EUROPEAN COOPERATION
IN THE FIELD OF SCIENTIFIC
AND TECHNICAL RESEARCH

EURO-COST

IC1004 TD(13) 08072
Ghent, Belgium
25-27 Septembre 2013

SOURCE: COMELEC Department, TELECOM ParisTech
Paris, France

A Disc of Scatterers Based Radio Channel Model for Secure Key Generation

Taghrid Mazloum and Alain Sibille
Telecom ParisTech
46, rue Barrault
75013 Paris
FRANCE
Phone: +33 1 45817468
Fax:
Email: taghrid.mazloum@telecom-paristech.fr

A Disc of Scatterers Based Radio Channel Model for Secure Key Generation

Taghrid Mazloum and Alain Sibille

***Abstract*—Physical layer security is a method to ensure the confidentiality of a wireless communication from encryption keys exploiting the randomness of the reciprocal propagation channel between a pair of legitimate users, Alice and Bob. This confidentiality is achieved owing to the decorrelation between these channels and that experienced by a third terminal (Eve), acting as an eavesdropper. In this work, we evaluate the secrecy capacity of a simple channel model, based on a disc of scatterers. The model allows to consider any distance between Alice and Eve within the disc and is thus not limited to a stationarity region. Moreover, we develop an analysis of the definition of radio channel scenarios for Alice, Bob and Eve, depending on their degree of knowledge of the environment. The practical relevance of these scenarios is discussed, in relation with the Gaussian or non Gaussian character of the channel statistics and its impact on the computation of the secrecy capacity.**

I. Introduction

Nowadays wireless communications have a major role in many fields of the society, hence their security becomes a crucial requirement. Secret keys are used to encrypt data to ensure the confidentiality of a wireless communication. Conventional methods of generating and distributing private keys may suffer from complexity and high computational cost. An alternative solution is physical layer security that exploits the inherent randomness of the reciprocal propagation channel between a pair of legitimate users, Alice and Bob, to generate a shared secret key. The confidentiality can be achieved exploiting the decorrelation between these channels and that experienced by a third terminal (Eve), acting as an eavesdropper [1], [2].

From an information-theoretic formulation of the problem, the maximum number of information bits I_K extracted from the estimated legitimate fading channels can be defined as the mutual information of these channels. However, in principle, not all of these bits are secure since the eavesdropper may have access to some insight about the legitimate channel. Therefore the secret key bits I_{SK} can be obtained by evaluating the mutual information between the channels seen by Alice and Bob, given Eves observation [1], [2], [3].

Several works can be found in the literature dealing with secrecy capacity for physical layer security based on different channel models or techniques (e.g. UWB, MIMO, etc.) [2], [3], [4]. In [3], for example, I_{SK} has been investigated in a worst-case scenario where Alice and Eve are both stationary and sufficiently close to each other. This scenario is not always realistic as the eavesdropper may be at a large distance from Alice and see a channel exhibiting a strong spatial decorrelation from Alices channel.

In this work we propose a simple channel model based on scatterers uniformly distributed within a disc centered at Alice. Eve is located within the disc, but can experience a channel really different from Alice, leading to a very good level of secrecy. Therefore, we investigate this secrecy in a simulated example.

However, a fundamental aspect, rarely discussed in the literature, is the relation between the definition of these scenarios and the degree of knowledge by Alice/Eve of their environment. Our analysis is based on the idea that the parameterization of the scenarios is intimately connected to this knowledge, which depends on the capability of Alice/Eve to acquire it. Furthermore, the practical relevance of scenarios is discussed in relation with the Gaussian or non Gaussian character of the channel statistics and its impact on the computation of the secrecy capacity.

The rest of the paper is organized as follows. In section II we describe the propagation scenario of the disc scattering model. We then define in section III four radio channel scenarios and discuss the terminal's knowledge about the environment with respect to the secrecy capacity. Section IV provides an evaluation of the secrecy in a non stationarity region. Finally we draw conclusions in section V.

II. Disc of scatterers based channel model

In order to study the effect of the difference between the channels seen by Alice and Eve on the secret key generation, we consider a geometry-based channel model where scatterers are uniformly distributed within a disc, as shown in Fig. 1. We also assume that Bob is far enough so that we can consider rays arriving to the local scatterers with a constant angle. This model can, for example, describe environments where the transmitter antenna (Bob) is highly elevated while the receiver terminals (Alice and Eve) are surrounded by a large number of local scatterers. This situation occurs mostly in urban macro-cells.

