Communications on Applied Electronics (CAE) – ISSN : 2394-4714
Foundation of Computer Science FCS, New York, USA
Volume 7 – No. 9, November 2017 – www.caeaccess.org

Channel-based Secret Key Establishment for FDD Wireless Communication Systems

Ali M. Allam
Associated Professor
Department of Electronic,
Communication and Computer Engineering,
Faculty of Engineering, Helwan University,
PO box 11792, Cairo, Egypt

ABSTRACT
Most of current research on channel-based key generation focused on a time division duplex (TDD) system as the channel reciprocity factor applied directly to the generation of a secret key. However, most of commercial cellular systems rely on a frequency division duplex (FDD) mode. In this paper, we study the utilization of the uplink and downlink of FDD systems for the generation of common secret key between two users in the presents of inactive eavesdropper. The clue of our work is to explore the fading gain of the wireless channel between two users to generate a symmetric key. We develop the upper bound of the generation rate for shared key of the suggested mechanism and give numerical examples to show the performance of our suggested approach.

General Terms
Information theoretical security.

Keywords
Source model; Key generation; FDD system; channel reciprocity.

1. INTRODUCTION
Lately, the method of utilizing the wireless channel characteristics in establishing shared secret keys based on the reciprocal feature of wireless link has attracted more interest [1] - [9]. The characteristics of wireless channel used as a common random resource for users to generate a secret key. If the distance between the Eavesdropper and any user in the network in a few centimeters, made his observation, not correlated with the other users' channels, this is generally the condition in wireless communications [10]. Therefore, the secrecy of the generated keys is perfect with the guarantee of theoretical information due to the environment of the wireless communication scheme, unlike the cryptographic cases, which depend on security assuming the complexity of some mathematical problems [11]-[14].

Based on random and reciprocity features of fading channel, various secret key agreement approaches were suggested for wireless communication systems in TDD mode [15] -[17]. But, in the FDD situation, the using of two different channels simultaneously for transmitting and receiving leads to lose the advantage of a reciprocal feature of the channel used in key generation as in TDD case. Therefore, the characteristics of channel status information (CSI) used in [15]-[17] to create a shared key could not be used directly in FDD mode. Lately, a number of approaches have been established for FDD systems [18]-[20]. In [18], the authors suggested an approach to create a shared key using the angle and delay of the transmitted signals, which are supposed to hold the reciprocity in FDD systems. But, the characteristics used to generate a shared key, i.e. angle and delay of a path are difficult to be estimated, beside that the generated key rate resulted from their scheme is not sufficient to be used in the real world even with high transmitted power. In [19], the author suggested a pilot- based channel estimation approach in a feedback system to estimate a virtual channel gain, but the author did not calculate the rate of his suggested algorithm.

In [20], the authors applied the Chinese remainder theorem on the angle of the path used for receiving signal to create a shared key between two nodes.

In [21], a probing-based channel estimation scheme used to estimate CSI of channels between the parties and generate from its real and imaginary portions a secret shared key.

According to [22], there are five stages to extract a secret key from the physical characteristics of a wireless channel between two parties: channel probing, randomness extraction, quantization, reconciliation and privacy application. The first stage responsibility is to estimate a common randomness source used for key generation; the other phases' responsibility is to extract number of bits from the signal resulted in the first stage to be the shared secret key. Of course, each step adds an error coefficient in the key generation process.

In the present paper, we focus only on the estimation of a common randomness source between two nodes and study the upper bound of the generated key rate resulted from this scheme.

The rest of the paper is organized as follows. Section 2 describes the wireless communication system model under investigation and provides the assumption necessary for our suggested scheme. We discuss the key generation for point-to-point FDD system and derive its secret key rate in sections 3. Numerical results are presented in section 4; finally, concluding notes is given in section 5.

2. SYSTEM MODEL
Fig.1 shows the system model under consideration. We consider a FDD mode for a common wireless communication network. The authentic node Alice transmits messages to the authentic node Bob in the existence of an inactive eavesdropper Eve. We assume that, Eve recognizes how the authentic nodes communicate, and can estimate the channel characteristic associated with the other nodes. We also assume that, Eve is a passive attacker, i.e. receives only transmitted signals in the range and did not interfere the transmission between Alice and Bob.

