Performance of secret key generation in non stationary channels

Taghrid Mazloum and Alain Sibille
Communication and Electronic Department, Telecom ParisTech/LTCI,
Paris, France
{taghrid.mazloum, alain.sibille}@telecom-paristech.fr

***Abstract*—Secret key generation from the randomness provided by random channels is currently considered as one way to improve security in wireless communications at the physical layer level. However, the relation between the performance of SKG schemes and the characteristics of the radio channel has been moderately investigated. In this work, we evaluate the security performance through a simple channel model based on scatterers distributed around the terminals, which enables going beyond the common assumption of spatial stationarity between the legitimate terminal and the eavesdropper. This performance is assessed both from information theory metrics and from a practical key extraction algorithm.**

***Index Terms*—physical layer, information security, propagation, spatial diversity.**

I. Introduction

Secret key generation (SKG) and distribution by conventional cryptography methods present a great issue especially in mobile radio communications. Therefore, accurate key generation schemes require that legitimate terminals (Alice and Bob) have access to a common source of randomness, which can be the propagation channel [1], [2], thereby avoiding the problems associated with the distribution of keys. Secret keys may be used then by upper layer protocols in order to ensure the confidentiality of wireless communications. Provided they use the same frequency, Alice and Bob observe nearly the same radio channel, owing to reciprocity. Moreover, the random character is ensured by multipath fading and by the decorrelation between the channels seen by two users in the spatial, temporal and frequency domains. Consequently an eavesdropper (Eve) has no direct access to the channel seen by the legitimate user (Bob) and, therefore, cannot easily crack the key when it is long enough.

In an information theoretic framework, the security brought by SKG has been evaluated in the literature through the computation of theoretical bounds for the key length. Simple analytical expressions are available in the case of jointly Gaussian channels [3], [4]. Nevertheless it is crucial to assess how much these bounds can be achieved in practical scenarios and also to evaluate privacy performance for arbitrary fading channels. This is provided by exploiting practical key extraction algorithms. The received signal strength [5], the phase information [6] and the channel impulse response [7], [8] have been exploited to generate key bit streams. Moreover, complex channel coefficients may be investigated to extract more random bits per single channel sample [3], [9], [10].

In the literature, SKG performance has been investigated statistically and empirically for a simple scenario where Eve is very close to a legitimate terminal, i.e. both of them sharing the same multipath components [3]. Indeed several works assumed that Eve is not able to access to correlated channel information when she is located more than a half or at most a few wavelengths away from both legitimate terminals [3], [5], [8]. However the authors in [7] proved by measurements that spatial correlation can be found even for larger separation distances. In particular, shadow fading seems to be critical in physical layer security, while shadow fading correlations [11] between Bob and Eve is likely to affect the information accessible to the eavesdropper and thus to impact the confidentiality.

Given these considerations, we here intend to evaluate the relation between the performance in terms of security and the characteristics of the radio channel, especially beyond the classical assumption of spatial stationarity between Bob and Eve (see also preliminary results in [9]). For that purpose, we use a channel model (described in section II), based on scatterers uniformly distributed within a disc. The SKG performance is assessed through metrics that are presented in section III and the results are discussed in section IV. Finally section V concludes the paper with a short summary.

II. A disc of scatterers based channel model

In real scenarios, the channel multipath components seen by Bob and Eve can change according to the relative distance between them and also according to the environment. For example, the propagation channel components are likely to be more sensitive to the separation distance in a dense scattering urban environment than in a rural one. Therefore, we aim in this paper to model the lack of spatial stationarity [12] between Bob and Eve and evaluate its impact on SKG behavior. For that purpose, we consider a 2-D geometry-based stochastic channel model where scatterers are uniformly distributed within a disc, see Fig. 1.

In this model, Bob is always located at the center of the disc and Eve is at a separation distance d from Bob within the disc. The maximum separation distance is kept to a value low enough to avoid edge effects due to the finite size of

the disc. Furthermore, the transmitter, Alice, is supposed far away from the disc so that we can consider rays arriving from a single direction $\vec{K}_A$ to the local scatterers. This situation occurs mostly in urban macro-cells, when the base station is located over rooftops. Each terminal is considered to be in non line-of-sight condition with respect to Alice. Hence all the rays received by Bob/Eve originate from the scatterers, acting as secondary sources. We assume that Bob and Eve are both equipped with an omnidirectional antenna.

