# Contribution Estimation of Dominant Partial Waves into Phase of Multipath Signal Used for Encryption Key Generation

Amir I. Sulimov – *Member IEEE*, Oleg N. Sherstyukov, Arkadiy V. Karpov – *Member IEEE*
Department of radio physics, Institute of physics
Kazan Federal University
Kazan, Russia
asulimo@gmail.com, lada-sher@mail.ru, arkadi.karpov@kpfu.ru

***Abstract*— Randomness of fast fading multipath channels has been used for encryption keys generation for a long time. It is believed that until an adversary is able to intercept all partial waves detected by legal users, generated keys are secure. In many cases, however, only one or two dominant waves may define the channel fading and generated key. In this work, we examine a possibility of creating a partial key highly-related to the legal key using information about only a few dominant partial waves. Based on simulation of multipath radio propagation, correlation of partial phase formed only by dominant waves and total phase of multipath signal is assessed for various contributions of the dominating component. A key interception probability is estimated for Multipath Key Generation systems exploiting randomness of carrier phase. An influence of the line-of-sight component and number of multipaths on the correlation of partial and total phases is considered. It is shown that a serious threat to security of the generated key exists only if the dominating component holds at least a 95%-share of the signal power, which is unlikely in practice.**

***Keywords— multipath radio propagation; encryption key; carrier phase; partial waves; partial phase; partial key; correlation.***

## I. Introduction

The Multipath Key Generation (MKG) exploits randomness of fast fading multipath channel to create identical copies of a shared encryption key at two nodes *A* and *B* [1]. Both nodes should exchange a series of probing signals. While propagating through a multipath environment, the signals are randomly modulated by the fast fading. By further demodulation of the received signal, the nodes generate two random bit strings $key_A$ and $key_B$. These strings are identical ($key_A = key_B$) due to the channel reciprocity and not known to anyone, except for the nodes *A* and *B*, which allows their use as a secret encryption key. Such scenario is natural for urban environment, which allows its implementation in cellular communications for secure distribution of secret keys between base transceiver stations and user mobile phones.

Various signal parameters are used for the key generation purposes. However, one of the most secure are phase methods [2][3]. Being both periodical and ambiguous, carrier phase cannot be intercepted reliably at distances greater than $\lambda/2$ from a legal node. Thus, security of the generated key relies on a rapid spatial decorrelation of the carrier phase. From a physical point of view, it means that an adversary is unable to eavesdrop to all partial waves detected by user. When analyzing wireless communications in urban environment, it is common to refer to the Rayleigh channel model that assumes equal power of all partial waves. A more general model based on the Nakagami-m distribution permits a presence of a few dominant waves in the received signal [4]. Such waves may define almost completely dynamics of the channel fading along with the generated key. Therefore, if the adversary focused his efforts on intercepting the dominant waves (or simply D-waves, for shortness), it would be a serious threat to security of the key.

This work was performed according to the Russian Government Program of Competitive Growth of Kazan Federal University.

Another malicious threat is the external modulation attack that completely compromises all amplitude-based MKG-systems [5][6]. In this attack, a set of high-power transmitters is arranged around the legal nodes to imitate a natural channel fading by modulated radio emissions. In essence, each malicious transmitter creates its own D-wave. Due to use of modulated phase samples, legal nodes create an unsecure key that follows the modulation law defined by the adversary.

The purpose of this work is to examine a possibility of creating a partial key highly-related to the legal key using information about only a few D-waves. We perform numerical estimates of correlation of partial phase formed only by a few D-waves and total phase formed by all multipaths for various contributions of the dominating component. By binary quantization of samples of total and partial phases, the legal and partial keys are created to assess a key interception probability. The estimates are done both for LOS and NLOS scenarios with typical (12-tap) and low (3-tap) number of multipaths.

The paper is structured as follows. Section II presents scenario model. Channel simulation is described in Section III. Correlation estimates of partial and total phases are given in Section IV. Section V gives estimates of the key interception probability. Conclusion summarizes our principal results.