Communications on Applied Electronics (CAE) – ISSN : 2394-4714
Foundation of Computer Science FCS, New York, USA
Volume 7 – No. 9, November 2017 – www.caeaccess.org

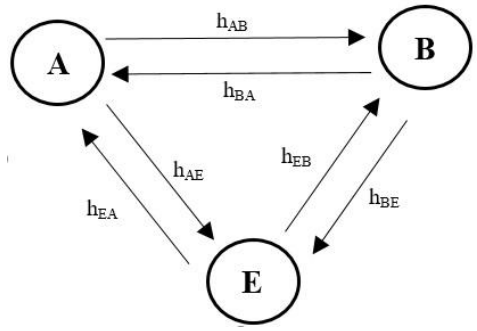

Fig.1 System Model

Alice and Bob would like to share a secret key without any information about it leakage to Eve. We assume that all the entities are full-duplex nodes.

More precisely, if Alice transmits a signal x_A over a channel, Bob and Eve will receive

$$y_B = h_{AB}x_A + n_B, \quad (1)$$
$$y_E = h_{AE}x_A + n_E, \quad (2)$$

in which h_{AB} is the channel gain of the path between Alice and Bob, n_B is a zero mean Gaussian noise with variance σ^2 at Bob, h_{AE} is the fading coefficient from Alice to Eve, and n_E is the noise at Eve. h_{AB} and n_B are both random variables and independent of each other. No channel gains in the system are known in a priori, but their distribution is known. Noise in all channels is independently and identically distributed.

Similarly, when Bob transmits x_B , Alice and Eve receive

$$y'_A = h_{BA}x_B + n_A, \quad (3)$$
$$y'_E = h_{BE}x_B + n_E, \quad (4)$$

in which h_{BA} is the channel gain of the path between Bob and Alice, n_A is a zero mean Gaussian noise with variance σ^2 at Alice, h_{BE} is the fading coefficient from Bob to Eve

In this paper, we assume that all the entities can transmit and receive simultaneously between each other, i.e., y'_A and y_B are at the same time. Also, we consider that the fading coefficient of the wireless channel remains unchangeable for a duration T, after that it changes randomly to another independent value. We assume all the channel gain distribution is a normal Gaussian distribution.

3. KEY GENERATION FOR POINT-TO-POINT FDD SYSTEM

Now, we are studying the idea of generating a shared secret key depending on physical layer features of wireless network in FDD mode. The following algorithm shows the suggested key generation scheme for point-to-point FDD communication mode.

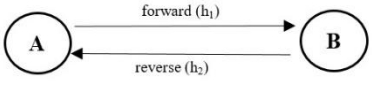

Fig. 2 Single Hop

The system model for the suggested protocol is shown in fig. 2, and the resource element of the scheme is shown in fig. 3. We split each fading period into two parts forward training allocation T_F and reverse training allocation T_R.

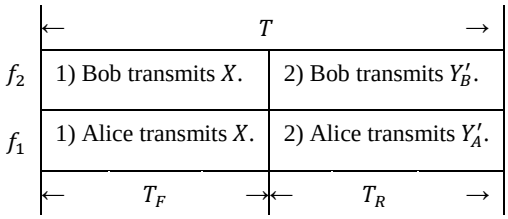

Fig. 3: Recourse Elements for single hop

Algorithm: Key Generation for Point-to-Point FDD mode.

Stage 1: Channel Estimation

1) Alice transmits an identified signal X with transmitted power P over channel h_1 using carrier frequency f_1 to Bob. Bob receives Y'_B. Simultaneously, Bob transmits a known signal X with transmitted power P over channel h_2 using carrier frequency f_2 to Alice. Alice receives Y'_A.

2) Alice transmits Y'_A with transmitted power P over channel h_1 to Bob. Bob receives Y_B from which it gets estimate $\tilde{h}_{12,B}$. Simultaneously, Bob transmits Y'_B with power P over channel h_2 to Alice. Alice receives Y_A from which it gets estimate $\tilde{h}_{12,A}$.

Stage 2: Key Agreement

Alice and Bob approve the sequence K as a shared key, using the correlated estimation pair $(\tilde{h}_{12,A}; \tilde{h}_{12,B})$.

