Security analysis of wireless communication systems of the millimeter waves band

Salnykov D.[1], Dudka A.[1],Tsopa A.[1]

[1]Radio-Technologies of Information and Communication Systems Department
Kharkov National University of Radio Electronics (KNURE), Kharkiv, Ukraine

dmytro.salnykov@nure.ua, knure.video@gmail.com

***Abstract* — The next-generation 5G wireless communication systems will provide extremely high data rates wit usage millimeter waves band (MM WB) and narrow signal beams. MM WB channel is often considered as difficult for interception by the infringer due to a high directivity and susceptibility to blocking by objects of environment. The general threat model for evaluating the security parameters of information transmission systems at the physical level using a millimeter wave band (MM WB) is considered and formed.**

Keywords — secrecy capacity, physical layer security, millimeter waves.

INTRODUCTION

Increasing the speed of information transfer in modern wireless communication systems, associated with increased traffic of multimedia information and the development of IP-TV technologies, requires a transition to higher frequency ranges of waves. The new standard of information transfer technology *IEEE 802.11ad* uses a range of 60 GHz [1].

However, small-scale objects inside the main beam of the propagation channel cause a reflection, which allows the interception devices to receive a signal outside the main beam. It was experimentally shown in [3] that even small reflectors allow to receive signals of MM WB from the violator. Modern communication devices with metal surfaces, such as mobile phones or laptops, can also cause sufficient signal reflection, which can pose a threat to interception of information.

The concept of a wiretap channel (WCh) [4-6] is currently widely used today to predict the security of wireless information transmission systems at the physical level.

The main objective of the report is the development of a threat model for the MM WB links and an assessment of the security of the wireless information transmission systems with a WCh.

MAIN PART

There are a necessary to take into account the propagation of radio waves and the effects that arise in the real operating conditions of the communication channel when developing a threat model for wireless data transmission systems at the physical level of the OSI model.

First of all, such factors as increase in the volume and speed of information transfer, high gain of antennas with their small aperture and increased noise immunity of the communication channel, the possibility of organizing the local broadband data transmission systems, the usage of highly directional antennas and some particularities of radio waves propagation in the MM WB it are necessary to note among the main advantages of using MM WB in communication systems.

A characteristic property of any radio signals is the decrease in signal level during propagation due to attenuation in free space, losses in atmospheric gases and some other types of additional losses. The essentially more values attenuation of radio-waves in atmospheric gases and hydrometeors [7] is the peculiarity of using MM WB for radio communication (terrestrial, satellite).

Figure 1 shows a systemic model of the wireless communication system of MM WB, which includes a channel for transmitting information from the transmitter of Alice to the receiver of Bob who is an information receiver. The Bob receiver is called as the main or legitimate channel of communication (main channel). Alice sends signals to Bob and uses a narrow beam pattern to improve channel security.

We assume that both the Alice and Bob antennas are perfectly aligned and transmit signals in the optimal direction.

Violator Eve is aimed at intercepting signals that Alice sends to Bob without disturbing her. She acts passively and only listens to signals and tries to receive reflected signals from objects located in the signal beam. For the

convenience of analysis, we assume that Eva uses the same hardware as Alice and Bob. The channel of tapping from the legitimate channel transmitter to the receiver of the unlawful consumer (intruder) is an WCh channel.

Three possible variants of the violator's behavior in the attack on the communication channel can be distinguished if one starts from the systemic model:

- Moving the object's manipulator and placing various objects in the signal beam to cause the signal reflecting toward the fixed intercept position;
- Moving the intruder himself and using reflection from existing objects in the propagation environment, which he cannot change;
- The stationary position of the intruder, who can neither move nor manipulate the objects of the environment and will only try to intercept the signal.

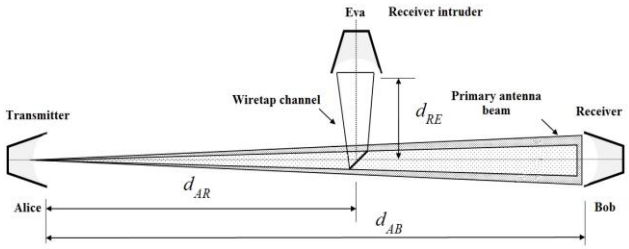

Fig. 1. Systemic model of wireless communication MM WB

Manipulating by an object. This attack model assumes that Eva offender is in a fixed position outside of the main signal beam and it is impossible to receive a signal directly from there. However, Eva places arbitrary objects in the environment to cause the signal deviating to the desired direction. She can control own antenna towards this object in order to optimally receive the part of the transmitted signal and seek to obtain sufficient signal quality for decoding information. At the same time, Eva tries to remain invisible to Alice and Bob, causing only a slight blockage of direct signal transmission.

