Hindawi Publishing Corporation
EURASIP Journal on Wireless Communications and Networking
Volume 2011, Article ID 628747, 7 pages
doi:10.1155/2011/628747

Research Article

Wireless Information-Theoretic Security in an Outdoor Topology with Obstacles: Theoretical Analysis and Experimental Measurements

Theofilos Chrysikos,[1] Tasos Dagiuklas,[2] and Stavros Kotsopoulos[1]

[1] *Department of Electrical and Computer Engineering, University of Patras, 26500 Rio Patras, Greece*
[2] *Department of Telecommunication Systems and Networks, TEI of Messolonghi, 30300 Nafpaktos, Greece*

Correspondence should be addressed to Theofilos Chrysikos, txrysiko@ece.upatras.gr

Received 15 June 2010; Accepted 20 August 2010

Academic Editor: Christos Verikoukis

This paper presents a Wireless Information-Theoretic Security (WITS) scheme, which has been recently introduced as a robust physical layer-based security solution, especially for infrastructureless networks. An autonomic network of moving users was implemented via 802.11n nodes of an ad hoc network for an outdoor topology with obstacles. Obstructed-Line-of-Sight (OLOS) and Non-Line-of-Sight (NLOS) propagation scenarios were examined. Low-speed user movement was considered, so that Doppler spread could be discarded. A transmitter and a legitimate receiver exchanged information in the presence of a moving eavesdropper. Average Signal-to-Noise Ratio (SNR) values were acquired for both the main and the wiretap channel, and the Probability of Nonzero Secrecy Capacity was calculated based on theoretical formula. Experimental results validate theoretical findings stressing the importance of user location and mobility schemes on the robustness of Wireless Information-Theoretic Security and call for further theoretical analysis.

1. Introduction

Security has maintained, over the last decades, a key role in wireless communications. Recent published works have renewed the interest of researchers for physical layer-based security, formulating the Wireless Information-Theoretic Security (WITS) concept, opening the way for fruitful advances in both academia and industry. Wireless Information-Theoretic Security suggests that perfect secrecy [1] in wireless communication between a transmitter and a legitimate receiver in the presence of an eavesdropper (passive intruder) is achievable even when the average Signal-to-Noise Ratio (SNR) of the main channel (established between the transmitter and the legitimate receiver) is less than the average SNR of the wiretap channel (established between the transmitter and the eavesdropper) if both channels are considered to be characterized by quasistatic Rayleigh fading. Thus, we are able to bypass the limitation of the classic Gaussian wiretap channel model [2–4], according to which the average SNR of the main channel had to be larger than that of the wiretap channel in order to establish Shannon's perfect secrecy.

Wireless Information-Theoretic Security can be implemented as an independent solution for security in wireless networks, or it can function in complementary fashion next to other implemented solutions [5–8]. Wireless Information-Theoretic Security key parameters such as the Probability of Nonzero Secrecy Capacity $P(C_s > 0)$, the Outage Probability $P_{\text{out}}(C_s < R_s) = P_{\text{out}}(R_s)$ for a given target secrecy rate $R_s > 0$, and the Outage Secrecy Capacity $P_{\text{out}}(C_{\text{out}})$ were thoroughly discussed in [9, 10]. Its theoretical findings are extended to include use of LDPC channel coding scheme as a means of opportunistic channel sharing [11, 12]. However, the lack of experimental measurements and empirical results challenged the scheme's reliability and robustness in relation to real-life conditions and actual propagation environments.

In this paper, Wireless Information-Theoretic Security has been determined in autonomic networks by considering

Rayleigh fading channels. Furthermore, a series of experimental measurements were conducted in order to provide a test bed for computation and evaluation of these fundamental metrics of Wireless Information-Theoretic Security, in the scenario of moving users in autonomic networks. An ad hoc network was set up, comprising of autonomic users (laptops connected via 802.11n embedded network adapters) moving in low-speed fashion (thus discarding any possible Doppler spread phenomena). The average SNRs of both main and wiretap channel were acquired via appropriate equipment and the Probability of Nonzero Secrecy Capacity was calculated in order to evaluate WITS in an actual outdoor environment with Obstructed-Line-of-Sight (OLOS) and Non-Line-of-Sight (NLOS) schemes that comply with WITS main and wiretap channel assumptions (Rayleigh fading). The results demonstrated a significant impact of relative user location on the WITS reliability as a physical security solution.