**978-1-5386-5824-6/18/$31.00 ©2018 IEEE**

## II. SCENARIO MODEL

In this section, we present a mathematical model of the multipath signal containing two D-waves and describe scenarios of both passive and active attack on the system.

In the assumed scenario, we consider multipath radio propagation in typical urban environment. Two nodes $A$ and $B$ (say, base transceiver station BTS and mobile terminal MT) exchange a series of probing signals in a half-duplex mode with a time slot of 0.1–10 ms. The nodes use radio frequency pulses at carrier frequency $f$ of the range from 1 to 5 GHz to probe the channel. At signal reception, each node observes random variations of carrier phase $\varphi$ caused by fading. As long as the channel is reciprocal, phase samples of both sides are identical ($\varphi_A = \varphi_B$). Based on this feature, the nodes collect $N$ samples of carrier phase and then convert the vectors $\{\varphi_A\}_N$ and $\{\varphi_B\}_N$ into the bit strings $key_A$ and $key_B$ using a binary quantization scheme. In real applications, key generation scheme is more complex. It includes some additional stages with randomness extraction, key reconciliation, and privacy amplification. Since our aim is physical layer analysis of the key leakage, we will omit these stages.

### A. Signal model

Our signal model assumes that the channel is probed with a clear sine wave of frequency $f$. The received signal is a superposition of ($n$+1) partial waves, of which two waves are dominant and the zero wave is a line-of-sight component (LOS). Complex amplitude of the received signal is given by:

$$A \cdot e^{i\varphi} = \sqrt{2k_R} \cdot A_0 \cdot e^{i\varphi_0} + G_1 A_1 \cdot e^{i\varphi_1} + G_2 A_2 \cdot e^{i\varphi_2} + \sum_{k=3}^{n} A_k \cdot e^{i\varphi_k} , \quad (1)$$

where $A_k$ and $\varphi_k$ are envelopes and phases of the partial waves, $k_R$ is the Rice factor, $G_1$ and $G_2$ are domination factors of the first and the second waves, respectively. The number of waves $n$ is implied to be a Poisson random process with the mean value $E(n)$. The model (1) implies the envelopes $A_k$ obeying the log-normal distribution law with mean value normalized to the received signal power $P_R$ as follows:

$$E(A_k) = \sqrt{\frac{P_R}{\{E(n) - 2 + G_1^2 + G_2^2\} \cdot (2k_R + 1)}} \ . \quad (2)$$

The received power $P_R$ is calculated along with the slow fading variance $var(A_k)$ of the partial envelopes in accordance with the chosen signal propagation model. In our study, we used the extended Hata-SRD model [7] proposed by the CEPT for this purpose. The phases $\varphi_k$ of the partial waves are defined almost completely by propagation delay, which makes their probability distribution essentially uniform.

With ability to consider various power ratios of the signal components, the model (1) allows contribution analysis of each D-wave and LOS into the total phase $\varphi$. We should also note here that in model (1) the total envelope $A$ obeys a two-mode Rice distribution rather than a single-mode as usual.

### B. Model of passive adversary

Passive scenario implies that an adversary $C$ can only receive but not transmit any signals. To intercept the key, the adversary eavesdrops to one of the legal nodes (say, node $B$) staying along at some distance. It is assumed that the node $C$ uses the same equipment perfectly synchronized with the legal nodes. Another powerful assumption is that the adversary $C$ knows exactly coordinates of both legal nodes, coordinates of scatterers $S_1$ and $S_2$ that create both D-waves detected by $B$, and, moreover, he also knows detected values $G_1A_1$ and $G_2A_2$ of amplitudes of the D-waves. As long as the LOS-wave is a deterministic component, parameters of the zero wave are also known to adversary. Using these data, adversary calculates the partial phase $\varphi_{012}$ by solving the following complex equation:

$$A_{012} \cdot e^{i\varphi_{012}} = \sqrt{2k_R} \cdot A_0 \cdot e^{i\varphi_0} + G_1 A_1 \cdot e^{i\varphi_1} + G_2 A_2 \cdot e^{i\varphi_2} . \quad (3)$$

This partial phase is taken as an estimate of the detected total phase $\varphi_B$. With such estimates, the adversary further tries to create a partial key $key_{012}$ correlated as much as possible with the legal key $key_B$ created from samples of the total phase. To analyze a contribution of various partial waves in details, we will also consider another three partial phases $\{\varphi_1, \varphi_{01}, \varphi_{12}\}$.