Positional interception. Unlike the previous model, Eve cannot change the environment but tries to use existing propagation effects. She can freely select a location outside the beam and direct the antenna to any reflector in the environment. Since she cannot affect the blocking in any way, Eva strives only to maximize the quality of the received signal, seeking to find the optimal antenna location and orientation for interception. Despite the fact that the use of existing objects can be more difficult, it is difficult to detect this attack, because nothing does not change in the environment and the communication system operate in normal regime.

Static (stationary) attack. In this model, Eve can neither manipulate the environment nor move to the optimal position of own antenna. This means that Eva must rely on environmental objects in the hope that the signal will be reflected in the necessary direction. As for positional interception, Eve does not affect the lock, but she can control here antenna only from a fixed location for better reception. This is the weakest model of the enemy, but the infringer Eve is almost impossible to detect, because nothing changes in the environment when the communication system works.

In general, a manipulated reflector can be used to perform a manipulation attack anywhere in the signal beam. To simplify the analysis problem, we will assume that the reflected objects should be directly on the center line of the narrow beam between Alice and Bob. This is the optimal case because both the largest signal reflection and signal blocking.

The transmitted and reflected radio rays have the same width when considering plane reflectors (Fig. 2, a). Reflectors with convex shapes (Fig. 2b) scatter the signal in different directions and reflectors with a concave shape (Fig. 2c) focus the signal to a certain focal point.

To analyze the security of the system, we will use the criteria [9], which characterize the information transfer system at the physical level: channel capacity, signal level, signal-to-noise ratio and bit error probability. We will not take into account additional reflections of the signal at several objects in our further analysis of the security of the communication channel.

One of the metrics for evaluating the security of a communication channel at the physical level is the secret performance [8] which is defined as the maximum difference between the information transfer rate in the legitimate and the diversion channels:

$$C_S = \max\{0, C_{AB} - C_{AE}\} = \\ = \left[\log(1+SNR_{AB}) - \log(1+SNR_{AE})\right]^+ \quad (1)$$

Where SNR_{AB} – is the signal-to-noise ratio in the primary channel; SNR_{AB} – signal-to-noise ratio in the branch channel.

The bandwidth of the communication channel between the transmitter and the receiver in the presence of additive white Gaussian noise is determined by the Shannon equation [9]:

$$C = W\log_2(1+SNR) = W\log_2\left(1+\frac{P_R}{N}\right) \quad (2)$$

where: W – channel bandwidth (Hz); P_R – received signal level (W); $N = W \cdot k \cdot T$ – the level of additive Gaussian white noise, k – the Boltzmann constant, which equal to, k =1.3807·W/Hz, $T = 290^o K$ - the temperature in degrees Kelvin.

The level of the received signal, with attenuation of the signal between the antennas according to the exponential law, is calculated by the Friis equation [9]:

$$P_R(d) = P_T \cdot G_T \cdot G_R \left(\frac{\lambda}{4\pi}\right)^2 \cdot \left(\frac{1}{d}\right)^n , \qquad (3)$$

where: P_T – transmitter power (W); G_T – transmission antenna gain; G_R - the gain of the receiving antenna; d – distance between antennas (m); λ – signal wavelength $\lambda = c/f$ (m); c – speed of light in vacuum, $c = 299{,}97245 \cdot 10^6$ m/s; f – signal frequency, Hz; n – coefficient, depending on the propagation conditions (2 ... 6) [10-12].

Table 1 shows the values of the coefficient for various propagation conditions.

We will characterize an efficiency of manipulation with an object in the main signal beam by reflection coefficient and coefficient of lock:

$$r = \frac{\max(P_{\mathrm{R}E})}{\max(P_{\mathrm{R}\,opt})}, \quad (4) \qquad b = 1 - \frac{\max(P_{\mathrm{R}B})}{\max(P_{\mathrm{R}\,opt})}, \qquad (5)$$

where: P_{OPT} – level of the signal accepted by Bob in case of absence of reflection and locks.

