On Polarization Diversity in Meteor Key Distribution Systems

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

***Abstrac* — Natural randomness of meteor burst channel can be used for establishing a shared encryption key. To improve a key generation rate, a new method is proposed that allows sampling of two independent measurements of carrier phase from each meteor radio reflection. The method relies on a time multiplexing of polarization of probing signal. By computer simulation based on numerical calculations of oblique diffraction of radio waves off ionized meteor trails, the first ever estimates of polarization coherence interval of meteor burst channel are made. Correlation functions of carrier phase versus polarization diversity of probing signals are presented both for cases of horizontal and vertical polarization of antennas. It is showed that the use of polarization diversity technique yields in generating two statistically independent encryption keys against a single key as in previous studies. However, the proposed method for generation of extra key demands a precise tuning of antenna polarization, which may cause some difficulties in its practical implementation.**

Keywords— meteor burst communication; diffraction of radio waves; radio reflection; channel nonreciprocity; encryption key; polarization diversity; correlation; channel coherence interval.

I. Introduction

Small meteor particles of both random mass and velocity constantly bombard the earth’s atmosphere. Burning up at the altitudes of 80-120 km they create ionized trails able to relay radio signals between two communication points. This effect is widely used for establishing communications [1][2]. Due to its complex astronomical and geophysical nature meteor burst channel is essentially a random propagation medium. Meteors occur instantly in random places creating trails of random spatial orientation, ionization level, and life time. Random propagation path along with unpredictable parameters of the medium both ensure randomness of meteor radio reflections (MRRs) detected by a receiver. Use of this randomness helps two communication points (say, “*A*” and “*B*”) to establish a shared secret encryption key by a simple exchange by series of probing signals [3]. For this purpose, each side measures parameters (carrier phase, for example) of detected MRRs then maps collected array of random values into a bit string. As long as channel is reciprocal, both sides create identical bit strings, which enables their use as a shared secret key.

A principal drawback of Meteor Key Distribution systems (MKD-systems) is low key generation rate, which in best case is only about 160 bits per hour [4]. That is why performance enhance is crucial for MKD. Unfortunately, there is nothing can be done with low meteor detection rate, which is only 50-350 events per hour. However, it is still possible to improve a data processing technique for detected MRRs in some way. In [3][4], only one single value of carrier phase has been sampled from each MRR due to high temporal correlation. On the other hand, in [5] it was shown that meteor burst channel is polarization sensitive. It means two probing signals of different polarizations might have uncorrelated carrier phases at the channel output. Such a feature could be able to provide two phase sample from each MRR, instead of one. Hence, it would double a key generation rate.

The purpose of this study is to validate a possibility of generation of two statistically independent encryption keys by polarization diversity of probing signals in meteor burst channel. In this paper, we present simulation results of phase correlation function versus polarization diversity. Numerical estimates of channel polarization coherence interval are made for the first time for meteor burst channel. By binary quantization of simulated phase-time responses of MRRs, two binary key strings are created from the probing signals of different polarizations to analyze their correlation. The analysis proves a possibility of generating an extra key string by using the polarization diversity technique in meteor burst channel.

II. Time Multiplexing of Probing Polarization

The channel polarization sensitivity forces two probing signals of different input polarizations γ_1 and γ_2 ($\gamma_i \in [0^\circ, 180^\circ], i = \{1,2\}$) to attain different output phase shifts φ_1 and φ_2, respectively. Here and below, we imply the use of linearly polarized radio waves of polarization angle γ. In the previous section, it was assumed that channel polarization sensitivity might help to double a performance of the MKD-systems by generation of extra encryption key. Conventional polarization diversity assumes using of differently polarized antennas both at the transmitter and the receiver [6]. In meteor burst communications, however, such technique is not feasible. Random direction of meteor trails along with random Faraday polarization twist both give rise to a depolarization effect that makes polarization of received signal arbitrary [5]. As a consequence, two probing signals of different input polarizations become inseparable at the channel output.

