Moscow Workshop on Electronic and Networking Technologies, MWENT 2018 - Proceedings, 2018, vol.2018-March, pages 1-7

Analisys of frequency-correlation properties of multipath channel for encyprion key generation using samples of differential phase

Kazan Federal University, 420008, Kremlevskaya 18, Kazan, Russia

Abstract

© 2018 IEEE. Wireless Key Generation exploits randomness of fast fading of a multipath radio channel to create identical copies of a shared encryption key at two communication nodes. A promising way for creating a highly secure key is use of samples of differential phase, which allows to overcome short-term instability of frequency standards and to make key generation devices smaller. This study examines frequency-correlation properties of the multipath channel to justify a feasibility of encryption keys generation with the differential phase method. By computer simulation, frequency autocorrelation functions of the envelope and carrier phase of a multipath radio signal are obtained, and estimates of the channel coherence bandwidth are made for a typical urban propagation environment. For random variations of the differential phase of a two-sine probe signal, a probability distribution is analyzed, its uniformity tests are done, and estimates of Shannon entropy at various frequency separations of the two probing tones are made. An effect of the line-of-sight wave and the number of multipaths on the channel frequency-correlation function and on probabilistic properties of the differential phase is considered.

http://dx.doi.org/10.1109/MWENT.2018.8337300

Keywords

differential phase, encryption key generation, frequency-correlation function, Multipath channel, Shannon entropy, synchronization

References

[1] J. Zhang et al, "Key generation from wireless channels: A review," IEEE Access, vol. 4, pp. 614-626, Jan. 2016.

[2] S. Jana 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.

[3] S. Mathur 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.

[4] A.D. Smolyakov et al, "Experimental verification of possibility of secret encryption keys distribution with a phase method in a multipath environment," Proc. X Int. IEEE Sib. Conf. on Cont. And Comm. (SIBCON-2013), pp. 1-5, Krasnoyarsk (Russia), Sept. 2013.

[5] A.I. Sulimov 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.

[6] A.D. Smolyakov et al, "Experimental extraction of shared secret key from fluctuations of multipath channel at moving a mobile transceiver in an urban environment," Proc. 12th Int. Conf. on Security and Cryptography (SECRYPT-2015), pp. 355-360, Colmar (France), 2015.

[7] A.A. Hassan, W.E. Stark, J.E. Hershey, S. Chennakeshu, "Cryptographic key agreement for mobile radio," Digital Signal Processing, vol.6, iss.4, pp. 207-212, 1996.

[8] D.W. Allan, "Time and frequency (time-domain) characterization, estimation, and prediction of precision cloks and oscillators," IEEE Trans.on ultrasonics, ferroelectrics, and freq. cont., vol. UFFC-34, no.6, pp. 647-654, Nov. 1987.

[9] B. Sklar, "Digital communications: fundamentals and applications," Prentice-Hall PTR, 1079 p., 2001.

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

[11] A.I. Sulimov et al, "Simulation of encryption key distribution process based on a multipath radio propagation," Proc. X Int. IEEE Sib. Conf. on Cont. And Comm. (SIBCON-2013), pp. 1-4, Krasnoyarsk (Russia), Sept. 2013.

[12] ETSI EN 300 910. Digital cellular telecommunication system (Phase 2+). Radio transmission and reception (GSM 05.05 ver. 8.5.1), European Standard (Telecommunication Series), 95 p., 1999.

[13] R.H. Clarke, "A statistical theory of mobile radio reception," Bell System Tech. Jour., vol. 47, pp. 957-1000, July 1968.

[14] G.A. Ponomaryov, A.M. Kulikov, E.D. Telpukhovskiy, "Propagation of UHF-radio waves in urban environment," Rasko, Tomsk (Russia), 223p., 1991 (in Russian).

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