The paper is structured as following. Section 2 presents the concept of Wireless Information-Theoretic Security and discusses its key parameters. Section 3 addresses a user movement scenario and its impact on the key parameters of Wireless Information-Theoretic Security, for a certain mobility model. Section 4 features the measurement topologies and the methodology of the experiment for the aforementioned case study of user movement. In Section 5, the results are discussed whereas Section 6 includes conclusions and, finally, in Section 7 open issues for future work are addressed.

2. Wireless Information-Theoretic Security

The possibility of a Nonzero (strictly positive) secrecy capacity $P(C_s > 0)$ is calculated, for Rayleigh fading channels instead of the classic Gaussian scheme, to be nonzero (strictly positive) even when the average main channel SNR $\overline{\gamma}_M$ is less than the wiretap channel SNR $\overline{\gamma}_W$, albeit with a possibility less than 0.5 [9]:

$$P(C_s > 0) = \frac{\overline{\gamma}_M}{\overline{\gamma}_M + \overline{\gamma}_W}. \tag{1}$$

In [10], the Probability of Nonzero Secrecy Capacity was provided as a function of the path loss exponent n and the distance ratio d_M/d_W, d_M being the distance between the transmitter and the legitimate receiver, and d_W is the distance between the transmitter and the eavesdropper:

$$P(C_s > 0) = \frac{1}{1 + (d_M/d_W)^n}. \tag{2}$$

In [9, 10], a path loss exponent of $n = 3$ was considered, based on an average path loss exponent value estimation in [13]. The channel-dependent variation of the path loss exponent [14–16] in outdoor and indoor environments, depending on the various mechanisms contributing to the signal attenuation, in an obstacle-dense environment, was proven to largely compromise the Wireless Information-Theoretic Security scheme [17], due to the rapid decrease of the Probability of Nonzero Secrecy Capacity. In [18], the closed-form expression for the Outage Secrecy Capacity was provided, allowing for the exact calculation of the maximum achievable secrecy rate for an upper-bound value of Outage Probability. This was accomplished via a Taylor series approximation of the exponential function, which was proven to be reliable for realistic values of the Secrecy Rate.

In [19, 20], the impact of user location (in relation to colluding eavesdropper(s)) on WITS robustness was addressed. However, the user movement was not taken into consideration, especially in a propagation environment with obstacles, a notion that falls into place with fundamental theoretical assumption of quasistatic Rayleigh fading for the WITS scheme. Moreover, the lack of central infrastructure calls for more specific inquiry.

3. Moving Users in Autonomic Network

In [21], the impact of user mobility on the boundaries of secure communications was addressed, in relation to the boundaries of secure communication from a physical layer standpoint. More specifically, the impact of the approaching eavesdropper on the decrease of the Probability of Nonzero Secrecy Capacity and Outage Secrecy Capacity (maximum Secrecy Rate for a given threshold of Outage Probability and a given average SNR for the legitimate receiver) was examined.

The ad hoc nodes employ a mobility model that realistically simulates mission critical situations [22, 23]. Physical obstacles are an indispensable part of the area under study. The destination points are selected by the nodes randomly based on a uniform distribution. Each node can move to every point in the network area as long as it does not reside within the boundaries of an obstacle. When a destination point is chosen, the node moves its way around the obstacles following a recursive procedure. If there is an obstacle in the way, the node sets as its next intermediate destination the vertex of the obstacle's edge directly visible that is closest to the destination and repeats the same process all over again with starting point its initial position and destination the chosen vertex. Otherwise, the node follows this direct line to get to the desired destination.

The Distance Ratio Factor (DRF) was defined as the distance ratio before and after user movement:

$$dR = \left(\frac{d'_M/d'_W}{d_M/d_W}\right) = \frac{d'_M d_W}{d_M d'_W} = \frac{d_W}{d'_W}, \tag{3}$$

where d'_M is the distance between the transmitter and the legitimate receiver after user movement, and d'_W is the distance between the transmitter and the eavesdropper after user movement as well.