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

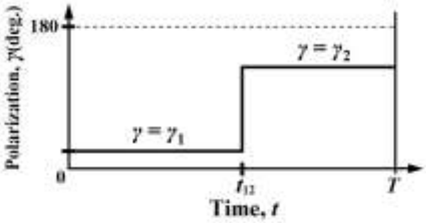

Fig. 1. Time diagram of TMPP

To overcome the signal depolarization, a multiplexing of probing polarization in a time domain as shown in Fig. 1 is proposed for diversity implementation. In practice, duration T of each MRR is limited by dissipation of meteor trails. Typical value of T ranges from 10 ms to 10 seconds with average value of about 300 ms. In Fig. 1, a time diagram of the Time Multiplexing of Probing Polarization (TMPP) is presented. According to the diagram, polarization of probing signal is switched from the γ_1-state into the γ_2-state at some intermediate moment $t_{12} \in [0, T]$. Linear antenna polarization is implied here. Such a switch provokes a leap of phase at the channel output from $\varphi_1 = \varphi(\gamma_1)$ to $\varphi_2 = \varphi(\gamma_2)$. To create independent key strings, we should find an appropriate polarization diversity $\Delta\gamma = |\gamma_2 - \gamma_1|$ that provides zero correlation of the phase values: $\rho = corr(\varphi_1, \varphi_2) \to 0$.

Another problem of TMPP is choice of the switching time t_{12}. Intrinsic features of meteor burst channel do not support an arbitrary choice. One principal peculiarity is incomplete channel reciprocity of a quite complicated electro dynamic nature [7]. The channel nonreciprocity is negative for encryption keys establishing, because it makes phase samples at both sides low-correlated: $\varphi_A \neq \varphi_B$. This results in some disagreement of the generated keys: $Key_A \neq Key_B$. The level of nonreciprocity is time-variant due to dissipation of meteor trail. Therefore, a moment t^* of minimum nonreciprocity exists for each MRR. One should use this moment to sample the carrier phase for key generation [3]. The nonreciprocity is a polarization sensitive feature. Therefore, for each probing polarization of γ its own minimum nonreciprocity time $t^*(\gamma)$ exists. This circumstance would not prevent the TMPP-implementation if the switching time t_{12} was chosen as the greatest of the two values: $t_{12} = \max\{t^*(\gamma_1); t^*(\gamma_2)\}$. Thus, choice of the switching time is justified by physical features of meteor burst channel.

This study focuses on estimation of required polarization diversity $\Delta\gamma$ and on assessing the mismatch $\Delta t^* = |t^*(\gamma_1) - t^*(\gamma_2)|$ of minimum nonreciprocity times of both probing polarizations to justify a feasibility of the TMPP-scheme. Considering a multifactoral nature of meteor burst channel, computer simulation seems to be a reasonable approach for solving these problems. Simulation scenario and modeling parameters are discussed in the next section.

III. Simulation Scenario

Strong signal depolarization in meteor burst channel [5] makes experimental studies on polarization coherence quite difficult. Such studies could probably be made with use of a code division of probing signals, when each polarization is assigned to a definite keying code. However, to the best of our knowledge, no such experiments have ever been done. On the other hand, theoretical study of phase correlation function with respect to polarization diversity $\rho(\Delta\gamma)$ requires consideration of a complete chain of polarization transforms in meteor burst channel including those that proceed due to diffraction off the meteor trail. The most of existing theoretical models of meteor burst channel do not support such capabilities. This fact made theoretical studies on the channel polarization correlation properties impossible for a long time.

TABLE I. Technical Specifications of Test Radio Links

Technical parameters	Moscow - Saint Petersburg	Saint Petersburg - Kazan
Link length, L (km)	635	1200
Carrier frequency, f_0 (MHz)	50	
Transmitter power, P_T (W)	2000	
Threshold level, P_0 (dBm)	-116	
Antenna type	5-dipole Yagi	
Antenna height, h_a (m)	4.4	13.9
Antenna polarization, γ (deg.)	γ_1 = 0 (horizontal, fixed), γ_1 = 90 (vertical, fixed), γ_2 = 0 to 180 (variable)	
Date and time	June 15th, 6 a.m.	
Number of samples, N	10 000 MRRs	

In this study, channel simulation was performed according to model [7]. At the moment, this is the only model that provides correct simulation of polarization features and nonreciprocal properties of meteor burst channel. To assess an influence of link length on the channel polarization coherence, two test radio links of different lengths were modeled during the simulations. The first test link Moscow (55.75° N., 37.60° E.) – Saint Petersburg (59.95° N., 30.30° E.) was of the moderate length of 635 km, while the second link Saint Petersburg – Kazan (55.75° N., 49.10° E.) was much longer with the length of 1200 km. Table I presents technical specification of the test links.