Scatterers may represent specular reflections from a building where the scattering coefficient changes with respect to the direction of departure. Hence Bob and Eve may not see the same power rays. Accordingly, each scatterer is assumed to act as a non-omnidirectional lossy re-transmitter, which is statistically independent from the others. Moreover, in order to account for the shadow fading correlation between Bob and Eve, we assume that each scattered path emitted from the same scatterer is spatially correlated [13] according to the following correlation coefficient [14]:

$$\rho_i = 0.5 + 0.5 \cos \Delta\phi_i \tag{1}$$

where $\Delta\phi_i$ is the angle of departure difference at the *i*th scatterer, as shown in Fig. 1. The shadowing coefficients a_{1i} and a_{2i} account for the shadow fading for each path [13]. These coefficients are i.i.d. and follow a normal distribution with zero-mean and standard deviation σ in dB. Furthermore the scattered wave undergoes free space attenuation according to the separation distance towards Bob/Eve [9], [15].

According to the scatterers distribution, physical path structures towards Bob/Eve are determined and the multipath fading channel can be computed [12]. Therefore the narrowband single input single output (SISO) channel seen by Bob is defined as follows:

$$h_B = \sum_{i=1}^{N_S} \frac{10^{\frac{a_{1i}}{20}}}{d_{Bi}} \exp[j(Kd_{Bi} + \vec{K}_A.\vec{r}_i)] \tag{2}$$

and that seen by Eve is as follows:

$$h_E = \sum_{i=1}^{N_S} \frac{10^{\frac{\rho_i a_{1i} + \sqrt{1-\rho_i^2} a_{2i}}{20}}}{d_{Ei}} \exp[j(Kd_{Ei} + \vec{K}_A.\vec{r}_i)] \tag{3}$$

where N_S, d_{Xi} and $\vec{r}_i$ are respectively the number of scatterers within the disc, the distance from an *i*th scatterer to X (Bob/Eve) side and the *i*th scatterer coordinate. Moreover, $K = \frac{2\pi}{\lambda}$ and $\vec{K}_A$ are respectively the wave number and the wave vector of the plane wave emitted by Alice towards the disc.

Owing to the reciprocity law, legitimate terminals see ideally the same propagation channels, i.e. $h_A = h_B$. However, in practice, their channel estimations are corrupted by noise. Hence we assume that $\hat{h}_i = h_i + n_i$ where $\hat{h}_i$ is the channel estimation and n_i is the noise estimation which can be modeled as zero-mean complex Gaussian random variable with variance σ_n^2. i denotes here A (Alice), B (Bob) and E (Eve).

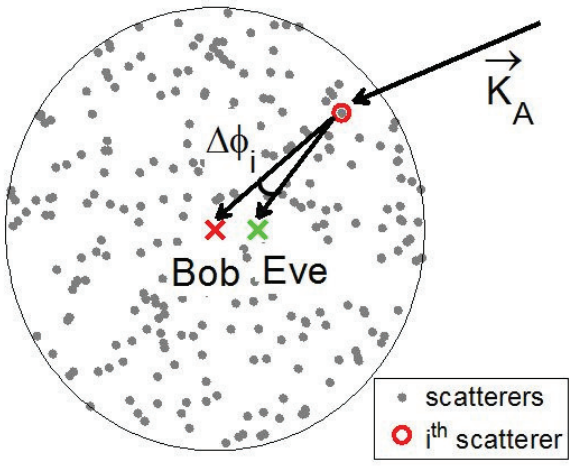

Fig. 1. Geometrical representation of the communication scenario

We aim to model both small scale fading (SSF) and shadow fading as explained in section III. For that purpose, we define how the random variables change according to these two fading types.

