Key Generation Based on Large Scale Fading

Junqing Zhang, Ming Ding, *Senior Member, IEEE,* Guyue Li, and Alan Marshall, *Senior Member, IEEE*

***Abstract*—This paper investigates key generation performance in environments with large scale fading including path loss and shadow fading. The path loss is found to be affected only by the distance between users and not secure for key generation. The shadow fading effect is caused by large obstacles such as buildings. The correlation relationships of the shadow fading are modelled and demonstrated to meet the requirements of key generation principles. Monte Carlo Simulations have been carried out and validated that shadow fading-based key generation is feasible and secure.**

***Index Terms*—Physical layer security, key generation, large scale fading, path loss, shadow fading**

I. Introduction

Key generation from wireless channels has become an emerging technique to establish cryptographic keys between legitimate users [1]. Wireless channels can be modelled with large scale fading and small scale fading [2]. Large scale fading occurs when mobile users move across a large distance and the signal is affected by path loss and shadow fading due to large obstacles such as buildings. On the other hand, small scale fading represents the constructive and destructive aggregation of multiple signal components due to reflection, refraction, and scattering in wave propagation.

The small scale fading is affected by the environment layout, scatterers' material and distributions, etc. These factors have been exploited by key generation prototyped with Wi-Fi [3], [4], and ZigBee [5]. All the experiments are conducted with limited communication ranges, e.g., less than 100 m. However, multipath leads to highly dynamic changes in channel phases, which is very sensitive to the carrier frequency and poses great challenges for key generation in frequency division duplex (FDD) systems [6]. In addition, the correlation of channel measurements is impacted by fast time-variant small scale fading, which limits its application in vehicular networks [4].

In addition to the above short range communication scenarios, many IoT applications will operate in a much longer range in the order of kilometers. This can be achieved by employing cellular networks such as LTE or low-power wide-area network (LPWAN) techniques, e.g., LoRa and NB-IoT, which are currently attracting much attention from both academia and industry. The wireless communications in such wide areas will suffer greatly from the large scale fading. There have been some practical explorations of applying key generation using LoRa [7], [8]. A disc model is proposed to analyze the effect of eavesdroppers' location, where scatterers are uniformly distributed within the disc [9], [10]. However, key generation principles, namely temporal variation, channel reciprocity, and spatial decorrelation, under large scale fading have not yet been properly modelled and studied.

This paper investigates key generation feasibility and performance when it is applied to large scale fading, e.g., vehicular networks where small scale fading is averaged out. We find that the path loss itself only depends on the distance and cannot offer sufficient randomness. Fortunately, shadow fading is correlated and affected by large obstacles such as buildings. In vehicle-to-vehicle (V2V) communications, it is experimentally observed that moving vehicles will cause shadow fading as well [11], which is different from small-scale fading. Based on the comprehensive analysis on the shadow fading correlation relationships, we show that shadow fading-based key generation is feasible and secure and further validate it via Monte Carlo simulation. The numerical results demonstrate that legitimate users are able to generate keys securely from shadow fading during the simulated period, and an eavesdropper does not have a better correlated observation on shadow fading than the legitimate users.

II. System Model

The system model is shown in Fig. 1, with two legitimate users, Alice and Bob, and one passive eavesdropper, Eve. Trusted/untrusted relays and multiple eavesdroppers are not considered. Interested readers please refer to [12], [13] and [14] for more information. A two-dimensional Cartesian coordinate system is adopted. Without loss of generality, Alice and Eve are configured stationary, located at $(0, 0)$ and $(0, y_E)$ with $y_E > 0$, respectively. This is a reasonable assumption as Alice can be a base station/gateway, which will usually be fixed. At time t, Alice transmits a downlink packet to Bob, who is located at (x_B, y_B). At time $t + \tau$, Bob moves to a new position (x'_B, y'_B) and replies an uplink packet to Alice. They will repeat the above transmissions until they get sufficient channel measurements for key generation. Eve will not inject any packets into the channel but quietly record all the transmissions.

