A novel scatterer model for the security of key generation based on DISC model

Yuanhang Yang\textsuperscript{1}, Xin Zeng\textsuperscript{1*} and Xiaoping Xue \textsuperscript{1}

\textsuperscript{1} Dept. of Information and Communication Engineering, Tongji University, Shanghai, Shanghai, 201804, China

\textsuperscript{*}Corresponding author’s e-mail: zengxin1@tongji.edu.cn

Abstract. Physical layer security is a method of extracting encryption keys according to the randomness of reciprocal propagation channels between legitimate users, and the security under normal circumstances is ensured according to the decorrelation between these channels and those tapped by eavesdropper. However, evidences show that in some scenarios, such as the environment of quasi-static or insufficient scattering, the tapped channel still has a strong correlation with the legitimate channel, leading to bits leakage and security imperilment of key generation. The effect of introducing scatterers has been experimentally proved, however, these studies are based on fixed positions or special models and there is yet a lack of research on the influences brought by various scatterer distributions. In this paper, we introduce scatterers into single-bounced DISC model and control their distributions through a probability density function with two degrees of freedom, aiming to deeply investigate the impacts of scatterer distribution on channel decorrelation as well as key security. Simulation results prove that spiral correlation between tapped channel and legitimate channel can be effectively reduced by increasing scatterers and arranging them around the legitimate receiver, which make contributions to reduce key leakage and improve security.

1. Introduction

Nowadays, wireless networks have been widely used in civilian and military applications for transmission of important/private information, such as credit card information, energy pricing, e-health data, command, and control messages. Therefore, security is a critical issue for future wireless networks\cite{1}. Conventional methods of generating and distributing secret keys may suffer from complexity and high computational cost\cite{2}, so new alternative security approaches are issued from information theory fundamentals and focus on the secrecy capacity of the propagation channel, which is referred as physical layer security.

The advantages of employing physical layer security techniques for wireless networks are on two aspects. First of all, different from the security of computation-based cryptography techniques, physical layer security based on channel characteristics is not easy to be compromised by eavesdroppers with sufficient computational capacities; second, the structures of future wireless networks, such as 5G, IoT and WSN, are usually decentralized, which imply network topology changes frequently on account of devices may randomly connect in or leave the network at any instant and make it a challenge for cryptographic key distribution and management. However, the physical layer security that encrypts according to the channel state in time has advantages for this, and is able to solve the challenges encountered in the distribution and management of encryption keys. With the deepening of research and implementation, physical layer security can be used to either perform
secure data transmission directly or as an additional level of protection on top of the existing security schemes in future networks.

Based on information theory, a pair of legitimate users can extract a shared secret key by exploiting the inherent randomness of their reciprocal propagation channels. Normally, thanks to the decorrelation between these fading channels and that experienced by a passive eavesdropper, network security can be significantly strengthened.

Figure 1 depicts a scenario where a pair of legitimate users denoted as Alice and Bob attempt to transmit information securely in presence of an eavesdropper named Eve. Public channels with common randomness are measured firstly by both legitimate sides to obtain channel estimations $h_{ba}$ and $h_{ab}$. Then, Alice and Bob quantify the received signals at the same time and quantitative results have a strong correlation due to the reciprocity of wireless channels, so shared secret key bits can be extracted respectively. However, there might be some discrepancies between the keys due to channel noise and time instants deviation, so Alice and Bob exchange information on public channel and use error correction coding schemes to reconcile the inconsistent parts. According to the openness of wireless channel $h_{ba}$ and $h_{ab}$, Eve attains part of the legitimate channel information to eavesdrop on keys and reduce communication security. The amount of relevant legitimate information obtained by the eavesdropper per unit time determines the key leakage rate, so the remaining part is the secure key rate. In this paper, we are interested in calculating the upper bound of the security key rate to evaluate the security at the channel estimation stage.