- Shadow fading statistic: It is defined by different realizations of the environment characterized by the macroscopic scatterers positions and the shadowing coefficients (a_{1i} and a_{2i}).
- SSF statistic: The macroscopic environment around Bob and Eve is fixed but scatterers are allowed to move on a square grid of surface 5λx5λ, providing SSF channels through varying phases over 0 to 2π.

III. SKG ASSESSMENT METRICS

A. Information theoretic security bounds

As mentioned in section I, information secret key capacity can be computed analytically for jointly Gaussian channels [3], [4]. Unfortunately, such a situation is not so commonly encountered in real life. In the present work, we turn around this difficulty by using the SSF channels as defined in the previous section. In other words, the secret key capacity and secret key vulnerability are conditional to the positions of Bob/Eve and to the macroscopic locations of the scatterers. The small scale randomness in the scatterers positions distinctly affect the channels seen by Bob and Eve and the common part between these channels is responsible for the key vulnerability.

By observing the same reciprocal propagation channel, the legitimate terminals are able to extract identical key bits. However the channel estimation noise limits the number of bits that can be generated. Therefore we define the available key bits I_K as the statistical maximum shared number of bits that can be extracted jointly by both Alice and Bob. I_K is then the mutual information between channels seen by both Alice and Bob, i.e. $I_K = I(\hat{h}_A, \hat{h}_B)$. If no information is available for Eve, all the I_K bits are secure and then serve to build the secret key. However if Eve measures a correlated channel with

the channel seen by Bob, the number of secure key bits is then reduced to the mutual information between channels measured by both Alice and Bob, conditionally knowing Eve channels, i.e. $I_{SK} = I(\hat{h}_A, \hat{h}_B / \hat{h}_E)$. Also we define the vulnerable key bits as $I_{VK} = I_K - I_{SK}$. In the case of jointly complex Gaussian channels, the mutual information can be calculated based on covariance matrices [3], [9].

B. Channel Quantization

After a channel estimation phase, legitimate terminals convert their channel observations into key bit streams through a quantization algorithm. Indeed they are interested in extracting a large number of identical key bits from a single channel sample. Using the channel quantization alternating (CQA) algorithm [3], we extract decorrelated key bits from the complex channel coefficients, since both real and imaginary parts are assumed independent for Gaussian channels [3], [10]. CQA makes use of alternating maps to avoid discarding symbols and to minimize the key bit disagreement. It was found to be a rather efficient and simple scheme to start with. Although this algorithm requires public discussion between Alice and Bob to agree on the map indices, it does not reveal useful information to Eve (refer to [3] for more information).

We intend to evaluate security performance by the computation of the bit error rate (BER) between keys extracted by both Bob and Eve, assuming noiseless channels. Hence we suppose that Alice and Bob are able to generate identical key bits with full reliability. The BER between Bob and Eve is considered as the ratio of bit disagreement between keys extracted by both Bob and Eve due to channel decorrelation.

C. Channel correlation

Given that the information security metrics recalled above are based on second order quantities, the correlation between channel coefficients is responsible of the imperfect security performance. We use the conventional channel correlation coefficient between two random complex variables X and Y of mean μ_X and μ_Y , defined as follows:

$$corr = \frac{E\{(X-\mu_X)(Y-\mu_Y)^*\}}{\sqrt{(E\{|X-\mu_X|^2\})(E\{|Y-\mu_Y|^2\})}} \quad (4)$$

where $(.)^*$ stands for complex conjugate. We consider two types of channel correlations: the complex channel correlation coefficient (referred as ρ_{BE}) where X and Y represent respectively the complex channel coefficients h_B and h_E and the power envelope correlation coefficient, where X and Y are replaced by the powers $|h_B|^2$ and $|h_E|^2$, respectively.

IV. SKG Performance Evaluation

The signal to noise ratio (SNR) is defined as the ratio of the average received power to the noise power:

$$SNR = \frac{E\{||h||_F^2\}}{\sigma_n^2} \quad (5)$$

where $E\{.\}$ and $||.||_F$ denote respectively for the expectation over SSF and the Frobenius norm. Tab. IV presents the simulation parameters values. We assume that all terminals have the same SNR and that 250 scatterers are distributed uniformly within the disc, unless differently stated. The maximum separation distance is 1000λ providing equivalence statistics for both Bob and Eve.

