is dedicated to a large number of publications. The paper Zakharov A. V. Specifications for advanced analyzer Wi-Fi networks (Electronic resource), examines the issues of the analysis of radio control systems (radiomonitoring) with different technical parameters, which combine one, they can only display and (at best) store panoramas of the spectrum of signals in the airspace. The task of analyzing digital legal channels does not solve them at all.

Krivtsun A. V. using the new features of the complex radio monitoring and digital signal analysis "Kassandra-M" to detect modern special technical means for the transmission of information by radio (Electronic resource), discusses Wi-Fi which is used in various wireless telemetry systems in transport. The 5 GHz Wi-Fi band is best for the organization of industrial local area networks in the presence of high-level interference. It is proved that the "classical" method of searching this frequency band can not be analyzed. That is, in order to look for IRI, other methods are needed.

Vlasov A. Article-office Wireless communication: DECT and Wi-Fi, the complex of radio monitoring "Delta" is considered, which continues the line of the most advanced and technological solutions in the field of radio monitoring. The complex provides a wide range of capabilities for detecting and identifying signal sources. The disadvantage of it is that there is no possibility of identifying IRI and automatic localization.

From the analysis of modern literature, one can conclude that there are practically no universal devices (devices, software complexes) for analyzing digital packages, in relation to the tasks of search radio control. Therefore, the task of detecting IRI working in the Wi-Fi range is relevant.

III.THE PURPOSE OF THE ARTICLE

The purpose of the article is based on the analysis of the digital frequency range of Wi-Fi and real spectrograms, to identify the characteristics of the identification of the external nature of the article and to improve the method of searching for digital IRI working in the Wi-Fi range.

IV.PRESENTING MAIN MATERIAL

By using highly loaded frequency bands for the work of the IRI, the attacker intends to maximize their detection, wisely using the commonly used and common communication standards in these ranges. For the Wi-Fi range, this greatly simplifies the production of IRI because of the use of common, affordable and inexpensive components (electronic radio components and modules) and well-designed engineering solutions.

But most importantly, it's difficult to distinguish between the work of two devices using the same digital communication standard without identifying their unique identifiers (IDs). In the case of Wi-Fi, this identifier is a MAC address or LLC. In this article, we will not touch on the security of legitimate Wi-Fi networks, this is a separate topic. In this case, we are interested in the use of Wi-Fi technology, which is used in the basis of OEM manufacturing, as well as what requirements need to be presented to modern means of analyzing Wi-Fi networks in terms of the field of search and localization of Outer Space for preventing the leakage of information over the frequency radio channel Wi- Fi.

The urgency of the foregoing, in addition to the theoretical justification, is also confirmed by the following example: only in an hour of travel in May this year on the route Maidan Nezalezhnosti street. Velyka Zhytomyrska Lvivska street The January drivers (Kyiv) specialists recorded 947 unique MAC addresses. Of these, 552 access points and 395 devices are in stand-by mode without a current connection (basically these are smartphones whose owners do not turn off Wi-Fi far from the registered access points). At the same time, 50 hidden networks were detected (point-to-point connection is organized).

Consider a high-quality mini recorder with a built-in Wi-Fi transmitter that combines a voice recorder and a Wi-Fi transmitter (Fig. 1.) And the Wi-Fi GEM-atom module (Fig. 2.), As an example of the use of OWN information transfer in the Wi-Fi frequency band. Data on these devices is available on the Acustek Ltd website [3]. Wi-Fi Micro Voice Recorder Micro Wi-Fi is a unique device for hidden audio surveillance that combines advantages and disadvantages of voice recorders and radio transmitters. Unlike ordinary voice recorders, reading a record from a MicroWi-Fi recorder with a Wi-Fi transmitter does not require physical access to the voice recorder. A voice recorder with a Wi-Fi transmitter only takes a few minutes a day on the radio to transmit recorded information. Therefore, it is

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 6, Issue 7 , July 2019

very difficult to detect such a recorder as a field detector and radio monitoring systems. The dimensions of the Wi-Fi dictophone do not exceed two cigarette lighter sockets.

