Experimental Extraction of Shared Secret Key from Fluctuations of Multipath Channel at Moving a Mobile Transceiver in an Urban Environment

Alexey D. Smolyakov, Amir I. Sulimov, Arkadiy V. Karpov and Aidar A. Galiev
Department of Radio Physics, Institute of Physics, Kazan Federal University, 18th Kremlyovskaya St., Kazan, Russian Federation

Keywords: Encryption Key Distribution, Shared Randomness, Multipath Radio Propagation, Mobile Communications, Carrier Phase, Wireless Synchronization, Entropy.

Abstract: The Wireless Key Distribution is one of the most promising and fast growing areas in modern applied cryptography. This area covers various techniques of secure secret key distribution between two legitimate users who share a common radio channel with unpredictable signal fading in a multipath environment. In essence, the pair of legitimate nodes uses their multipath radio channel as a source of common randomness to establish a shared encryption key. There are a number of studies have been presented in recent publications devoted to experimental implementation of the Wireless Key Distribution using random variations in the received power of fading signal. Despite a number of valuable benefits, there is a much fewer experimental verifications of phase method with all of them are limited to a key distribution within some indoor environments only. Apparently, this is due to the technical difficulties of precise synchronization of legitimate users' equipment to provide coherent carrier phase measurements in a microwave radio frequency range. In this regard, our experiments can be considered as the first experimental verification of secure Wireless Key Distribution by observing random variations in the carrier phase of multipath signal at moving a mobile user within a real outdoor environment. To perform this, we used wireless Internet transmission of concurrent service data to maintain a required level of synchronization of one stationary and one mobile legal nodes. Despite the humble key generation rates we have achieved in practice, our results show possibility of secure wireless key distribution between the base station and mobile subscriber in a cellular communications scenario.

1 INTRODUCTION

Information security in wireless systems is vital in developing the modern telecommunications. Being the most popular type of wireless systems, the cellular communications continuously increase their demands for confidentiality of traffic data of mobile subscribers. To fulfill these severe requirements, a secure secret key distribution between the base station and legal subscriber's cell phone could be used. The Wireless Key Distribution (WKD) proposed firstly in (Hershey, 1995; Hassan, 1996) solves this problem along with unpredictable variation in time of naturally random secret key. The key is established through observing the stochastic fluctuations in characteristics of communication channel between the base station and mobile phone arising due to signal fading in an urban environment.

To establish a shared key, two legal nodes (say, Alice as mobile phone and Bob as base station) exchange with a series of radio signals to measure their stochastic fluctuations at receiving. The channel reciprocity property ensures the measurements to be identical at both sides. Such common randomness is a source to create two copies of the shared key. Due to a rapid spatial decorrelation of radio signal in real multipath environments (Prettie, 2002; Hamida, 2009; Madiseh, 2009) a key interception is very unlikely in practice.

In (Zhu, 2013) an experimental verification of WKD has been presented for the case of mobile communications established in an outdoor environment. In this study, two legitimate nodes placed into the moving cars created a secret key by establishing a common multipath channel and observing random variations in the received signal

D. Smolyakov A., I. Sulimov A., Karpov A. and V. Galiev A..
Experimental Extraction of Shared Secret Key from Fluctuations of Multipath Channel at Moving a Mobile Transceiver in an Urban Environment.
DOI: 10.5220/0005561703550360
In *Proceedings of the 12th International Conference on Security and Cryptography* (SECRYPT-2015), pages 355-360
ISBN: 978-989-758-117-5