TABLE I
Simulation Parameters

Frequency	2 GHz
SNR	15 dB
Disc radius	5000λ
Scatterers number N_S	250

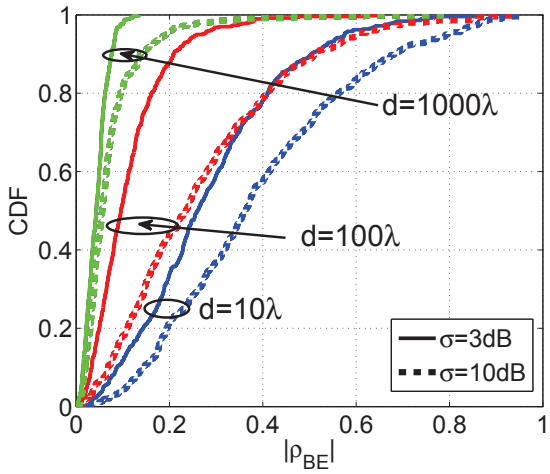

Fig. 2. CDF of complex channel correlation

Each statistical quantity (correlation coefficient, information theoretic key bound and BER value) is computed from an SSF statistics. Then statistical distributions for these quantities are obtained from the combined macroscopic scatterers randomness and the shadow fading parameters randomness.

A. Channel correlation

Fig. 2 shows cumulative distribution functions (CDF) of complex channel correlation coefficients for both shadow fading standard deviation $\sigma = 3dB$ and $\sigma = 10dB$ and for several separation distances (d) between Bob and Eve. For $N_S = 250$, the average distance between scatterers is almost 600λ. For $d > 600\lambda$, the interferences seen by Bob and Eve become independent and the complex correlation vanishes. Consequently $|\rho_{BE}|$ decreases when d increases. Furthermore we notice that $|\rho_{BE}|$ increases when σ increases. Usually increasing σ yields more rapidly channel decorrelations. However this is not the case here. This is due to the fact that our channel model is able to reproduce both Rayleigh and Rician distributions. The proportion of these two distributions is impacted by the value of σ. When σ increases, the proportion of Rician channels increases. We here consider that channel amplitudes are Rician distributed if the Rician K factor is greater or equal to 1. The results show that almost 18% of the channels are Rician for $\sigma = 3dB$ whereas we have 30% for $\sigma = 10dB$. Indeed