Fig.1 MicroWi-Fi Recorder

Fig.2. Wi-Fi GEM-atom module

The Wi-Fi dictophone supports variable micro SD cards. The amount of memory supported allows you to record for 300 hours. Built-in battery provides dictaphone for up to 120 hours of battery life. Downloading daily audio tracking on a high-quality Wi-Fi connection takes only a few minutes. Included with the Micro Wi-Fi dictophone comes a mini router. The Wi-Fi voice recorder can be configured to automatically detect the network of the mini-router, connect to it, and make audio downloads. In this mode, the operator is sufficiently close to the laptop with the connected router at the distance of the Wi-Fi network (up to 50 meters indoors) to download all the accumulated information. A voice recorder can also be configured to work on a regular (such as office) Wi-Fi network. In this case, Micro Wi-Fi can download the accumulated audio information to the remote computer according to the schedule of the user.

Taking into account the foregoing, one can distinguish the main features of the means of secret reception of information in the range of Wi-Fi:

- possibility of digital audio recording with saving on micro SD card;
- standard size recorder matchbox;
- Built-in microphone allows recording at a distance of up to 10 m;
- presence of an input for connecting an external microphone;
- presence of modes of activation of the recording by schedule and by voice;
- stand-alone operation for one charge of the battery up to 120 hours;
- remote management and forwarding of records using Wi-Fi connection;
- downloading 24 hours of recording takes only about 5 minutes;
- use of flexible schedule of switching on / off Wi-Fi transmitter;
- the possibility of audio monitoring in real time via Wi-Fi connection;
- Possibility of automatic recognition and downloading of records at the appearance of a mobile access point in the zone of action (up to 50 m);
- the ability to connect to any stationary Wi-Fi access point.

Means of tacit reception of information can be found at the time of data transmission, but in the mode of recording only to detect such a dictophone with the help of radio control is difficult, its spurious electromagnetic radiation (SER) is unlikely to be able to identify most of the specialists in radio control. Below is an example of the spurious electromagnetic radiation (SER) of the recorded dictation in recording mode, which can only be detected on very sensitive equipment and at a distance of several centimeters (Fig. 3). The SER spectrum was recorded using the radio control and digital analysis of the "Kassandra-K21" signals [6].

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 6, Issue 7 , July 2019

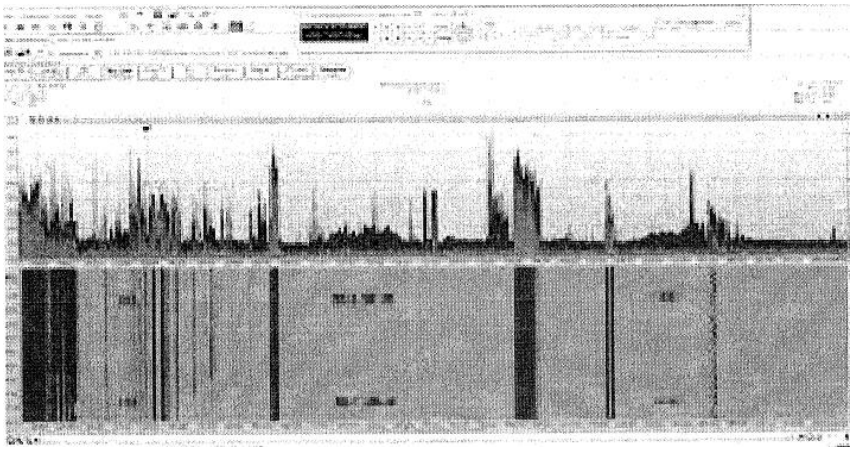

Fig. 3. Secondary electromagnetic radiation of the dictophone in the mode of recording only

So the device is most likely to be detected at the moment of the transfer of accumulated information over the Wi-Fi network (the half hour's transmission of the conversation is carried out in 30 seconds (Fig. 4) [3]). A voice recorder can be detected on the network as an access point, with the unique identifier of the wireless network (SSID) (Service Set Identifier) can assign any name. After testing this dictaphone in real conditions it is possible to determine its main TTX.