A low-speed moving scenario was considered (discarding any chances of Doppler spread effect), where a malicious user is approaching the static transmitter in the presence of an equally static legitimate receiver with a constant velocity u for a time window Δt:

$$d'_W = d_W - u\Delta t. \tag{4}$$

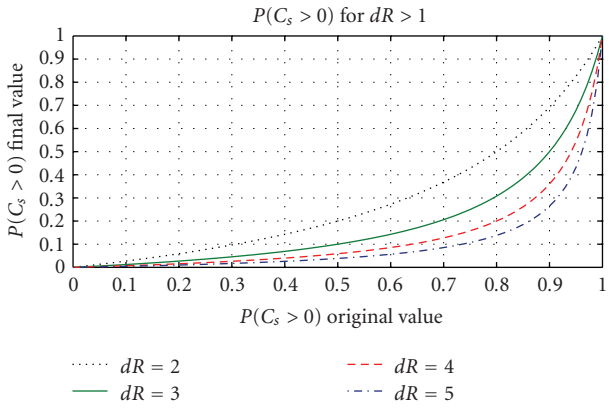

Figure 1: Probability of Nonzero Secrecy Capacity for DRF > 1.

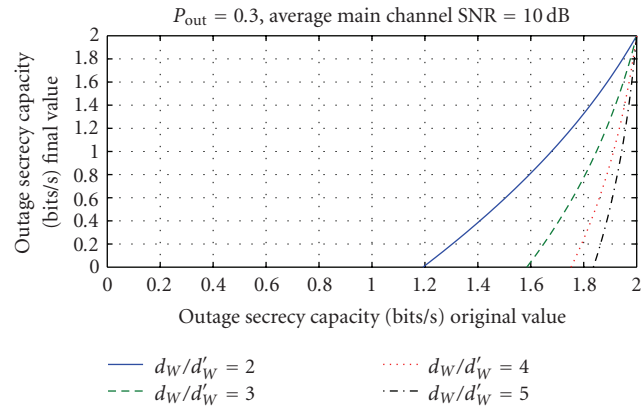

Figure 2: Outage Secrecy Capacity before and after eavesdropper's movement.

The Probability of Nonzero Secrecy Capacity and Outage Secrecy Capacity before and after user movement were expressed in terms of the DRF as

$$\frac{1}{dR} = \frac{d'_W}{d_W} = \sqrt{\frac{(1 - P(C_s > 0))P(C_s > 0)'}{\left(1 - P(C_s > 0)'\right)P(C_s > 0)}},$$

$$C'_{\text{out}}(p) = \log_2\left(\frac{p + 1/\overline{\gamma}_M}{dR^2\left(\left(p + 1/\overline{\gamma}_M\right)/2^{Rs} - 1/\overline{\gamma}_M\right) + 1/\overline{\gamma}_M}\right), \quad (5)$$

where $C'_{\text{out}}(p)$ is the Outage Secrecy Capacity (maximum Secrecy Rate) after user movement, p is the Outage Probability threshold (upper-bound), and R_s is the Secrecy Rate before user movement.

Results proved, as shown in Figure 1, that by reducing the original separation from the transmitter, the eavesdropper can achieve a radical decrease in $P(C_s > 0)$. If the mobility scheme and the user velocity are known, we can calculate the time window in which this decrease is accomplished. The impact of user (eavesdropper) movement on Outage Secrecy Capacity further confirms that if the legitimate receiver remains static, then the Secrecy Rate would require, before the eavesdropper's movement, unrealistically large values so that there will be a marginally nonzero Secrecy Rate after the movement. The results are depicted in Figure 2, where a suboptimal scheme has been considered in terms of Outage Probability (upper-bound at 0.3) and average main channel SNR (10 dB).