The effect of the small scale fading can be averaged out by means of filtering at the receivers, therefore, the received signal power is mainly affected by the large scale fading, including path loss and shadow fading. Path loss describes the power decay due to the transmission distance and shadow fading represents the power absorption by large obstacles [2]. By considering the popular log-normal shadow fading model

Manuscript received xxx xx, 2018; revised xxx xx, 2018; accepted xxx xx, 2018. Date of publication xxx xx, 2018; date of current version xxx xx 2018. The associate editor coordinating the review of this paper and approving it for publication was xxx xxx.

J. Zhang and A. Marshall are with the Department of Electrical Engineering and Electronics, University of Liverpool, Liverpool, L69 3GJ, United Kingdom. (email: junqing.zhang@liverpool.ac.uk; alan.marshall@liverpool.ac.uk)

M. Ding is with Data61, CSIRO, Australia (e-mail: Ming.Ding@data61.csiro.au)

G. Li is with the School of Cyber Science and Engineering, Southeast University, Nanjing, China. (e-mail: guyuelee@seu.edu.cn.)

Digital Object Identifier xxx

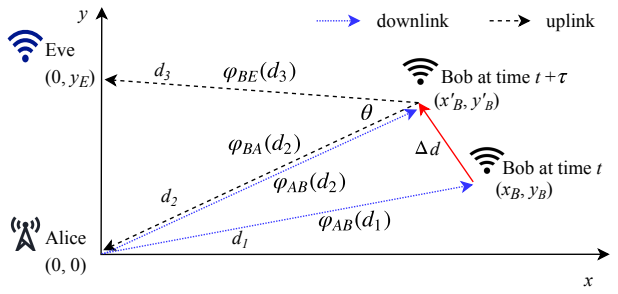


Fig. 1. A key generation system with two legitimate users, Alice and Bob, and one eavesdroppers, Eve.

and empirical path loss models such as Hata model, the received power, P_r, in dB, can be written as

$$P_r = P_t - K_1 - 10\alpha \log_{10}(d) - K_2 \log_{10}(f_c) + \varphi, \quad (1)$$

where P_t is the transmission power in dB, K_1 and K_2 are constants determined by the environments, α is the path loss exponent, d is the distance between transmitter u and receiver v, f_c is the carrier frequency, and φ is the shadow fading effect which follows a normal distribution, i.e., $\varphi \sim \mathcal{N}(0, \sigma_\varphi^2)$. We assume all the links have the same standard deviation, σ_φ, ranging from 6 to 12 dB [15].

Key generation extracts the randomness from a dynamic channel, hence the constant components in (1) do not contribute. In particular, although the carrier frequencies of uplink and downlink are not the same in FDD systems, they are always fixed. We therefore analyze the variable components of (1), namely $P_r^{\text{PL}} = \log_{10}(d)$ and $P_r^{\text{SF}} = \varphi$.

III. Path Loss

During the uplink transmission (from Bob to Alice), the components of the path loss at Alice and Eve can be given by

$$P_{r,BA}^{\text{PL}} = \log_{10}(d_2) = \frac{1}{2}\log_{10}\left(x_B^2 + y_B^2\right), \quad (2)$$

$$P_{r,BE}^{\text{PL}} = \log_{10}(d_3) = \frac{1}{2}\log_{10}\left(x_B^2 + (y_B - y_E)^2\right), \quad (3)$$

respectively. The subscript $()_{uv}$ represents a link from a transmitter u to a receiver v. Because Eve is fixed, the variations of $P_{r,BA}^{\text{PL}}$ and $P_{r,BE}^{\text{PL}}$ are only caused by the movement of Bob. It is not secure for key generation, as will be analyzed below.

The partial derivative of $P_{r,BA}^{\text{PL}}$ and $P_{r,BE}^{\text{PL}}$ with respect to x_B can be written as

$$\frac{\partial P_{r,BA}^{\text{PL}}}{\partial x_B} = \frac{x_B}{x_B^2 + y_B^2}, \quad (4)$$

$$\frac{\partial P_{r,BE}^{\text{PL}}}{\partial x_B} = \frac{x_B}{x_B^2 + (y_B - y_E)^2}, \quad (5)$$

respectively. Note that both (4) and (5) will always have the same monotonicity, determined by x_B. Accordingly, their partial derivation with respect to y_B can be given by

$$\frac{\partial P_{r,BA}^{\text{PL}}}{\partial y_B} = \frac{y_B}{x_B^2 + y_B^2}, \quad (6)$$

$$\frac{\partial P_{r,BE}^{\text{PL}}}{\partial y_B} = \frac{y_B - y_E}{x_B^2 + (y_B - y_E)^2}, \quad (7)$$

respectively. When $y_B > y_E$ or $y_B < 0$, they have the same monotonicity; otherwise, they have the opposite monotonicity.

