Characterization of Secrecy Capacity of Time Reversal Technique for Wireless Physical Layer Security

Hassan El-Sallabi and Abdulaziz Aldosari
Department of Technical Affairs, QAF
Qatar

Abstract—**Secrecy capacity with time reversal technique is characterized and investigated for both specular and dense diffuse scattering radio channels. The characterization of secrecy capacity of specular radio channel is conducted for two clustered channels with 6 and 60 clusters that are composed of 120 and 1200 rays, respectively. Diffuse scattering channels are tested under different delay spread values. The investigation addresses the behavior in increasing the secrecy capacity with SNR. The increase in secrecy capacity with SNR saturates at particular values of SNR for specular channels but that is not the case with diffuse radio channels. The SNR saturation threshold varies with number of multipath components in specular channels.**

I. Introduction

Governments have become more and more dependent on data that is created and/or collected to extract information out of it. So, the illegitimate access to this data and extracted information are highly important concern. Information security for government, military, banks, etc is a very crucial issue in wireless communication systems. In communications systems, the upper network layers of the protocol stack manage issues related to authentication, privacy, etc, using private-key and public-key cryptosystem. Huge effort has been placed to accomplish this mission but challenges are still being faced and need to be tackled. Different techniques have been applied in different network layers [1]. For instance, based on some assumption, data encryption and decryption algorithms have been applied in application layer. The assumption that the eavesdroppers have limited computational resources may not be valid due development of efficient algorithms that can be used to break the encryption/decryption algorithms with increased power of modern computers.

The upper layers-specific security protocol ignore the most fundamental layer in wireless communications. Wireless devices communicate via wireless channels through encoding and modulation of information data to waveforms. Wireless channels lack physical boundaries. Any nearby receiver may listen to transmitted signals or may jam transmission. Hence, wireless communications systems are security vulnerable [2],[3]. It is very important by design to guarantee wireless transmission with low probability of intercept (LPI) and do not depend on upper layer encryption and secret keys. Spread spectrum technology is the most widely known for LPI but due to increasing bandwidth of wireless communications leads to reduction in spread processing gain [4] in addition to possibility of estimation of spreading codes [5]. Some work has appeared in literature based on antenna array, channel diversity, and channel deconvolution [6-8]. Research results from information theory, signal processing and cryptography showed that much security can be obtained from imperfect wireless channel conditions [9]. Physical layer security is of increasing interest [10],[11]. It is focused on exploiting random nature and reciprocity of wireless channel with no assumption of computational capability of eavesdroppers. These features can be used to generate secure keys against eavesdropping. It should be noted that the proposed procedure applies for slow fading channels, when the propagation delays, processing delay at Rx for channel state estimation and processing delay at Tx to construct a pulse shaping is less than coherence time of the channel.

II. Background on Time Reversal Technique

Recent research on wireless information security has focused on physical layer properties, [12],[13]. One of the main ideas is to obtain highly position specific channel properties between transmitter and receiver to generate spatial and temporal variant secret keys to secure information transmission, *i.e.,* time reversal technique. Time reversal technique is based on utilizing the dense multipath random channel. The time reversal technology has the capability to focus energy both in time and spatial domains [14],[15]. This energy harvesting may have an important role in high spatial resolution that secures data transmission between transmitter and intended receiver and become very difficult for eavesdropper. The idea is based on fact that each receiver including the eavesdropper has a unique spatial and temporal channel impulse relative to the position of the transmitter. This is reflected in terms of azimuth and elevation angle of arrivals of multipath components as well

`

their delays and amplitudes. The bandwidth of the system has an important role in resolving the multipath components for proper design of radio receiver.

The concept of time reversal is based on utilizing the invariance of wave equation under time reversal. For lossless media the wave equation is given as [16]

$$\nabla^2 \bar{E}(\bar{r},t) - \mu(\bar{r})\epsilon(\bar{r})\frac{\partial^2}{\partial t^2}\bar{E}(\bar{r},t) = 0$$