The above confirms that eavesdropper's movement towards the transmitter compromises the WITS scheme, as long as the legitimate receiver remains static, and eavesdropper movement does not alter the main channel characteristics. In order to provide measurements for this scenario, a test-bed has been implemented so that realistic values of Probability of Nonzero Secrecy Capacity could be provided for an outdoor environment in the presence of obstacles. The topology and measurements acquisition are described in the following section.

4. Measurements Topology and Acquisition

An autonomic network consisting of three users was set up for the purposes of the experimental measurements. Three laptops equipped with embedded 802.11n wireless adapters created an ad hoc network: the first laptop served as transmitter, the second laptop was the legitimate receiver, and the third laptop was the passive eavesdropper.

Without loss of generality, the total EIRP of transmitting laptop was at 10 dBm. Both receivers (legitimate and eavesdropper) were equipped with the NetStumbler software that provides received power values for any given wireless network (802.11) in range [24]. In our scenario, both the transmitter and the legitimate receiver (quasistatic Rayleigh fading for main channel) were considered to be static, and the eavesdropper is allowed to move, in the presence of obstacles.

All measurements were conducted in the campus of the University of Patras. Three different schemes were considered: two OLOS (Obstructed-Line-of-Sight) case studies, depicted in Figure 3, and one NLOS (Non-Line-of-Sight) scenario, depicted in Figure 4. Since WITS requires quasistatic Rayleigh fading for both main and wiretap channel, no LOS scheme was considered. In all cases, the (low-speed) movement of the eavesdropper (depicted by the dotted line whereas the arrow points the direction of movement) does not have any impact on the main channel characteristics. In Figure 3, T3 and T4 represent transmitter's locations for each OLOS scheme, and all other locations mark legitimate receiver positions. Locations C3 and D3 are in higher ground level than the movement of the eavesdropper (red dotted line) so that the main channel characteristics are not altered.

5. Results and Discussion

Table 1 illustrates the average received power levels and SNR for all legitimate receiver (main channel) locations whereas Table 2 presents the calculated values for the Probability of Nonzero Secrecy Capacity. Average received power values were obtained via the NetStumbler software for both legitimate receiver and eavesdropper.

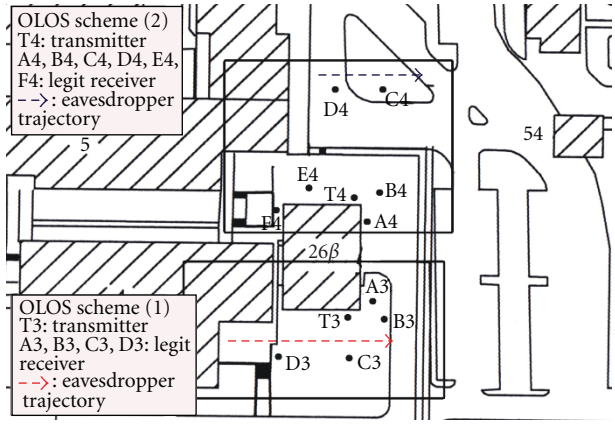

Figure 3: Measurement topology for OLOS schemes.

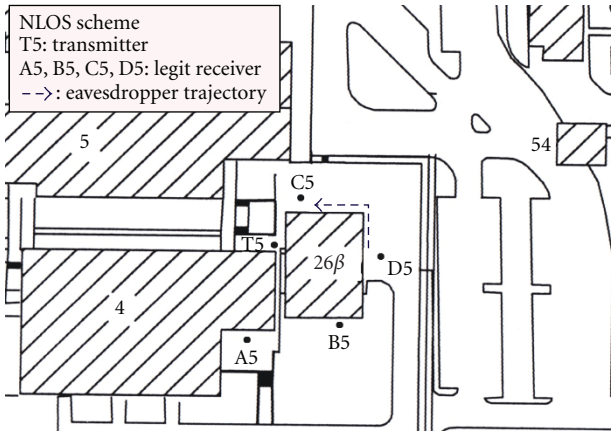

Figure 4: Measurement topology for NLOS scheme.

Table 1: Average received power and SNR for OLOS-1 (T3) scheme.