strength (RSSI). However, we believe that the measurements of signal carrier phase have a number of valuable benefits and would be more appropriate for cryptographic applications. There are at least three advantages of the carrier phase approach. Firstly, the probability distribution of carrier phase is usually closer to uniform as opposed to the distribution of RSSI, which is a Rician random variable (Rappaport, 1996). Secondly, the RSSI based method is mainly limited to a fixed link length communication scenario. On the other hand, the link length is extremely variable in a mobile scenario. This leads to a strong variation in the median RSSI level. Therefore, a continuous system adjustment is required to maintain the RSSI based key generation. Finally, the phase measurements have the ambiguity property making key interception more complicate in practice. This property follows directly from the fact that the same carrier phase value $\varphi \in [-\pi;\pi]$ can be simultaneously observed at infinite set of receiving points separated by an integer number of wavelengths λ. As a result, if the separation between a possible eavesdropper and a legal node is larger than $\lambda/2$ then unconditional recovering of the phase value detected by user is impossible. According to the prognosis of development of wireless communications given by (Rappaport, 2013), a move of the 5G cellular systems into the 30GHz frequency range is expected in the nearest 5-10 years. The corresponding wavelengths of the order of 1 centimeter exclude any practical possibility of a key interception.

Despite all the above benefits, there are a few experimental verifications of the phase method have been presented in recent publications. The main difficulty in its implementation is the need for precise carrier frequency synchronization of both legitimate nodes. In (Smolyakov, 2013; Sulimov, 2014) a WKD with the phase method has been implemented but within the test indoor environment only. The synchronization issue was solved by a direct cable connection between the two key generation parties. Apparently, such a solution is inappropriate in the outdoor mobile scenario. Therefore, it is necessary to keep the sides synchronized within a few nanoseconds precision by wireless methods solely. Though being technically difficult, this problem is resolvable.

The aim of our research was an experimental WKD verification by extracting a common randomness from the fluctuations of carrier phase of multipath signal at moving a mobile user within a real urban environment. As will be shown in the following sections, we succeeded in our goal, but a further wireless synchronization enhancement is required to achieve better system performance.

2 SCENARIO OF THE EXPERIMENTS

A pair of identical transceiving test devices (M1 and M2) has been designed to implement the experimental verification. The M1 test device (let's call it Bob) was placed at the 14th floor of our research facility at approximately 45 meters above the mean roof height to serve as a base station. The M2 test device (let's call it Alice) was placed into a car to be moved on the closed route within the surrounding urban environment (see Fig.1). The route was of 1680 meters in length with the average car speed of about 10 *m/s*. The data collecting time was T_{OBS} = 300 seconds, which allowed the car to pass two full laps on the route.

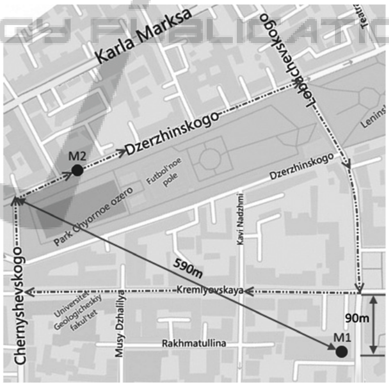

Figure 1: Moving route of mobile user.

During the data collecting procedure Alice and Bob kept on transmitting the sounding signals at the carrier frequency f = 963 *MHz* in a time-division duplex mode. At receiving the signal each node was measuring its amplitude and carrier phase to observe random fluctuations of the multipath channel. The signal amplitude values were used to track a current channel quality that possibly could be unsatisfactory due to deep fades. However, only the phase measurements were used to create a secret key.

To ensure synchronous operationing of Alice and Bob with the required accuracy of phase measurements, each side has been equipped with the FS725 rubidium frequency standard. In addition to the test device M1 and frequency standard FS1, mobile user Alice also used a laptop L1 to manage all the equipment and WKD process. The base station Bob used a laptop L2 in a similar way to manage his test device M2 and frequency standard FS2. The L1 and L2 laptops were connected through the wireless Internet to transmit all the service data needed to maintain the WKD process. This Internet connection served just as an auxiliary open communication channel and was not used to transfer any secret phase measurements. The software implementation of the WKD protocols stack was running both on the L1 and L2 laptops and included synchronization procedure for the FS1 and FS2 frequency standards.