TABLE I

Propagation conditions	n
Free space	2
Open space in the city	2,7-3,5
Space in the city with the dense building	3-5
In buildings of LOS	1,76-1,8
In buildings of NLOS	4-6

Using ratios (4) and (5) it is possible to write the appropriate expressions for productivity of the main channel, the diversion channel and confidential productivity (6):

$$C_S = C_{AB} - C_{AE} = W \log_2 \left\{ \frac{\left[1 + \frac{P_{TA} \cdot G_{TA} \cdot G_{RB}}{W \cdot k \cdot T} \left(\frac{\lambda}{4\pi}\right)^2 \cdot \left(\frac{1}{d_{AB}}\right)^n\right]}{\left[1 + \frac{P_{TA} \cdot G_{TA} \cdot G_{RE}}{W \cdot k \cdot T} \left(\frac{\lambda}{4\pi}\right)^2 \cdot \left(\frac{1}{d_{AE}}\right)^n\right]} \right\} \qquad (6)$$

Where: G_{RB} – gain amount of the receiving antenna of Bob; d_{AB} – distance between the transferring Alice's antenna and the receiving antenna of Bob (m); G_{RE} – gain amount of the receiving antenna of Eve; d_{AE} – distance (m) between the transferring antenna of Alice and receiving antenna of Eve.

To evaluate confidential productivity, we used simulation in a mathematical MATLAB packet. The provided model is simplified and considers actually throughput of the channel and depending on gain of the antenna of Eve and distance from Alice to Bob and Eve.

In a real case we will have no information, as about distance and gain of antennas, as and other parameters of the device of the malefactor. In view of this we used the following optimum model parameters for creation of our model and the analysis (Table II).

TABLE II

Parameter value	**Value**
W (bandpass range of the channel)	1 *GHz*
P_A (power of the transmitter of Alice)	30 *mW*
G_{TA} (gain amount of the transferring Alice's antenna)	20 dB
G_{RB} (gain amount of the receiving antenna of the Bob)	20 dB
G_{RE} (gain amount of the receiving antenna of Eve)	29 dB
D_{AB} (distance between Alice and Bob's antennas)	1:20 m
D_{AE} (distance between Alice and Eve's antennas)	1:50 m
F (wireless signal frequency)	60GHz.

In fig. 3 it is shown the 2D and 3D representation of dependence of confidential productivity as functions of distance from the user Alice to Bob and to the violator. The surface in fig. 3(b) represents the maximum speed.

ANALISIS OF RESULTS

There is possibility to select the main advantages of this model and advantage this 3D diagrams if it been based on these obtained results.

First, the obtained results confirm relevance of usage this metrics according to security of communication link at the physical layer in MM WB, as well as one gives the further possibility to use this model as a basis for formation of more torn and difficult model of a wireless communication system.

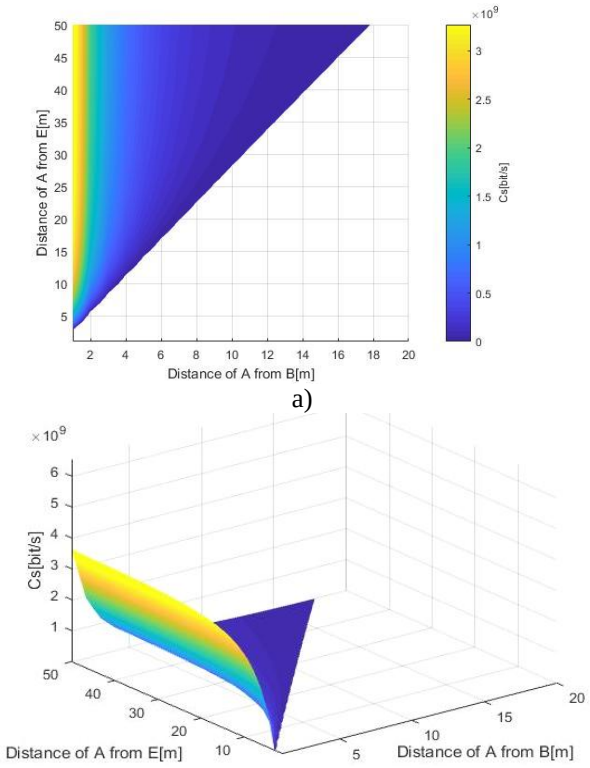

Fig. 3. 2D (a) and 3D (b) dependence of confidential productivity on the user Alice to Bob and to the violator Eve.

In future we will consider additional reflections of a signal on several objects, and also application of the narrow direction characteristic for case of creation and the analysis of security of communication link.

Secondly, thanks to 3D diagrams there is possibility to visually see the feature of dependence of confidential productivity on distance when using MM WB. So for fixed distance d_{AB}, there is the minimum distance d_{AE} where minimum speed of the main channel can be satisfied, and communication at the same time remains is safe. For example, the confidential productivity practically becomes maximum thanks to millimeter waves and specifics of their distribution in space if Eve is in 15 m from Alice for parameters considered in this article.