A two-way radio propagation of the probing signals emitted synchronously from both ends of the link was being modeled during the simulations. A set of ten thousand MRRs was being generated in each simulation. Note that, unlike a real practice, in simulation we were able to accurately distinguish at the reception the probing signals with different input polarizations. This allowed straight simulation of simultaneous coexistence of two parallel channels with diverse polarizations. Therefore, there was no need in actual simulation of the TMPP-scheme with time division of the diverse channels. Instead of this, a simultaneous propagation of two probing signals with different input polarizations was simulated. The diversity channel 1 (CH1) was established with use at both link ends of linearly polarized antennas of the polarization angle γ_1, whereas for the diversity channel 2 (CH2) analogous antennas of different polarization γ_2 were used. In practice, implied neighborhood of two differently polarized antennas would imminently cause a coupling effect leading to a polarization violation. However, no such effects were modeled, which ensured observation of actual polarization correlation properties of meteor channel.

Antenna polarization was tuned through a rotation of antenna plane, in which all the dipoles were collocated, around the antenna arrow direction. A horizontal polarization was set either by the rotation angles of $\gamma = 0°$ or $\gamma = 180°$. The vertical polarization was set by the angle of $\gamma = 90°$. The CH1 was considered as a reference channel, so its polarization remained constant throughout all simulation. Both horizontal ($\gamma_1 = 0°$) and vertical ($\gamma_1 = 90°$) reference polarizations were modeled. The polarization γ_2 of the CH2 was varied to achieve various polarization diversities of $\Delta\gamma$ needed to observe desired phase correlation function $\rho(\Delta\gamma)$.

The following four phase-time dependencies $\{\varphi_A(t,\gamma_1);\varphi_B(t,\gamma_1);\varphi_A(t,\gamma_2);\varphi_B(t,\gamma_2)\}$ were synthesized for each meteor to imitate time-variant properties of all MRRs synchronously detected at both ends of the link. These data allowed identification of the minimum channel nonreciprocity times $t^*(\gamma_1)$ and $t^*(\gamma_2)$. Further, a minimum allowable switching time t_{12} was assessed as the difference Δt^* of these times. The Pearson's correlation $\rho(\Delta\gamma) = corr\{\varphi_A(t,\gamma_1),\varphi_A(t,\gamma_2)\}$ of the carrier phases was calculated in order to estimate the channel polarization coherence interval. The averaging was done both over the duration ($t \in [0,T_i]$) and the whole set of simulated MRRs ($i = 1..N$). Despite the nonreciprocity, average indicators of the channel were in a good agreement at the both sides "*A*" and "*B*". This allowed analysis of the data at one side only (at the side "*A*"). For the generation of independent key strings, we used the phase values of $\varphi_1 = \varphi_A(t^*(\gamma_1))$ and $\varphi_2 = \varphi_A(t^*(\gamma_2))$ sampled exactly at the minimum nonreciprocity times. The above operations were done for each simulated meteor to gather a necessary statistics.

IV. Estimation of Channel Polarization Coherence

The results of simulation of the phase correlation function versus polarization diversity are shown in Fig. 2 for both test links using two different reference polarizations. The obtained correlation curves are non-symmetric due to asymmetrical statistics of angle of arrival of MRRs. It can be seen from Fig. 2 that there were some specific diversities $\Delta\gamma_0$ that nullified the phase correlation. Physically, it means that the change of $\Delta\gamma_0$ in the probing polarization made the detected phases to be shifted on π/2 on average that ensured a mutual orthogonality of the CH1 and CH2. Subsequently, greater diversities caused greater phase shifts leading to a negative correlation. The revealed possibility of the zero correlation is favorable for the key generation purposes. Another notable result is that orthogonal polarizations, generally, do not eliminate a correlation of the phase samples. As seen from Fig. 2, a typical polarization coherence interval ranges from 40° to 90° depending on parameters of the link, and the average interval is about 65°.

Fig. 2 also indicates that the polarization coherence interval is narrower at shorter links. Apparently, this is due to a higher spatial scatter of meteor trails at shorter links [8]. With higher variance of parameters of meteors, even small alteration in the probing polarization causes a large phase change. Conversely, at longer links all detected meteors have nearly the same parameters, and this similarity retains a high correlation. Fig. 2 also points at weaker negative correlation at longer links, which means that the scattered waves of different incident polarizations rarely have phase mismatch greater than π/2.