From the above analysis, we can conclude that the path loss effect is deterministic and cannot be used for key generation. The user location is the only variable in a free space communication or an environment with strong line-of-sight, e.g., the unmanned aerial vehicle (UAV) air-to-air channel. The eavesdropper can use other techniques, e.g., radar or ultrasonic, to localize the legitimate users, which will compromise the key generation process.

IV. Shadow Fading

Shadow fading is affected by large obstacles, whose location and distribution are difficult to predict and replicate, especially in dense urban environments. It is usually due to electromagnetic waves attenuated by obstacles, which is affected by the size, shape, depth, material type, surface smoothness, relative positions of such obstacles as well as the angles of incidence/refraction [2]. According to empirical measurements [2], [11], when eavesdroppers are located a certain distance away, e.g., 20 meters, they get uncorrelated channel observation. Shadow fading information is thus secure in this sense.

Key generation relies on temporal variation, channel reciprocity, and spatial decorrelation [1], which can be quantified by autocorrelation, cross correlation between legitimate measurements, and cross correlation between legitimate and eavesdropping observations, respectively. And the cross correlation is defined as

$$\rho(s_1, s_2) = \frac{\mathbb{E}\{s_1(t)s_2(t)\} - \mathbb{E}\{s_1(t)\}\mathbb{E}\{s_2(t)\}}{\sigma_{s_1}\sigma_{s_2}}, \quad (8)$$

where $\mathbb{E}\{\cdot\}$ denotes the expectation operation, s_1 and s_2 are random variables. When $s_2(t) = s_1(t+\tau)$, it becomes the autocorrelation.

A comprehensive feasibility analysis on the correlation modelling of shadow fading can be found in [16]. This section will first analyze these correlation relationships and then derive the secret key capacity.

A. Correlation Relationship

1) Temporal Variation - Autocorrelation: The autocorrelation of the shadow fading describes the correlation relationship between the shadowing effects of the same link at two time. The sample delay τ leads to a movement of Bob, Δd, and the shadowing effects are $\varphi_{AB}(d_1)$ and $\varphi_{AB}(d_2)$ in Fig. 1. The authors in [17], [18] describe the autocorrelation function as an exponential one, which can be written as

$$r(\Delta d) = \exp\left(-\frac{\Delta d}{d_c}\ln 2\right), \quad (9)$$

where d_c is the decorrelation distance, which is dependent on the environment, e.g., a decorrelation distance of 20 meters is applied in the vehicular environment [19]. The model is validated by many empirical measurements with sufficient accuracy [11], [20] and also adopted in this paper.

2) Channel Reciprocity - Correlation Between Uplink and Downlink: Channel reciprocity indicates that the uplink and downlink with the same transmission path and carrier frequency will have identical features at both ends. In a TDD system the channel reciprocity is affected by the sampling delay between uplink and downlink in a mobile scenario [21]. The cross correlation in this case is the same as the autocorrelation coefficient, $r(\Delta d)$. On the other hand, the channel reciprocity in a FDD system is affected by the different carrier frequencies separated by Δf, and their shadow fading effects of uplink and downlink are assumed to be correlated with a coefficient $R(\Delta f)$ [22]. In summary, the correlation coefficient between uplink and downlink can be given as

$$\rho(\varphi_{AB}, \varphi_{BA}) = \begin{cases} r(\Delta d), & \text{TDD systems;} \\ R(\Delta f), & \text{FDD systems.} \end{cases} \tag{10}$$

A high cross correlation between the shadow fading of uplink and that of downlink has been found by measurements [23].

3) Spatial Decorrelation - Correlated Eavesdropping Channel: Spatial decorrelation describes the correlation relationship between the legitimate and eavesdropping channels, namely $\varphi_{BA}(d_2)$ and $\varphi_{BE}(d_3)$ in Fig. 1. According to the modelling based on the empirical measurements, it usually takes a new approach from the autocorrelation modeling [16].