For channels h_1 and h_2, after the forwarding channel estimation phase, Bob and Alice receive

$$Y'_B = h_1X + N_B \quad (5)$$
$$Y'_A = h_2X + N_A \quad (6)$$

simultaneously. After that both of them feedback their received signals, after the reverse channel training phase, Alice and Bob receive

$$Y_A = h_2Y'_B + N_A$$
$$= h_1h_2X + h_2N_B + N_A \quad (7)$$
$$Y_B = h_1Y'_A + N_B$$
$$= h_1h_2X + h_1N_A + N_B \quad (8)$$

simultaneously. From these observations, Alice and Bob get the following estimates

$$\tilde{h}_{12,A} = \frac{X^T}{\|X\|^2} Y_A = h_1h_2 + h_2 \frac{X^T}{\|X\|^2} N_B + \frac{X^T}{\|X\|^2} N_A \quad (9)$$

$$\tilde{h}_{12,B} = \frac{X^T}{\|X\|^2} Y_B = h_1h_2 + h_1 \frac{X^T}{\|X\|^2} N_A + \frac{X^T}{\|X\|^2} N_B \quad (10)$$

Note that, from [25], the product of two Gaussian random variables is also Gaussian. So that $\tilde{h}_{12,A}$ is a zero mean Gaussian random variable with variance $\sigma_1^2\sigma_2^2 + \frac{\sigma_2^2\sigma^2}{\|X\|^2} + \frac{\sigma^2}{\|X\|^2}$, and similarly $\tilde{h}_{12,B}$ is a zero mean Gaussian random variable with variance $\sigma_1^2\sigma_2^2 + \frac{\sigma_1^2\sigma^2}{\|X\|^2} + \frac{\sigma^2}{\|X\|^2}$.

Assuming that Alice and Bob transmit signals with transmitted power P during the channel estimation phase, we have $\|X\|^2 = T_FP$ and $\|Y'_A\|^2 = \|Y'_B\|^2 = T_RP$.

Based on the lemma of data processing in [23], it is easy to observe, the validation of the following Markovian relationship [1]:

$$\tilde{h}_{12,A} \leftrightarrow Y_A \leftrightarrow h_1 h_2 \leftrightarrow Y_B \leftrightarrow \tilde{h}_{12,B}$$

which implies $I(\tilde{h}_{12,A}; \tilde{h}_{12,B}) \leq I(Y_A; Y_B)$.

Similarly, from the Markovian relationship

$$Y_A \leftrightarrow \tilde{h}_{12,A} \leftrightarrow h_1 h_2 \leftrightarrow \tilde{h}_{12,B} \leftrightarrow Y_B$$

we have $I(\tilde{h}_{12,A}; \tilde{h}_{12,B}) \geq I(Y_A; Y_B)$.

As the result of lemma 3.1 in [1], $I(\tilde{h}_{12,A}; \tilde{h}_{12,B}) = I(Y_A; Y_B)$, which indicates that $\tilde{h}_{12,A}$ and $\tilde{h}_{12,B}$ maintain the mutual information between Y_A and Y_B; which can be used to compute the rate of a generated secret key between Alice and Bob.

From $(\tilde{h}_{12,A}, \tilde{h}_{12,B})$, one can evaluate the secret key rate from [24], as following

$$R_S = \frac{1}{T} I(\tilde{h}_{12,A}; \tilde{h}_{12,B}) \quad (11)$$

$$R_S = \frac{1}{2T} log\left(1 + \frac{(\sigma_1^2 \sigma_2^2 P T_F)^2}{\sigma_1^4 \sigma_2^2 P T_F \sigma^2 + \sigma_1^2 \sigma_2^4 P T_F \sigma^2 + \sigma_1^2 \sigma_2^2 \sigma^4 + \sigma_2^2 P T_R \sigma^2 + \sigma_1^2 P T_R \sigma^2 + \sigma^4}\right) \quad (12)$$

one can conclude rate of generated key is constrained by factor $\frac{1}{T}$, this is due to the changing of channel characteristics every T sequences times, i.e., the path gain between parties remain consists only for a block of T sequences times.

To show the effect of the main variables and coefficients in (12) on the derived rate, we assume that the coherence time T is equally divided over the forward and reverse training sequences T_F and T_R, respectively, and the channel gains variance of the two paths is same, i.e., $\sigma_1^2 = \sigma_2^2 = \sigma_L^2$.