Our synchronization protocol consisted of two stages. At the first stage, the FS1 and FS2 frequency standards were being adjusted by the GPS 1PPS-clock pulses. At the second stage, Alice and Bob were exchanging with a series of test signals to collect a correcting sample of phase measurements. After that, Bob sent Alice his sample to allow her to perform calculations of necessary correction coefficient to adjust the FS2 output frequency. The resultant correction data transmitted to Alice through the Internet connection. Such synchronization allowed keeping a relative frequency mismatch between the FS1 and FS2 standards within the $3*10^{-12}$ bound that was enough to provide desired coherent measurements of the carrier phase. However, our experimental data showed that a large short-term instability remained causing an instrumental error of phase measurement up to 30 degrees in magnitude.

3 DATA ANALYSIS

Two samples of 30000 phase measurements in size have been collected at each node during the data collecting procedure of $T_{\text{OBS}} = 300$ seconds duration. Unfortunately, a large part of the collected data corresponded to a nonlinear operating mode of phase detectors caused by deep fades and power lack of the received signal. Therefore, all the phase measurements with strong nonlinear distortion have been eliminated from the sample with only $N = 4575$ measurements left after that. Nevertheless, even reduced amount of experimental data was sufficient to assess basic probability properties of the observed parameters of multipath signal.

As was shown in (Smolyakov, 2013; Sulimov, 2014) the maximum achievable rate of encryption key distribution can be estimated by the formula (1). Here we denote the entropy of observed signal parameter (in our case, this is the carrier phase) as $H(\varphi)$, and N_0 is the amount of phase measurements that are suitable for the key generation. As follows from the formula (1), the key generation rate is defined mainly by the physical properties of multipath channel.

$$R_{\max} = H(\varphi) N_0 / T_{OBS} \qquad (1)$$

Collected experimental data allowed estimation of the entropy of carrier phase $H(\varphi)$ along with the proportion of the sample (N_0/N) suitable for the key generation in the mobile scenario close to actual practice of mobile communications.

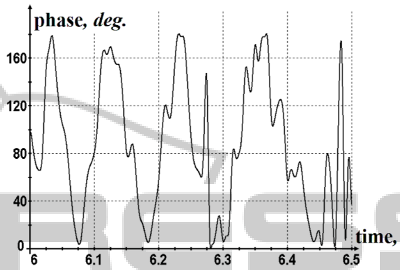

Figure 2: An extract of carrier phase fluctuations observed at mobile side while moving in an outdoor environment.

Fig. 2 shows a fragment of carrier phase fluctuations of received multipath signal as it was observed by Alice while she was moving on the car within the urban environment. The presented fluctuations clearly show a presence of some deterministic component along with random variations caused by fast fading. Obviously, such deterministic component is caused by the line-of-sight wave (LOS), which presence reduces entropy of carrier phase. Unfortunately, our attempt to suppress the LOS wave resulted in such low received signal strength that it was insufficient for the correct operation of the phase detector. For this reason, the samples $\{\varphi_A\}_N$ and $\{\varphi_B\}_N$ that were collected by Alice and Bob, respectively, contained only the measurements corresponding to the dominance of LOS wave within the received signal.

A significance of the multipath component and fading phenomena is commonly characterized by the Rician factor k_R (Rappaport, 1996). An analysis of the data, collected while Alice was moving along the route depicted at Fig.1, shows that the value of k_R was varying in the range from 11 to 20 dB with the average value about 15 dB. Thus, the LOS wave was at 15 dB stronger than the multipath component. In (Sulimov, 2013) was shown that in the case of the fixed link length scenario such k_R value causes the carrier phase to have a non-uniform probability distribution with a pronounced peak located at the phase of the LOS wave. However, in a mobile scenario the dominant mode of probability distribution is moving within the entire range of phase variation $\varphi \in [-\pi;\pi]$. This slightly improves a uniformity of the phase sample but does not exclude a high temporal autocorrelation of successive measurements. The presence of such autocorrelation reduces the N_0 value.

