Experimental Study of Performance and Security Constraints on Wireless Key Distribution Using Random Phase of Multipath Radio Signal

Amir I. Sulimov, Alexey D. Smolyakov, Arkadij V. Karpov and Oleg N. Sherstyukov
Department of Radio Physics, Institute of Physics, Kazan Federal University,
18th Kremlyovskaya St., Kazan, Russia

Keywords: Encryption Keys Distribution, Common Randomness, Multipath Radio Propagation, Channel Reciprocity, Randomness of Carrier Phase, Rate of Encryption Key Distribution, Spatial Correlation, Key Interception.

Abstract: The paper presents the results of experimental distribution of encryption keys based on random carrier phase of fading radio signal measured in a multipath environment. The random bits extraction scheme was proposed and tested in practice. The proposed scheme is universal and applicable to measurements digitizing of any observable random variable. Experimental study of spatial correlation of multipath signal phase in the case of transverse spatial diversity is carried out. Experimental estimation of the key generation rate and the probability of its passive interception at different distances between the legal user and potential eavesdropper are also performed. It is shown that the parameters of bit extraction procedure significantly affect on the performance and security of the key distribution process.

1 INTRODUCTION

The problem of secure distribution of encryption keys is one of the most important in cryptography. Amongst the others, the wireless key distribution methods firstly proposed in (Hershey, 1995; Hassan, 1996) have been actively investigated in the recent decade. Under this method, a multipath radio channel is considered as a shared source of randomness used for the creation of secret key. The key is generated by observing random variations in the parameters of fading radio signal received in a multipath environment. To do this, two nodes (say, Alice and Bob) transmit to each other a series of radio signals and measure their parameters when receiving. The channel reciprocity ensures the measured signal parameters will be identical at both sides. Due to a rapid spatial decorrelation of signal characteristics in a multipath environment the key interception is very unlikely at practice.

Several methods of the key generation using different parameters of multipath signal have been considered in prior publications. An experimental verification of the amplitude method based on measurements of random values of received signal strength has been carried out in (Mathur, 2008; Wilhelm, 2010; Liu & Trappe, 2010; Wei, 2011; Croft, 2011; Zan, 2012). An experimental verification of the channel impulse response (CIR) method based on measurements of random values of signal quadrature components has been performed in (Li, 2006; Wilson, 2007; Hamida, 2009; Madiseh, 2009). However, the phase method seems to be the most appropriate for the key generation. Unlike the amplitude and signal quadrature components, the signal phase often shows uniform probability distribution, which is desirable for the key generation. Unfortunately, the prior publications (Hassan, 1996; Korzhik, 2012; Shehadeh, 2011) on the phase method are mostly limited to theoretical analysis and simulation. The only paper (Smolyakov, 2013) we know, where an attempt of its experimental verification was made, does not concern any key interception issues.

The purpose of this paper is to clarify experimental evaluations of the performance and security of key distribution based on observation of the signal phase in a multipath environment.

Sulimov A., D. Smolyakov A., V. Karpov A. and N. Sherstyukov O..
Experimental Study of Performance and Security Constraints on Wireless Key Distribution Using Random Phase of Multipath Radio Signal.
DOI: 10.5220/0005101004110416
In *Proceedings of the 11th International Conference on Security and Cryptography* (SECRYPT-2014), pages 411-416
ISBN: 978-989-758-045-1

2 SCENARIO OF THE EXPERIMENTS

To perform all the experiments, we designed three identical test devices (or simply nodes). The two of them (nodes *A* = Alice and *B* = Bob) worked as legitimate users, and the third one (node *E* = Eve) served as a passive eavesdropper, who tried to intercept the measurements of signal phase on the side of node *B* (or simply Bob). Alice and Bob transmitted to each other a series of probing signals at carrier frequency *f* = 962 MHz in a half-duplex mode with the time frame of activity of 50 ms. The transmitted power was set at 10 dBm. When receiving a signal, each node measured the carrier-phase and stored the data into a built-in SD-memory card. Thus, each node was performing twenty measurements of the carrier-phase in one second. The reference oscillators of all the three nodes have been synchronized via coaxial cables. To provide the most intense random variations of the signal phase, an omni-directional antenna has been used in each node for the signal reception.

