Wireless Information-Theoretic Security: Theoretical analysis & experimental measurements with multiple eavesdroppers in an outdoor obstacle-dense MANET

Theofilos Chrysikos [1], Konstantinos Birkos [1], Tasos Dagiuklas [2] & Stavros Kotsopoulos [1]

[1]Department of Electrical & Computer Engineering, University of Patras, Greece
[2] Division of Computer Science and Informatics, London South Bank University, UK
txrysiko@ece.upatras.gr, kmpirkos@ece.upatras.gr, tdagiuklas@lsbu.ac.uk,
kotsop@ece.upatras.gr

Corresponding Author:
Theofilos Chrysikos, P.O.BOX 1182, Patras, 26223, Greece.
Phone: +306937152344. Email: txrysiko@ece.upatras.gr

Abstract. Wireless Information-Theoretic Security (WITS) has been suggested as a robust security scheme, especially for infrastructure-less networks. Based on the physical layer, WITS considers quasi-static Rayleigh fading instead of the classic Gaussian wiretap scenario. In this paper, they key parameters of WITS are investigated by implementing an 802.11n ad-hoc network in an outdoor obstacle-dense topology. Measurements performed throughout the topology allow for a realistic evaluation of a scenario with multiple moving eavesdroppers. Low speed user movement has been considered, so that Doppler spread can be discarded. A set of discrete field test trials have been conducted, based on simulation of human mobility throughout an obstacle-constrained environment. Average Signal-to-Noise Ratio (SNR) values have been measured for all moving nodes, and the Probability of Non-Zero Secrecy Capacity has been calculated for different eavesdropping cooperative schemes (Selection Combining and Maximal-Ratio Combining). In addition, the Outage Probability has been estimated with regard to a non-zero target Secrecy Rate for both techniques. The results have been compared with the respective values of WITS key parameters derived from theoretical analysis.

Keywords. Wireless Security; Rayleigh channels; Ad-hoc networks; Diversity

WITS: Wireless Information-Theoretic Security
HUMO: Human Mobility Model
NS-2: Network Simulator - 2

1 Introduction

Physical Layer 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. The classic Gaussian wiretap channel scenario has suggested that perfect secrecy as defined by Shannon [1] in wireless communication between a transmitter and a legitimate receiver in the presence of an eavesdropper (passive intruder) is achievable when the average Signal-to-Noise Ratio (SNR) of the main channel (established between the transmitter and the legitimate receiver) is larger than the average SNR of the wiretap channel (established between the transmitter and the eavesdropper) [2-4]. This limitation proved to be a major setback for further research in the field of physical layer based security, and attention turned to other solutions [5]-[7].

Recently, however, the concept of Wireless Information-Theoretic Security (WITS) was introduced in [8] and further developed in [9], providing a new resurgence in interest for physical security. According to the WITS fundamental principle, if both channels are considered to be characterized by quasi-static Rayleigh fading, then wireless security can be achieved even when the average Signal-to-Noise Ratio (SNR) of the main channel is less than the average SNR of the wiretap channel, albeit with a probability smaller than 0.5. The theoretical findings of Wireless Information-Theoretic Security are extended to include the use of LDPC channel coding scheme as a means of opportunistic channel sharing [10], [11]. In [12], a theoretical work for multiple eavesdroppers was presented, inquiring the impact of multiple eavesdropping antennas on the robustness of WITS. However, the lack of experimental work and even more, the lack of combining multiple eavesdroppers with user movement, especially in an infrastructure-less networking case study, left a significant gap in related research which motivated our work.

In this paper, WITS has been studied via both theoretical analysis and experimentation for multiple eavesdroppers' scenarios. Moving nodes of an ad-hoc network provide a realistic scenario for investigating WITS for multiple eavesdroppers and providing values for its key parameters. Two different cooperative techniques for eavesdropping have been examined: Selection Combining (SC) and Maximal-Ratio Combining (MRC).

The paper is structured as following: Section 2 presents key parameters of Wireless Information-Theoretic Security and discusses past contributions. Section 3 addresses a user movement scenario on the basis of a mobility model that assumes a certain obstacle presence of specific dimensions. Section 4 discusses the findings from a previously conducted experimental measurement scenario for a single eavesdropper and presents the theoretical analysis for comparative discussion. Section 5 features the measurement topologies and the methodology of the experiment for the multiple eavesdroppers' scheme; the results are presented followed by a brief discussion, whereas Section 6 includes conclusions and finally Section 7 addresses open issues for future work.

2 Wireless Information-Theoretic Security

The possibility of a Non-Zero (strictly positive) secrecy capacity $P(C_s > 0)$ is calculated, for Rayleigh fading channels instead of the classic Gaussian scheme, to be non-zero (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 [8]:

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

In [9], the Probability of Non-Zero Secrecy Capacity was provided as a function of the path loss exponent n and the distance ratio d_M / d_W, where d_M is the distance between the transmitter and the legitimate receiver, and d_W is the distance between the transmitter and the eavesdropper:

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

The outage probability for a given Secrecy Rate $R_s > 0$ is also calculated as an expression of the average main and wiretap channel SNR, $\overline{\gamma}_M$ and $\overline{\gamma}_W$ respectively [9]:

$$P_{out}(C_s < R_s) = P_{out}(R_s) = 1 - \frac{e^{\left(-\frac{2^{R_s} - 1}{\overline{\gamma}_M}\right)}}{1 + 2^{R_s} \frac{\overline{\gamma}_W}{\overline{\gamma}_M}} \tag{3}$$

By substituting the SNR faction with the distance ratio, the Outage Probability is expressed as:

$$P_{out}(C_s < R_s) = P_{out}(R_s) = 1 - \frac{e^{\left(-\frac{2^{R_s} - 1}{\overline{\gamma}_M}\right)}}{1 + 2^{R_s} \left(\frac{d_M}{d_W}\right)^n} \tag{4}$$

In [9], a path loss exponent of n=3 has been considered, based on an average path loss exponent value estimation in [13]. However, the path loss exponent [14]-[16] at both outdoor and indoor environments has been found to be heavily dependent on the various mechanisms contributing to the signal attenuation, in an obstacle-dense environment. In addition, the lack of a mathematical factor representing the losses from the independent shadowing phenomenon meant that the path loss exponent would have to incorporate shadow fading losses alongside free space, distance-dependent attenuation and scattering phenomena. It was shown [17] that the channel-dependent variation of the path loss exponent severely compromised the WITS scheme, due to the rapid decrease of the Probability of Non-Zero 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 addition, the shadow fading losses and their impact on the mathematical formulae and the robustness of the WITS solution have been considered, incorporating obstacle losses into the path loss calculation as a mechanism independent of free space, distance-dependent attenuation [35].

3. Mobility models

There are several mobility models that have been proposed in the bibliography aiming to provide tools for realistic movement for nodes in a mobile ad hoc network [19], [20]. The most dominant mobility model is the Random Waypoint mobility (RWP) model. In the RWP model, nodes select a random destination in the simulation area and they move around using a random uniformly distributed speed [21]. After a certain pause time, the same process is repeated. Several variations of RWP consider extensions of the aforementioned procedure. Typical examples are considered the Random Direction (RD) mobility model (the nodes determine speed and direction and they move until they reach the boundary of the area) [22], Realistic Mobility Model (speed and direction follow distributions that yield that mimic node movement) [23].