Wireless channel environment is usually assumed to have sufficient scattering capability, which implies that the fading process between legitimate channel and eavesdropping channel can be regarded as independent. Majority of works consider that Eve gets no side information about the key from her observations of the pilots transmitted by Alice and Bob[3-5]. In this case, the information bits extracted from the estimated legitimate fading channels $h_{ba}$ and $h_{ab}$ can be regarded as the maximum mutual information $I_k$:

$$I_K = I(h_{ba}, h_{ab})$$

However, it often occurs in practical scenarios that scattering environment is not rich or scatterers are clustered with small angular spread rather than being discretely distributed, as was shown in practical 3GPP channel models[6], the spatial correlation is non-negligible. In [7, 8], experiments were conducted in quasi-static environment to evaluate the spatial correlation of the eavesdropper's observations, which confirmed that the correlation exists and even strong when Eve is close to one side. The work of [9] studied the impact of channel spatial correlation on the secret-key capacity in presence of a correlated eavesdropper. In [10], the authors adopt an indoor experimental approach and verify results of cross-correlation, mutual information and secret-key rates are related to the eavesdropper’s position. In principle, part of bits in (1) are no longer secure in account of Eve’s insight into legitimate channels. At this time, the security key bits $I_{SK}$ can be extracted from the mutual information of Alice and Bob under the observation of Eve:
In [11], the impact of the number of paths and the eavesdropper separation was analytically studied. Besides, it was proved that many of the same multipath components can be seen when Eve is pretty close to Bob in [12]. Literatures show that several authors have tried to make a difference in multipath components by exploiting scatterers. However, scatterers are usually placed in fixed positions or in Jakes model[13], making the results lack sparsity and universality.

In the present work, we propose an improvement on the DISC model centered at Bob in [14] and introduce a circularly symmetric scattering distribution function with two degrees of freedom in [15] to dynamically generate eligible scatterer positions. A more realistic situation in different Eve-Bob distance ranges will be simulated according to adjusting the shape and range of scatterer, then corresponding security level will be evaluated.

The rest of this paper is organized as follows. Section 2 describes the propagation scenario of the disc scattering model and combines it with the scattering distribution function. In Section 3, we provide an assessment of the available key bits in non-fixed areas. Finally, we draw conclusions in Section 4.

2. Geometric disk scattering model and assumptions

To simulate real communication scenarios, we adopt a 2D geometric DISC channel model with Bob as the center. Eve is inside the DISC at a distance $d$ from the center for she needs to be closer to one of the legitimate nodes than the other to obtain stronger spatial correlation. Under normal circumstances, Alice is located outside the DISC and farther away from Bob. The additional scatterers bring distinction to the multipath components seen by Bob and Eve respectively, leading to spatial decorrelation between channels and key leakage. At this point, a basic DISC model with additional scatterers as shown in figure 2 can be established.

![Geometric DISC model for a single-bounce scattering scenario.](image)

In [11], the impact of the number of paths and the eavesdropper separation was analytically studied. Besides, it was proved that many of the same multipath components can be seen when Eve is pretty close to Bob in [12]. Literatures show that several authors have tried to make a difference in multipath components by exploiting scatterers. However, scatterers are usually placed in fixed positions or in Jakes model[13], making the results lack sparsity and universality.

In the present work, we propose an improvement on the DISC model centered at Bob in [14] and introduce a circularly symmetric scattering distribution function with two degrees of freedom in [15] to dynamically generate eligible scatterer positions. A more realistic situation in different Eve-Bob distance ranges will be simulated according to adjusting the shape and range of scatterer, then corresponding security level will be evaluated.

The rest of this paper is organized as follows. Section 2 describes the propagation scenario of the disc scattering model and combines it with the scattering distribution function. In Section 3, we provide an assessment of the available key bits in non-fixed areas. Finally, we draw conclusions in Section 4.