### C. Model of active adversary

In the passive scenario, there was an impractical assumption on perfect knowledge of parameters of D-waves by an adversary. Unlike the passive, an active adversary can interfere into the system by imitating some signals. The perfect knowledge would be more likely achievable in practice if there were some self-made D-waves in channel. To attack the system, adversary arranges two pairs $\{C_{A1}; C_{A2}\}$ and $\{C_{B1}; C_{B2}\}$ of high-power transmitters around the legal nodes $A$ and $B$, respectively. These devices imitate a couple of D-waves for each party. Since modulation law of all the false waves is defined by the adversary, he can predict precisely what will be detected in the node $B$. Knowing parameters of the signal dominating component, the adversary calculates a partial phase and creates a partial key just as in the passive scenario.

## III. CHANNEL SIMULATION

For correlation $corr(A_{012}, A)$ of the partial and total envelopes compact analytic expressions can be derived. Unfortunately, such expressions cannot be derived for phase values. Therefore, computer simulation seems to be a reasonable approach for solving the problem. In our study, we used the simulation model described in [8]. The model simulates a channel between a base transceiver station BTS (node $A$) and a user mobile terminal MT (node $B$) of cellular communication system. At the first stage, $n$ randomly spaced multipath scatterers are generated, and then all partial waves are traced to a receiver. Amplitudes of the D-waves and LOS are adjusted according to given values of the Rice factor $k_R$ and factors $\{G_1, G_2\}$. Further, the total carrier phase $\varphi$ is calculated according to (1) and (2), and a set of partial phases $\{\varphi_1, \varphi_{01}, \varphi_{12}, \varphi_{012}\}$ is found by nullifying appropriate terms in (3).

The instant number of waves $n$ is modeled as a Poisson random process with the mean value $E(n)$. At the physical layer, number of waves varies due to random motions of the mobile MT. To simulate a typical urban environment, a 12-tap

TABLE I. CHANNEL SIMULATION PARAMETERS

| Simulation parameter | Parameter value |
|---|---|
| Initial link length, $d$(m) | 200 |
| Carrier frequency, $f$ (MHz) | 1000 |
| Antennas height | $h_{BTS}$ = 30 m, $h_{MT}$ = 1.5 m |
| Antennas type | omnidirectional (0 *dBi*) |
| Signal-to-noise ratio, *SNR* (dB) | 20 |
| Mean number of partial wave, $E(n)$ | 12 or 3 |
| Rice factor, $k_R$ (dB) | -∞ or 15 |
| Domination factors, $G_{1,2}$ (dB) | -40…60 |
| Mobile speed, $V$ (m/s) | 10 |
| Communication duration, $T_S$ (s) | 30 |

channel ($E(n)$ = 12) was modeled. A 3-tap channel ($E(n)$ = 3) was used as an example of low-multipath environment. The LOS-wave was also assumed to come to the receiver. Its power was set by the Rice factor $k_R$. To assess a contribution of LOS into the total phase $\varphi$, the following two scenarios were modeled: 1) $k_R \to -\infty$ (NLOS), 2) $k_R$ = 15 dB (strong LOS).

A 30-second communication session was simulated for each pair of values of the factors $\{G_1, G_2\}$. The mobile MT was moved along a random path with a constant speed $V$ = 10 m/s. Thus, the total mobile path was about 300 meters. Instant values of the partial and total phases were sampled with the sampling time of 0.4 ms. In such a way, each simulation brought about 750 000 phase samples, which was sufficient both for partial phase correlation analysis and for estimation of key interception probability. Table I presents principal parameters of simulation.