So,

$$R_S = \frac{1}{2T} log\left(1 + \frac{\left((\sigma_L^2)^2 P \frac{T}{2}\right)^2}{((\sigma_L^2)^3 + \sigma_L^2) PT\sigma^2 + (1 + (\sigma_L^2)^2)(\sigma^2)^2}\right) \quad (13)$$

From (13), we conclude that the secret key rate is a function of the transmitted power P and the coherence period T. The secret key rate is directly proportional to the transmitted power P, i.e. as the transmitted power P increases, the secret key rate increases at an order of $\frac{1}{2T} logP$. Conversely, as the fading, changes slowly, i.e. as T increases, the key rate decreases at an order of $\frac{1}{2T} logT$, which tends to zero. Also, there is two coefficients channel gain variance σ_L^2 and noise variance σ^2.

4. NUMERICAL RESULTS

In this section, we show the effect of the variables and the coefficients in (13) on the rate through a numerical illustration.

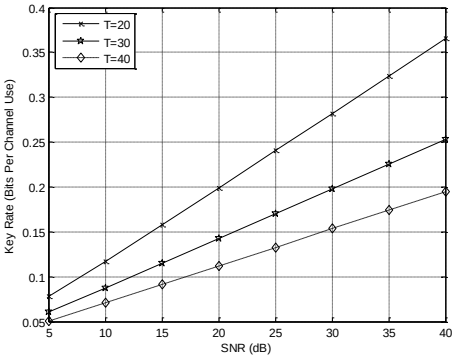

Fig. 4. Comparison of key rates for different coherence periods

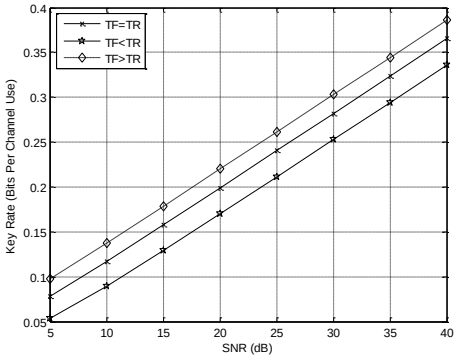

Fig. 5. Comparison of key rates for different channel training allocation.

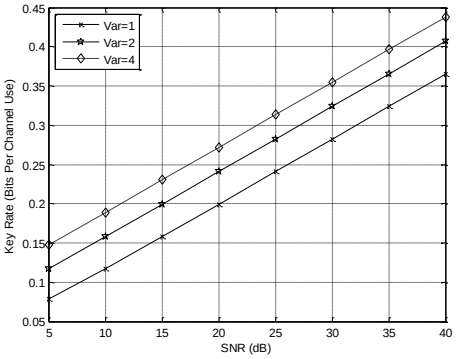

Fig. 6. Comparison of key rates for different channel gain variances.

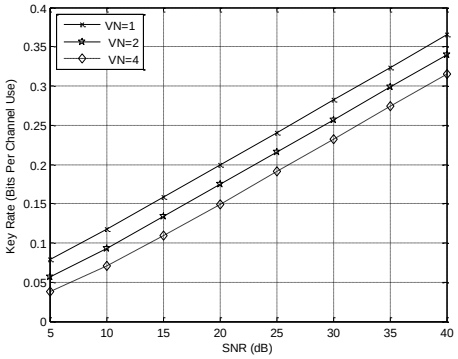

Fig. 7. Comparison of key rates for different noise variances.

All the figures show the rate of the generated secret key (key rate) in bits per channel use in the vertical coordinate vs the signal-to-noise ratio (SNR) in dB in the horizontal coordinate, corresponding to different values of the variables and the coefficients.

In figure 4, we examine the effect of coherence pariod on the rate with three different values. We assume the entire channel gains variances and noise variances to be 1. The figure shows that the increase in the coherence pariod decrease the generation rate of the secret key per channel use, for that we suggest to use this technique in the slow fading scenario.

In figure 5, we examine the effect of the time allocation for the training process for the forward channel and the reverse channel on the rate with three different distributions. We assume the entire channel gains variances and noise variances to be 1. The figure shows that as the time allocation for forward channel training increase with respect to the part allocated for reverse channel training, the generation rate of the secret key per channel use increase. This result drive us for improving the rate of our suggested technique, and utilize it for a future work.