In this regard, model "0.8/0.4 RX" is a popular model, which takes angle-of-arrival difference, θ, and distance into consideration [24]. In more detail, such model is defined as

$$\rho(\varphi_{BA}, \varphi_{BE}) = \begin{cases} f(X,\kappa)(0.6 - \frac{|\theta|}{150}) + 0.4, & \text{if } |\theta| \leq 60^\circ, \\ 0.4, & \text{if } |\theta| > 60^\circ, \end{cases} \tag{11}$$

where

$$f(X,\kappa) = \begin{cases} 1 - \kappa/X, & \text{if } \kappa \leq X, \\ 0, & \text{if } \kappa > X, \end{cases} \tag{12}$$

where X ranges from 6 to 20 dB, and $\kappa = |10\log_{10}(\frac{d_2}{d_3})|$. Intuitively, the larger θ and κ, the lower the cross correlation.

B. Secret Key Capacity

As we mentioned in Section II, $P^{\text{SF}}_{r,uv} = \varphi_{uv}$. Therefore, we can extract the randomness residing in the shadow fading effect from measuring the received power. Because φ_{uv} follows a Gaussian distribution, $P^{\text{SF}}_{r,BA}$, $P^{\text{SF}}_{r,AB}$, and $P^{\text{SF}}_{r,BE}$ will also follow Gaussian distributions. Their mutual information can be calculated as [25]

$$I(P^{\text{SF}}_{r,uv}, P^{\text{SF}}_{r,u'v'}) = -\frac{1}{2}\log_2\Big(1 - \rho(P^{\text{SF}}_{r,uv}, P^{\text{SF}}_{r,u'v'})\Big). \tag{13}$$

Because Alice and Eve are fixed, $P^{\text{SF}}_{r,AE}$ will remain constant, which does not include any randomness. When Bob moves around, $\rho(\varphi_{BA}, \varphi_{BE})$ will vary its value. We take the maximum value, $\rho^{\max}(\varphi_{BA}, \varphi_{BE})$, as the worst case. The secret key capacity, defined per channel realization, can then be given by

$$\begin{aligned} C^{\min}_{sk} &= I(P^{\text{SF}}_{r,BA}, P^{\text{SF}}_{r,AB}) - I^{\max}(P^{\text{SF}}_{r,BA}, P^{\text{SF}}_{r,BE}) \\ &= -\frac{1}{2}\log_2\Big(\frac{1 - \rho(\varphi_{AB}, \varphi_{BA})}{1 - \rho^{\max}(\varphi_{BA}, \varphi_{BE})}\Big). \end{aligned} \tag{14}$$

When $\rho(\varphi_{AB}, \varphi_{BA}) > \rho^{\max}(\varphi_{BA}, \varphi_{BE})$, the $C^{\min}_{sk}$ will always be larger than 0. In this case, we will be able to generate keys securely from the correlated shadow fading.

In order to collect random key sequences, legitimate users can either use an optimal sampling interval [21] or employ decorrelation methods such as principal component analysis [26] to obtain the uncorrelated measurements.

V. Simulation Evaluation and Discussion

Unless otherwise specified, the following simulation setup was used in this section. Alice and Eve were located at the origin and (x_E, y_E) = (0, 100m), respectively. Bob was originally located at (x_B, y_B) = (10m, 60m) and moved randomly with a speed of v km/h.

A. Path Loss

We carried out two simulations to analyze the effect of increasing x_B (y_B) on the received power and the results are shown in Fig. 2(a). The monotonicities of the received powers are deterministic, which validates our analysis in the Section III. We conducted another simulation by randomly changing the values of x_B and y_B, each with a step of 0.5 meters. The results are shown in Fig. 2(b), showing $\rho(P^{\text{PL}}_{r,BA}, P^{\text{PL}}_{r,BE}) = 0.8628$. In most of the cases, especially after the sample index of 200, Eve can get a highly correlated observation of the channel that will compromise the security performance.