## IV. CORRELATION ANALYSIS OF PARTIAL PHASE

A series of simulations at various domination factors was done to assess a contribution of D-waves into the total signal phase. The factors $\{G_1, G_2\}$ were varied in a wide range from minus 40 dB to 60 dB, where $G_i(dB) = 20\lg G_i$ ($i = \{1,2\}$). A single D-wave channel was modeled as a particular case of $G_2$ = 0 dB. For a channel with two D-waves two different power distributions among them were considered: 1) D-waves of equal power ($G_2 = G_1$); 2) the first D-wave was two-times greater ($G_2 = G_1/2$ or, equivalently, $G_2$(dB) = $G_1$(dB) – 6).

Fig. 1 presents simulation results for a dependence of correlation coefficient $R(\varphi_1, \varphi)$ of partial phase $\varphi_1$ of the first D-wave and the total phase $\varphi$ on the domination factors $\{G_1, G_2\}$. The solid line describes a NLOS-channel ($k_R$ = 0), whereas the dashed line is for the LOS-scenario ($k_R$ = 15 dB). The results are shown for both power ratios of the D-waves. In Fig. 1, the single D-wave case of $\{G_2 = 1\}$ describes both passive and active adversaries. The cases of $\{G_2 = G_1/2\}$ and $\{G_2 = G_1\}$ with two D-waves describe a passive adversary that knows only parameters of the first D-wave.

It can be seen from Fig. 1 that significance of the first D-wave increases with rise of its domination factor until the partial phase correlation reaches a definite marginal level at values of $G_1$ ~ 1000. In a single D-wave channel, the marginal level corresponds to a perfect correlation. In channel with two D-waves, the marginal levels are close to $1/\sqrt{2}$ in case of $\{G_2 = G_1/2\}$ and to $1/\sqrt{2\pi}$ in case of $\{G_2 = G_1\}$, respectively.

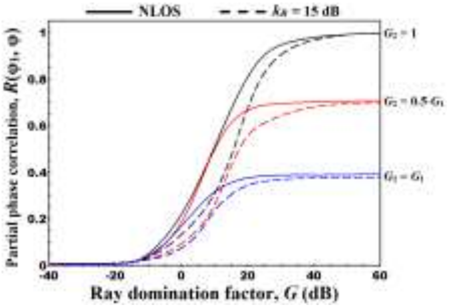



Fig. 1. Correlation of partial and total phases ($E(n)$ = 12)

Note that these values differ from intuitive estimates equal to 2/3 and 1/2. In presence of LOS, significance of the D-wave was lower leading to a decrement in the correlation level up to 0.25. In typical urban environment ($E(n)$ = 12, NLOS), the only D-wave of channel made a major contribution into the total phase $\varphi$ when its power was about 10 to 11 times greater than the mean power of ordinal partial waves. It seems that the boundary condition is simple equality of the D-wave power to summary power of the rest multipaths. A 90%-correlation allowing successful interception of each bit of generated key with a 95%-probability was observed for domination factors $G_1$ > 25 dB, which corresponds to at least a 96.5%-share of the received signal power.

Fig. 2 shows a comparison of correlation levels of the partial $\varphi_1$ and total $\varphi$ phases for the typical (solid line) and low (dash-dotted line) number of multipaths in NLOS-scenario. As can be seen, significance of each partial wave is higher at lower number of multipaths. However, the marginal levels of correlation do not depend on the number of waves but only depend on a share of signal power belonging to a considered dominating component. In a 3-tap channel, the only D-wave made a major contribution into the total phase $\varphi$ at factors $G_1$ > 1.3 dB, while at factors $G_1$ > 17.5 dB the correlation exceeded the 90%-level. Such domination also corresponds to a 96.5%-share of power as it was in the 12-tap channel.