Each terminal is considered to be equipped with an omnidirectional antenna and is in non line-of-sight

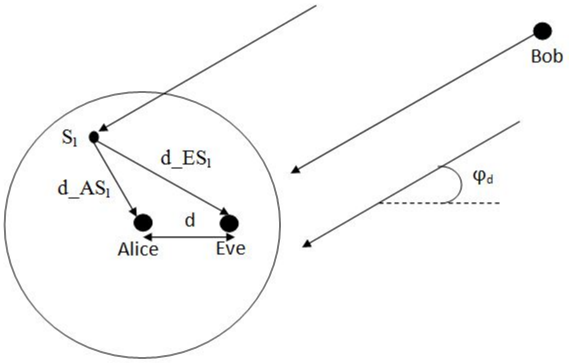

Fig. 1. Graphical representation of the disc of scatterers scenario

propagation from Bob. Hence all the rays received by Alice/Eve originate from the scatterers, acting as secondary sources. Each scatterer is also assumed to act as an omnidirectional re-transmitter, statistically independent from the other scatterers. Therefore the narrowband complex baseband channel gain connecting Bob antenna to Alice or Eve antenna can be defined as follows:

$$h = \sum_{l=1}^{N_S} \frac{1}{d\_iS_l} \beta_l \exp[j(K.d\_iS_l + \vec{K}_{B\_S}.\vec{r}\_S_l)] \quad (1)$$

where N_S is the number of scatterers surrounding Alice and d_iS_l is the distance from Alice (if $i = A$) or Eve (if $i = E$) to each scatterer. $\vec{r}\_S_l = [x\_S_l, y\_S_l]$ and β_l are respectively the scatterers coordinate and the complex scattering coefficient. $K = \frac{2\pi}{\lambda}$ and $\vec{K}_{B\_S} = K[\cos(\phi_d), \sin(\phi_d)]$ are respectively the wave number and the wave vector of the plane wave emitted by Bob towards the disc, where ϕ_d is the angle of departure from Bob and λ is the wavelength. We further assume that the power of the incoming wave from Bob is diffused by scatterers and attenuated according to the separation distance towards Alice/Eve.

III. Radio channel scenarios

A. General considerations

The available key bits I_K and the secret key bits I_{SK} are statistical quantities computed from the observed channels. We can also define the vulnerability key bits I_{VK} as the number of bits leaked to the eavesdropper so that $I_{VK} = I_K - I_{SK}$. The computation of these quantities is impacted by the channels statistics depending on the knowledge of the terminals about their environment. In fact, according to the relative position of Eve against Alice and the environment where they are, Eve may measure a channel different from the one measured by Alice. The complexity of the multipath channel and the difference on the scatterers directions and distances, seen from Alice or Eve are the causes of the decorrelation between the channels.

The number of secret key bits is the length of the private key that can't be obtained by an enemy whatever the amount of correlated information he got. Therefore, in order to reduce the secrecy, Eve might use several methods in order to obtain information about the common channel of Alice and Bob and, thus, reduce the number of secret key bits [4]. For example if, in addition to measuring the channel, Eve knows the positions of legitimate terminals, she can exploit this information to reduce the exploration of possible Alice-Bob channels. In other words, the information owned by the triplet Alice-Bob-Eve determines the relevant statistical ensembles of the three channel pairs. The resulting randomness directly impacts the degree of secrecy, in other words the number of vulnerable key bits.

Based on this analysis, we define in the following four scenarios and address the differences in the terminals' knowledge about their environment to evaluate the secrecy. A consideration is that of the Gaussian or non Gaussian character of the channel coefficients. Indeed, in the former case the various number of key bits defined above are easy to compute from the covariance matrices [6] while in the latter there is no simple way to do it. Therefore, we are mainly interested in exploiting Gaussian channels.

B. Scenario 1: Nearly perfect environment knowledge

Here we assume that Alice knows the departure angle ϕ_d of rays emitted by Bob as well as the locations of scatterers. With the full knowledge of the environment (ϕ_d and the scatterers locations), Alice can estimate accurately the channel between herself and Bob. However, for any secrecy to exist, there must be some randomness that will create difficulties for Eve to guess the key bits. Here, the randomness stems from two features: firstly we assume there is a residual uncertainty on Bob's position and environment, which results in Rayleigh fading for the incoming wave ; secondly we consider two cases for β_l:

- In the first (Rayleigh fix) we assume that the scattering coefficients of all scatterers are identical, in other words β_l is a pure constant.
- In the second (Rayleigh β) we assume that diffused waves exhibit random Rayleigh fading towards Alice/Eve.