where $\bar{E}(\bar{r},t)$ is the vector electric field in space and time is the solution of the wave equation, the time reversal of it $\bar{E}(\bar{r},-t)$ is also a solution to the same wave equation, $\bar{r} = \hat{x}x + \hat{y}y + \hat{z}z$ is the spatial vector position, the medium is characterized by μ and ϵ. This wave equation says that for every electromagnetic wave diverges away from a source, there is an exact reversed electromagnetic wave from destination follows precisely the path back to the source. For a communication system perspective, if the source has *M* transmit antennas and receiver has *N* receive antennas, the impulse response at time *t* from antenna at $\overline{r_m}$ to receive antenna at $\overline{r_n}$ is $h_{n,m}(t,\tau,\ \overline{r_m} \rightarrow \overline{r_n})$, with τ denoting the delay of multipath components of impulse response. The channel impulse response is estimated at receiver and time reversed and sent back to the transmitter [15]. The time-reversed complex conjugate of the estimated impulse response is applied as precoding filter g(t) at transmitter side, is applied, which can be written as

$$g_m(t;\tau) = K \cdot h^*_{n,m}(t,-\tau,\overline{r_m} \rightarrow \overline{r_n})$$

where *K* is a power normalization factor and $*$ denotes complex conjugate. The received signal $y_{n,m}(t)$ can be written as

$$y_{n,m}(t) = h_{n,m}(t,\tau,\overline{r_m} \rightarrow \overline{r_n}) \otimes g_m(t;\tau) \otimes x(t) + n(t)$$

where $x(t)$ is the input transmitted signal, $n(t)$ is receiver additive noise, $\otimes$ denotes the convolution operator. During coherence time of the channel, the equivalent impulse response from transmit antenna m to receive antenna n can be written as [15]

$$h^{eq}_{n,m}(t,\tau,\overline{r_m} \rightarrow \overline{r_n}) = h_{n,m}(t,\tau,\overline{r_m} \rightarrow \overline{r_n}) \otimes h^*_{n,m}(t,-\tau,\overline{r_m} \rightarrow \overline{r_n})$$

which is the autocorrelation function of channel impulse response $h_{n,m}(t,\tau,\overline{r_m} \rightarrow \overline{r_n})$. This autocorrelation function indicates that, in time domain, the energy is compressed at the center of the $h^{eq}_{n,m}$ and very low power elsewhere.

III. System Model

Security of wireless networks can be classified into mainly two major aspects that are referred to active attack and passive attack. The first is related to intrusion with faked authentication or network sabotage via malicious jamming. Passive attack is also referred as eavesdropping. Its aim is to break secure communications and acquire private communications. This is the more common threat. Physical layer security research focuses on preventing eavesdropping to ensure secure communications. The active attack problem is studied under physical layer authentication. Figure 1 shows system level scenario of legitimate channel between transmitter (Alice) and receiver (Bob) and illegitimate channel between transmitter and eavesdropper (Eve) [11]. Eve does not make any active attack but passively tries to extract information from transmission between Alice and Bob.

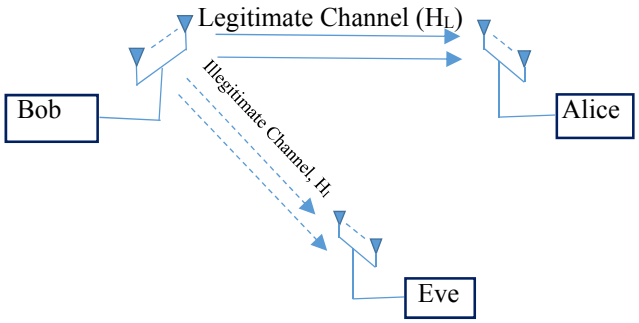


Figure 1. System model.

The received signal at the intended receiver (Bob), $\mathbf{Y_L}$, is given by

$$\mathbf{Y_L} = \mathbf{H_L X} + \mathbf{n_L}$$

$\mathbf{X}$ is the matrix of transmitted signals, $\mathbf{n_L}$ is the matrix of additive Gaussian noise at legitimate receiver (Bob), $\mathbf{H_L}$ is the matrix of impulse response between transmitter (Alice) antenna and legitimate receiver (Bob) antenna and is given by

$$\mathbf{H_L} = \begin{bmatrix} h_{11} & h_{12} & \cdots & h_{1M} \\ h_{21} & h_{22} & \cdots & h_{2M} \\ \vdots & \vdots & \ddots & \vdots \\ h_{N1} & h_{N2} & \cdots & h_{NM} \end{bmatrix}$$