OLOS T3	Pr (nW)	Pr (dBm)	SNR (dB)
A3 (main)	1,26	−59	26
B3 (main)	0,32	−65	20
C3 (main)	0,03162	−75	10
D3 (main)	0,03162	−75	10
X31 (eaves)	0,00631	−82	3
X32 (eaves)	0,5	−63	22
X33 (eaves)	0,5	−63	22
X33 (eaves)	10	−65	20
X35 (eaves)	2,51	−56	29
X36 (eaves)	1,58	−58	27

Table 2: $P(C_s > 0)$ for OLOS-1 (T3) scheme.

Pr legit. (nW)	Pr eaves. (nW)	SNR ratio	$P(C_s > 0)$
1,26	0,00631	0,005007937	0,995
1,26	0,5	0,396825397	0,716
1,26	0,5	0,396825397	0,716
1,26	10	7,936507937	0,112
1,26	2,51	1,992063492	0,334
1,26	1,58	1,253968254	0,444
0,32	0,00631	0,01971875	0,981
0,32	0,5	1,5625	0,390
0,32	0,5	1,5625	0,390
0,32	10	31,25	0,031
0,32	2,51	7,84375	0,113
0,32	1,58	4,9375	0,168
0,03162	0,00631	0,199557242	0,834
0,03162	0,5	15,81277672	0,059
0,03162	0,5	15,81277672	0,059
0,03162	10	316,2555345	0,003
0,03162	2,51	79,38013915	0,012
0,03162	1,58	49,96837445	0,020

Average SNR for both the main and the wiretap channel was calculated considering a noise-interference level of −85 dBm (for all schemes), based on actual commercial (COTS) systems (802.11g Wi-Fi) operating at the same frequency as the ad hoc 802.11n network within range. Environmental noise was considered −98 dBm (all schemes).

The notations Xxy (i.e., X31) refer to eavesdropper's locations, sampled from the trajectory of the eavesdropper's movement in each scheme. All possible combinations between main channel and eavesdropper average SNRs were considered and the respective Probability of Nonzero Secrecy Capacity has been determined.

As it can be seen from the results, average received power levels are in the nW scale. Average SNR for both main and wiretap channel range from a few dB above zero up to almost 30 dB. Therefore, the calculated values of Probability of Nonzero (strictly positive) Secrecy Capacity range from worst-case (a value of 0,003) where the WITS scheme is largely compromised ($\overline{\gamma}_M \ll \overline{\gamma}_W$), up to 0,995, where $\overline{\gamma}_M \gg \overline{\gamma}_W$.

As in the case of OLOS-1 (T3) scheme, the average received power levels remains in the nW scale, with slightly lower values than the first case. This is due to the fact that whereas this is still an OLOS scenario, the existence of dense plantation (trees with large branches of leaves) that meddles with the signal path adds to the shadowing and the attenuation of the transmitted signal. This is evident in the legitimate receiver locations B4, C4, D4, and E4. As in the first OLOS scheme for location A3, locations A4 and F4 are considered to be behind the building surface in relation to the transmitter. However, the knife-edge diffraction effect deems this an OLOS case instead of a classic NLOS scheme.

In addition, the trajectory of the eavesdropper's movement (walking speed) was considered to be even further from the transmitter. Again, the eavesdropper low-speed movement does not cause any Doppler spread phenomena and does not alter the main channel characteristics. Average SNR values for both legitimate receiver and eavesdropper range significantly from a few dB's up to nearly 30 dB, and the calculated values of Probability of Nonzero (strictly positive)

Table 3: Average received power and SNR for OLOS-2 (T4) scheme.

OLOS T4	Pr (nW)	Pr (dBm)	SNR (dB)
A4 (main)	0,32	−65	20
B4 (main)	0,32	−65	20
C4 (main)	0,0158	−78	7
D4 (main)	0,32	−65	20
E4 (main)	1	−60	25
F4 (main)	0,05012	−73	12
X41 (eaves)	0,1	−70	15
X42 (eaves)	0,32	−65	20
X43 (eaves)	0,63	−62	23
X44 (eaves)	1	−60	25
X45 (eaves)	1,58	−58	27
X46 (eaves)	2,51	−56	29

Table 4: $P(C_s > 0)$ for OLOS-2 (T4) scheme.