Fundamentally put, the more information Eve can get the less the security between Alice and Bob. In this scenario we assume that Alice/Eve use techniques (an accurate eye, a telemeter...) that enable them to know perfectly (Rayleigh fix) or accurately (Rayleigh β) the positions of scatterers and also to know the positions of both terminals.

In summary, to compute a single value of I_K, we fix the direction of departure of signals emitted by Bob and we also fix the distribution of the scatterers within

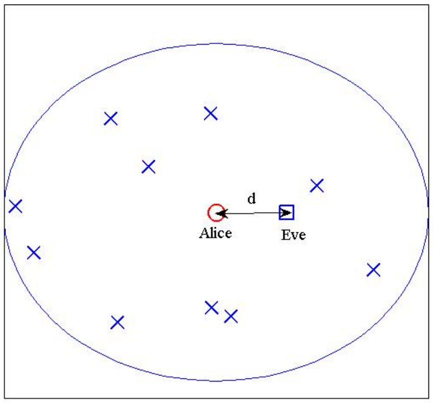

Fig. 2. A random realization for 10 scatterers within the disc centered at Alice

the disc. The evaluation of the mutual information is based on the statistics of the path amplitude through covariance matrices.

Now it is clear that the computed value of I_K corresponds to a given set of scatterers and a given direction of Bob. In order to obtain a more representative view of the various environments, it is interesting to do this for various sets of scatterers and various Bob's directions. In order to take into account these variabilities, we compute several values of I_K over with we can obtain a statistical description of the various possible environments. Since simulations show that the channel is actually Gaussian, we are able to compute easily the statistical distribution of the numbers of available or vulnerable key bits.

The simple geometry-based channel model considered in this work allows considering any distance between Alice and Eve within the disc. Moreover Eve is supposed to know the scatterers positions. So Eve has full knowledge about the physical environment. Different scenario realizations are taken into account so that ϕ_d varies uniformly in $[0, 2\pi]$ and also the scatterers positions changes following a uniform distribution in two dimensions. Anyway, the separation distance between Alice and Eve is fixed for the evaluation of a mean value of I_K to highlight the impact of this separation on the security performances.

C. *Scenario 2: Knowledge of Bob's direction*

Consider now the case where Alice knows only the direction of arrival of rays emitted by Bob towards the disc of scatterers. To estimate the legitimate channel, she fixes the parameters given by her knowledge of the environment and she tries to define statistically the other parameters, such as the complex scattering coefficient and the scatterers locations. If the channel is Gaussian, we can compute a value of I_K by fixing an angle of departure ϕ_d and considering different statistical realizations of scatterers locations uniformly distributed on the disc. To take into account different channel realizations, we compute different values of I_K for different direction of departure. This scenario can be a quasi-realistic scenario where Alice can have the knowledge of Bob's position but not the distribution of the scatterers surrounding herself. However the statistics of the channel show non Gaussian behavior then the available key bits cannot be easily obtained.

D. *Scenario 3: Knowledge of scatterers' positions*

In this scenario, the assumptions that Alice has information about the locations of scatterers but not about the position of Bob are made. This scenario isn't anymore practical because it's very difficult that Alice has access to techniques enabling her to know the positions of scatterers. But if we suppose that, in this scenario the channel has a Gaussian behavior, so we can evaluate easily the security performances. In this scenario we assume that Eve is able to know Alice location, so that she knows the separation distance with her. She's able too to know the scatterers positions. Based on this knowledge, we can evaluate the secret key bits for a fixed separation distance between the eavesdropper and the legitimate terminal.

E. *Scenario 4: No information*

We assume that Alice/Eve don't know anything about their environment, which is expressed by a statistical ensemble to compute a single value of e.g. I_K where we have a large set of realizations of the scatterers and also a large set of Bob's directions, again taking that ϕ_d is uniformly distributed over $[0, 2\pi]$. Under these assumptions, the channel doesn't have a Gaussian behavior and so we are not able to evaluate the secrecy for this scenario. Nevertheless this scenario seems to be the more practical one because it is the most realistic one, where Alice has no channel state information.

