CORE
Metadata, citation and similar papers at core.ac.uk
Provided by Kazan Federal University Digital Repository

Conference Proceedings - 2017 Radiation and Scattering of Electromagnetic Waves, RSEMW 2017, 2017, pages 146-149

On possibility of using of measurements of random polarization of radio reflections from meteor trails for generating shared encryption keys

Sulimov A.
Kazan Federal University, 420008, Kremlevskaya 18, Kazan, Russia

Abstract

© 2017 IEEE. Meteor burst channel is formed by a scattering of radio waves from the ionized trails left by fast meteor particles. Meteor phenomena make the channel to be stochastic. Using this randomness along with approximate reciprocity of radio propagation, two communication points are able to generate a purely random shared encryption key by joint observation on the channel parameters. In previous studies, it was shown that the randomness of carrier phase and propagation time of detected meteor radio reflections can be used for the key generation purposes. However, a polarization of the radio reflections is also random, and it might be used to generate the keys too. In this study, the first ever attempt on examining a possibility of generating of purely random encryption keys using the samples of random polarization of meteor radio reflections is made. By computer simulation based on a rigorous solution to the problem of oblique diffraction of radio waves on meteor trails, statistical properties of the polarization of meteor radio reflections are studied. The estimates of the cross-correlation between the values of polarization measured synchronously at both sides of a radio link and differing due to non-perfect reciprocity of meteor burst channel are presented. Some preliminary results on the testing generation of a random key are also presented in the end of the paper.

http://dx.doi.org/10.1109/RSEMW.2017.8103590

Keywords

Diffraction of radio waves, Encryption key, Meteor burst propagation, Meteor radio reflection, Polarization

References

[1] A.I. Sulimov, "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.

[2] A.I. Sulimov, "Performance evaluation of meteor key distribution, " Proc. 12th Int. Conf. on Security and Cryptography (SECRYPT-2015), pp. 392-397, Colmar (France). Jul. 2015.

[3] P.S. Cannon, "Polarization rotation in meteor-burst communication systems, " Radio Science, vol. 21, no. 3, pp. 501-510, May-June 1986.

[4] R.I. Desourdis Jr., "Nonreciprocity of meteor scatter radio links, " Proc. Ionospheric Effects Symposium (IES), pp.165-173, 4-6 May 1993.

[5] R.G. Khuzyashev, "Calculation of the amplitude and phase characteristics of a signal scattered obliquely off a meteor trail, " Radiophysics and Quantum Electronics, vol. 27, 9, pp. 778-782, 1984.

[6] A. Karpov, "The computer model KAMET: The new generation version, " Proc. Meteroids 2001 Conf., pp.367-370, Kiruna (Sweden), 6- 10 Aug, 2001.

[7] J.A. Weitzen, "Characterizing the Multipath and Doppler Spreads of the High-Latitude Meteor-burst Communication Channel, " IEEE Trans. on Comm., vol. 35, pp.1050-1058, 1987.

[8] D. W. R. McKinley, "Meteor science and engineering, " McGraw-Hill, 1961.