The impulse response between transmit antenna m and receive antenna n can be represented as diffuse scattering channel or multipath specular channel. The diffuse is given as

$$h_{nm}(t) = \sum_{q=0}^{Q-1} \alpha_q^{nm} \delta\left(t - \tau_q^{nm}\right)$$

where Q is very large number represent of multipath diffuse components, α_q^{nm} and τ_q^{nm} are the amplitude and delay of multipath diffuse component q between transmit antenna m and

receive antenna n. The delay of diffuse component is even distribution in all slots of excess delay domain, i.e., the delay domain is filled up of multipath energy due to diffuse phenomena. The amplitude of multipath component q follows a Rayleigh statistical distribution, whose probability density function is

$$f_{\alpha_q}(x) = \frac{x}{\sigma_q^2} e^{\frac{-x^2}{2\sigma_q^2}}, \quad 0 \le q \le Q-1$$

where σ is the scale parameter of the distribution. For specular channel, the adopted channel model in this work is the spatial channel model (SCM) model [17]. It is multi-cluster model of each cluster has constant delay with angular spread of arrivals and departure. Each cluster represents a resolvable multipath in delay domain and the within multipath are called subpaths. The impulse response of each cluster path can be written as

$$h_{u,s,n}(t) = \sqrt{\frac{P_n \sigma_{SF}}{M}} \times \sum_{m=1}^{M} \begin{pmatrix} \sqrt{G_{BS}(\theta_{n,m,AoD})} \exp\left(j\left[kd_s \sin(\theta_{n,m,AoD}) + \Phi_{n,m}\right]\right) \times \\ \sqrt{G_{MS}(\theta_{n,m,AoA})} \exp\left(jkd_u \sin(\theta_{n,m,AoA})\right) \times \\ \exp\left(jk\|\mathbf{v}\| \cos\left(\theta_{n,m,AoA} - \theta_v\right) t\right) \end{pmatrix}$$

The details and definitions of parameters can be traced in [17].

IV. Secrecy Capacity

In wireless networks, secrecy is as important feature as capacity. The relationship of secrecy and channel capacity in a networking system was examined by Wyner [18] for wire-tap channel model. This work has been extended for more sophisticated channels and scenarios in literature. Large amount of works has been published focusing on designing physical layer security. In scenario of secure transmission based time reversal technique during existence of eavesdroppers, the channel properties can be exploited to maximize the channel capacity to legitimate users and minimize the channel capacity to illegitimate transmission. The security maximization can be reached by maximizing the secrecy capacity [19],[20]. Secrecy capacity characterizes a system in terms of maximum transmission rate for achieved perfect transmission. Wireless channels are unbounded and hence there is no guarantee that the eavesdropper has worse channel. If the eavesdropper channel is better than the intended receiver, the secrecy capacity zero. The design of wireless communications system for secure communications should take into account such cases where the eavesdropper has better radio channel. This where the physical layer security plays a role to obtain non-zero secrecy capacity. For single channel scenario of legitimate receiver (Bob) channel impulse response, i.e., h_L, and illegitimate receiver channel, i.e., h_I, the secrecy capacity can be computed as

$$C_s = C_L - C_I = max(\log_2(1 + SNR_L|h_L|^2) - \log_2(1 + SNR_I|h_I|^2), 0)$$

where SNR_L and SNR_I are the signal to noise ratios at legitimate and illegitimate receivers. The implicit assumption of iid noise is made between Alice and Eve Rx. For the case of MIMO channel, the channel capacity of MIMO system for intended legitimate user (Bob) can be calculated with

$$C_L = \log_2\left(\det\left(\mathbf{I}_N + \frac{SNR_L}{N_t}\mathbf{H}_L^H\mathbf{H}_L\right)\right)$$

The superscript H denotes complex conjugate transpose of matrix $\mathbf{H}_L$ transmitter (Alice) and legitimate receiver (Bob). The channel capacity of MIMO system at the eavesdropper is given as

$$C_I = \log_2\left(\det\left(\mathbf{I}_N + \frac{SNR_I}{N_I}\mathbf{H}_I^H\mathbf{H}_I\right)\right)$$

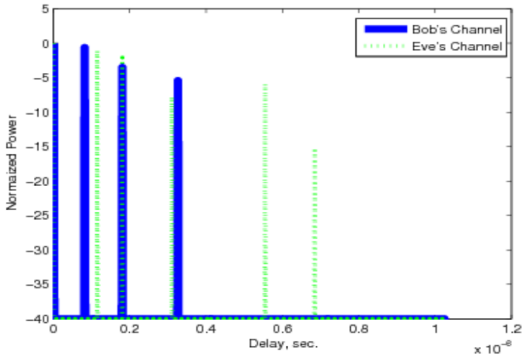
$\mathbf{H}_I$ is the channel matrix between transmitter (Alice) and eavesdropper receiver (Eve). The approximate distribution of MIMO capacity of fading channel can be traced in [21].