We have designed and developed a mobility model that mimics human mobility in an environment with obstacles. This model is called Human Mobility Model (HUMO) and has been developed to simulate realistically mobile ad hoc networks that operate in areas with obstacles under mission critical applications [24], [25]. In general, under the HUMO model, each node moves towards the chosen destination point with a random speed that lies between *Umin* and *Umax*. When the node reaches this point, it waits for a certain pause time *P* in order to accomplish a specific mission and then repeats the above process all over again. The destination point is selected using a uniform distribution and models the assignment of a mission to the node about an event that occurred at this specific point. Each node can move freely in the area under study as long as the point does not reside within the boundaries of an obstacle. Without loss of generality, the obstacles are considered as rectangular that have two primitives. The first one regards the restriction of the node's mobility towards a specific point. The second one regards the introduction of signal attenuation in order to simulate phenomena such as fading, multipath etc.

Each node moves around the obstacles follow a recursive process in order to reach the selected destination point. If there is an unobstructed line of sight connecting the node with the destination point, the node follows this direct line to get to the desired destination. Otherwise, the node sets as its next intermediate destination the vertex of the directly visible obstacle edge 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. This is repeated until an unobstructed direct line until the current destination is reached. This procedure is illustrated in Figure 1 [26].

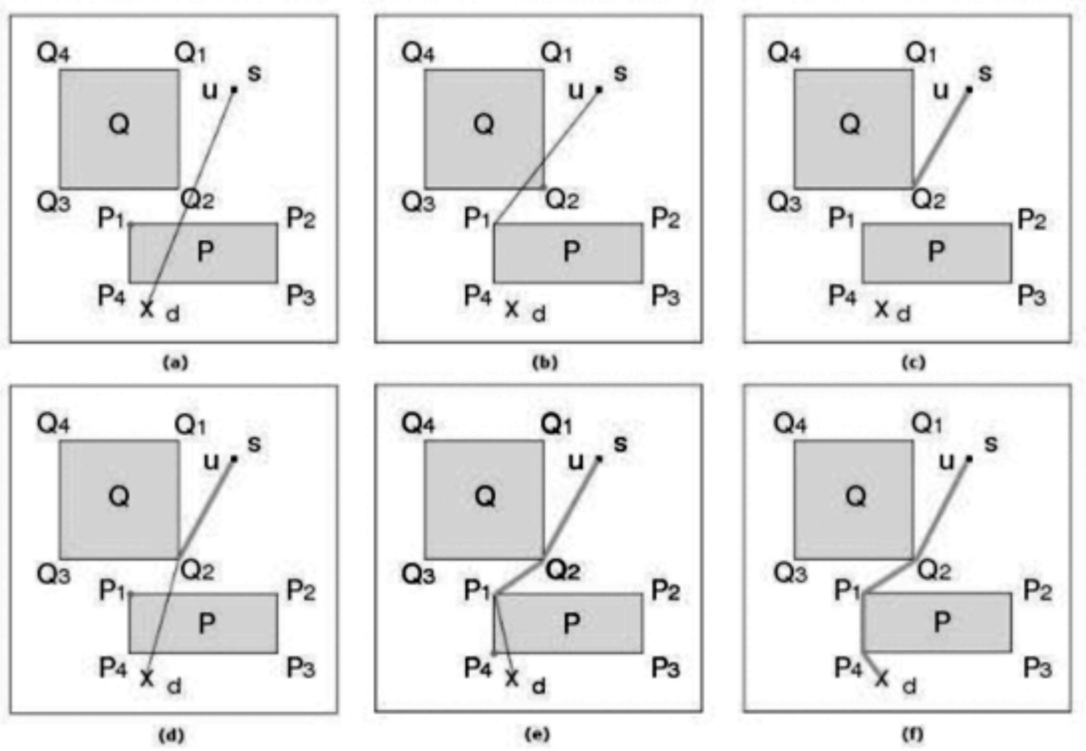

Figure 1: Node mobility within the obstacles using the HUMO mobility model

4. Wireless Information-Theoretic Security with a single eavesdropper

4.1 Theoretical Analysis

In [27], [28] the impact of user location on WITS robustness was addressed. However, the user movement has not been taken into consideration, especially in an obstacle-constrained propagation environment. In [29], the impact of user mobility on the boundaries of secure communications has been addressed, from a physical layer point of view. More specifically, the impact of the approaching eavesdropper on the decrease of the Probability of Non-Zero 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) has been examined. 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.

Results have confirmed that by reducing the original separation from the transmitter, the eavesdropper can achieve a radical decrease in $P(C_s > 0)$. For a given mobility scheme and the user velocity, the time window in which this decrease is accomplished can be calculated.

Therefore, the impact of user (eavesdropper) movement on Outage Secrecy Capacity may compromise the boundaries of secure communication, depending of course on the location and mobility of the legitimate receivers.

Figure 2 illustrates the theoretical PDF of the Probability of Non-Zero Secrecy Capacity P(Cs>0) for a single transmitter-single receiver scenario in the presence of a single eavesdropper. The following assumptions have been considered to measure PDF of the Secrecy Capacity: the mobility area is a rectangular 5x5 grid, the obstacle is a rectangular located at the centre of the grid, both the legitimate receiver and the eavesdropper move at low-speed (1 m/s) in accordance with the HUMO mobility model, the transmitter is considered to be at a fixed location.

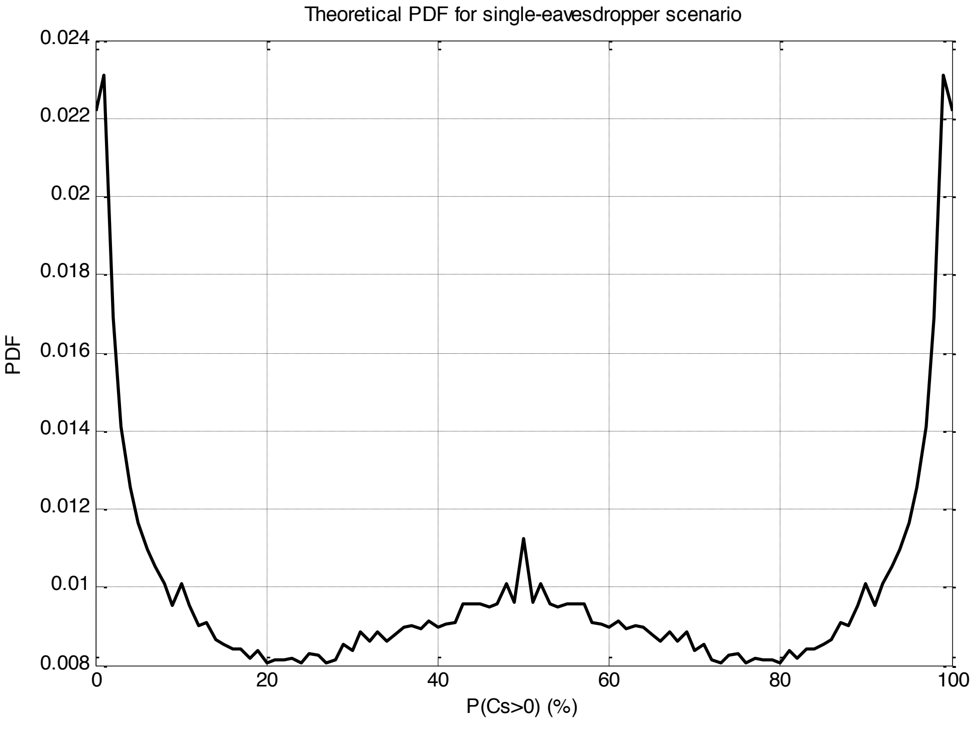

Figure 2: Theoretical PDF of P(Cs>0) for single-eavesdropper scenario

4.2 Experimental Measurements

In [30], a series of experimental measurements have been conducted in order to provide a test bed for computation and evaluation of the key parameters of WITS, in the presence of moving users (both legitimate receiver and eavesdropper).