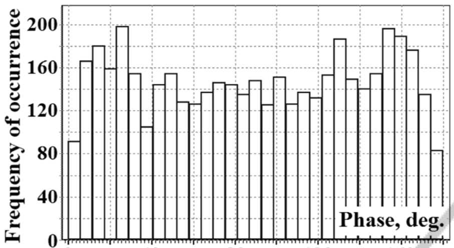

Figure 3: Probability distribution histogram of the collected sample of phase measurements.

Fig. 3 shows empirical probability distribution histogram of the phase measurements sample collected by Alice. As expected, due to presence of strong LOS wave the histogram is non-uniform. This weakens entropy of the generated key. In addition, non-uniformity of probability distribution complicates the bit extraction procedure at processing the phase measurements. In particular, the sample pre-randomization becomes necessary. Although, the probability histogram does not reveal any dominant mode, the sample autocorrelation function $R[n]$ clearly indicates the cross-correlation of neighboring measurements (see Fig. 4).

The presented sample autocorrelation function (ACF) also indicates a need for sample decorrelation to create unpredictable binary key sequence. The decorrelation step n_0 is determined by the condition: $R[n_0] \le \varepsilon$, where ε is a threshold correlation level. After the sample decorrelation is finished, its effective size is reduced to $N_0 = N/n_0$ measurements. From the physical point of view, the step n_0 characterizes a channel coherence time that depends on the channel variability determined by Alice's movement speed.

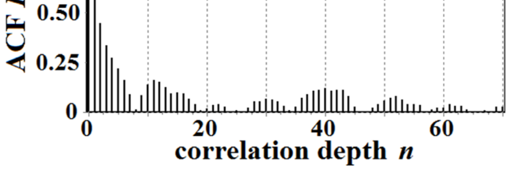

Figure 4: Autocorrelation function of the collected sample of carrier phase measurements.

Given the probability histogram of phase measurements presented at Fig.3, we were able to estimate a value of the carrier phase entropy using the formula (2). Here $\hat{p}_i$ is a normalized empirical frequency of occurrence of phase measurements within the i-th column of the histogram, $\Delta\varphi$ is a quantization interval width and $H_e(\delta\varphi)$ is entropy of the phase measurement error caused by both channel noise and imperfection of measuring equipment.

$$\hat{H}(\varphi) = -\sum_i \hat{p}_i \log_2(\hat{p}_i / \Delta\varphi) - H_e(\delta\varphi) \qquad (2)$$

In our experiments, standard deviation $\sigma(\delta\varphi)$ of the phase measurement error did not exceed 1°. An estimation of the measurement error entropy showed the value of $H_e(\delta\varphi) \sim 0.01$ *bits*. At the same time, estimation of the carrier phase entropy showed the value $\hat{H}(\varphi) = 7.5$ *bits*. Thus, theoretically we could extract up to 7.5 random bits in average from every single measurement of the carrier phase. However, these values characterize only the maximum achievable key generation rate $R_{\max}$. In the Section 5 we present actually achieved values R_K of the key generation rate.

4 STATISTICAL PROPERTIES OF EXTRACTED KEY SEQUENCE

The main reason for the statistical properties of generated key sequence to degrade is autocorrelation within the primary sample of phase measurements. To eliminate its effect, a sample decorrelation procedure should be performed (Croft, 2011). The decorrelation implies secondary sampling of the primary sample with the step n_0 determined by the condition: $R[n_0] \le \varepsilon$, where ε is a permissible correlation level. After this the decorrelated sample takes the form $\{\varphi_1, \varphi_{n_0+1}, \varphi_{2n_0+1} \ldots\}$ with effective size reduced to $N_0 = N/n_0$ measurements. It may be said that the improvement of statistical properties of the key is achieved through the n_0-times waste in its generation rate.