V. Numerical Results

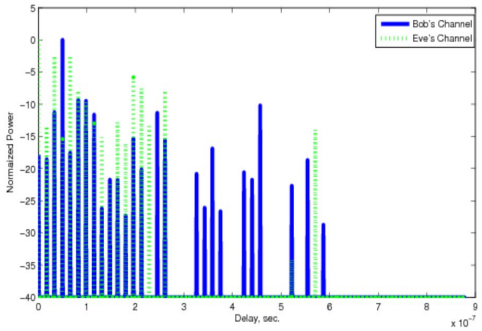
A simulation environment has been built to investigate the time reversal performance on secrecy capacity under both specular and diffuse radio channels. The specular channel is multi-path countable paths channels. The simulation results are for both single input single output (SISO) and MIMO communication systems. The specular channels have been simulated with SCM MIMO channels with urban microcellular propagation environment, which can be used for SISO channel. The simulated number of clusters are 6 and 60, where each cluster has 20 subpaths. This leads to 120 and 1200 rays channels. The operating frequency is 2 GHz. The simulated sample density is 2 samples per half-wavelength. The MIMO channel is 2x2 scenario with element spacing of half-wavelength. Large number of power delay profiles have been generated. Figure 2 shows samples of specular power delay profiles for both intended receiver, which is Bob's power delay profile channel and eavesdropper's power delay profile. The impulse response of the Bob's radio channel is sent back to the transmitter and used its conjugate time reversal as precoding filter in transmitter side. This is the key part in time reversal physical security. The function of the filter is to compress the signal in time domain for Bob's receiver and spread the signal in time domain at Eve's

`

receiver. Compressing the signal will boost the SNR at Bob's receiver and minimize the SNR at the Eve's receiver. This shown in Figure 3. It is clear that the side that multipath components around the center compressed energy is less for the case when there are 60 cluster for both Bob's and Eve's channel. This makes the time location of compressed energy is the major energy temporal power to Bob's channel and minimum to Eve's channel in addition to minimizing the inter-symbol interference. The secrecy capacity for both SISO and MIMO systems based in time reversal technique is shown Figure 4. It is clear that the case of radio channel that has more clusters (i.e., 60 clusters) leads to more secrecy capacity as SNR increases. It can be noticed that there is a saturation limit to increase in secrecy capacity. The saturation limit to SISO channel of 6 clusters is at around SNR = 20 dB, then, there is no more noticeable increase in secrecy capacity. The similar trend can be observed for case of specular radio channel of 60 clusters but the saturation is at around SNR = 30 dB. The MIMO channel clearly shows better secrecy capacity in both specular radio channels. The saturation behavior is also observable for MIMO specular channel. Figure 5 shows sample of diffuse radio channels for both Bob's (blue) and Eve's (red) radio channels for three different values of root mean square (RMS) delay spread. The diffuse radio channel have extremely large number of multipath components that makes spatial energy focusing and temporal energy compression very efficient. This adds significance to physical layer security based on time reversal technique. The secrecy capacity for SISO diffuse radio channels is shown in Figure 6 for different values of RMS delay spread. It is clear that the higher the RMS delay spread the higher increase in secrecy capacity. This is due to characteristics of time reversal technique, which performs better higher RMS delay spread. Furthermore, the diffuse radio channel shows no saturation in secrecy capacity increase.

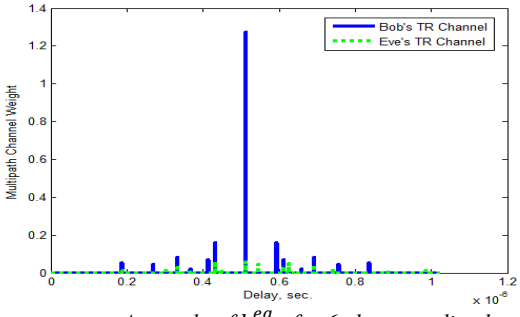


a. A Sample of 6 Cluster Specular Channel.