A mobile ad-hoc network has been set up, comprising of autonomic users (laptops) moving in low-speed fashion (thus discarding any possible Doppler spread phenomena). Three laptops have been connected via 802.11n embedded network adapters: the first laptop served as transmitter, the second laptop was the legitimate receiver and the third laptop was the passive eavesdropper. All measurements have been conducted in the campus of the University of Patras-Greece[1], in very close proximity to a building belonging to the Department of Electrical and Computer Engineering, assuming Obstructed-Line-of-Sight (OLOS) and Non-Line-of-Sight (NLOS) schemes that comply with WITS channel considerations (Rayleigh fading).

The topology for the experimental measurements is shown in Figure 3. Buildings 4 and 5 include the main faculty offices and research areas of the Department. Building 26 hosts the Wireless Telecommunications Laboratory, and a number of other labs and offices belonging to the Department. Buildings 30 and 54 belong to the Department of Civil Engineering of the University of Patras. The transmitter has been set in a fixed position, just outside of Building 26, near the external wall. In the single eavesdropping scenario [30], movement has been confined in close proximity around Building 26, constituting two OLOS case studies (the first being a typical obstruction scenario and the second one a more severe scenario of obstruction with plantation and greater transmitter-receiver separation distance) and one NLOS case study.

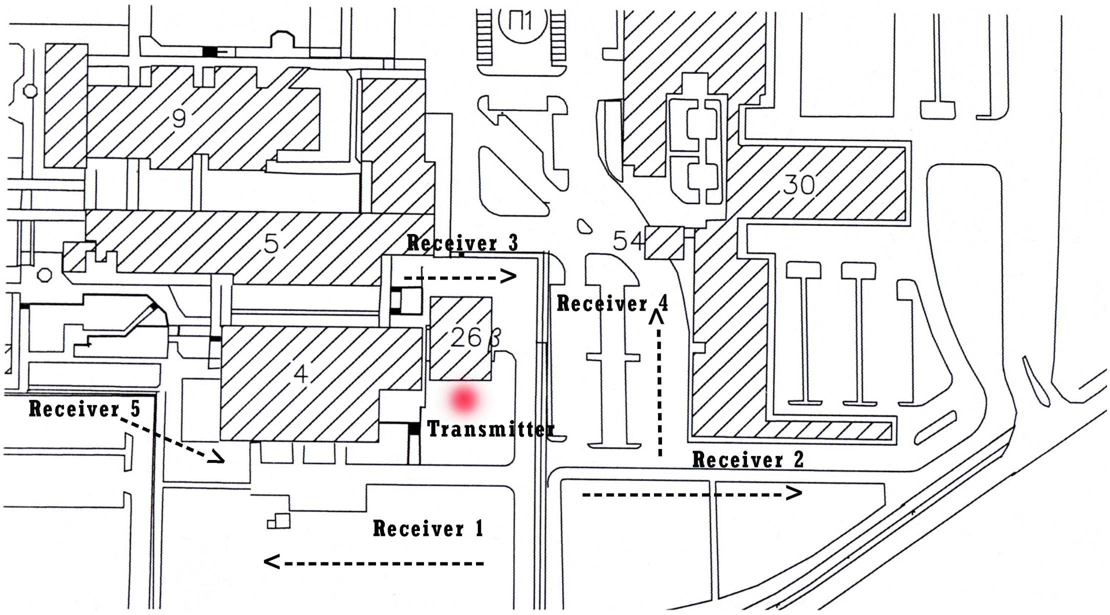

Figure 3: Outdoor topology for Ad-Hoc Network Measurements

[1] http://www.ece.upatras.gr

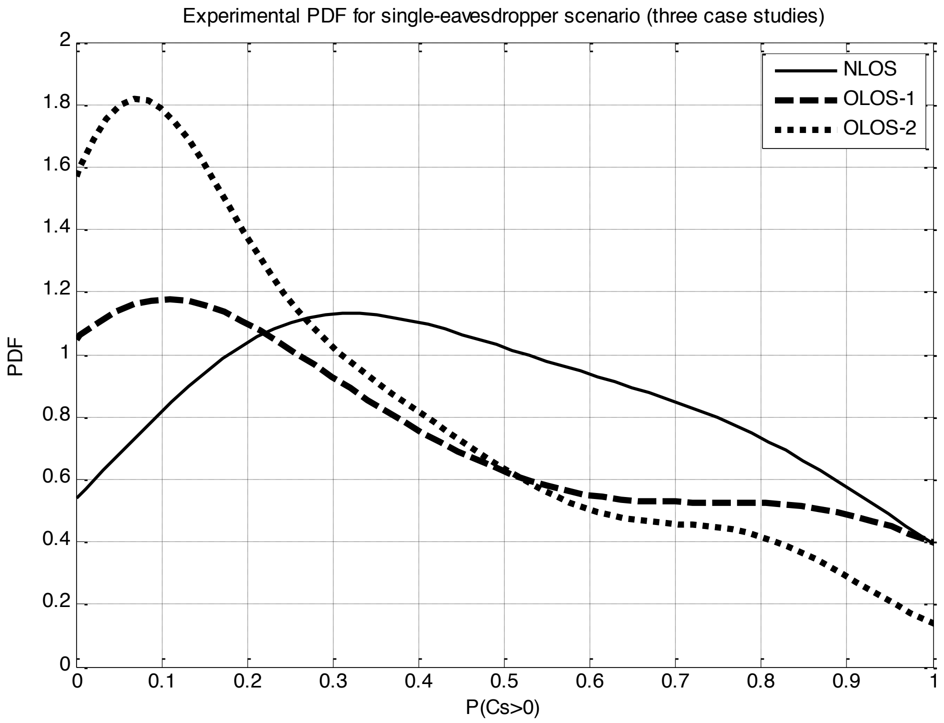

Figure 4: Empirical PDF of P(Cs>0) for single-eavesdropper scenario

The average SNRs of both main and wiretap channel have been measured and the Probability of Non-Zero Secrecy Capacity has been calculated in order to evaluate WITS in an actual obstacle-constrained outdoor environment. The results demonstrated in Figure 4, manifest a significant impact of relative user location on WITS reliability as a physical security solution.

More specifically, the OLOS-2 case study provides the worst results in terms of P(Cs>0), with an average value of 0.269. In the OLOS-1 case study, P(Cs>0) is slightly improved with an average value of 0.354. This is due to the fact that the HUMO mobility model has an impact on relative user location, with the eavesdropper's channel quality (average SNR) being superior compared to the legitimate receiver's. In the NLOS case study, channel conditions for both legitimate receiver and eavesdropper are really bad, therefore the values of the average SNR for both moving nodes are quite similar, resulting in a smoother PDF, with an average value of 0.461 for P(Cs>0).