2. Geometric disk scattering model and assumptions

To simulate real communication scenarios, we adopt a 2D geometric DISC channel model with Bob as the center. Eve is inside the DISC at a distance $d$ from the center for she needs to be closer to one of the legitimate nodes than the other to obtain stronger spatial correlation. Under normal circumstances, Alice is located outside the DISC and farther away from Bob. The additional scatterers bring distinction to the multipath components seen by Bob and Eve respectively, leading to spatial decorrelation between channels and key leakage. At this point, a basic DISC model with additional scatterers as shown in figure 2 can be established.

![Geometric DISC model for a single-bounce scattering scenario.](image)

Single omnidirectional antenna is assumed to be equipped with all nodes and its polarization effects are neglected. Taking the high path loss into account, we ignore the component from remote scatterers and assume that the wave emitted from Alice reaches Bob after being single bounced by one of the scatterers inside the model. Every scatterer is independent and regarded as an omnidirectional lossless transponder for both Bob and Eve, which means that legitimate signal undergoes equal attenuation after refracted by same scatterer.

Different from the common methods of fixing the scatterers uniformly, we introduces a scatterer distribution model of vehicular communication networks in [15], which summarizes a new probability density function in Cartesian coordinates to fit the distribution of local scatterers positions in real scenes as follows:

$$I_{sk} = I(h_{sk} | h_{sn}, h_{sm})$$ (2)
In the equation above, local scatterers are distributed within a disk of radius $R$, which determines the location range. On the basis of radius $R$, a new additional degree of freedom $k$ named shape factor is introduced. Shape factor $k$ is a real value greater than -1 and controls the distribution of the scatterers within the model proposed in figure 2. It has been proved that the model with two degrees of freedom is able to be accurately curve-fitting to some empirical data and established scattering models, such as Uniform Circular, Hollow-DISC, Ring Clarke and Gaussian. The term $2\pi$ clarifies the fact that the angle-of-arrival is uniformly distributed between $-\pi$ and $\pi$, other constant terms ensure the unity of area and cumulative distribution function.

In terms of narrowband communication, multipath components with different delays can be superimposed rather than causing interference, so Turin model is suitable to describe the narrowband complex channel gain between Alice and Bob / Eve as follows:

$$h_{ab/e} = \sum_{i=1}^{N_s} \frac{\beta_i}{d_i} \exp[j(2\pi f_c \tau_i + \phi_i)]$$

(4)

In equation (4), we number a total of $N_s$ scatterers within radius $R$ from 1 to $N_s$. Assuming that scattering coefficient of the $i$th scatterer is $\beta_i$, following Rayleigh Scattering and distance $d_i$ can be obtained according to the coordinates of Bob/Eve and the $i$th scatterer. During the time delay $\tau_i$, Bob/Eve receives a plane wave vector from Alice after being directionally reflected by the $i$th scatterer. Phase shift of incoming wave in free space is determined by the time delay $\tau_i$, and additional phase shift of multipath channel is related to direction of incoming wave and position vector of the $i$th scatterer.

Since Bob and Eve are fixed at a relatively close distance, the channel between Bob to Eve is obviously different from the result observed by Alice and can be regarded as independent, therefore the secret key evaluated in (2) is simplified as:

$$I_{SK} = I(h_{ab}, h_{in} | h_{me})$$

(5)

Multipath components in narrowband communication are superimposed after single-bounce reflection from scatterers, making the channel in this multipath environment could be approximated by complex Gaussian distribution, so mutual information can be simplified based on the covariance matrix of the channel observations:

$$I_K = I(h_{ab}, h_{in}) = \log_2 \frac{|R_{aa}| |R_{bb}|}{|R_{ab}|^2}$$

(6)

$$I_{SK} = I(h_{ab}, h_{in} | h_{me}) = \log_2 \frac{|R_{aa}| |R_{bb}|}{|R_{ab}|^2 |R_{ee}|^2 |R_{ae}|}$$

(7)

where covariance matrix $R_{xy} = E\{h_x h_y^*\}$ and $R_{XY-Z} = E\{[h_x h_y^* \cdots h_z h_y^*] [h_x h_y^* \cdots h_z h_y^*]^*\}$.