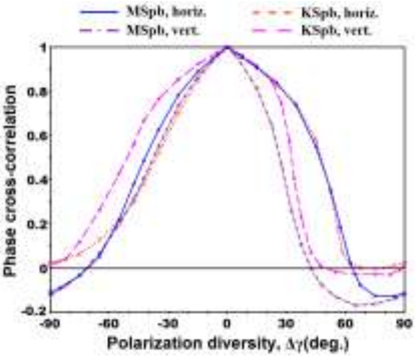

Fig. 2. Phase cross-correlation versus polarization diversity $corr\{\varphi_A(t,\gamma_1), \varphi_A(t,\gamma_2)\}$

Fig. 2 presented an instant correlation function with a zero time shift. However, for generation of independent keys according to the TMPP-scheme, the phase values of $\varphi_1 = \varphi_A(t^*(\gamma_1))$ and $\varphi_2 = \varphi_A(t^*(\gamma_2))$ with mutual time delay of Δt^* should be used. An account of additional decorrelation due to the time shift of Δt^* should provide a more accurate estimate of the channel polarization coherence interval. The obtained channel polarization correlation function $\rho(\Delta\gamma,\Delta t^*) = corr\{\varphi_A(t_1^*,\gamma_1),\varphi_A(t_2^*,\gamma_2)\}$ of the phase samples measured at the moments of minimum nonreciprocity is shown in Fig. 3. Comparison with the Fig. 2 reveals only small changes in the correlation level seen mostly in the region of low diversities. The effect of additional time shift was most pronounced with vertical polarization of the reference channel, it narrowed the channel coherence interval by 10° on average.

For implementation of the TMPP-scheme, it is desirable to have the moments $t^*(\gamma_1)$ and $t^*(\gamma_2)$ of minimum channel nonreciprocity be sufficiently distant. The time gap is needed for such operations as detection of MRR, tuning of transceivers, sampling of carrier phase in the CH1, and, finally, for switch of antenna polarization. Fig. 4 shows obtained dependence of mismatch Δt^* of the minimum nonreciprocity times on the polarization diversity of the CH1 and CH2. Our estimates of Δt^* ranged from 15 ms to 55 ms, which is sufficient for implementation of all required operations. The nonreciprocity time mismatch, generally, follows the channel correlation level observed at Fig. 2 and Fig. 3. The local maxima of the Δt^* value fit well with the correlation zeroes. An analysis showed that the sign of Δt^* is not random and that it has a systematic dependence on the diversity $\Delta\gamma$. Therefore, it

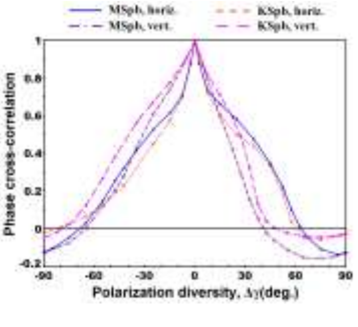

Fig. 3. Cross-correlation of phase samples versus polarization diversity $corr\{\varphi_A(t^*(\gamma_1),\gamma_1), \varphi_A(t^*(\gamma_2),\gamma_2)\}$

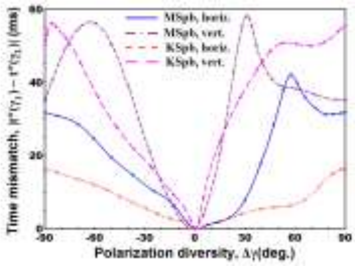

Fig. 4. Mismatch of minimum nonreciprocity times for diversity channels.

is possible to predict the minimum nonreciprocity time of which polarization is earlier to correctly choose the values of γ_1 and γ_2 compliant with the Fig. 1.

The presented results confirm feasibility of the TMPP-scheme proposed in Section II. For exhaustive verification, we will perform a test generation of two independent key strings using the phase samples of different probing polarizations.

V. Analisys of Encryption Keys Correlation

The phase samples $\{\varphi_1\}_N$ and $\{\varphi_2\}_N$ formed by processing of simulated MRRs were mapped into the key strings K_1 and K_2, respectively. About 3% of the samples had been discarded due to inappropriate nonreciprocity. All remained samples were mapped into bits using a binary quantization scheme [5]. After the keys were generation, their linear correlation coefficient was calculated. According to [9], two bit strings of 9700-bit length may be considered as uncorrelated if their correlation is under the 0.02-level. To validate a statistical independence of the generated key strings, their correlation coefficient $corr(K_1,K_2)$ was compared to the critical level 0.02. The analysis results obtained with several different polarization diversities are presented in Table II.