5 Wireless Information-Theoretic Security with Multiple Eavesdroppers

5.1 Theoretical Analysis

Our research motivation is to study a scenario with multiple eavesdroppers. Without loss of generality, a number of k=4 eavesdroppers has been considered. In order to evaluate a possible joint action of eavesdropping from all passive intruders which are active within the range of transmission, two methods will be employed: Selection

Combining (SC) and Maximal-Ratio Combining (MRC). In the case of SC, the best signal is chosen among the pool of available power levels, whereas in the case of MRC, the final received signal is the sum of all signals from all active eavesdroppers [31]. Comparing the findings from each method will also help validate whether for k=4 eavesdroppers, the gain from adding all independently received signals exceeds significantly the largest independently received signal.

Figures 5 and 6 illustrate the theoretical PDF and CDF respectively for the multiple (k=4) eavesdroppers scenario for both SC and MRC cooperative schemes. The extraction of these graphs was performed on simulating the mobility model. the user density and user movement scenario which was implemented for the experimental measurements.

According to the CDF, the MRC scheme provides a higher probability that P(Cs>0)<0.2. In the region where the probability is below a threshold (P(Cs>0)>0.2), the two schemes converge. For both MRC and SC, the probability that P(Cs>0) will exceed the 0.5 threshold is low (approximately 0.2), with slightly higher values for the SC scheme.

The PDF for MRC confirms a higher concentration of P(Cs>0) values in the lower region, i.e. less than 0.2. It is interesting to note a peak of density of P(Cs>0) values for SC around the 0.5 value. On a theoretical level, the multiple eavesdroppers' scenario for the SC technique converges with the single eavesdropper theoretical scheme. This is due to the fact that no other specifications have been considered for the multiple eavesdroppers, and this is an unbiased multi-user case study.

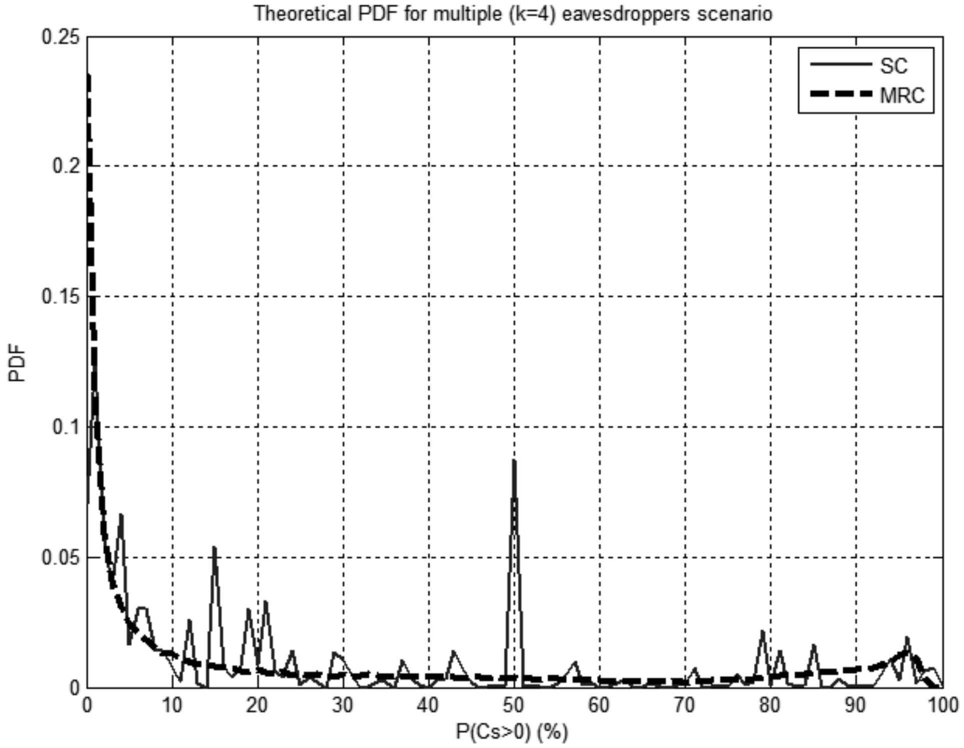

Figure 5: Theoretical PDF of P(Cs>0) for multiple (k=4) eavesdroppers scenario

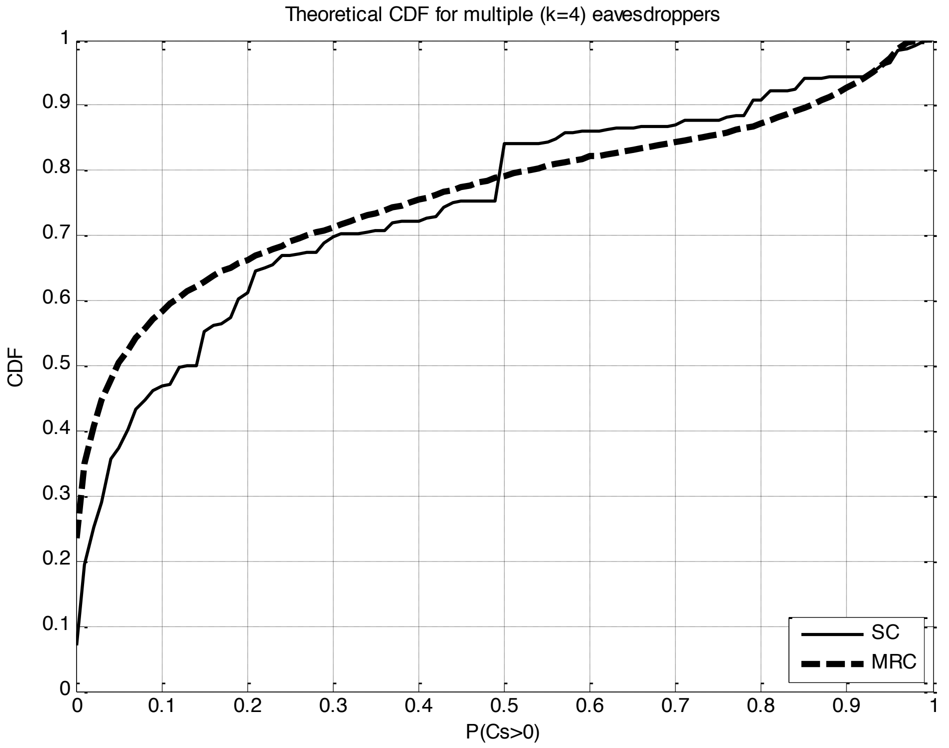

Figure 6: Theoretical CDF of P(Cs>0) for multiple (k=4) eavesdroppers scenario

5.2 Experimental Measurements

5.2.1 Methodology

For the purpose of the experimental measurements, an 802.11n ad-hoc network with 6 nodes has been implemented, in order to provide empirical values for the key parameters of WITS. The first node serves as the transmitter, the second as the legitimate receiver and the other 4 served as passive malicious users (eavesdroppers).

All nodes move within the area of interest by considering the HUMO mobility model, which has been implemented as an add-on module in NS-2 [32]. The output of NS-2 trace stores the coordinates of the new destination point, the mobility speed and the pause time of each node.