Pr legit. (nW)	Pr eaves. (nW)	SNR ratio	$P(C_s > 0)$
0,32	0,1	0,3125	0,762
0,32	0,32	1	0,500
0,32	0,63	1,96875	0,337
0,32	1	3,125	0,242
0,32	1,58	4,9375	0,168
0,32	2,51	7,84375	0,113
0,0158	0,1	6,32911392	0,136
0,0158	0,32	20,2531646	0,047
0,0158	0,63	39,8734177	0,024
0,0158	1	63,2911392	0,016
0,0158	1,58	100	0,010
0,0158	2,51	158,860759	0,006
1	0,1	0,1	0,909
1	0,32	0,32	0,758
1	0,63	0,63	0,613
1	1	1	0,500
1	1,58	1,58	0,388
1	2,51	2,51	0,285
0,05012	0,1	1,99521149	0,334
0,05012	0,32	6,38467678	0,135
0,05012	0,63	12,5698324	0,074
0,05012	1	19,9521149	0,048
0,05012	1,58	31,5243416	0,031
0,05012	2,51	50,0798085	0,020

Secrecy Capacity, presented in Table 4, range from worst-case (a value of 0,006), where the WITS scheme is largely compromised ($\overline{\gamma}_M \ll \overline{\gamma}_W$), up to 0,909, where $\overline{\gamma}_M \gg \overline{\gamma}_W$.

Finally, the NLOS scenario is presented in Figure 4. The transmitter is fixed in location T5 whereas the legitimate receiver is situated in locations A5, B5, C5, and D5. All four locations comply with classic NLOS scenario, with D5 compensating for being behind the building with the fact that the transmitted signal penetrates the glass doors of front (left-side) and back entrance (right-side) of the building, thus reducing the attenuation that would be caused in the case of wall penetration.

Table 5: Average received power and SNR for NLOS (T5) scheme.

NLOS T5	Pr (ρW)	Pr (dBm)	SNR (dB)
A5 (main)	15,8	−78	7
B5 (main)	10	−80	5
C5 (main)	100	−70	15
D5 (main)	3,16	−85	0
X51 (eaves)	10	−80	5
X52 (eaves)	31,62	−75	10

Table 6: $P(C_s > 0)$ for NLOS (T5) scheme.

Pr legit. (ρW)	Pr eaves. (ρW)	SNR ratio	$P(C_s > 0)$
15,8	10	0,632911	0,612
15,8	31,62	2,001266	0,333
10	10	1	0,500
10	31,62	3,162	0,240
100	10	0,1	0,909
100	31,62	0,3162	0,760
3,16	10	3,164557	0,240
3,16	31,62	10,00633	0,091

The eavesdropper follows the trajectory shown in Figure 4. Two sampled locations have been acquired along the movement. As it can be seen from Table 5, the NLOS scheme is evidently different than the two OLOS case studies in terms of average received power, which is in pW levels. Table 6 provides the average SNR combinations and the respective calculated values of Probability of Nonzero (strictly positive) Secrecy Capacity.

6. Conclusions

Three different case studies in consistence within the OLOS/NLOS scenario were examined for an autonomic network of low-speed moving nodes (laptops connected via 802.11n ad hoc network). Additive noise and interference levels were considered to be −85 dBm for all scenarios, based on environmental noise assumption of −98 dBm and recorded interference from other operating 802.11g networks in the same frequency (2.4 GHz) within range. The NetStumbler software was used for acquisition of average received power levels.

The first OLOS scheme took into consideration knife-edge diffraction and obstruction of signal path whereas sampling eavesdropper locations along a movement trajectory. Average received power levels were in nW scale and all possible average SNR combinations provided calculated values of Probability of Nonzero (strictly positive) Secrecy Capacity ranging from worst-case, where the WITS scheme is compromised and deemed inappropriate, up to best-case, where $P(C_s > 0) \cong 1$.

The second OLOS scheme took into consideration dense plantation shadowing that leads to further signal attenuation, still however in nW scale. Finally, the NLOS scheme offered

Table 7: Average SNR and $P(C_s > 0)$ values for each scheme and overall.