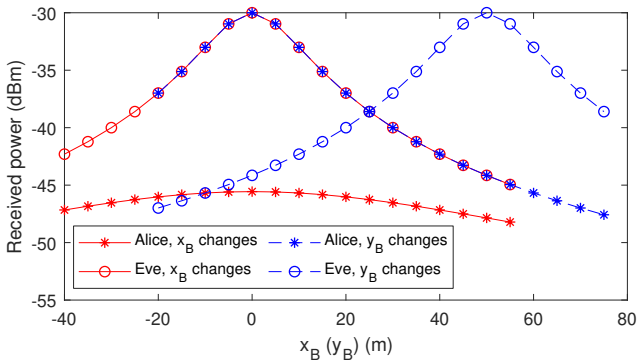
B. Shadow Fading

We analyze the correlation between uplink and downlink by taking TDD LTE as an example. The delay for transmitting ACK/NACK ranges from 4 subframes to 7 subframes for the downlink hybrid automatic repeat request (HARQ) and from 4 subframes to 13 subframes for the uplink HARQ [27]. Each subframe lasts 1 ms, and hence $\tau^{\min}$ = 4 ms and $\tau^{\max}$ = 13 ms. When $v = 60$ km/h, a typical vehicle moving speed, the distance is $\Delta d^{\min} = \tau * v$ = 0.067 m and $\Delta d^{\max} = 0.217$ m. The Δd thus ranges from 0.067 m to 0.247 m in the simulation.

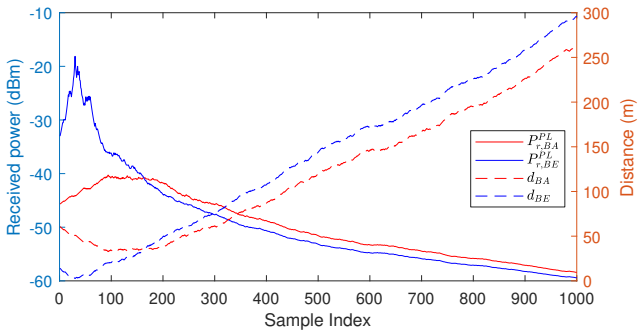
The variation of the mutual information and autocorrelation coefficient against Δd in a TDD LTE system is investigated by fixing $y_E = 100$ and the results are shown in Fig. 3. Besides calculating $I(P^{\text{SF}}_{r,AB}, P^{\text{SF}}_{r,BA})$ using (13), we also numerically calculated the mutual information by employing a k-nearest neighbor (knn) distances-based method [28]. The results match each other very well. We also calculated the $I(P^{\text{SF}}_{r,BA}, P^{\text{SF}}_{r,BE})$ using the knn-based method, and $I(P^{\text{SF}}_{r,AB}, P^{\text{SF}}_{r,BA}) > I(P^{\text{SF}}_{r,BA}, P^{\varphi}_{r,BE})$ always holds in these cases, which indicates key generation can be carried out successfully, because the incurred distance Δd is very small.

Similarly, we studied the effect of the eavesdropper location on the mutual information by fixing $\Delta d = 0.067$ m but varying y_E. As shown in Fig. 4, even when y_E is as small as 1, i.e., the eavesdropper is only one meter away from Alice, $I(P^{\text{SF}}_{r,AB}, P^{\text{SF}}_{r,BA})$ is still larger than $I(P^{\text{SF}}_{r,BA}, P^{\text{SF}}_{r,BE})$. This ensures Alice and Bob can generate keys securely.

The secure key generation can be achieved when $\rho(\varphi_{AB}, \varphi_{BA}) > \rho(\varphi_{BA}, \varphi_{BE})$, which will be determined



(a)



(b)

Fig. 2. Received power affected by the location of Bob. The initial coordinates of the users were $(x_A, y_A) = (0, 0)$, $(x_B, y_B) = (10, 60)$, and $(x_E, y_E) = (0, 50)$. (a) Bob was moving towards x-axis or y-axis. $x_B = [-40 : 5 : 55]$, $y_B = 60$ and $x_B = 10$, $y_B = [-20 : 5 : 70]$; (b) Bob was moving randomly, both in x-axis and y-axis, with a step of 0.5 meter.