The above mentioned methodology for assessing the level of protection of IIS in the main and bypass communication channels at the physical level of the OSI interaction model allows for a comparative assessment of the various methods which an attacker uses and to predict the series in order to meet the requirements of information security.

CONCLUSIONS

A general threat model for evaluating the security parameters of information transmission systems at the physical level using a millimeter wave band (MM WB) is considered and formed. A more detailed model of the threat is based on the dependence of the channel capacity on the antenna gain and the distance in the main and bypass channel.

This model demonstrates the initial capabilities of MM WB in the concept of use in modern communication systems, namely, security at the physical level.

However, with further addition of additional parameters such as the reflection coefficient and the blocking ratio by environmental objects, we will obtain a detailed model of threats at the physical level. This model provides an accurate understanding of specific vulnerabilities and thereby emphasizes the relevance of the concept of a wiretap (branch) channel.

REFERENCES

[1] *Nitsche T., Cordeiro C., Flores A. B., Knightly E. W., Perahia E. and Widmer J. C.* IEEE 802.11ad: directional 60 GHz communication for multi-Gigabit-per-second Wi-Fi. // IEEE Communications Magazine. – 2014. – vol. 52, № 12, – pp. 132–141.

[2] *Yang N., Wang L., Geraci G., Elkashlan M., Yuan J. and. Renzo M. D.* Safeguarding 5G wireless communication networks using physical layer security. // IEEE Communications Magazine, – 2015. – vol. 53, №4. – pp. 20–27.

[3] *Steinmetzer D., Chen J., Classen J., Knightly E., Hollick M.* Eavesdropping with Periscopes*:* Experimental Security Analysis of Highly Directional Millimeter *Waves* // Proceedings of the IEEE Conference on Communications and Network Security (CNS). – 2015, September 2015, Florence.

[4] *Wyner A. D.* The wire-tap channel. // Bell System Technical Journal. – 1975. – Vol. 54, № 8. – pp. 1355-1387.

[5] *Liu R. and Trappe W.* Securing Wireless Communications at the Physical Layer. // New York: Springer, 2010.

[6] Forecasting methods of security of departmental communication systems on the basis of the concept of the diversion channel. / Under the editorship of. A.I. Tsopa, V.M. Shokalo. – Kharkiv: RC "City printing house", 2011. – 502 pages. (in Russian)

[7] Bystrov R. P., Petrov A.V., Sokolov A.V. Millimeter waves in communication systems//Log of radiotronics, No. 5, 2000. 8. Barros J. and Rodrigues M. R. D. Secrecy Capacity of Wireless Channels.//IEEE Int. Symp. on Information Theory, 2006.

[8] *Shu Sun, George R. MacCartney Jr., Rappaport Theodore S.* Millimeter-Wave Distance-Dependent Large-Scale Propagation Measurements and Path Loss Models for Outdoor and Indoor 5G Systems // 10th European Conference on Antennas and Propagation – Davos, Switzerland. – April 2016, pp. 1-5.

[9] *Chrysikos T., Dagiuklas T., Kotsopoulos S.* A Closed-Form Expression for Outage Secrecy Capacity in Wireless Information-Theoretic Security // Proceedings of Security in Emerging Wireless Communication and Networking Systems (*SEWCN'09*). – Springer, 2010. – Vol. 42 of Lecture Notes in Computer Science. – pp. 3–12.

[10] *Tsopa O.I.* Estimation of the probability to detect signal with wiretap channels with antennas apertures of different sizes and relative position /A.A. Strelnitskiy, A.E. Strelnitskiy, O.I. Tsopa, V.M. Shokalo, E.V. Yagudina // International journal «Telecommunication and Radio Engineering». – Begell House, 2011. – Vol. 70(7). – P. 601-606.

[11] *Ganshyn D. G., Dudka A. A., Bitchenko A. N., Tsopa A. I.* Analysis of structural secrecy of multi-frequency signals of broadband communication systems / // International journal «Telecommunication and Radio Engineering». – Begell House, 2016. – Vol. 75(13). – P. 1209-1219.

[12] *Tsopa O.I.* Prediction model of energy security for the systems of subscriber radio access with branched street and corridor communications channels / *A. A. Strelnitskiy, A. E. Strelnitskiy, O. I. Tsopa and V. M. Shokalo* // Radioelectronics and Communications Systems. – Allerton Press, Inc., 2011. – Vol. 54. – No. 2, – pp. 61-67.