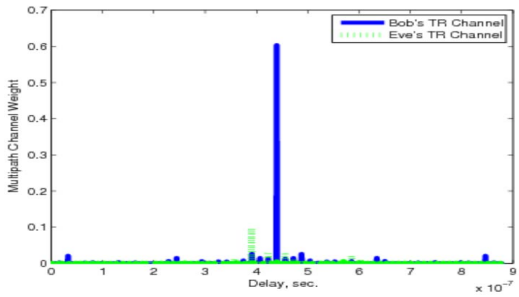


b. A Sample of 60 Cluster Specular Channel.

Figure 2. Samples of power delay profiles for specular channel of 6 and 60 rays for both Bob's and Eve's radio channels.



a. A sample of $h_{n,m}^{eq}$ for 6 cluster radio channel.



b. A sample of $h_{n,m}^{eq}$ for 60 cluster radio channel.

Figure 3. Samples of PDP with Bob's time reversal physical security for both 6 and 60 specular channels.

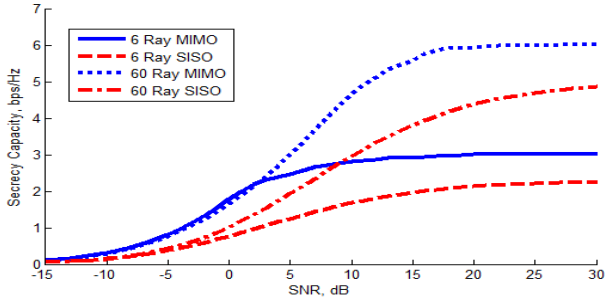


Figure 4. Secrecy capacity of specular channel.

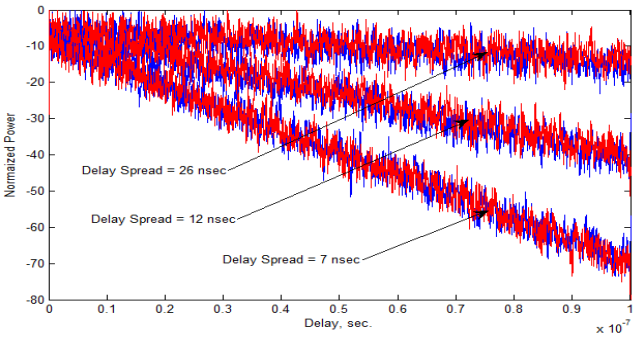


Figure 5. Power delay profiles of dense diffuse channels. Blue for Bob's channel and red for Eve's channel.

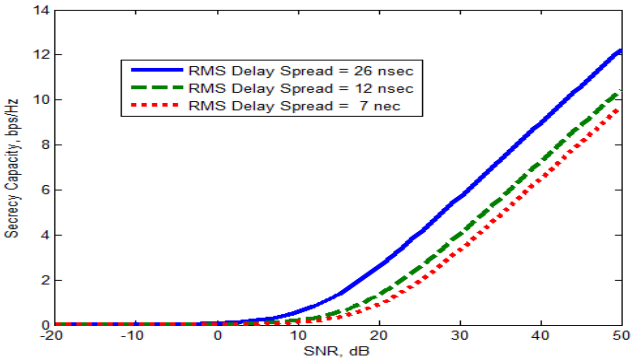


Figure 6. Secrecy capacity of diffuse channels.

VI. Conclusion

This work presented characterization of secrecy capacity based on time reversal technique for physical layer security. The characterization is based on two types of radio channels: 1) Specular channels, 2) Diffuse channels. The specular channels are simulated for both 6 radio clusters (120 rays) and 60 clusters (1200 rays). The diffuse channel is simulated as a very dense multipath channel. It has been observed that the specular channel reach some threshold SNR values in increasing secrecy capacity. This SNR threshold depends on number of clusters and their rays in specular channels. After this SNR threshold, the increase in secrecy capacity is not noticeable. However, this threshold in SNR for increase in secrecy capacity is not observed in diffuse radio channels. The relationship is linear after the kickoff increase with SNR starts, which is around SNR = 10 dB. The kickoff increase in secrecy capacity for specular channel is much lower than that of diffuse channel, i.e., around SNR = - 10 dB.