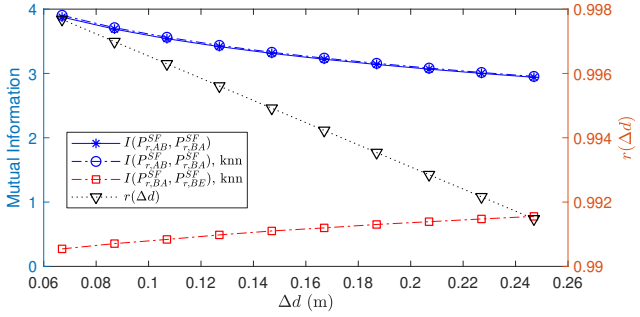


Fig. 3. Mutual information and autocorrelation against Δd. $(x_E, y_E) = (0, 100)$ m, $d_c = 20$ m.

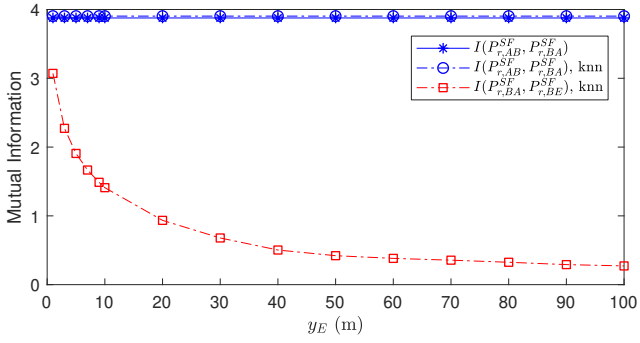
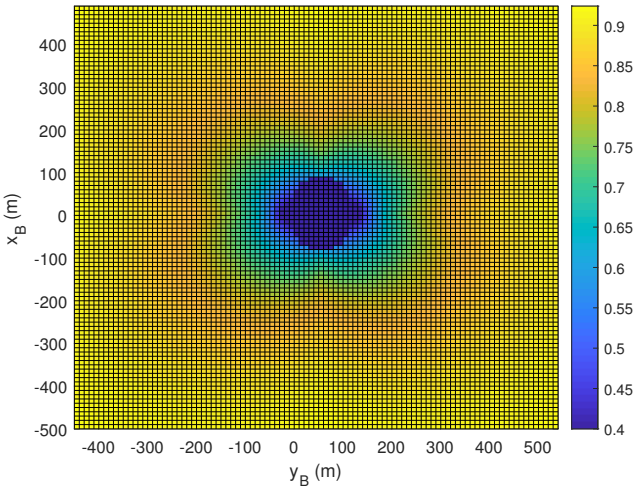
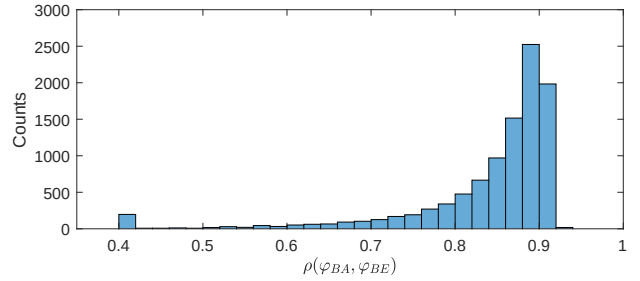


Fig. 4. Mutual information against y_E. $x_E = 0$, $\Delta d = 0.067$ m, $d_c = 20$ m.



(a)



(b)

Fig. 5. $\rho(\varphi_{BA}, \varphi_{BE})$ when Bob moves. $X = 6$ dB, $(x_E, y_E) = (0, 100)$. (a) The distribution of $\rho(\varphi_{BA}, \varphi_{BE})$ versus (x_B, y_B); (b) The statistical distribution of $\rho(\varphi_{BA}, \varphi_{BE})$.

by the relative locations of Alice, Bob, and Eve, and also the movement of Bob. A site survey of the cross correlation between φ_{BA} and φ_{BE}, i.e., $\rho(\varphi_{BA}, \varphi_{BE})$ when Bob moves, can be carried out by simulation to reveal the statistical distribution of $\rho(\varphi_{BA}, \varphi_{BE})$, and an example is exemplified in Fig. 5. The site survey may not be practical in real scenarios because Eve will usually hide its presence and location. However, as observed in Fig. 3 and Fig. 4, a site survey is not a prerequisite because $I(P^{\text{SF}}_{r,AB}, P^{\text{SF}}_{r,BA})$ is always larger than $I(P^{\text{SF}}_{r,BA}, P^{\text{SF}}_{r,BE})$ in the simulated period. As shown in Fig. 5(a), when Bob moves further from Alice, $\rho(\varphi_{BA}, \varphi_{BE})$ becomes higher, because both θ and κ approach to zero. Therefore, Bob will only carry out key generation when it is in the proximity of Alice.