The experiments have been carried out in a typical academic environment, which is a good example of multipath propagation medium (see Figure 1). The placements of nodes *A* and *B* were fixed, and the distance between them (length of the test link) was 4.5 m. The *E* node has been placed at various spatial diversities *d* from Bob in a transverse relative to the link direction. The value of *d* has been varied in the range from 0 cm to 100cm with 5 cm increment. The zero spacing (*d* = 0 cm) has been implemented by using a common receiving antenna for both *B* and *E* nodes.

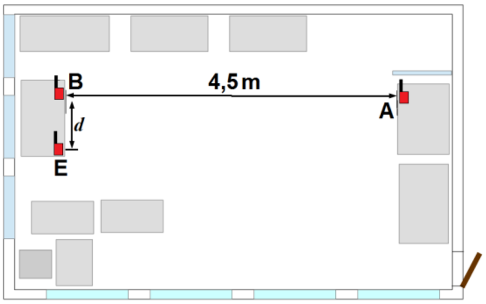


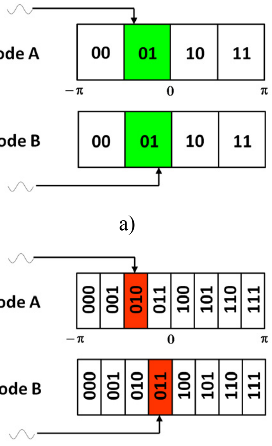
Figure 1: Experimental setup.

A sample of 9000 measurements has been collected at each node for every fixed placement of the nodes *A*, *B* and *E*. In a typical multipath environment, such a small sample is insufficient to create a long enough key. The reason is the low channel variability (Madiseh, 2009). To ensure a high channel variability (or high Doppler frequency f_D) the researchers were actively walking within the test room in various directions while the sample was being collected. In addition, antenna of the node *A* was being randomly shifted in the range ±50cm in perpendicular (relative to the link axis) plane. Such actions provided quite a satisfactory Doppler frequency $f_D = 10 \div 30$ Hz, which made it possible to keep up to 50% of a primary sample after implementing the measurements decorrelation.

The collected measurement data $\{\varphi_A\}$, $\{\varphi_B\}$ and $\{\varphi_E\}$ has been copied on a laptop, where with the help of a special software it has been converted into the keys K_A, K_B and K_E, respectively. After this, we have examined a bit disagreement rate of the generated keys and a cross-correlation between the phase samples.

3 BIT EXTRACTION

To generate the keys from the collected samples of signal phase measurements a bit extraction procedure is necessary to be performed. To extract random bits, the full range of the signal phase variation $\varphi \in [-\pi;\pi]$ is divided into 2^m quantization intervals. The variable *m* denotes the number of bits we want to extract from a single phase measurement. We called it a “codeword length” and expressed the values of *m* in bits per measure (or simply bpm for short).



a)

b)

Figure 2: Extraction of bits from the carrier phase measurements: a) *m*=2bpm, b) *m*=3bpm.

In our bit extraction scheme, each quantization interval is mapped into a binary codeword of length *m*. When the phase measurement falls into some quantization interval, an associated codeword is formed at the output. An encryption key is generated by combining or hashing all the resultant codewords. To increase entropy of the key, the measurements decorrelation procedure (Croft, 2011) is performed before the bit extraction.

Another important requirement is to ensure uniformity of the generated key. To fulfil this requirement, the phase measurements should fill all the quantization intervals uniformly. This is possible if the carrier phase will be a uniformly distributed random variable. However, this is not always true in practice. For example, the presence of intense line-of-sight wave violates the signal phase uniformity. In this case, we should use non-uniform quantization of measurements with the variable-width intervals.

The choice of optimal codeword length is the most important step at the bit extraction. It is obvious, that the rise of m will increase a key generation rate R_K, but it will also increase a bit disagreement rate between the K_A and K_B keys. It should be noted, that due to measurement errors and impact of the channel noise the perfect cross-correlation between the $\{\varphi_A\}$ and $\{\varphi_B\}$ samples collected by Alice and Bob is impossible in practice. As a result, the φ_A and φ_B measurements always have some deviation $\Delta\varphi = \varphi_A - \varphi_B \neq 0$. If the width of quantization intervals is sufficiently large, the deviation $\Delta\varphi$ will not cause any mismatch between the codewords formed by Alice and Bob (see fig.2a). However, the rise of m increases probability of codewords mismatch (see fig.2b). Thus, there must be an optimal value m^*, which maximizes the key generation rate and minimizes the probability of bit disagreement between the K_A and K_B keys.