The presence of the tapping channel makes $I_{SK}$ smaller than the key capacity $I_K$, the difference is the vulnerability key bits defined as $I_{VK}$:

$$I_{VK} = I_K - I_{SK}$$

(8)

It is the best option for Eve to be a passive attacker to conceal herself, so she obtains $I_{VK}$ according to wiretapping instead of interfering the legitimate fading channel.
3. Secrecy evaluation

Both $I_K$ and $I_{SK}$ are statistical values affected by different channel implementations. In each implementation, formula (2) is used to generate various eligible scatterers with corresponding scattering coefficient, which is regarded as the same cost for Bob and Eve. Then average $I_K$ and $I_{SK}$ values are calculated over various simulation implementations. Parameters are shown in table 1.

Table 1. Simulation parameters.

| Parameters                           | Values               |
|--------------------------------------|----------------------|
| Carrier frequency $f_c$              | 2 GHz                |
| Disc radius $R$                      | $100 \lambda$        |
| Shape factor $k$                     | 0, 3, 8              |
| SNR                                  | 15 dB                |
| Eavesdropper separation distance $d$ | $0.1$ to $100 \lambda$ |
| Scatterers number $N_S$              | 10                   |
| Footer                               | $100 \lambda$        |

Under simulation process, the location of scatterers should be determined at the beginning of the modeling. According to the adjustment of parameters $k$ and $R$, several scattergrams with 5000 points are depicted in figure 3 for better visualizations. Figure 3(a) shows the distribution of random scatterers generated where the shape factor $k$ is set to 0. In this case, equation (3) is related to the first moment of distance, leading scatterers to be uniformly distributed on x-axis and y-axis respectively. When $k=1$, the probability density function becomes a constant, and scatterers are two-dimensional uniform distribution on the circular area. With $k$ increasing, scatterers gradually approach the edge of circle and eventually become a ring distribution when $k$ is large enough.

![Figure 3. Scatter diagram illustrating with different shape factor values.](image)

Since usual researches tend to fix the scatterers in even distance, we take $k=0$ as an example to study and consider comparison between channel correlations and relative vulnerable bits in various number of scatters, the results are shown in figure 4. Thanks to the difference in the multipath components provided by scatterers, better spatial decorrelation and higher security can be obtained according to the increase in scatterers number. However, the additional effects tend to be easing for the rise in the number leads to stable sum.
Figure 4. Channel correlations and relative vulnerable bits in various scatterers numbers.

Relative vulnerable bits are positively correlated with correlation coefficient, both decrease when Eve approaches the border of DISC because of the spatial decorrelation. The separation of Eve to Bob also changes the relative position between Eve and scatterer, which means distribution of the scatterers may also affect the correlation and relative vulnerable bits. We experiment with different shape factors in $N_s=10$ and get the results as shown in figure 5.

Figure 5. Channel correlations in different shape factor values.

Figure 5 shows that correlation is negatively correlated with the increase of shape factor $k$, because larger shape factor makes scatterers closer to the edge, then smaller differences are brought to Bob and Eve. Based on this idea, we explore the impact of adjusting another degree of freedom $R$ and get the result shown in figure 6.
In figure 6, the correlation and relative vulnerable bits are reduced with the decrease of DISC radius, because in this case scatterers are more likely to distribute near Bob, providing components with greater differences and improving security.

4. Conclusion

In this paper, we proposed an evaluation of key capacity through a DISC channel model and scatterer distribution function. Any distance between Bob and Eve within the model can be considered and is thus not limited to a stationarity region. We use various values of shape factor and distribution radius of scatterer as well as different eavesdropper separation distances to evaluate channel correlation and relative vulnerable bits. Simulation results show that better security can be achieved according to increasing the number of scatterers or placing them around Bob, both of which make contributions to fading channel richness.