`

References:

[1] H. Bidgoli, *Handbook of Information Security, Threats, Vulnerabilities, prevention, Detection and Management,* vol. 3, John Wiley, 2006.

[2] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: a survey," *IEEE communications Surveys and Tutorials*, vol. 16, no. 3, pp. 1550–1573, 2014.

[3] Y. Liang, H. V. Poor, and S. Shamai, ''Secure communication over fading channels,'' *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2470–2492, Jun. 2008.

[4] Y. Hwang and H. C. Papadopoulos, "Physical-layer secrecy in AWGN via a class of chaotic DS/SS systems: analysis and design," *IEEE Trans. Signal Processing*, vol. 52, no. 9, pp. 2637-2649, Sept. 2004.

[5] M. J. Mihaljevic and J. D. Golic, "Convergence of a Bayesian iterative error-correction procedure on a noisy shift register sequence," in *Advances in Cryptology*, vol. 658, pp. 124-137, Berlin, Germany: Springer-Verlag, 1993.

[6] X. Li, M. Chen and P. Ratazzi, "A randomized spacetime transmission scheme for secret-key agreement," *CISS'2005*, Johns Hopkins University, Mar. 2005.

[7] X. Li, M. Chen and E. P. Ratazzi, "Array-transmission based physical-layer security techniques for wireless sensor networks," *the 2005 IEEE Int. Conf. on Mechatronics and Automation (IEEE ICMA'2005)*, Niagara Falls, Ontario, Canada, July 2005.

[8] X. Li, J. Hwu and E. P. Ratazzi, "Array redundancy and diversity for wireless transmissions with low probability of interception," *ICASSP'2006*, Toulouse, France, May 2006.

[9] M. Bloch and J. Barros, *Physical-Layer Security: from Information Theory to Security Engineering*, 2011, Cambridge University Press

[10] R. Bassily, E. Ekrem, X. He et al., "Cooperative security at the physical layer: a summary of recent advances," IEEE Signal Processing Magazine, vol. 30, no. 5, pp. 16–28, 2013.

[11] A. Yener and S. Ulukus, "Wireless physical-layer security: lessons learned from information theory,"Proceedings of the IEEE, vol. 103, no. 10, pp. 1814–1825, 2015.

[12] R. Liu and W. Trappe, *Securing Wireless Communications at the Physical Layer*, 2010, Springer

[13] F. Renna, N. Laurenti and H. V. Poor, "Physical-layer secrecy for OFDM transmissions over fading channels", *IEEE Trans. Inf. Forens. Security*, vol. 7, no. 4, pp. 1354-1367, 2012.

[14] Xiao, S., J. Chen, X. Liu, and B.-Z. Wang, "Spatial focusing characteristics of time reversal UWB pulse transmission with different antenna arrays," *Progress In Electromagnetics Research B*, Vol. 2, 223-232, 2008.

[15] H. El-Sallabi, P. Kyritsi, A. Paulraj, and G. Papanicolaou, "Experimental Investigation on Time Reversal Precoding for Space Time Focusing in Wireless Communications," IEEE Trans. Instr. Measur., vol. 59, no. 6, pp. 1537–1543, 2010.

[16] M. E. Yavuz and F. L. Teixeira, "Ultrawideband Microwave Sensing and Imaging Using Time-Reversal Techniques: A Review," Remote Sensing 1(3), Sep. 2009.

[17] 3rd Generation Partnership Project (3GPP), "Spatial channel model for multiple input multiple output (MIMO) simulations (3gpp tr 25.996 version 6.1.0 release 6)," ETSI, Tech. Rep., 2003.

[18] A.D. Wyner. The Wire-Tap Channel. The Bell System Technical Journal, 1975

[19] P. K. Gopala, L. Lai and H. El-Gamal, "On the secrecy capacity of fading channels", *Proc. IEEE Int. Symp. Information Theory*, pp. 1306-1310, 2007.

[20] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels", *Proc. IEEE Int. Symp. Information Theory*, pp. 356-360, 2006.

[21] J. Salo, P. Suvikunnas, H. El-Sallabi and P. Vainikainen, "Approximate distribution of capacity of Rayleigh fading MIMO channels", Electron. Lett., vol. 40, no. 12, pp. 741-742, 2004.