In order to prove that the available key bits calculated in scenario 1 corresponds to a realistic value, we conjecture that the mean of I_K computed in the scenario 1 where the channel estimated is Gaussian corresponds to a single value computed in this last scenario.

IV. Secrecy evaluation in non stationarity region

We adopt scenario 1 to evaluate the secrecy with respect to Eve, since the statistics of the channel are Gaussian. The channel model employed here permits to consider any distance between Alice and Eve within the disc. Fig. 2 shows a random realization for the disc of scatterers centered at Alice. It shows too the relative distance between Alice and Eve in an environment of 10 scatterers. Clearly, the distance between the scatterers and Alice differs from the one between the scatterers and Eve. So the two terminals compute different complex channel coefficients due to the attenuation related

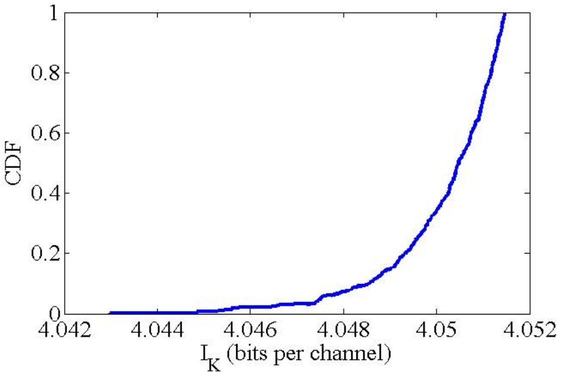

Fig. 3. Cumulative distribution of I_K for the scenario 1

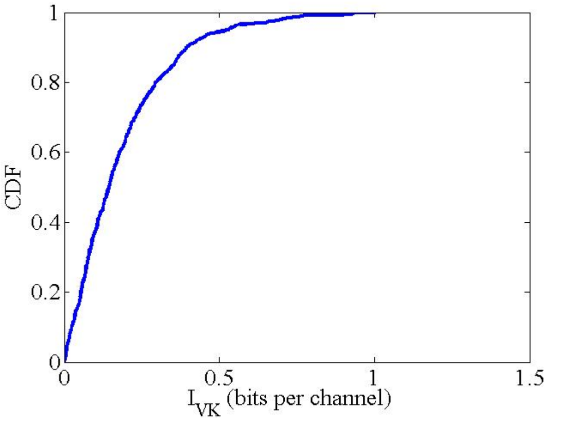

Fig. 4. Cumulative distribution of I_{VK} for the scenario 1

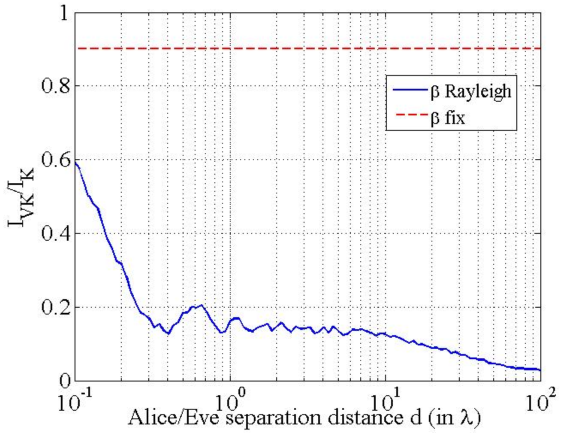

Fig. 5. Vulnerability key bits for scenario 1 where β can be Rayleigh or fix

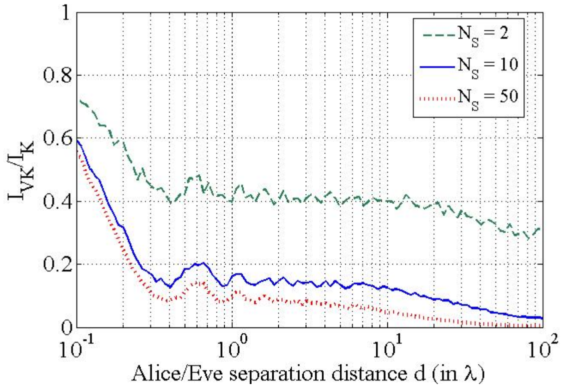

Fig. 6. Vulnerability key bits for different number of scatterers for the scenario 1

to the distance of separation with the scatterers. Table I shows the values of the simulation parameters.