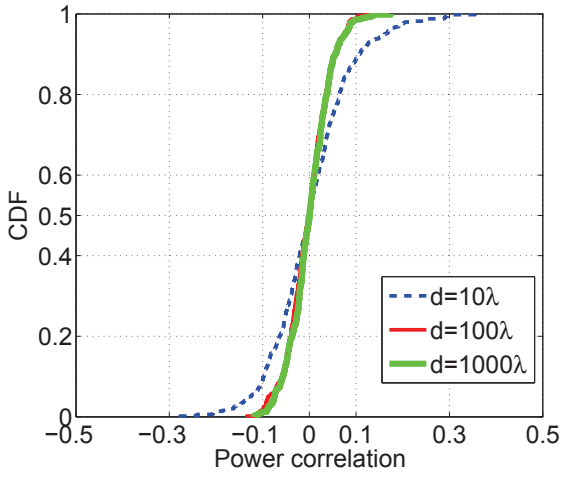

Fig. 3. CDF of power envelope correlation for $\sigma = 3dB$

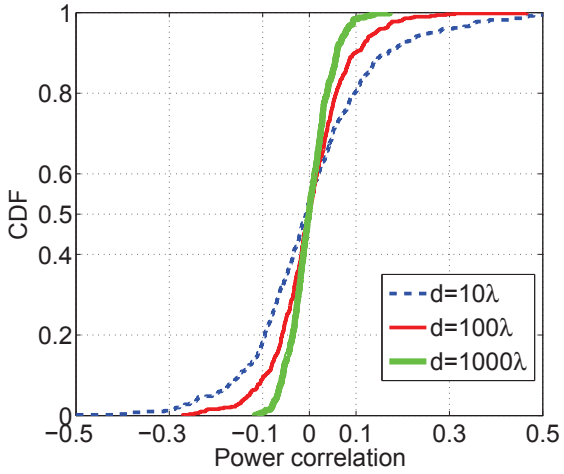

Fig. 4. CDF of power envelope correlation for $\sigma = 10dB$

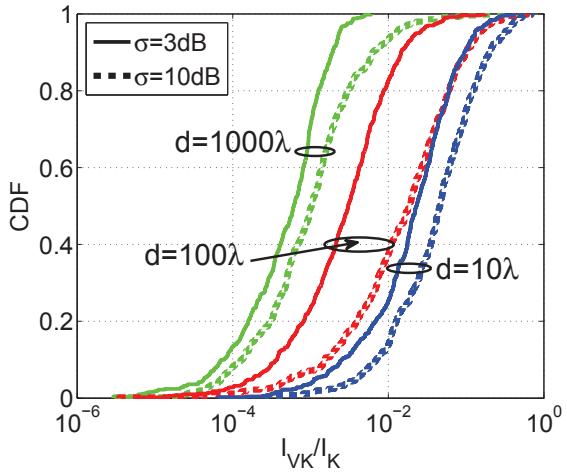

Fig. 5. CDF of relative vulnerable key bits

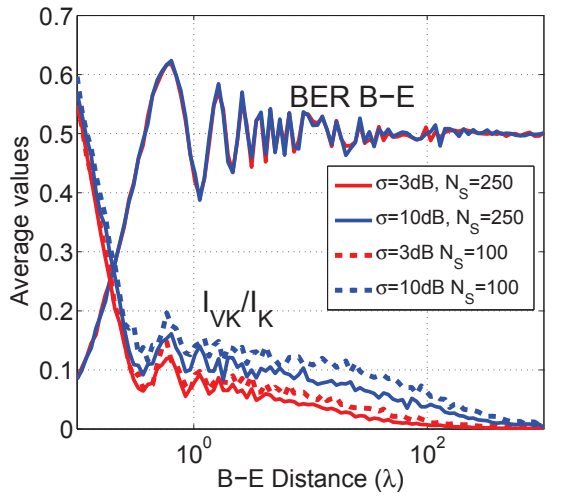

Fig. 6. Averaged BER and vulnerable key bits as function of the separation distance d between Bob and Eve

we find that the correlation increases for Rician channels, where a dominant predictable path exists. This is the reason why we still have large correlation values for large separation distances.

Fig. 3 and Fig. 4 depict the variation of the CDF of power correlation for several Bob-Eve distances and for $\sigma = 3dB$ and $\sigma = 10dB$, respectively. As expected, the power correlation decreases when d increases. When Eve goes away from Bob, they see different multipath components, leading to a decrease in both complex and power envelope correlations. Due to the high proportion of Rician channels for $\sigma = 10dB$, the variance is the largest in this case, which can be explained by more correlations resulting from less significant scatterers in the presence of a dominant path.

B. Vulnerable key bounds performance

According to the chosen SNR, the maximum number of key bits (I_K) is nearly equal to 4 per channel observation. Nevertheless the vulnerable key bits (I_{VK}) depend on spatial channel correlations. Since channel correlations decrease when either d increases or σ decreases, the amount of information gathered by Eve about the legitimate channel and subsequently about the secret key decreases, i.e. I_{VK}/I_K decreases, as shown in Fig. 5 and Fig.6. Regarding the variance of I_{VK}/I_K, shown in Fig. 7, the security behavior changes according to the environment realization with more significant variation for moderate d values and for large σ values. Good security performance is provided for dense multipath propagation channels, whereas it is degraded for environments where a predictable dominant path exists.