Fig. 3 presents a comparison of correlation levels obtained for all considered partial phases in a 12-tap channel both in LOS (Fig. 3a) and NLOS (Fig. 3b) scenarios. An analysis showed that the correlation level $R(\varphi_{12}, \varphi)$ obtained for the partial phase $\varphi_{12}$ was nearly the same as the correlation $R(\varphi_1, \varphi)$ observed for the partial phase $\varphi_1$ in case of single D-wave ($G_2$ = 1), indifferently to power of LOS. Presumably, in a 12-tap channel with two D-waves the partial phase $\varphi_{12}$ plays the same role what the partial phase $\varphi_1$ plays in an 11-tap channel with

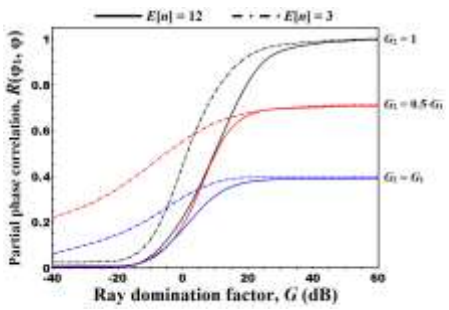
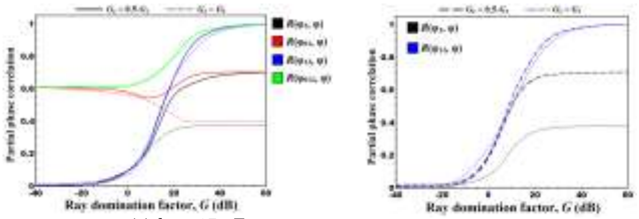



Fig. 2. Correlation of partial and total phases (NLOS)



(a) $k_R$ = 15 дБ (b) NLOS

Fig. 3. Correlation of partial and total phases for various partial components (E(n) = 12)

single D-wave. This rule, apparently, could be observed in channels with a greater number of D-waves, but this assumption requires additional verification. An account of both the second D-wave and LOS made the partial phases closer to true phase $\varphi_B$ detected by $B$. At the same time, for partial phases containing both D-waves the correlation level was weakly dependent on the ratio of $(G_2/G_1)$. Particularly, the curves obtained for the cases of $\{G_2 = G_1/2\}$ and $\{G_2 = G_1\}$ lay close to each other. The LOS-wave with a 15 dB predominance over the ordinal multipath component played a decisive role in the total signal phase until the domination factor $G_1$ reached the value of 10 dB. In other words, the LOS was decisive as long as it had more than a 50%-share in the received power. Rise of significance of the second D-wave reduced quite expectedly the correlation level $R(\varphi_{01}, \varphi)$ observed for the partial phase $\varphi_{01}$, and it made it to fall asymptotically down to the marginal correlation of the partial phase $\varphi_1$. For all considered partial phases, correlation with the total phase reached a flat level at domination factors $G$ of the order of 20–25 dB, which corresponded roughly to a 95%-share in the received power.

Comparing the results at Fig. 3(a) and Fig. 3(b), we came to an unexpected conclusion on an advantage of presence of LOS for the adversary. Intuitive consideration suggests that the channel becomes more predictable in presence of a powerful LOS, which should simplify estimation of the total phase and facilitate to key interception. While at low domination factors, this concept was fulfilled unconditionally, it did not work at large values of $G$. Specifically, at $G_1$ greater than 12 dB the correlation $R(\varphi_1, \varphi)$ observed in the NLOS-scenario was higher than the correlation $R(\varphi_{01}, \varphi)$ observed in presence of LOS. The same situation was also with the correlation $R(\varphi_{12}, \varphi)$ in the NLOS-scenario that was higher than the correlation $R(\varphi_{012}, \varphi)$ in the LOS-scenario at the values of $G_1$-factor higher than 17 dB. It seems like the presence of LOS did not facilitate but impede estimation of the total phase. Apparently, this effect is explained by probabilistic nature of interference of D-waves with the LOS-wave that causes additional oscillations in partial phase, which weaken its correlation with the total phase.