Next we implemented an entropy-based bit extraction scheme (Sulimov, 2014) to create a shared key. To assess its uniformity, we used the NIST statistical tests suite (NIST, 2010). Among the 15 tests in the NIST suite, we run only 10-12 tests and find that the extracted bits can pass these tests. The other tests require larger input size, and we plan to run them in the future. The testing has been performed for the two following values of the allowable correlation: $\varepsilon_1 = 0.3$ and $\varepsilon_2 = 0.1$. The decorrelation steps corresponding them are $n_0(\varepsilon_1) = 4$ and $n_0(\varepsilon_2) = 14$, respectively. The generated key sequence has successfully passed all the enabled tests. By using the ε_1 threshold the smallest *p*-value equal to 0.43 was observed in the «Non Overlapping Template» test. Similarly, by using the ε_2 threshold the smallest *p*-value equal to 0.55 was observed in the «Longest Run» test. In summary, by reducing the permissible correlation ε from 0.3 down to 0.1 we were able to improve statistical properties of the key sequence and to increase average *p*-value at 33%.

The testing results also revealed their sensibility to the number of bits *m* extracted from each single phase measurement. In the following, we will refer to this variable as the *codeword length*. During the bit extraction procedure we were varying the codeword length *m* within the range from 1 to 6 bits per measure. The best testing results were achieved with the *m* = 2 and *m* = 3 values. In the case of *m* = 1 the resultant key sequence was too short to provide a good statistics. On the other hand, at high values of *m* there was insufficient size *N* of the primary phase measurements sample to provide its accurate randomization. Even at *m* = 6 to succeed in the sample randomization, it is required that the carrier phase values to fill all the 64 quantization intervals uniformly with equal frequencies of occurrence within them. The amount of our experimental data (4575 values) was insufficient to fulfill this requirement, because we had only 71 values of carrier phase in average for each quantization interval.

Summarizing the testing results, we can conclude that the generated key sequence satisfies the criteria of randomness.

5 KEY DISTRIBUTION RESULTS

The samples of carrier phase measurements $\{\varphi_A\}_N$ and $\{\varphi_B\}_N$ collected by Alice and Bob allowed generation of two copies K_A and K_B of the shared secret key. Unfortunately, the $\{\varphi_A\}_N$ and $\{\varphi_B\}_N$ samples revealed a significant mismatch $|\varphi_A - \varphi_B|$ leading to samples low cross-correlation: $cor(\varphi_A,\varphi_B)=0.571$. Based on this value of cross-correlation a preliminary estimation of the key mismatch rate gives $p_e \sim 32\%$ (Sulimov, 2014). From the technical point of view, such a high phase measurements mismatch is explained by a strong short-term instability of output frequencies of the FS1 and FS2 rubidium standards. This was due to large ping delay (up to 1 second and more) of the wireless Internet channel. Therefore, the required synchronization data sent by Bob was reaching Alice with a significant time-lag. During this time-lag the measuring equipment of Alice and Bob was going out of the synchronized state.

The presence of phase measurements mismatch required implementation of a key reconciliation procedure. We used the cyclic redundancy codes (CRC-16) for the K_A and K_B reconciliation. This is similar to a more secure approach based on the privacy amplification (Bennet, 1995) but easier to implement. In this case, the choice of optimal codeword length *m** for the bit extraction procedure becomes a crucial moment. Increasing the value of *m* we can extract more random bits from each single carrier phase measurement but causing a higher key mismatch rate p_e. It's a trap because high key mismatch rate may result in total rejection of the key at its reconciliation. By denoting the efficiency of key reconciliation as η the actual key generation rate R_K may be expressed by the formula (3).

$$R_K = mN\eta/(n_0 \cdot T_{OBS}). \tag{3}$$

Fig. 5 shows the dependence of achieved key generation rate calculated by the formula (3) as the function of the codeword length. Due to a high mismatch in the phase measurements of Alice and Bob the optimal codeword length takes its minimum possible value *m** = 1. All our attempts to extract more random bits from each carrier phase value led to a sharp increase in the key mismatch rate p_e and to expected decrease in the reconciliation efficiency η.