TABLE II. Correlation of Generated Key Strings

Polarization diversity		“MSpb” link	“KSpb” link
γ_1 = 0°	γ_2 = 55°	0.117	0.085
γ_1 = 0°	γ_2 = 57°	0.185	**0.010**
γ_1 = 0°	γ_2 = 58°	0.233	-0.058
γ_1 = 0°	γ_2 = 60°	0.076	-0.116
γ_1 = 0°	γ_2 = 63°	**0.011**	-0.133
γ_1 = 0°	γ_2 = 65°	-0.037	-0.144
γ_1 = 0°	γ_2 = 90°	-0.223	-0.141
γ_1 = 0°	γ_2 = 118°	**-0.018**	**0.009**
γ_1 = 0°	γ_2 = 120°	0.043	0.029
γ_1 = 90°	γ_2 = 0°	-0.233	-0.141
γ_1 = 90°	γ_2 = 45°	-0.107	-0.117
γ_1 = 90°	γ_2 = 50°	**0.001**	**0.002**
γ_1 = 90°	γ_2 = 55°	0.117	0.207
γ_1 = 90°	γ_2 = 150°	0.028	0.177
γ_1 = 90°	γ_2 = 153°	**-0.011**	0.111
γ_1 = 90°	γ_2 = 154°	-0.021	0.088
γ_1 = 90°	γ_2 = 157°	-0.060	0.022
γ_1 = 90°	γ_2 = 158°	-0.073	**0.001**
γ_1 = 90°	γ_2 = 160°	-0.099	-0.032
γ_1 = 90°	γ_2 = 180°	-0.231	-0.146

The results in Table II confirm an existence of definite polarization diversities ensuring generation of two uncorrelated bit strings. These cases (marked in bold) are in a good agreement with the results in Fig. 2 and Fig. 3 as they fit well to the points of zero correlation. Again, it can be seen from Table II that use of orthogonal polarizations does not eliminate a correlation of the key strings, because it does not provide orthogonality of the detected phases. A serious barrier to the TMPP-implementation is a strong sensitivity of the keys correlation level to small variations in the diversity $\Delta\gamma$. Table II shows that the tuning error of antenna polarization of simply one or two degrees leads to an unacceptable correlation of the key strings. Technical implementation of such precise tuning of antenna polarization may be quite problematic.

VI. Conclusions

In this study, a possibility of meteor generation of statistically independent encryption keys using the polarization diversity technique has been examined for the first time. Based on numerical calculations of the diffraction of radio waves, polarization correlation curves of carrier phase of meteor radio reflections (MRRs) have been obtained. The very first estimates of polarization coherence interval of meteor burst channel have shown the values of about 55°-65°. A time multiplexing of probing polarization scheme has been proposed for implementation of polarization diversity. Its feasibility has been verified through simulations. By binary quantization of the phase samples of MRRs corresponded to diverse probing polarizations, a possibility of generating two uncorrelated key strings has been proven. A principal barrier to implementation of proposed technique is a strong sensitivity of the keys correlation level to small errors in tune of antenna polarization. The estimates have shown that admissible tune errors should not exceed one degree.

References

[1] McKinley D. W. R. Meteor science and engineering. McGraw-Hill. 1961.

[2] Oetting J.D. An analysis of meteor burst communications for military applications. IEEE Trans. on comm. Vol. COM-28. No. 9. Pp. 1591-1601. 1980.

[3] Sulimov A.I. et al. Secure key distribution based on meteor-burst communications. Proc. 11th Int. Conf. on Security and Cryptography (SECRYPT-2014). Pp. 445-450. Vienna (Austria). Aug. 2014.

[4] Sulimov A.I. et al. Performance evaluation of meteor key distribution. Proc. 12th Int. Conf. on Security and Cryptography (SECRYPT-2015). Pp. 392-397. Colmar (France). Jul. 2015.

[5] Sulimov A.I. On possibility of using of measurements of random polarization of radio reflections from meteor trails for generating shared encryption keys. Proc. 2017 Int. Conf. on Radiation and Scattering of Electromagn. Waves (RSEMW-2017). Pp. 146-149. Divnomorskoe (Russia). June-July 2017.

[6] Saunders S.R. Aragon-Zavala A. Antennas and propagation for wireless communication systems. 2nd ed. John Wiley and Sons. 2007.

[7] Sulimov A.I. et al. Analysis and simulation of channel nonreciprocity in meteor burst communications. IEEE Trans. Ant. and Prop. Vol. 65. No. 4. Pp. 2009-2019. Apr. 2017.

[8] Weitzen J.A. Performance of short- and long-range meteor scatter communication with different antennas. IEEE J. Sel. Areas Com. Vol. 10. Pp. 491-496. April 1992.

[9] Knuth D.E. The art of computer programming. Vol. 2. 3rd ed. Addison Wesley Longman. 1998. 762 p.