These data have been used as an input in this current work in order to define the route that each node will follow in each field test trial, the fixed transmitting node notwithstanding. A total of 15 field trials have been selected, resulting in a total of 125 different node routes, produced by the simulation in NS-2. These correspond to 125 set of measurements for the average (local-mean) SNR of each moving node.

The legitimate receiver and the 4 eavesdroppers move throughout the topology depicted in Figure 3, around Building 26, between and around Buildings 4 and 5, and in the surrounding area, at a low speed (approximately 1 m/s), so that any Doppler spread phenomena can be discarded.

5.2.2 Average SNR values for all moving nodes

The total EIRP of transmitting node is 10 dBm. All moving receivers (legitimate and eavesdropper) have been equipped with the NetStumbler 0.40 software [33], that measures local-mean received power and SNR values from any given wireless network (802.11b/g/n) in range. Separating different sources of transmission, namely 802.11 Access Points (APs), the NetStumbler software allows for experimental calculation of the interference levels (whereas all unwanted sources of transmission are considered to contribute to the interference level). Environmental noise was considered -98 dBm for all field trials. In all 125 node routes, the total noise-interference level was found to be approximately constant and equal to -85 dBm. Results for the local-mean SNR values for all moving nodes are depicted in Table 1 for each field test trial.

Table 1: Measured Local-Mean SNR values for moving ad-hoc nodes

Field Test Trials	Leg. Rc. SNR (dB)	Eaves. 1 SNR (dB)	Eaves. 2 SNR (dB)	Eaves. 3 SNR (dB)	Eaves. 4 SNR (dB)
1	6.81	-4.57	11.17	9.35	11.64
2	12.68	-5.66	7.19	10.75	21.94
3	12.84	1.26	*N/A*	18.85	*N/A*
4	5.57	7.91	*N/A*	10.9	*N/A*
5	5.93	22.7	16.42	-0.6	*N/A*
6	12.85	18.07	22.52	4.42	*N/A*
7	13.14	6.64	14.02	0	-0.44
8	20.66	9.7	1.62	3.08	1.88
9	26.81	-2.08	*N/A*	1.46	*N/A*
10	38.14	-5.46	-0.14	7.39	*N/A*
11	6.71	10.68	10.33	2.5	*N/A*
12	3.57	-2.92	7.63	*N/A*	*N/A*
13	2.78	6.17	17.21	4.6	*N/A*
14	2.64	12.21	6.29	2.48	*N/A*
15	6.92	3.12	7.23	*N/A*	*N/A*

It is important to note that in certain field test trials, as shown in Table 1, not all 4 eavesdroppers were able to receive any signal from the fixed transmitting 802.11n node. This is because the selected field trials and respective node routes have been produced on the basis of the HUMO mobility model with regard to the obstacles of the topology under study and did not take into consideration the probability that in a certain route the signal level arriving from the transmitting node is below the receiver's sensitivity level.

This means that in certain cases, i.e. field test trials 7 and 8, all 4 eavesdroppers are within range of receiving signal from the transmitting 802.11n ad-hoc node. In other cases, 1 or 2 eavesdroppers could be "disconnected", i.e. field test trials 12 and 15. However, in all field test trials, at least 2 eavesdroppers are within reception area (mean value of 2.93≈3 eavesdroppers), so that the single eavesdropping scenario is always avoided.

Figure 7 depicts the number of eavesdroppers, which are "active" in each field test trial, i.e. that fall within range of the 802.11n ad-hoc network in terms of signal reception from the fixed eavesdropper. Table 2 presents the statistical properties of the 'fluctuation' of the number of active eavesdroppers.

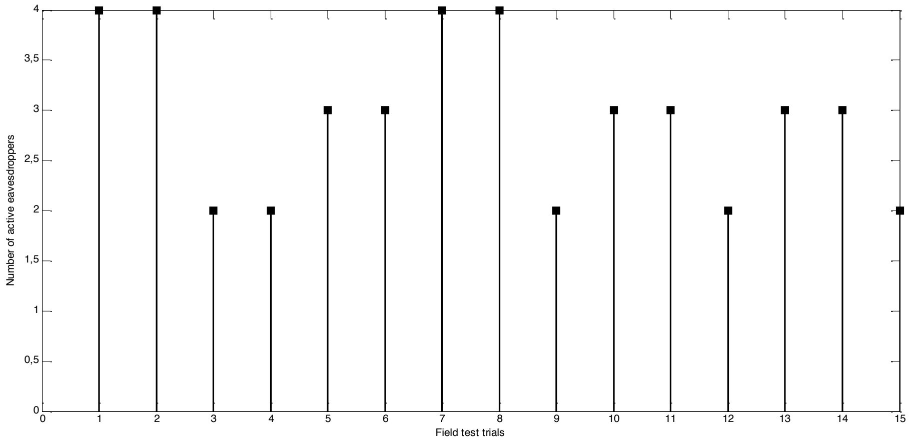

Figure 7: Number of active eavesdroppers in each field test trial

Table 2: Statistical properties of 'active' eavesdroppers

Metrics	Mean	Median	Min	Max	Std Dev
No. of Eavesdroppers	2.93	3	2	4	0.8

It must be pointed out that this adds to the realistic nature of our experiment. WITS has been notably recommended for infrastructure-less networks, including emergency scenarios where ad-hoc networks of rescue teams and safety workers might move in an obstacle-dense environment, where a possible natural or man-made disaster may have occurred. In such an environment, the mobility of the nodes can be appropriately simulated by the HUMO mobility model. At the same time, the obstacle-constrained topology will have a severe impact on the signal attenuation, both large-scale (shadowing from obstructing materials) and small-scale (multipath propagation, scattering from small obstacles). As it has been confirmed in [34], an obstacle-dense topology produces a dynamic shadowing throughout the topology. In that case, a mathematical description of large-scale fading with an area-mean value of shadowing deviation does not provide reliable results and a more thorough methodology on local-mean scale can describe the phenomenon adequately.

5.2.3 Probability of Non-Zero Secrecy Capacity

Employing the formula from Equation1, the Probability of Non-Zero Secrecy Capacity can be calculated. All P(Cs>0), values have been calculated by Eq.1, assuming that the eavesdropper SNR is adjusted according to the scheme. MRC assumes the contribution of all eavesdroppers, whereas for the SC scheme the SNR of the “strongest” eavesdropper is considered. Results are presented in Figure 8 for all field test trials.