Fig.6 shows the variation of the mean values of both vulnerability bits and the BER as a function of distance and for different σ values and different scatterers densities. If the density of scatterers decreases, the effective number of scatterers seen by Bob and Eve decreases, resulting in more vulnerability. Consistently, the variability of I_{VK}/I_K

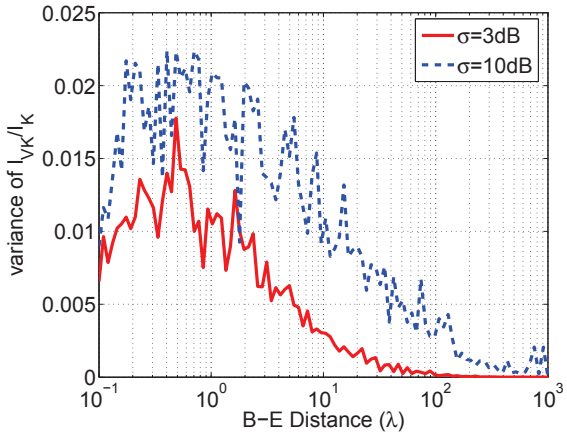

Fig. 7. The statistical variance of I_{VK}/I_K as a function of d

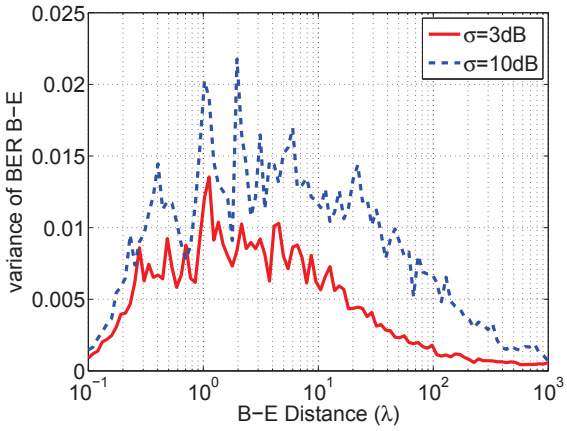

Fig. 9. The statistical variance of BER as a function of d

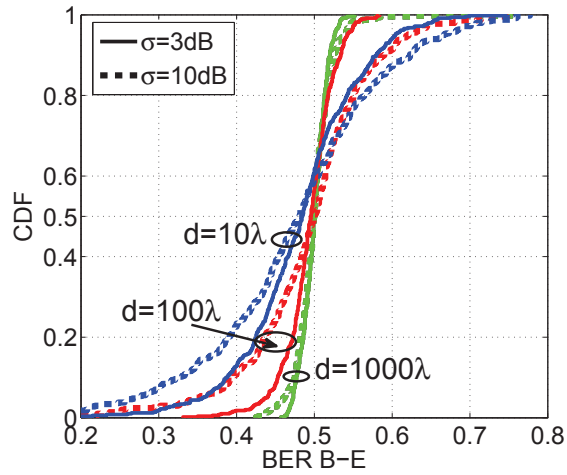

Fig. 8. CDF of BER between Bob and Eve

increases with the shadow fading statistics for $N_S = 100$ (the results is omitted for the clarity of the figure).

C. CQA performance

Alice, Bob and Eve quantify their channel complex coefficients into stream bits by extracting 1 bit from each I and Q parts. Fig.8 shows the CDFs of BER for different values of σ and d. Although we have almost the same average value for different values of both d and σ, the behavior changes from one environment to another, as shown implicitly by the variance of each CDF, see also Fig. 9. While σ does not impact the mean of BER whatever d, it impacts the variance of BER as shown in Fig. 9.

When Eve goes away from Bob, the security is enhanced since the mean BER converges towards 0.5 and this is consistent with the behavior of the average I_{VK}/I_K. Actually, the BER simply expresses the raw difference between the key bits directly extracted from the channel coefficients seen by Bob and Eve. The algorithm doesn't attempt to develop more powerful strategies in order to exploit the common characteristics between these channels. This is the reason why the remaining vulnerability expressed in I_{VK} beyond about one wavelength distance between Bob and Eve, is not reflected in the BER.