Scheme	Av. main SNR (dB)	Av. eaves SNR (dB)	$P(C_s > 0)$
OLOS-1 (T3)	16,5	23	0,354
OLOS-2 (T4)	17,3	21,5	0,269
NLOS (T5)	6,8	7,5	0,461
Overall	13,53	17,33	0,361

classic NLOS cases and demonstrated a radical decrease in average received power values, in pW scale whereas calculated values of Probability of Nonzero (strictly positive) Secrecy Capacity still ranged from worst-case to best-case. This leads us to the conclusion that a severe degeneration of the channel topology and characteristics does not necessarily compromise the WITS scheme in terms of Probability of Nonzero (strictly positive) Secrecy Capacity, as long as this degeneration applies for both the legitimate receiver and the eavesdropper. The most critical factor in WITS is the relative locations of both users in reference to the transmitter that holds a definitive impact on the robustness of the WITS scheme, confirming our theoretical assumptions and findings.

It is also evident, as shown in Table 7, that our theoretical assumptions are also confirmed from these experimental measurements. In each scheme, average main channel SNR is slightly lower than average wiretap channel SNR (eavesdropper) and has an overall value of slightly above 10 dB, which was our theoretical main channel SNR assumption [21]. Also $P(C_s > 0)$ has an overall average value of 0,361, confirming the WITS notion [9, 10] that when $\overline{\gamma}_M < \overline{\gamma}_W$, Perfect Secrecy is achievable for Rayleigh fading channels instead of the classic Gaussian wiretap scenario, albeit with a possibility less than 0.5.

7. Future Work

The experimental measurements acquired in this work provide some more open issues for immediate research in the field of Wireless Information-Theoretic Security. The issue of shadowing needs to be furthermore inquired. Site-specific measurements and channel modeling have led to an empirical method for calculation of shadowing deviation based on obstacles meddling with the signal path [25], providing a novel approach for an accurate large-scale consideration of shadowing phenomena. The method was originally implemented for indoor topologies at 2.4 GHz but is valid for any topology and any frequency in question. This should be taken into consideration for the mathematical expressions of WITS key parameters.

In addition, as proven from the OLOS and NLOS topologies examined in this paper, interference from other operating networks in the same frequency needs to be taken into consideration in the SNR denominator. In the case of nonuniform interference for all concerned users of the network, a noise-interference factor needs to be implemented into the mathematical expressions of WITS key parameters, and the impact of its numerical variation (for realistic scenarios) on the WITS reliability needs to be thoroughly examined.

Finally, the issue of Doppler spread should be addressed for higher values of the user velocity, where both the channel characteristics and the Secrecy Rate are affected by Doppler shift.

Acknowledgments

The authors would like to acknowledge Mr. Giannis Georgopoulos for his assistance during the experimental work. The authors wish to acknowledge the support of the ICT European Research Programme and all the partners in PEACE: PDMF&C, Instituto de Telecomunicaes, FhG Fokus, University of Patras, Thales, Telefonica, and CeBit.

References

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell Systems Technical Journal*, vol. 29, pp. 656–715, 1949.

[2] A. D. Wyner, "The wire-tap channel," *Bell Systems Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[3] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339–348, 1978.

[4] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wiretap channel," *IEEE Transactions on Information Theory*, vol. 24, no. 4, pp. 451–456, 1978.

[5] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Transactions on Information Theory*, vol. 39, no. 3, pp. 733–742, 1993.

[6] U. M. Maurer, "Information-theoretically secure secret-key agreement by NOT authenticated public discussion," in *Advances in Cryptology—EUROCRYPT '97*, vol. 1233 of *Lecture Notes in Computer Science*, pp. 209–225, Springer, Heidelberg, Germany, 1997.

[7] U. M. Maurer, "Information-theoretic key agreement: from weak to strong secrecy for free," in *Advances in Cryptology—EUROCRYPT 2000*, vol. 1807 of *Lecture Notes in Computer Science*, pp. 351–368, Springer, Heidelberg, Germany, 2000.