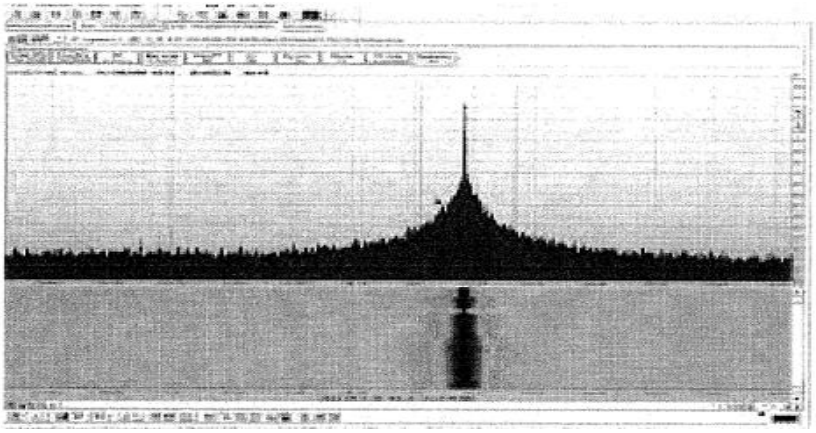

Fig.4 Fix the transfer of record information to the Wi-Fi recorder

A unique wireless network identifier (SSID) is a very important signal regarding the need for a complete revision of the Wi-Fi network monitoring concept. An ongoing and time-consuming analysis of Wi-Fi networks is now becoming relevant, as is radio monitoring on objects with limited access information.

Now, for comparison, imagine, for example, a business center in a big city. Or a great modern office, which has several connected to the common access point network having the same SSID. Today, at some sites, hundreds of Wi-Fi devices are simultaneously accepted (Fig. 5).

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 6, Issue 7 , July 2019

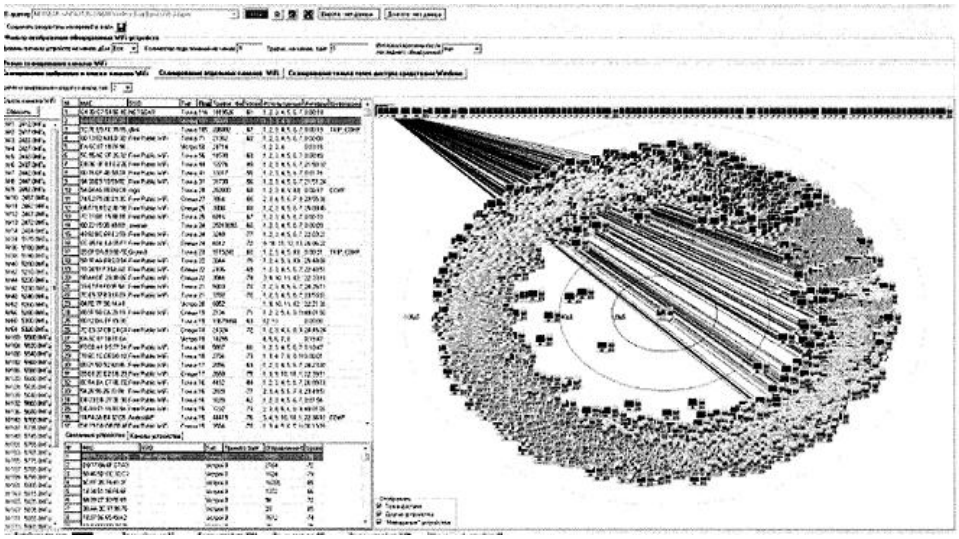

Fig. 5 Vector analysis of Wi-Fi devices of a large office center.