Regarding FDD systems, their correlation relationship is affected by different carrier frequencies. As shown in (10), $R(\Delta f)$ and $r(\Delta d)$ have similar effects on the $\rho(\varphi_{AB}, \varphi_{BA})$, therefore, the simulation under the FDD system is omitted for simplicity.

VI. Discussion

Consider a typical vehicular communication context with a vehicle moving at a speed of $v = 60$ km/h and a TDD LTE mode with carrier frequency $f_c = 2$ GHz. The coherence time

of the small scale fading will be in the order of

$$T_c \propto \frac{1}{f_m} = \frac{c}{v}\frac{1}{f_c} = 9 \text{ ms}, \quad (15)$$

where c is the speed of light. Compared to the minimum sampling delay, $\tau^{\min} = 4$ ms, the small scale fading is varying relatively fast; it is thus challenging to obtain correlated channel measurements and apply key generation in such a dynamic scenario [4]. Shadow fading has a large decorrelation distance, e.g., 20 meters as specified in [19]. When leveraging the data and ACK frames in TDD LTE systems for key generation, the maximum movement $\Delta d^{\max}$ is 0.217 m, which is much shorter than the decorrelation distance. A high cross correlation between the shadowing fading can thus be obtained.

On the other hand, shadow fading changes much slower than small-scale fading, which results in less randomness and hence a slower key generation rate. In addition, shadow fading is coupled with small-scale fading, so additional signal processing such as filtering is required.

VII. Conclusion

This paper investigated key generation based on the large scale fading, including path loss and shadow fading. We found that path loss cannot be used for key generation, because it is deterministic with respect to the distance. On the other hand, shadow fading is affected by large obstacles such as buildings, and exhibits a good autocorrelation property. We modelled the correlation relationship of the shadow fading among legitimate users and the eavesdropper. We demonstrate by simulation that legitimate users can carry out key generation securely in the simulated period. Our future work will experimentally validate the feasibility of key generation considering correlated shadow fading.

References

[1] 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.

[2] A. Goldsmith, *Wireless Communications*. Cambridge University Press, 2005.

[3] O. Gungor, F. Chen, and C. Koksal, "Secret key generation via localization and mobility," *IEEE Trans. Veh. Technol.*, vol. 64, no. 6, pp. 2214–2230, Jun. 2015.

[4] X. Zhu, F. Xu, E. Novak, C. C. Tan, Q. Li, and G. Chen, "Using wireless link dynamics to extract a secret key in vehicular scenarios," *IEEE Trans. Mobile Comput.*, vol. 16, no. 7, pp. 2065–2078, 2017.

[5] B. Zan, M. Gruteser, and F. Hu, "Key agreement algorithms for vehicular communication networks based on reciprocity and diversity theorems," *IEEE Trans. Veh. Technol.*, vol. 62, no. 8, pp. 4020–4027, 2013.

[6] G. Li, A. Hu, C. Sun, and J. Zhang, "Constructing reciprocal channel coefficients for secret key generation in FDD systems," *IEEE Commun. Lett.*, vol. 22, no. 12, pp. 2487–2490, 2018.

[7] H. Ruotsalainen and S. Grebeniuk, "Towards wireless secret key agreement with LoRa physical layer," in *Proc. ARES*, Hamburg, Germany, Aug. 2018, p. 23.

[8] J. Zhang, A. Marshall, and L. Hanzo, "Channel-envelope differencing eliminates secret key correlation: LoRa-based key generation in low power wide area networks," *IEEE Trans. Veh. Technol.*, vol. 67, no. 12, pp. 12 462–12 466, 2018.

[9] T. Mazloum, F. Mani, and A. Sibille, "A disc of scatterers based radio channel model for secure key generation," in *Proc. 8th European Conf. Antennas and Propagation (EuCAP)*, Hague, The Netherlands, 2014, pp. 1290–1294.

[10] T. Mazloum and A. Sibille, "Performance of secret key generation in non stationary channels," in *Proc. 9th European Conf. Antennas and Propagation (EuCAP)*, Lisbon, Portugal, 2015, pp. 1–6.