In figure 6, we examine the effect of the channel gain variances of reverse and forward paths on the rate with three different values. We assume the entire channel gains variances are equal and the noise variances are equal to 1. The figure shows that as we increase the channel gain for the paths, the rate increase. This result is because the increase in the channel gain increases the randomness of the common observation between the nodes, which use as the source for the key generation.

In figure 7, we examine the effect of the noise variances on the rate with three different values. We assume the entire channel gains variances are equal to 1. The figure shows that as the noise variance increase, the key rate per channel use decrease. This is due to the effect of the noise on the common observation of the users, which leads to decrease the signal to noise ratio of the common observation, which decrease the number of bits shared by two nodes.

5. CONCLUSION

We have suggested a new mechanism to establish a shared secret key for point-to-point communication in FDD systems. In the suggested scheme, we explore the common observation between nodes as a randomness source for a secret key generation between them. We derive the key generation rate for our suggested scheme and the numerical simulation showed that, we can improve the rate by increasing the training allocation for the forward channel with respect to the time allocation for the reverse channel for every coherence period.

6. REFERENCES

[1] L. Lai, Y. Liang, and H. V. Poor, "A unified framework for key agreement over wireless fading channels," *IEEE Trans. Inf. Forens. Security*, vol. 7, pp. 480–490, Apr. 2012.

[2] L. Lai, Y. Liang, and H. V. Poor, "Key agreement over wireless fading channels with an active attacker," in *Proc. Allerton Conf. on Communication, Control, and Computing*, (Monticello, IL), Sept. 2010.

[3] R. Wilson, D. Tse, and R. A. Scholtz, "Channel identification: Secret sharing using reciprocity in ultra-wide band channels," *IEEE Trans. Inf. Forens. Security*, vol. 2, pp. 364–375, Sept. 2007.

[4] T.H. Chou, A. M. Sayeed, and S. C. Draper, "Minimum energy per bit for secret key acquisition over multipath wireless channels," in *Proc. IEEE Intl. Symposium on Inform. Theory*, (Seoul, Korea), Jun. 2009.

[5] T.H. Chou, A. M. Sayeed, and S. C. Draper, "Impact of channel sparsity and correlated eavesdropping on secret key generation from multipath channel randomness," in *Proc. IEEE Intl. Symposium on Inform. Theory*, (Austin, TX), Jun. 2010.

[6] A. Sayeed and A. Perrig, "Secure wireless communications: Secret keys through multipath," in *Proc. IEEE Intl. Conf. on Acoustics, Speech, and Signal Processing*, (Las Vegas, NV), Apr. 2008.

[7] C. Ye, S. Mathur, A. Reznik, W. Trappe, and N. Mandayam, "Information-theoretic key generation from wireless channels," *IEEE Trans. Inf. Forens. Security*, vol. 5, pp. 240–254, Jun. 2010.

[8] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radiotelephathy: Extracting a secret key from an unauthenticated wireless channel," in *Proc. ACM International Conference on Mobile Computing and Networking*, (San Francisco, CA), 2008.

[9] K. Zeng, D. Wu, A. Chan, and P. Mohapatra, "Exploiting multipleantenna diversity for shared key generation in wireless networks," in *Proc. IEEE Conf. Computer Communications (Infocom)*, (San Diego, CA), Mar. 2010.

[10] D. Tse and P. Viswanath, "*Fundamentals of Wireless Communication*," Cambridge, UK: Cambridge University Press, May 2005.

[11] Ali M. Allam, Ihab A. Ali and Shereen M. Mahgoub , "A provably secure certificateless organizational signature schemes", International Journal Of Communication Systems, vol. 30, no. 5, March 2017.

[12] Kai Chain, Kuei-Hu Chang, Wen-Chung Kuo and Jar-Ferr Yang , "Enhancement authentication protocol using zero-knowledge proofs and chaotic maps", International Journal of Communication Systems, vol. 30, no.1, January 2017.

[13] Dheerendra Mishra, Saru Kumari, Muhammad Khurram Khan and Sourav Mukhopadhyay , "An anonymous biometric-based remote user-authenticated key agreement scheme for multimedia systems", International Journal of Communication Systems, vol. 30, no. 1, January 2017.