[8] U. Maurer and S. Wolf, "Secret-key agreement over unauthenticated public channels—part I: definitions and a completeness result," *IEEE Transactions on Information Theory*, vol. 49, no. 4, pp. 822–831, 2003.

[9] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *Proceedings of IEEE International Symposium on Information Theory (ISIT '06)*, pp. 356–360, IEEE Press, July 2006.

[10] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2515–2534, 2008.

[11] M. Bloch, A. Thangaraj, S. W. McLaughlin, and J.-M. Merolla, "LDPC-based Gaussian key reconciliation," in *Proceedings of IEEE Information Theory Workshop (ITW '06)*, pp. 116–120, IEEE Press, March 2006.

[12] T. J. Richardson, M. A. Shokrollahi, and R. L. Urbanke, "Design of capacity-approaching irregular low-density parity-check codes," *IEEE Transactions on Information Theory*, vol. 47, no. 2, pp. 619–637, 2001.

[13] T. Rappaport, *Wireless Communications: Principles and Practice*, Prentice Hall, Upper Saddle River, NJ, USA, 2001.

[14] J. D. Parsons, *The Mobile Radio Propagation Channel*, Wiley Interscience, Hoboken, NJ, USA, 2000.
[15] A. Özgür, O. Lévêque, and E. Preissmann, "Scaling laws for one- and two-dimensional random wireless networks in the low-attenuation regime," *IEEE Transactions on Information Theory*, vol. 53, no. 10, pp. 3573–3585, 2007.
[16] J. Seybold, *Introduction to RF Propagation*, Wiley Interscience, Hoboken, NJ, USA, 2005.
[17] T. Chrysikos and S. Kotsopoulos, "Impact of channel-dependent variation of path loss exponent on Wireless Information-Theoretic Security," in *Wireless Telecommunications Symposium 2009*, pp. 1–7, IEEE Press, Prague, Czech Republic, April 2009.
[18] T. Chrysikos, T. Dagiuklas, and S. Kotsopoulos, "A closed-form expression for outage secrecy capacity in Wireless Information-Theoretic Security," in *Proceedings of Security in Emerging Wireless Communication and Networking Systems (SEWCN '09)*, vol. 42 of *Lecture Notes in Computer Science*, pp. 3–12, Springer, 2010.
[19] P. C. Pinto, J. Barros, and M. Z. Win, "Physical-layer security in stochastic wireless networks," in *Proceedings of 11th IEEE Singapore International Conference on Communication Systems (ICCS '08)*, pp. 974–979, IEEE Press, November 2008.
[20] P. C. Pinto, J. Barros, and M. Z. Win, "Wireless physical-layer security: the case of colluding eavesdroppers," in *Proceedings of IEEE International Symposium on Information Theory (ISIT '09)*, pp. 2442–2446, IEEE Press, July 2009.
[21] T. Chrysikos, T. Dagiuklas, and S. Kotsopoulos, "Wireless information-theoretic security for moving users in autonomic networks," in *IFIP Wireless Days (WD '10)*, Venice, Italy, 2010.
[22] C. Papageorgiou, K. Birkos, T. Dagiuklas, and S. Kotsopoulos, "An obstacle-aware human mobility model for ad hoc networks," in *Proceedings of the 17th IEEE International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems (MASCOTS '09)*, London, UK, September 2009.
[23] C. Papageorgiou, K. Birkos, T. Dagiuklas, and S. Kotsopoulos, "Simulating mission critical mobile ad hoc networks," in *Proceedings of the 4th ACM International Workshop on Performance Monitoring, Measurement, and Evaluation of Heterogeneous Wireless and Wired Networks (PM2HW2N '09)*, Tenerife, Spain, October 2009.
[24] http://www.netstumbler.com/.
[25] T. Chrysikos, G. Georgopoulos, and S. Kotsopoulos, "Empirical calculation of shadowing deviation for complex indoor propagation topologies at 2.4 GHz," in *Proceedings of International Conference on Ultra Modern Telecommunications (ICUMT '09)*, pp. 1–6, IEEE Press, St. Petersburg, Russia, October 2009.