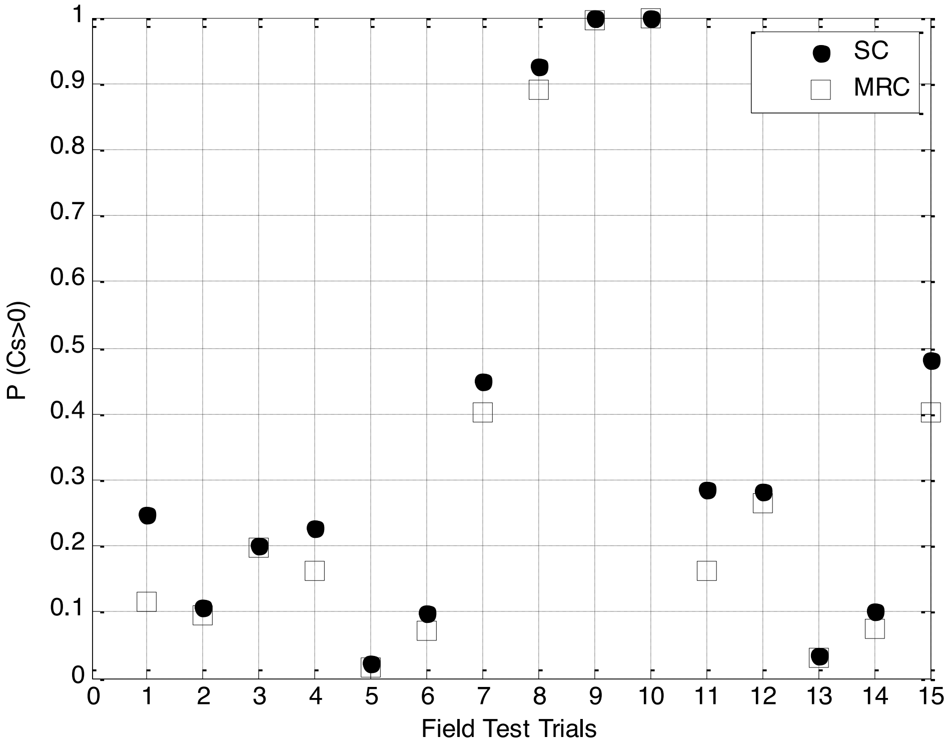

Figure 8: P(Cs>0) values for multiple (k=4) eavesdroppers scenario

Table 3 : P(Cs>0) local-mean values for SC and MRC schemes

Field Test Trials	**P(Cs>0) SC**	**P(Cs>0) MRC**
1	0.247	0.116
2	0.106	0.096
3	0.200	0.198
4	0.227	0.163
5	0.021	0.017
6	0.097	0.073
7	0.450	0.401
8	0.926	0.890

9	0.997	0.996
10	0.999	0.999
11	0.286	0.162
12	0.282	0.265
13	0.035	0.031
14	0.099	0.075
15	0.482	0.401

Table 4: P(Cs>0) area-mean values for SC and MRC schemes

Metrics	Area-mean values	Median	Min	Max	Std Dev
P(Cs>0) - SC	0.364	0.247	0.021	0.999	0.343
P(Cs>0) - MRC	0.326	0.163	0.017	0.999	0.350

Tables 3 and 4 provide respectively the local-mean and area-mean values for the Probability of Non-Zero Secrecy Capacity. For field test trials 8, 9, 10, $P\left(C_s > 0\right) \cong 1$, leading to perfect secrecy. Field test trials 7 and 15 are middle-of-the-road, where $P\left(C_s > 0\right) \cong 0.5$. For all other field test trials, the WITS scheme is compromised, since $P\left(C_s > 0\right) < 0.3$.

Comparing the values of P(Cs>0) for the same field test trial between the two cooperative schemes, results vary from nearly-identical (field test trials 9, 10) to substantially deviating, as in field test trials 1 and 11, where MRC provides significantly smaller values of Probability of Non-Zero Secrecy Capacity (53% and 43% respectively). Overall, the MRC technique provides an average (mean value) 16.73% reduction in the values of P(Cs>0) compared to the respective values of the SC scheme.

Figure 9 depicts the empirical CDF of the P(Cs>0) values for both schemes. It is very interesting to observe that the results are very close to the theoretical values of P(Cs>0) provided by the respective theoretical CDF in Figure 6. The empirical PDF of the experimentally calculated values of P(Cs>0), depicted in Figure 10, provides a generic agreement with the respective theoretical PDF.

In the lower region of 0<P(Cs>0)<0.2 the MRC provides a higher density of values, similarly to the theoretical analysis. The experimental values deviate from the theoretical ones in the higher region where 0.85< P(Cs>0) <1: the empirical values provide higher density of values than the theoretical scheme.