[14] Han-Yu Lin , "Efficient mobile dynamic ID authentication and key agreement scheme without trusted servers", International Journal Of Communication Systems, vol. 30, no. 1, January 2017.

[15] Chunxuan Ye; Reznik, A.; Shah, Y.," Extracting Secrecy from Jointly Gaussian Random Variables," *Information Theory, 2006 IEEE International Symposium on* , vol., no., pp.2593,2597, 9-14 July 2006.

[16] Patwari, N.; Croft, J.; Jana, S.; Kasera, S.K., "High-Rate Uncorrelated Bit Extraction for Shared Secret Key Generation from Channel Measurements," *Mobile Computing, IEEE Transactions on* , vol.9, no.1, pp.17-30, Jan. 2010

[17] S. Mathur, W. Trappe, N. Mandayam, C. Ye, A. Reznik, "Radiotelepathy: Extracting a secret key from an unauthenticated wireless channel," *Proc. ACM Conf. Mobile Comput. Network.*, Sept. 2008.

[18] Wang W J, Jiang H Y, Xia X G, et al. "A wireless secret key generation method based on Chinese remainder theorem in FDD systems," Sci China Inf Sci, 2012.

[19] Goldberg S J, Shah Y C, Reznik A., "Method And Apparatus For Performing JRNSO In FDD," TDD AND MIMO COMMUNICATIONS, U.S. Patent Application 12/106,926[P]. 2008-4-21.

[20] W. Wang, H. Jiang, X. Xia, P. Mu, Q. Yin, "A wireless secret key generation method based on chinese remainder theorem in FDD systems", *Science China Information Sciences*, vol. 55, no. 7, pp. 1605-1616, 2012.

[21] X. Wu, Y. Peng, C. Hu, H. Zhao, L. Shu, "A secret key generation method based on CSI in OFDM-FDD system", *Proc. IEEE Globecom Workshops*, pp. 1297-1302, Dec. 2013.

[22] J. Zhang, T. Q. Duong, A. Marshall, and R. Woods, "Key generation from wireless channels: A review," IEEE Access, vol. 4, pp. 614–626, Mar. 2016

[23] T. M. Cover and J. A. Thomas, "*Elements of Information Theory*," New York: Wiley, 1991.

[24] R. Ahlswede and I. Csisz´ar, "Common randomness in informationtheory and cryptography, Part I: Secret sharing," *IEEE Trans. Inf. Theory*, vol. 39, pp. 1121–1132, July 1993.

[25] P. Bromiley, "Products and convolutions of Gaussian distributions," Medical School, Univ. Manchester, Manchester, UK, Tech. Rep, vol. 3, p. 2003, 2003.

[26] Lai, Lifeng, Yingbin Liang, and Wenliang Du, "Cooperative key Generation in wireless Networks", IEEE Journal on Selected Areas in Communications, 2012.

[27] J.-K. Hwang, J. H. Winters, "Sinusoidal Modeling and Prediction of Fast Fading Processes", *IEEE Global Telecommunications Conference (GLOBECOM '98)*, vol. 2, pp. 892-897, 1998.

[28] J. B. Andersen, J. Jensen, S. H. Jensen, F. Frederiksen, "Prediction of Future Fading Based on Past Measurements", *IEEE Vehicular Technology Conference (VTC fall '99)*, vol. 1, pp. 151-155, 1999.

[29] T. Eyceoz, A. Duel-Hallen, H. Hallen, "Deterministic Channel Modeling and Long Range Prediction of Fast Fading Mobile Radio Channels", *IEEE Communications Letters*, vol. 2, no. 9, pp. 254-256, 1998.

[30] S. Semmelrodt, R. Kattenbach, "A 2-D Fading Forecast of Time-Variant Channels Based on Parametric Modeling Techniques", *Proc. of the 13th IEEE International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC '02)*, pp. 1640-1644, 2002.

[31] H. Hafez, Y.A. Fahmy and M.M. Khairy, "LTE and WiMAX: performance and complexity comparison for possible channel estimation techniques", International Journal of Communication Systems, vol. 26, no. 6, pp. 792–805, June 2013.