4 EXPERIMENTAL RESULTS

Comparison of phase measurements collected by the nodes A and B showed a high cross-correlation $\rho_\varphi = 0.95 \div 0.99$ between the samples, which confirmed reciprocity of the multipath channel. Some mismatch of the $\{\varphi_A\}$ and $\{\varphi_B\}$ samples is explained by non-ideal calibration of experimental equipment and by impact of the channel noise. Despite the high correlation between measurement data of Alice and Bob, the K_A and K_B keys contained a large fraction of bits in mismatch. The minimum experimentally achieved key disagreement rate p_e was about 3%.

In (Liu & Trappe, 2010; Korzhik, 2012) the key disagreement rate p_e has been considered as a function of cross-correlation coefficient ρ_φ between the measurement data of Alice and Bob. This concept is very useful in practice, since it allows estimation of the key disagreement rate even before implementing the bit extraction procedure. Figure 3 shows such dependence observed at the experiments. Despite the lack of experimental data for the range $\rho_\varphi \in [0.3;0.8]$, the curve in Figure 3 is in a good agreement with the results in (Liu & Trappe, 2010), but shows slightly lower values of probability p_e. It should be noted, that the curve in Figure 3 is applicable not only for estimating the p_e value of disagreement rate between the K_A and K_B keys, but it also can be used for evaluating the p_{int} value of disagreement rate between the K_B and K_E keys. In the latter case, we should use a cross-correlation between the $\{\varphi_B\}$ and $\{\varphi_E\}$ samples as an argument.

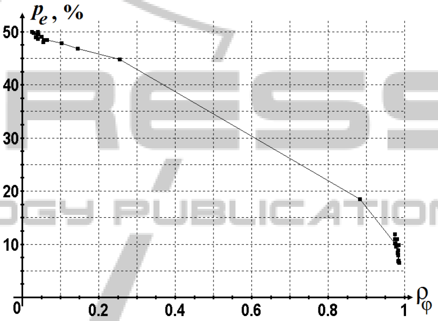


Figure 3: Probability of bit disagreement as a function of cross-correlation between the phase measurements.

To eliminate a mismatch between the K_A and K_B keys, their reconciliation with a cyclic redundancy codes (CRC) of the CRC-16-CCITT standard was being performed. The use of CRC-codes is analogous to the well-known method of privacy amplification (Bennet, 1995) but easier to implement. Just as in the privacy amplification method, after successful check of some fragment of the K_A and K_B keys we should remove at least 16 arbitrary bits. In our experiments, the optimal length of verified fragment of the K_A and K_B keys was in the range from 18 to 41 bits of which we removed 16 arbitrary bits. It is clear, that the keys reconciliation led to a huge loss. An efficiency of the key reconciliation process was characterized by the $\eta = (N_+/N)$ parameter. Here N_+ is the key length after and N is the key length before the reconciliation, respectively. Due to high values of the key disagreement rate p_e the maximum experimentally achieved value of η was about 10%.

Figure 4 presents achieved key generation rate R_K expressed in bits per second (or simply in bps) as a function of the codeword length m. The key generation rate was estimated as $R_K=(N_+/T)$, where T is duration of the samples collecting. In our experiments, it was T = 9000•50 ms = 450 s. The curves in Figure 4 are presented for three different values of the cross-correlation coefficient between the $\{\varphi_A\}$ and $\{\varphi_B\}$ samples. It can be clearly seen, that small changes in the ρ_φ value lead to a significant reduction in the key generation rate. Relatively high values of the key disagreement rate p_e resulted in small values of optimal codeword length m*, which in the experiments were only 1 or 2 bpm. All attempts to extract more random bits from each measurement caused a rapid rise in the key disagreement rate p_e and to an expected sharp decrease in the efficiency of key reconciliation η. The maximum achieved key generation rate slightly exceeded 2 bps, which is in correspondence with the results of other verifications of the wireless key distribution (Madiseh, 2009).

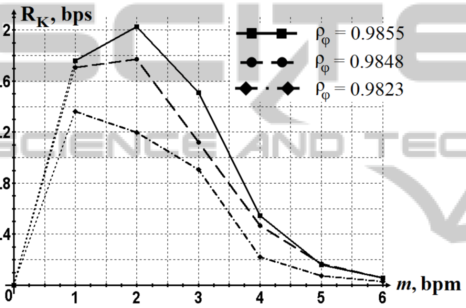


Figure 4: Key generation rate as a function of the codeword length.