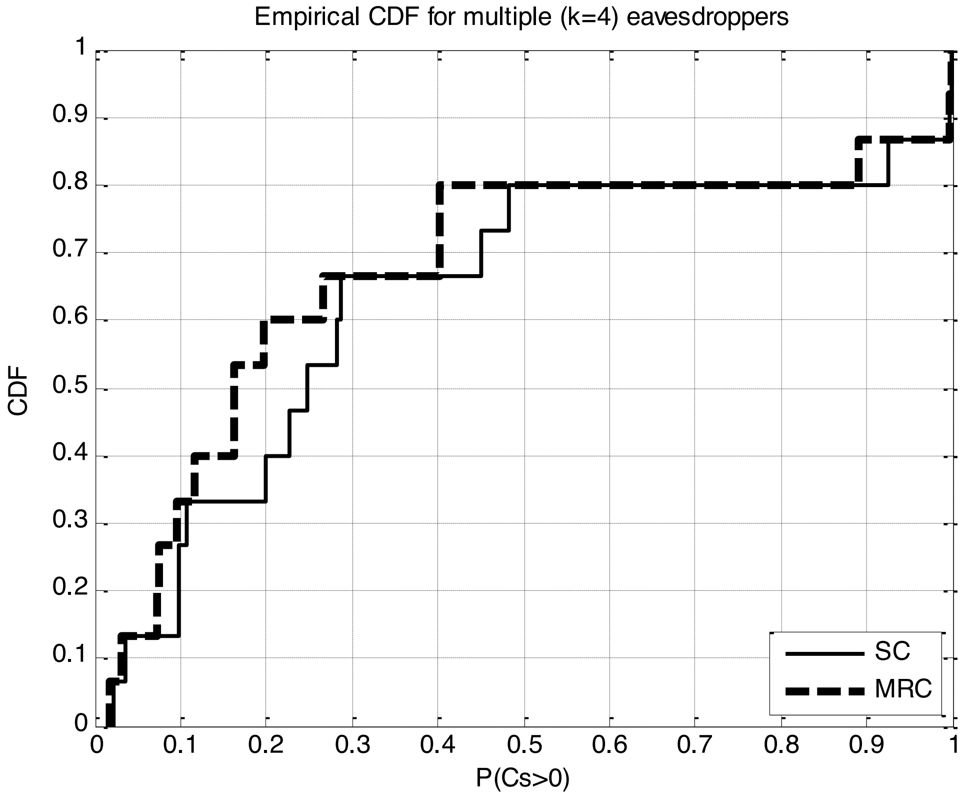

Figure 9: Empirical CDF of P(Cs>0) for multiple (k=4) eavesdroppers scenario

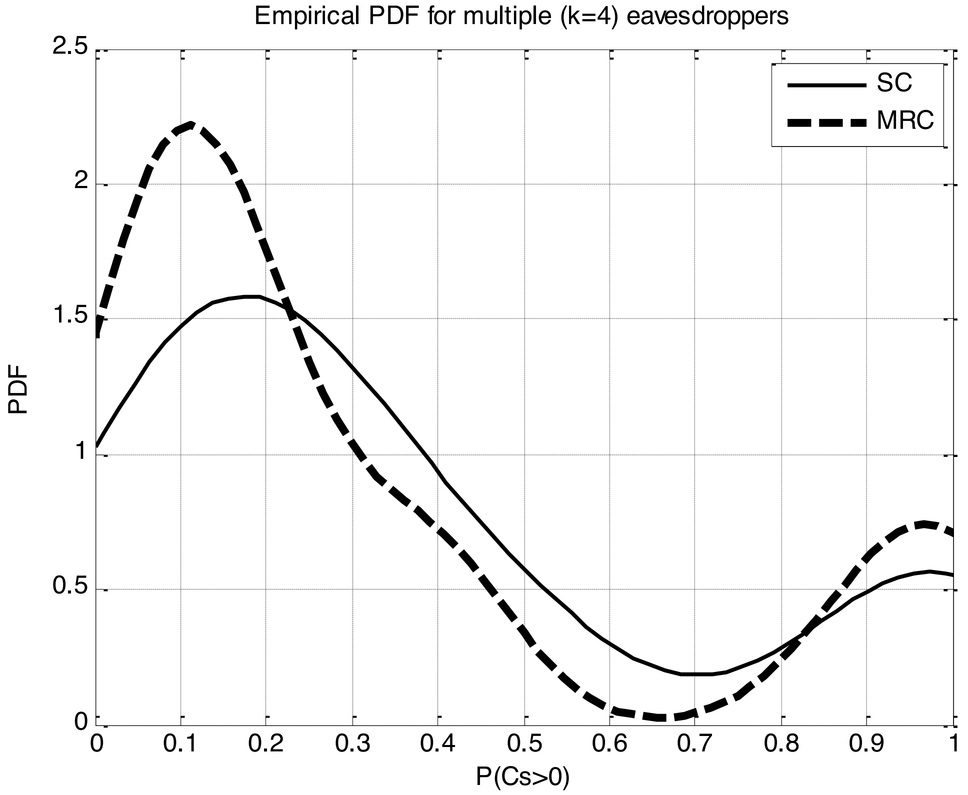

Figure 10: Empirical PDF of P(Cs>0) for multiple (k=4) eavesdroppers scenario

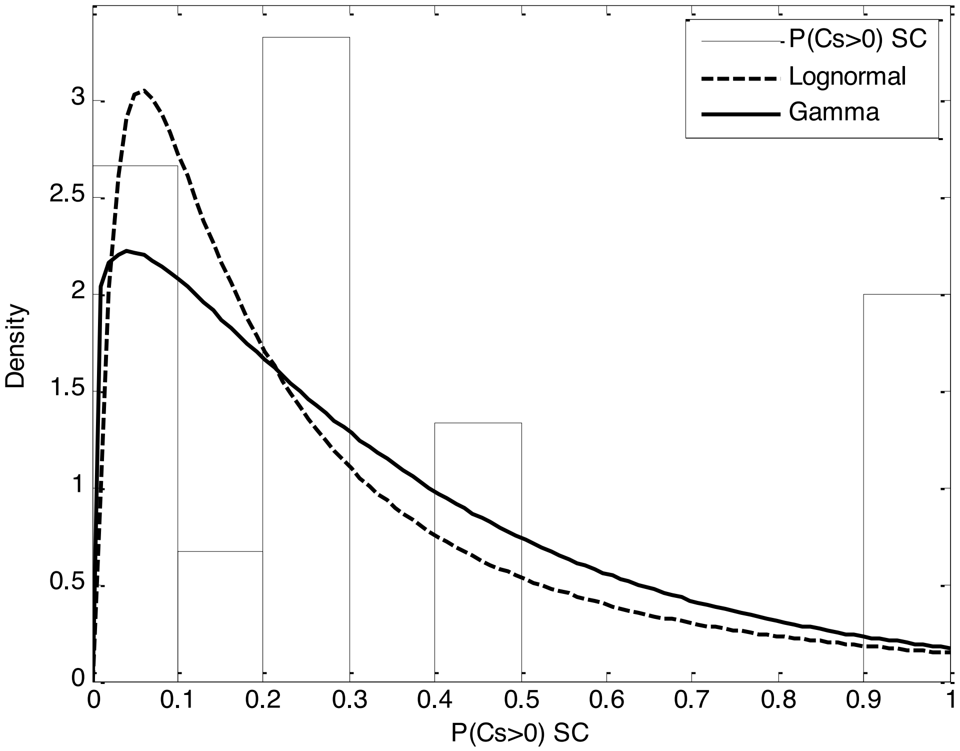

Figure 11: Data-fitting PDF of P(Cs>0) values for SC scheme

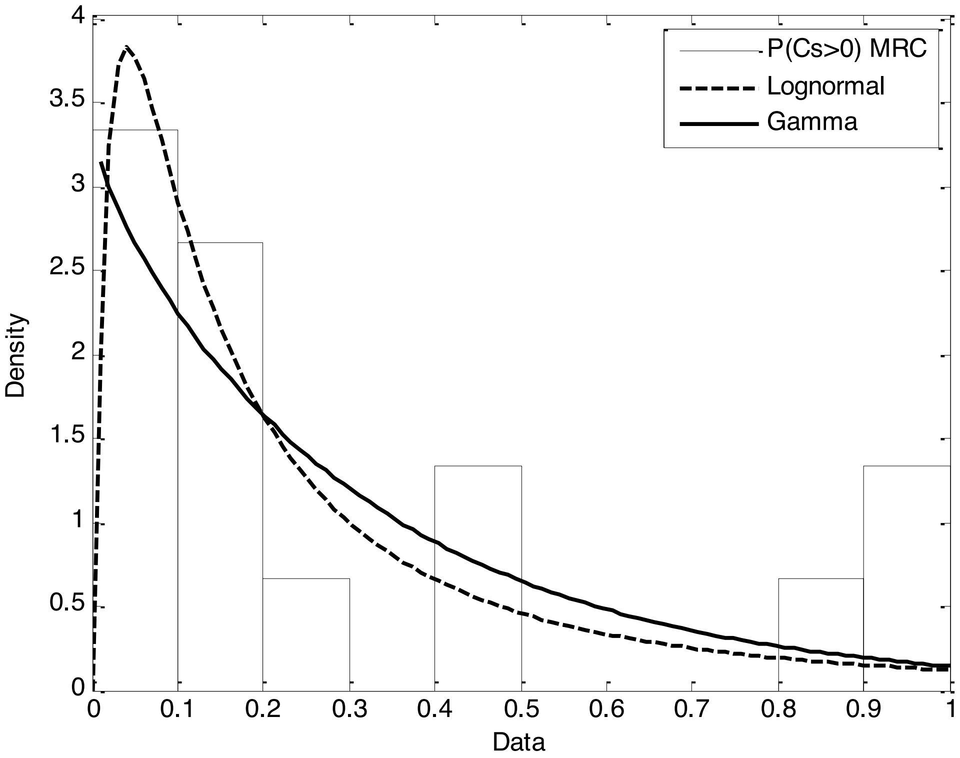

Figure 12: Data-fitting PDF of P(Cs>0) values for MRC scheme

Figures 11 and 12 illustrate the histogram of the experimentally calculated values of P(Cs>0) for both SC and MRC schemes respectively. In each case, the Log-normal and Gamma distributions are employed for data-fitting purposes, and the statistical properties are depicted in Table 7. Both Log-normal and Gamma distributions describe the same large-scale fading (shadowing) process of the fluctuation of local-mean values of received signal power (or SNR) around an area-mean value [14]. Both distributions assume a normal (Gaussian) distribution of logarithmic values of received signal power around the (logarithmic) area-mean value, however the Gamma distribution provides a closed-form expression which can be implemented more adequately than the Log-normal formula [16]. The data fitting in Figures 11 and 12 demonstrates that the Gamma distribution fits the data more smoothly than the Log-normal, while at the same time describing the same type of fluctuation.