The correlation analysis showed that, in some cases, exact knowledge of parameters of a few dominant waves provides an effective estimation of the total multipath phase, which causes a key leakage threat. In the next section, we present relevant estimates of the key interception probability.

## V. Estimation of Key Interception Probability

To generate the key strings, we processed samples of the total and partial phases using the procedure of [3]. At the first stage of the processing, a cross-correlation of sequential phase samples had been eliminated. After that, a binary quantization scheme was used to map the samples into bits. The samples of total phase were mapped into the legal key *key*, while other partial phases $\{\varphi_1, \varphi_{01}, \varphi_{12}, \varphi_{012}\}$ were mapped into respective set of partial keys $\{key_1, key_{01}, key_{12}, key_{012}\}$. The length of each key string was about 12 000 bits. For the estimation of a key interception probability, the fraction $p_e$ of unmatched bits between the legal and considered partial keys was counted.

Fig. 4 presents estimated key disagreement rate between the partial key $key_1$ and the legal key *key* as a function of the domination factors $\{G_1, G_2\}$. Following the Fig. 1, the three different power ratios of the D-waves were considered both in presence and absence of LOS. The results show that taking into account of only one of two D-waves does not allow the adversary to reach low values of the disagreement rate $p_e$. In case of $\{G_2 = G_1/2\}$, the lower boundary was about 11.5%, whereas for $\{G_2 = G_1\}$ it was about 27%. An account of the LOS-wave affected much the key interception possibility. In a single D-wave channel without LOS, each bit of the generated key string can be intercepted with a success probability of 99% only if the $G_1$-factor exceeds 35 dB, which corresponds to an overwhelming share of power of 99.6% in the received signal. In a more realistic case, when the dominating component has an 80%-share, the key disagreement rate $p_e$ is about 11.3%. In case of a 50%-share, it has an order of 20%. As can be seen from the beginning region in Fig. 4, a contribution of the partial waves, whose power is 17 dB lower than the level of ordinal waves (corresponds to a 0.2%-share of power), is negligible.

Fig. 5 presents estimates of a bit disagreement rate between the partial and legal keys for the same examples as in Fig. 3. All curves clearly show that the use of both D-waves increases much an interception probability of the key. Moreover, power distribution among the D-waves has a weak effect on values of $p_e$. As seen from Fig. 5(a), in channel without any D-waves, knowledge of the deterministic phase $\varphi_0$ of the LOS-wave only ensured a successful interception of each bit of the legal key with probability of nearly 70%. However, as was noted in Section IV, the presence of LOS at large domination factors, conversely, increased the key disagreement rate. As for example, in the NLOS-scenario, domination factors of the order of 45 dB ensured the disagreement rate to be lower 0.5%, whereas in the LOS-scenario this rate was nearly ten times greater.

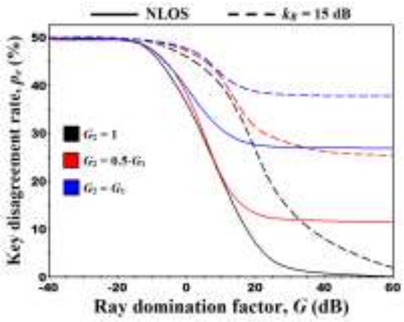
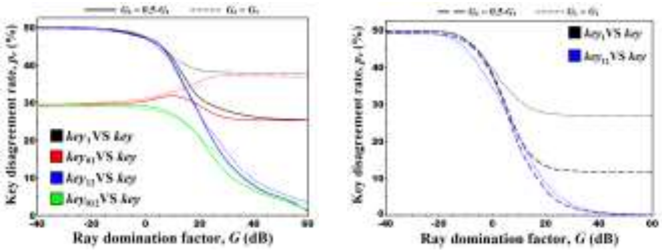



Fig. 4. Bit disagreement rate between the legal key and the partial key of the first dominant wave ($E(n)$ = 12).