A spatial correlation of the signal phase and its relationship with the key disagreement rate has also been investigated during the experiments. To do this, the cross-correlation coefficient between the $\{\varphi_B\}$ and $\{\varphi_E\}$ samples along with the key disagreement rate p_{int} of the K_B and K_E keys have been determined for each value of the spatial diversity d. The observed dependencies are presented at Figures 5 and 6, respectively.

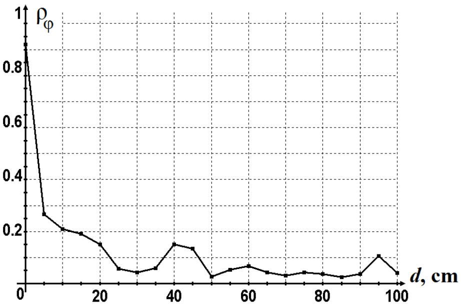


Figure 5: Spatial autocorrelation function of carrier-phase.

The maximum correlation between the $\{\varphi_B\}$ and $\{\varphi_E\}$ samples has been detected when Bob and Eve used a common antenna for the probing signals reception. The highest value was 0.8828. A mutual influence of input circuits of both nodes prevented correlation between the $\{\varphi_B\}$ and $\{\varphi_E\}$ samples to be higher. This mutual influence caused additional distortions in the signal phase which made deviation of the φ_B and φ_E measurements much greater. Furthermore, the closer receiving antennas of the B and E nodes were the stronger antenna array effect we observed. When the spatial diversity d of nodes became less λ, we observed strong distortions of radiation pattern of both the receiving antennas.

The curves in Figure 6 actually reproduce the profile of autocorrelation function presented at Figure 5. It should be clarified, that value p_{int} = 0 indicates absolute identity of the K_B and K_E keys, which means perfect key interception by Eve. Conversely, value p_{int} = 50% means absolute independence of the K_B and K_E keys and absence of the key interception threat. Figure 6 shows the two curves obtained for different values of the codeword length m. It can be seen, that the reduction of m increases a key interception probability. This is

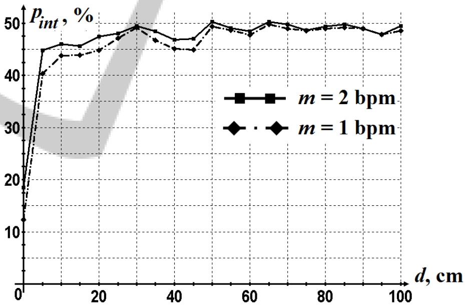


Figure 6: Probability of bit disagreement between the K_B and K_E keys as a function of spatial diversity of Bob and Eve.

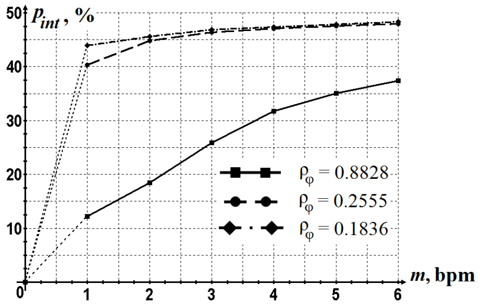


Figure 7: Probability of bit disagreement between the K_B and K_E keys as a function of the codeword length.

reasonable, because with a decrease in the number of quantization intervals the probability 2^{-m} of a simple guessing the codewords increases.

Figure 7 illustrates this effect in more details. It presents the dependence of key disagreement rate between the K_B and K_E as a function of the codeword length m for three values of cross-correlation coefficient between the {φ_B} and {φ_E} samples. The presented curves demonstrate sharp decline in the probability of key interception with increase in m at low values of cross-correlation coefficient. This result is in agreement with the conclusions of fundamental work (Maurer, 1993), where it has been shown, that not only the number of successfully distributed bits N_+ should be considered for the key generation rate R_K estimation, but the amount of mutual information $I(K_E;K_B)$ between the K_B and K_E keys is also should be taken into account.