[11] T. Abbas, K. Sjöberg, J. Karedal, and F. Tufvesson, "A measurement based shadow fading model for vehicle-to-vehicle network simulations," *Int. J. Antennas Propag.*, p. 190607, 2015.

[12] C. D. T. Thai, J. Lee, and T. Q. Quek, "Physical-layer secret key generation with colluding untrusted relays," *IEEE Trans. Wireless Commun.*, vol. 15, no. 2, pp. 1517–1530, 2016.

[13] M. Waqas, M. Ahmed, Y. Li, D. Jin, and S. Chen, "Social-aware secret key generation for secure device-to-device communication via trusted and non-trusted relays," *IEEE Trans. Wireless Commun.*, vol. 17, no. 6, pp. 3918–3930, 2018.

[14] X. Wang, Y. Hou, X. Huang, D. Li, X. Tao, and J. Xu, "Security analysis of key extraction from physical measurements with multiple adversaries," in *Proc. IEEE ICC Workshops*, Kansas City, MO, USA, 2018, pp. 1–6.

[15] "Further enhancements to LTE time division duplex (TDD) for downlink-uplink (DL-UL) interference management and traffic adaptation," Tech. Rep. 3GPP TR 36.828 V11.0.0, Jun. 2012. [Online]. Available: www.3gpp.org/dynareport/36828.htm

[16] S. S. Szyszkowicz, H. Yanikomeroglu, and J. S. Thompson, "On the feasibility of wireless shadowing correlation models," *IEEE Trans. Veh. Technol.*, vol. 59, no. 9, pp. 4222–4236, 2010.

[17] M. Gudmundson, "Correlation model for shadow fading in mobile radio systems," *Electronics Lett.*, vol. 27, no. 23, pp. 2145–2146, 1991.

[18] M. Ding, M. Zhang, D. López-Pérez, and H. Claussen, "Correlated shadow fading for cellular network system-level simulations with wraparound," in *Proc. IEEE ICC*, London, UK, Jun. 2015, pp. 2245–2250.

[19] G. Senarath, "Multi-hop relay system evaluation methodology (channel model and performance metric)," Tech. Rep., 2007. [Online]. Available: http://ieee802.org/16/relay/docs/80216j-06_013r3.pdf

[20] R. He, Z. Zhong, B. Ai, and C. Oestges, "Shadow fading correlation in high-speed railway environments," *IEEE Trans. Veh. Technol.*, vol. 64, no. 7, pp. 2762–2772, 2015.

[21] J. Zhang, A. Marshall, R. Woods, and T. Q. Duong, "Efficient key generation by exploiting randomness from channel responses of individual OFDM subcarriers," *IEEE Trans. Commun.*, vol. 64, no. 6, pp. 2578–2588, 2016.

[22] H. Kim and Y. Han, "Enhanced correlated shadowing generation in channel simulation," *IEEE Commun. Lett.*, vol. 6, no. 7, pp. 279–281, 2002.

[23] E. Perahia and D. C. Cox, "Shadow fading correlation between uplink and downlink," in *Proc. IEEE Veh. Technol. Conf.*, vol. 1, Rhodes, Greece, Greece, May 2001, pp. 308–312.

[24] T. Klingenbrunn and P. Mogensen, "Modelling cross-correlated shadowing in network simulations," in *Proc. IEEE Veh. Technol. Conf.*, vol. 3, 1999, pp. 1407–1411.

[25] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd ed. John Wiley & Sons, 2006, p. 252.

[26] G. Li, A. Hu, J. Zhang, L. Peng, C. Sun, and D. Cao, "High-agreement uncorrelated secret key generation based on principal component analysis preprocessing," *IEEE Trans. Commun.*, vol. 66, no. 7, pp. 3022–3034, 2018.

[27] "Evolved Universal Terrestrial Radio Access (E-UTRA); physical layer procedures," Tech. Rep. 3GPP TR 36.213 V15.3.0, Sep. 2018. [Online]. Available: www.3gpp.org/dynareport/36213.htm

[28] A. Kraskov, H. Stögbauer, and P. Grassberger, "Estimating mutual information," *Physical Review E*, vol. 69, no. 6, p. 066138, 2004.