V. Conclusion

In this paper we presented an analysis of SKG based on channel randomness in relation to characteristics of the propagation by investigating a disc of scatterers-based channel model. This has been done by considering channel correlations, by computing relative vulnerable key bits and by extracting key bits via the CQA algorithm, providing a direct evaluation of the SKG scheme performance. A separation distance by a few wavelengths is not enough to guarantee the maximal level of security, especially for environments where a dominant path exists. Consistently this level is impacted by the detailed features of the environment itself and differs significantly between Rayleigh and Rician channels. Complementary results, making use of experimental data, can be found in [10].

Acknowledgment

This work has been supported by the PHYLAWS project (EU FP7-ICT 317562, www.phylaws-ict.org).

References

[1] R. Ahlswede and I. Csiszar, "Common randomness in information theory and cryptography-Part I: Secret sharing," *IEEE Trans. Inform. Theory*, vol. 39, pp. 1121-1132, July 1993.

[2] U. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inform. Theory*, vol. 39, no. 3, pp. 733-742, May 1993.

[3] J. Wallace and R. Sharma, "Automatic secret keys from reciprocal MIMO wireless channels: measurement and analysis," *IEEE Trans. Inf. Forensics and Security*, vol. 5, no. 3, pp. 381-392, Sep. 2010.

[4] C. Ye, A. Reznik, and Y. Shah, "Extracting secrecy from jointly Gaussian random variables," *IEEE Int. Symp. on Inform. Theory*, Seattle, WA, Jul. 9-14, 2006, pp. 2593-2597.

[5] T. Aono, K. Higuchi, T. Ohira, B. Komiyama, and H. Sasaoka, "Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels," *IEEE Trans. Antennas and Propagation*, vol. 53, no. 11, pp. 3776-3784, Nov. 2005.

[6] A. Sayeed and A. Perrig, "Secure wireless communications: Secret keys through multipath," *Int. Conf. Acoustics, Speech and Signal processing*, Las Vegas, Nevada, Mar. 31-Apr. 4, 2008, pp. 3013-3016.
[7] M.G. Madiseh, S. He, M. McGuire, S. Neville, and S. Dong, "Verification of secret key generation from UWB channel observations," *IEEE Int. Conf. Communications*, Dresden, Germany, Jun. 14-18, 2009, pp. 1-5.
[8] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. Mandayam, "Information-theoretically secret key generation for fading wireless channels," *IEEE Trans. Inform. Forensics and Security*, vol. 5, no. 2, pp. 240-254, Jun. 2010.
[9] T. Mazloum, F. Mani, and A. Sibille, "A disc of scatterers based radio channel model for secure key generation," *Eur. Conf. Antennas and Propagation*, The Hague, Netherlands, April 6-11, 2014, pp.1290-1294.
[10] T. Mazloum, F. Mani, and A. Sibille, "Analysis of secret key robustness in indoor radio channel measurements," *IEEE Vehicular Tech. Conf.*, Glasgow, Scotland, May 11-14, 2015, in press.
[11] M. Gudmundson, "Correlation model for shadow fading in mobile radio systems," *Electron. Lett.*, vol. 27, no. 23, pp. 2145-2146, Nov. 1991.
[12] A. Borhani and M. Patzold, "Modelling of non-stationary mobile radio channels using two-dimensional brownian motion processes," *Int. Conf. Advanced Technologies for Communications*, Oct. 16-18, 2013, pp.241-246.
[13] L. Vuokko, V.-M. Kolmonen, J. Salo, and P. Vainikainen, "Measurement of large-scale cluster power characteristics for geometric channel models," *IEEE Trans. Antennas and Propagation,* vol. 55, no. 11, pp. 3361-3365, Nov. 2007.
[14] F. Grazioso, M. Pratesi, M. Ruggieri, and F. Santucci, "A multicell model of handover initiation in mobile cellular networks," *IEEE Trans. Vehicular Tech.*, vol. 48, no. 3, pp. 802-814, May 1999.
[15] F. Amoroso and W.W. Jones, "Geometric model for DSPN satellite reception in the dense scatterer mobile environment," *IEEE Trans. Commun.*, vol. 41, pp. 450-453, Mar. 1993.