5 CONCLUSIONS

The experiments showed feasibility of wireless key distribution based on measurements of carrier-phase in a multipath environment. The key generation rate R_K ~ 2 bps has been achieved at the Doppler frequency f_D ~ 30Hz and cross-correlation between the measurement samples of Alice and Bob close to 0.99. Investigation of spatial autocorrelation of the signal phase showed an existence of the passive key interception threat even at distances more than 3λ. Furthermore, it was found that absolute correlation between the measurement data of two closely spaced nodes is hardly achievable in practice. The complex effects of mutual influence of antennas and input circuits of both nodes restrict the ability to intercept generated keys. Experimental results have shown that the behaviour of probability of passive key interception when varying a spatial diversity of legitimate user and eavesdropper basically repeats the profile of the spatial autocorrelation function for the measurement data. It was also shown an existence of optimal number of bits, which should be extracted from a single measurement of observable random variable to maximize the key generation rate and to reduce the probability of its interception.

REFERENCES

Bennet, C.H., Brassard, G., Crepeau, C., Maurer, U.M., 1995. Generalized privacy amplification. In *IEEE Transactions on Information Theory*, vol.41, iss.6, pp. 1915-1923.

Croft, J.E.D., 2011. *Shared secret key establishment using wireless channel measurements*. Ph.D. thesis, Dept. Elect. Eng., University of Utah, USA.

Hamida, S.T.B., Pierrot, J.B., Castelluccia, C., 2009. An adaptive quantization algorithm for secret key generation using radio channel measurements. In *NTMS'09, Proceedings of 3rd International Conference on New Technologies, Mobility and Security*, pp. 1-5.

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

Hershey, J.E., Hassan, A.A., Yarlagadda, R., 1995. Unconventional cryptographic keying variable management. In *IEEE Transactions on Communications*, vol.43., iss.1, pp.3-6.

Korzhik, V., Yakovlev, V., Kovajkin, Y., 2012. Secret key agreement over multipath channels exploiting a variable-directional antenna. In *International Journal of Advanced Computer Science and Applications*, vol. 13, No. 1, pp. 172–178.

Li, Z., Xu, W., Miller, R. and Trappe, W., 2006. *Securing wireless systems via lower layer enforcements*. In *WiSec '06, Proceedings of the 5th ACM workshop on Wireless Security*, pp. 33-42.

Liu, R. and Trappe, W., 2010. *Securing wireless communications at the physical layer*, Springer, NY, 396 p.

Madiseh, M.G., He, S., McGuire, M.L., Neville, S.W., Dong, X., 2009. Verification of secret key generation from UWB channel observations, In *ICC'09, Proceedings of the IEEE International Conference on Communications*, pp. 593-597.

Mathur, S., Trappe, W., Mandayam, N., Ye, C., Reznik, A., 2008. Radio-Telepathy: extracting a secret key from an unauthenticated wireless channel. In *MobiCom'08, Proceedings of the 14th ACM international conference on Mobile computing and networking*, pp. 128-139.

Maurer, Ueli M., 1993. Protocols for secret key agreement by public discussion based on common information. In *Advances in Cryptology (CRYPTO '92). Lecture Notes in Computer Science*, vol. 740, pp. 461–470.

Shehadeh, E.H., Alfandi, O., Tout, K., Hogrefe, D., 2011. Intelligent mechanisms for key generation from multipath wireless channels. In *WTS'2011, Proceedings of the Wireless Telecommunications Symposium*, pp.1-6.

Smolyakov, A.D., Sulimov, A.I., Karpov, A.V., Sherstyukov, O.N., 2013. Experimental Verification of Possibility of Secret Encryption Keys Distribution with a Phase Method In a Multipath Environment. In *SIBCON-2013, Proceedings of 2013 IEEE International Siberian Conference on Control and Communications*.

Wei, Y., Zeng, K., Mohapatra, P., 2011. Adaptive wireless channel probing for shared key generation based on PID Controller. In *Proceedings of IEEE INFOCOM'2011*, pp. 2165-2173.

Wilhelm, M., Martinovich, I., Schmitt, J.B., 2010. Secret key from entangled sensor motes: implementation and analysis. In *WiSec'10, Proceedings of the 3rd ACM*

conference on Wireless network security, pp. 139-144.
Wilson, R., Tse, D., Scholtz, R.A., 2007. Channel identification: Secret sharing using reciprocity in ultrawideband channels. In *Proceedings of IEEE Transactions on Information Forensics and Security*, Part 1, vol.2, iss.3, pp. 364-375.

Zan, B., Gruteser, M., Hu, F., 2012. Improving robustness of key extraction from wireless channels with differential techniques. In *ICNC'2012, Proceedings of International Conference on Computing, Networking and Communications*, pp. 980-984.