Acknowledgments

This work was supported in part by the National Natural Science Foundation of China (Grant No. 61871290) and Shanghai Sailing Program (Grant No. 19YF1451500).

References

[1] Wu, Y., Khisti, A., Xiao, C., Caire, G., Wong, K. K., Gao, X. (2018) A survey of physical layer security techniques for 5g wireless networks and challenges ahead. IEEE Journal on Selected Areas in Communications, 36: 679-695.

[2] Aono, T., Higuchi, K., Ohira, T., Komiyama, B., Sasaoka, H. (2005) Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels. IEEE Transactions on Antennas and Propagation, 53: 3776-3784.

[3] Ye, C., Mathur, S., Reznik, A., Shah, Y., Trappe, W., Mandayam, N.B. (2010) Information-theoretically secret key generation for fading wireless channels. IEEE Transactions on Information Forensics and Security, 5: 240-254.

[4] Chen, C., Jensen, M.A. (2011) Secret key establishment using temporally and spatially correlated wireless channel coefficients. IEEE Transactions on Mobile Computing, 10: 205-215.

[5] Jorswieck, E.A., Wolf, A., Engelmann, S. (2014) Secret key generation from reciprocal spatially correlated MIMO channels. In: IEEE Globecom Workshops. Atlanta. pp. 1245-1250.
[6] Rottenberg, F., Doncker, P.D., Horlin, F., Louveaux, J. (2020) Impact of realistic propagation conditions on reciprocity-based secret-key capacity. In: IEEE 31st Annual International Symposium on Personal, Indoor and Mobile Radio Communication. London. pp. 721-727.

[7] Pierrot, A.J., Chou, R.A., Bloch, M.R. (2013) Experimental aspects of secret key generation in indoor wireless environments. In: IEEE 14th Workshop on Signal Processing Advances in Wireless Communications. Darmstadt. pp. 669-673.

[8] Chou, T.H., Draper, S.C., Sayeed, A.M. (2010) Impact of channel sparsity and correlated eavesdropping on secret key generation from multipath channel randomness. In: IEEE International Symposium on Information Theory-Proceedings. Austin. pp. 2518-2522.

[9] Prabhu, V.U., Rodrigues, M.R.D. (2011) On wireless channels with -antenna eavesdroppers: characterization of the outage probability and outage secrecy capacity. IEEE Transactions on Information Forensics and Security, 6: 853-860.

[10] Zenger, C., Vogt, H., Zimmer, J., Sezgin, A., Paar, C. (2016) The passive eavesdropper affects my channel: secret-key rates under real-world conditions. In: IEEE Globecom Workshops. Washington. pp. 54-60.

[11] Wallace, J.W., Chen, C.C.C., Jensen, M.A. (2009) Key generation exploiting MIMO channel evolution: Algorithms and theoretical limits. In: European Conference on Antennas and Propagation. Berlin. pp. 1499–1503.

[12] Wallace, J.W., Sharma, R.K. (2010) Automatic secret keys from reciprocal MIMO wireless channels: measurement and analysis. IEEE Transactions on Information Forensics and Security, 5: 381-392.

[13] Zhang, J., He, B., Duong, T.Q., Woods, R. (2017) On the key generation from correlated wireless channels. IEEE Communications Letters, 21: 961-964.

[14] Mazloum, T., Mani, F., Sibille, A. (2014) A disc of scatterers-based radio channel model for secure key generation. In: European Conference on Antennas and Propagation. The Hague. pp. 1290-1294.

[15] Borhani, A., Patzold, M. (2013) A unified disk scattering model and its angle-of-departure and time-of-arrival statistics. IEEE Transactions on Vehicular Technology, 62: 473-485.