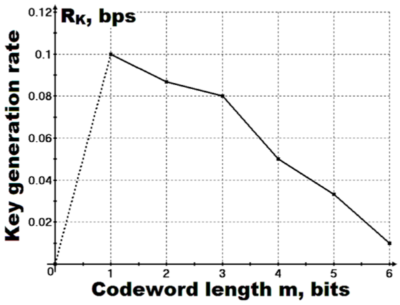

Figure 5: Key generation rate as a function of the codeword length.

We used the $\varepsilon_1 = 0.3$ allowable correlation to implement the bit extraction procedure. Given the value of decorrelation step $n_0(\varepsilon_1) = 4$, 1144 random bits have been extracted at each channel side, of which 324 bits were in a mismatch indicating the key mismatch rate p_e = 28.3%. During the key reconciliation each block of 23 key sequence bits in length has been verified with the CRC-16 code. After successful block verification we excluded 16 arbitrary bits from this block to prevent a key leakage caused by the CRC-code transmission. The achieved reconciliation efficiency was about η = 2.6%. Thus, collecting the multipath fluctuations data for 300 seconds Alice and Bob were able to extract 30-bit shared key sequence. Despite the humble key generation rate achieved in practice, our experiments prove a feasibility of the Wireless Key Distribution based on the carrier phase fluctuations in a mobile communications scenario.

6 CONCLUSIONS

Our experiments proved a feasibility of the Wireless Key Distribution based on the carrier phase method for the case of mobile communications within a real urban environment. The key generation rate about $R_K \sim 0.1$ bits per second (bps) has been achieved at satisfactory statistical properties of the generated key. Despite the humble key generation rates achieved in practice, we believe in a great potential of the method for the secure wireless key distributing between the base station and mobile subscriber in a cellular communications scenario. However, a further improvement of synchronization protocol for the legitimate users' equipment is required to achieve better system performance.

A key interception probability evaluation and its spatial decorrelation problem should be addressed in the following experiments.

REFERENCES

Bennett, C. H., Brassard, G., Crepeau, C., Maurer, U. M., 1995. Generalized privacy amplification. In *IEEE Trans. on Inf. 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 Int. Conf. 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.

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

NIST, 2010. *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*. NIST Special Publication 800-22.

Prettie, C., Cheung, D., Rusch, L., Ho, M., 2002. Spatial correlation of UWB signal in a home environment. In *Proceedings of IEEE Conference on Ultra Wideband Systems and Technologies*, pp. 65-69.

Rappaport, T., 1996. *Wireless communications: Principle & Practice*, IEEE Press, Prentice Hall, 641 p.

Rappaport, T. S., Sun, S., Mayzus, M. et al., 2013. Millimeter Wave Mobile Communications for 5G Cellular: It Will Work!. In *IEEE Access*, vol.1, pp. 335-349.

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, Proc. of 2013 IEEE Int. Siberian Conf. on Control and Communications*.

Sulimov, A. I., Sherstyukov, O. N., Karpov, A. V., Smolyakov A.D., 2013. Simulation of Encryption Key Distribution Process Based on a Multipath Radio Propagation. In *SIBCON-2013, Proc. of 2013 IEEE Int. Siberian Conf. on Control and Communications*.

Sulimov, A. I., Smolyakov, A. D., Karpov, A. V., Sherstyukov, O.N., 2014. Experimental Study of Performance and Security Constraints on Wireless Key Distribution Using Random Phase of Multipath Radio Signal. In *Proceedings of the 11th International Conference on Security and Cryptography (SECRYPT-2014)*, pp. 411-416.

Zhu, X., Xu, F., Novak, E. et al., 2013. Extracting secret key from wireless link dynamics in vehicular environments, In *Proc. of IEEE INFOCOM 2013*, pp. 2283-2291.