In Fig. 5, the vector analysis made by the search engine in the conditions of the real work of the office center is presented. A circular diagram shows the number of Wi-Fi devices in the office, and the lines indicate the directions on the Wi-Fi device of a specific room.

In such conditions it is very difficult to notice the appearance of another access point with the same name and the one which is almost identical to the other level of the signal. Without knowledge of the MAC addresses of all their devices, nobody is able to understand whether this access point is legal or not.

Based on the foregoing, as well as analysis of new threats, it is possible to form an advanced method for the search for IRI and analysis of Wi-Fi networks. To detect digital radio bookmarks:

1.Continuously (round the clock), control the Wi-Fi network of all standards (IEEE 802.11 a / b / g / n), with the binding of all measurements on time.

2. Searchable MAC address modules should be located directly in the monitored premises (without the need to install additional PCs) and connected to a single network.

3. The analysis should behave without the need to connect to the PC to store the archive of accumulated data for a long time.

4. Must maintain a list of legitimate MAC addresses for the rapid detection and identification of new Wi-Fi transmitters and detect all MAC addresses of all devices.

5. For the ultimate detection of digital radio bookmarks, you need a lightweight, mobile, and economical receiver direction finding module. This module is needed to solve operational tasks.

For permanent maintenance of the countermeasures of technical intelligence requires the availability of multi-server software, support for the zonal placement of a large number of search modules (servers) that will perform tasks for the search of digital radio tabs on a permanent basis. It is in this way that according to the proposed methodology and with the help of the automated search complex (ASC) that can accomplish these tasks it is possible to detect and localize the digital radio tabs that operate under the umbrella of the Wi-Fi frequency range, that is to do work in the area of counteracting the means of technical intelligence.

V. CONCLUSION

1. An analysis of the Wi-Fi frequency range has been carried out, which showed the highest loading of various devices and devices that will be further developed in the future and even more load this frequency range.

2. To look at applications that are most likely to be used, devices for data capture work in the frequency range of Wi-Fi.

3. Real spectrographs and vector analysis of the IRI working on the Wi-Fi range have been carried out, the most optimal conditions for their detection have been discovered.

4. Advanced search engine for digital OEMs that detects digital radio tabs that work in the Wi-Fi range.

ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 6, Issue 7 , July 2019

Directions of further research. Further research is advisable to improve the software for agribusiness, in order to automate the localization of devices with MAC addresses that do not belong to the computer network of the checked premises

REFERENCES

1. Resolution of the Cabinet of Ministers of Ukraine from may 14, 2015 No. 295 "About modification of the Plan of use of radio frequency resource of Ukraine".

2. IEEE Standard for Information technology Telecommunications and information exchange between systems. Local and metropolitan area networks. Specific requirements. Part 11: Wireless LAN Medium Access Control and Physical Layer (PHY) Specifications.

3. The website of the company Acustek Ltd https / [Electronic resource]- access Mode: //www.acustek.com/en (05.06.2019).

4. Zakharov A. V. specifications for advanced analyzer Wi-Fi networks [Electronic resource]Mode of access: http://www.analitika.info/stati3.php?page=1&full=block_article241 (25.05.2019).

5. Ananskikh E. V. what is the eavesdropping devices and how to find them? (part 2), journal "security Service" [Electronic resource] mode of access: http://www.kvirin.com/articles/267/

6. A. V. Krivtsun using the new features of the complex radio monitoring and digital signal analysis "Kassandra-M" to detect modern special technical means for the transmission of information by radio [Electronic resource] /A. V. Krivtsun, A. V. Zakharov access mode: http://www.inspectorsoft.ru/article.php?id=388 (24.05.2019)

7. Vlasov A. office Wireless communication: DECT and Wi-Fi. [Electronic resource]. Mode of access: http://www.dect.ru/dect.html (05.05.2016)

8. Search complexes. [Electronic resource]: https://www.das-ua.com/documents/catalog/search-appliances. (03.05.2019)