(a) $k_R$ = 15 дБ (b) NLOS

Fig. 5. Bit disagreement rate between the legal key and various partial keys of dominating signal components ($E(n)$ = 12)

Our estimates showed that the use of information about a few dominant waves could be an effective method to attack a Multipath Key Generation system but only in case of overwhelming dominance, when the partial component known to adversary shares at least 95% of the received signal power. Such conditions are unlikely to be fulfilled in practice. Thus, the phase-based MKG-systems can be considered as strongly resistant to the active attack with an imposed external modulation.

## VI. Conclusion

In this paper, a contribution estimation of dominant partial waves (D-waves) into total phase of multipath signal received in a typical urban environment was performed. The estimates were obtained both for NLOS and strong LOS propagation scenarios for channels with typical (12-tap) and low (3-tap) number of multipaths. By simulation of multipath radio propagation, a dependence of correlation level of partial and total phases of the multipath signal on a share of received power given to the dominant waves was studied. Our estimates showed that the only D-wave of channel provides a major contribution into the total signal phase if its power exceeds summary power of the rest multipaths. A 90%-correlation of the partial and total phases is achieved if the only D-wave has at least a 96.5%-share of power, which is unlikely in practice. In channel with two D-waves, similar correlation level is achieved only if the dominating component takes at least 98%-99% of the received power. The results showed that at fixed share of power given to the dominating component the lower the number of D-waves the higher the correlation of the partial and total phases.

By binary quantization of samples of the total and partial phases, test key strings were generated to estimate a key interception probability. The estimates showed that the bit disagreement rate between the partial and legal keys under a 1%-level is achievable only if the single D-wave in channel has at least a 99.6%-share of power. In a more realistic case, when the dominating component has an 80%-share, the key disagreement rate is about 11.3%. In case of a 50%-share, it has an order of 20%. The partial waves, whose share of power does not exceed 0.2%, produce a negligible contribution into the total signal phase. In a LOS-scenario with Rice factor of 15 dB, knowledge of deterministic phase of the LOS-wave ensures a success probability of interception of each bit of the legal key up to 70%.

The obtained results showed that the use of information about a few D-waves could be an effective method to attack a Multipath Key Generation system (MKG-system) but only in case of overwhelming dominance, when the dominating component known to adversary shares at least 95% of received power. Such conditions are unlikely in practice. This proves a strong resistance of the phase-based MKG-systems to the active attack with an imposed external modulation.

## References


[1] Zhang J. et al. Key generation from wireless channels: a review. IEEE Access. Vol. 4. Pp. 614-626. Jan. 2016.

[2] Hassan A.A., Stark W.E., Hershey J.E., Chennakeshu S. Cryptographic key agreement for mobile radio. Digital Signal Processing. Vol. 6. Iss. 4. Pp. 207-212. 1996.

[3] Sulimov A.I. et al. Experimental study of performance and security constraints on wireless key distribution using random phase of multipath radio signal. Proc. 11th Int. Conf. on Security and Cryptography (SECRYPT-2014). Pp. 411-416. Vienna (Austria). Aug. 2014.

[4] Saunders S.S., Aragon-Zavala A. Antennas and propagation for wireless communication systems. John Wiley & Sons. 553 p. 2007.

[5] Jana S. et al. On the effectiveness of secret key extraction from wireless signal strength in real environments. Proc. 15th Ann. Int. Conf. on Mob. Comp. and Networking (MobiCom' 09). Pp. 321-332. Sept. 2009.

[6] Mathur S. et al. ProxiMate: Proximity-based secure pairing using ambient wireless signals. Proc. 9th Int. Conf. on Mob. systems, applications, and services (MobiSys' 11). Pp. 211-224. Bethesda (Maryland, USA). June 2011.

[7] SEAMCAT: Spectrum Engineering Advanced Monte Carlo Analysis Tool. Handbook. European Communication Office (CEPT). 221p. 2010.

[8] Sulimov A.I. et al. Analysis of frequency-correlation properties of multipath channel for encryption key generation using samples of differential phase. Proc. Moscow Workshop on Electronic and Networking Technologies (MWENT-2018). Pp. 1-7. Moscow (Russia). March 2018.