Fig. 3 shows the cumulative distribution function of the available key bits. The values are very close to 4 bits. This is normal because for single-input single-output SISO systems, this quantity depends only on the signal to noise ratio SNR, defined as follows:

$$SNR = \frac{||h||_F^2}{N\sigma^2} \tag{2}$$

where $||.||_F$ denotes the Frobenius norm, N is the number of channel realizations to compute a single value of I_K and σ^2 is the mean power of the noise. We can remark that the variance of the curve is very small and that is because of the elevated value of the parameter N. Table II shows the variation of I_K with the SNR. It's clear that the secrecy capacity increases with the SNR. Fig. 4 represents the cumulative distribution function of the secret key bits for scenario 1 where Eve is in the middle distance between Alice and the border of the disc. We notice a significant security at this stage where the vulnerable key bits are very few (as shown by the fig. 4, we almost have 4.6% of the available key bits as vulnerable key bits).

Fig. 5 shows the vulnerable key bits in two cases: same scattering coefficient for all scatterers or different scattering coefficient for each scatterer. In the first case, we assume that all the scatterers act in the same manner. In the second case, the scatterers retransmit the signal with a certain complex attenuation and we assume that β follows a zero-mean complex Gaussian distribution, as explained in the description of scenario 1 above. Due to this randomness, we have more variability on the channel and then Eve finds it more difficulty to guess the key. So in the first case, almost all the bits are vulnerable. However we have a certain level of secrecy for the second case and this security is improved when the decorrelation between the legitimate channel and Eve's channel becomes significant, due to their separation distance.

Fig. 6 shows the vulnerable key bits for different number of scatterers found within the disc. If the number of scatterers increases, the diversity of the channel increases consequently and the work of the eavesdropper becomes more complicated. Then the vulnerability key bits decrease as shown by the results in Fig. 6.

For the scenario corresponding of the knowledge of the scatterers positions, we have the same results as the first scenario of nearly perfect knowledge. This result is reasonable since we work with SISO systems where the angle of departure isn't relevant. Moreover, in scenario 3, the angle of departure ϕ_d contributes to the randomness in addition to the complex scattering coefficient that changes from a scatterer to another one. Therefore, we already have a variation on the phase with or without the variability of ϕ_d.

Frequency	2 GHz
Disc radius	20 λ
SNR	15 dB
Scatterers number	10
N	1000

TABLE I. Simulation parameters

SNR	I_K (bits per channel)
15 dB	4.05
20 dB	5.67
25 dB	7.31

TABLE II. I_K with respect to the SNR

V. Conclusion

In this paper we have presented an evaluation of the performance of the security in a simple channel model, based on a disc of scatterers. This model allows to consider any distance between Alice and Eve within the disc and is thus not limited to a stationarity region. We evaluate the secrecy capacity with respect to the terminals knowledge about the environment. Unfortunately the Gaussian character of the channel coefficients is not always respected, which seriously complicates the computation of the secrecy capacity. We can assess the decrease of the vulnerable key bits when Eve moves away from Alice and when the number of scatterers increases in the disc area. The model has been studied for single frequency SISO systems but can easily extended to MIMO systems and/or wideband systems.

Acknowledgments

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

References

[1] U. Maurer, "Secret key agreement by public discussion from common information", *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733742, May 1993.

[2] M. Bloch, J. Barros, M.R.D. Rodriques and S.W. McLaughlin, "Wireless information-theoretic security", *IEEE Trans. Inf. Theory*, vol. 54, pp. 25152534, June 2008.

[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] R. Wilson, D. Tse and R.A. Scholtz, "Channel identification: Secret sharing using reciprocity in ultrawideband channels", *IEEE Trans. Inf. Forensics and Security*, vol. 2, no. 3, pp. 364375, Sep. 2007.

[5] Y. Liu, S.C. Draper and A.M. Sayeed, "Exploiting channel diversity in secret key generation from multipath fading randomness", *IEEE Trans. Inf. Forensics and Security*, vol. 7, no. 5, pp. 1484-1497, Oct. 2012.

[6] J. Wallace, "Secure physical layer key generation schemes : Performance and information theoretic limits", *in Proc. IEEE Int. Conf. Communications (ICC 09)*, Dresden, Germany, Jun. 1418, 2009, pp. 15.