Table 7: Statistical properties of distributions describing P(Cs>0) values

SC	**MRC**
Distribution: Lognormal	**Distribution: Lognormal**
Log likelihood: -0.215512	Log likelihood: 2.0626
Domain: 0 < y < Inf	Domain: 0 < y < Inf
Mean: 0.428065	Mean: 0.375604
Variance: 0.511524	Variance: 0.478336
Parameter Estimate Std. Err.	Parameter Estimate Std. Err.
μ -1.51487 0.29808	μ -1.71895 0.314055
σ 1.15446 0.222176	σ 1.21633 0.234083
Estimated covariance of parameter estimates:	Estimated covariance of parameter estimates:
μ 0.0888519 1.02299e-017	μ 0.0986307 1.2978e-017
σ 1.02299e-017 0.0493622	σ 1.2978e-017 0.0547948
Distribution: Gamma	**Distribution: Gamma**
Log likelihood: 0.245152	Log likelihood: 1.83866
Domain: 0 < y < Inf	Domain: 0 < y < Inf
Mean: 0.3636	Mean: 0.325533
Variance: 0.116865	Variance: 0.109158
Parameter Estimate Std. Err.	Parameter Estimate Std. Err.
a 1.13126 0.367631	a 0.970808 0.311305
b 0.321412 0.130376	b 0.335322 0.138864
Estimated covariance of parameter estimates:	Estimated covariance of parameter estimates:
a 0.135153 -0.0383994	a 0.0969107 -0.0334734
b -0.0383994 0.0169979	b -0.0334734 0.0192833

5.2.4 Outage Probability

Employing the formula presented in Equation 3, the Outage Probability (*Pout*) can be calculated as a function of a non-zero target Secrecy Rate (*Rs*). For each field test trial, the respective SNR faction and local-mean main channel SNR (corresponding to the legitimate receiver) are substituted in Eq.2 for both SC and MRC techniques. The results are depicted in Figures 13- 22. Without loss of generality, we present the Outage Probability for Field Trials 1, 2, 4, 6, 7, 8, 10, 11, 12 and 15. These are the scenarios that demonstrate the different behavior on the performance of SC and MRC techniques.

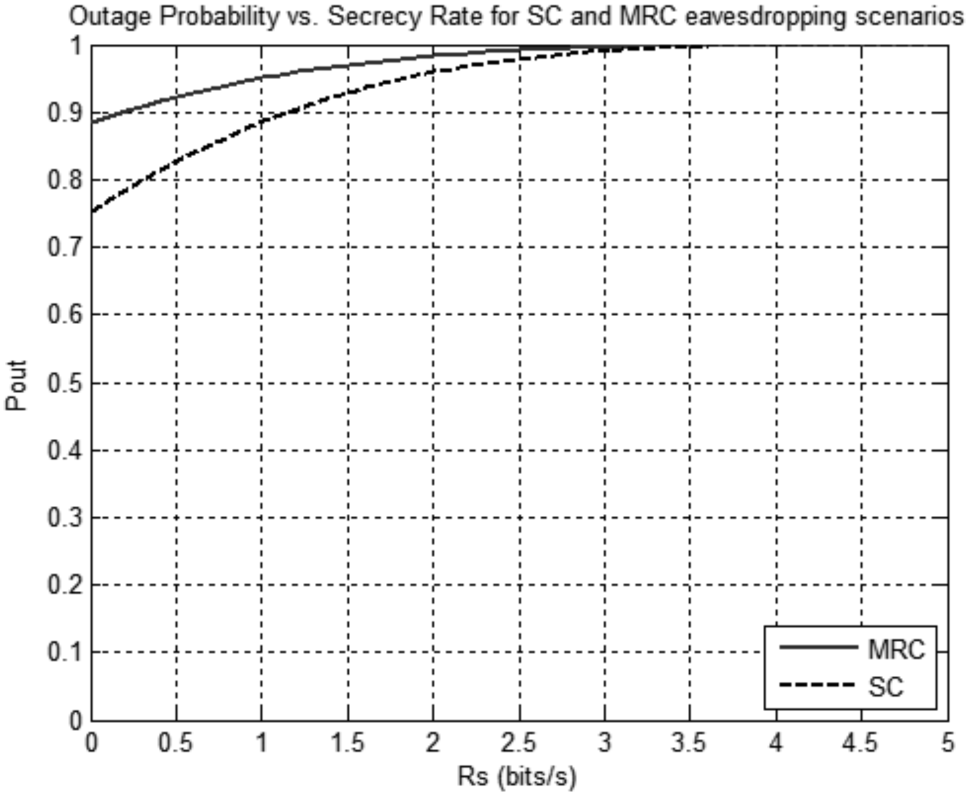

Figure 13: Outage Probability vs. Secrecy Rate for Field Test Trial 1

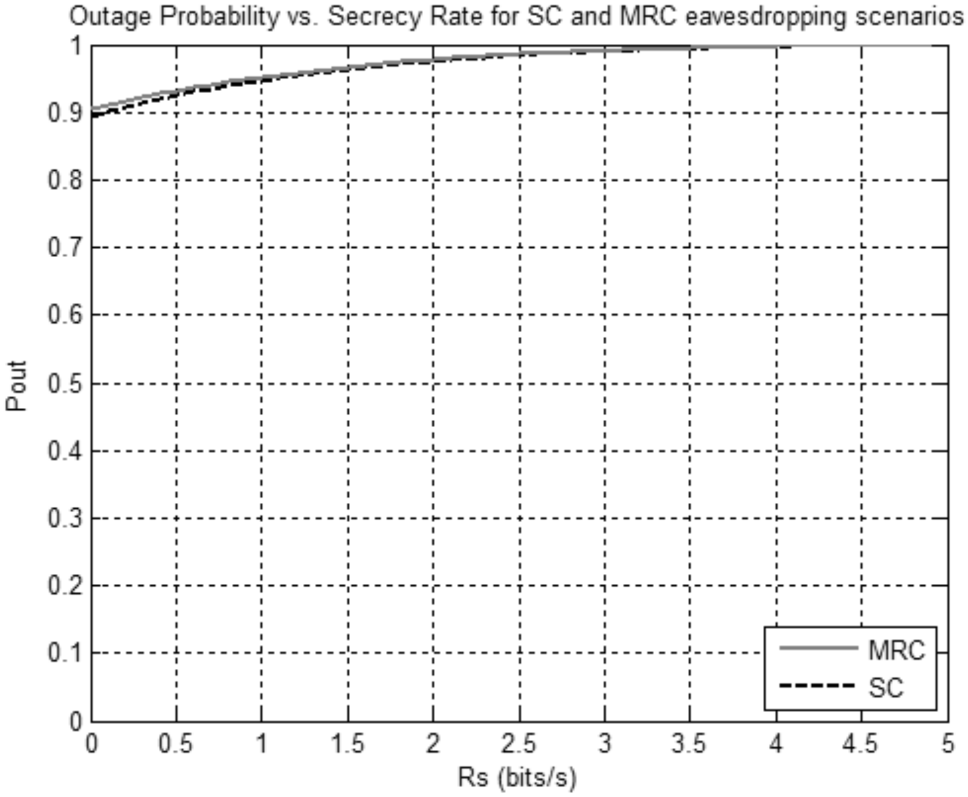

Figure 14: Outage Probability vs. Secrecy Rate for Field Test Trial 2

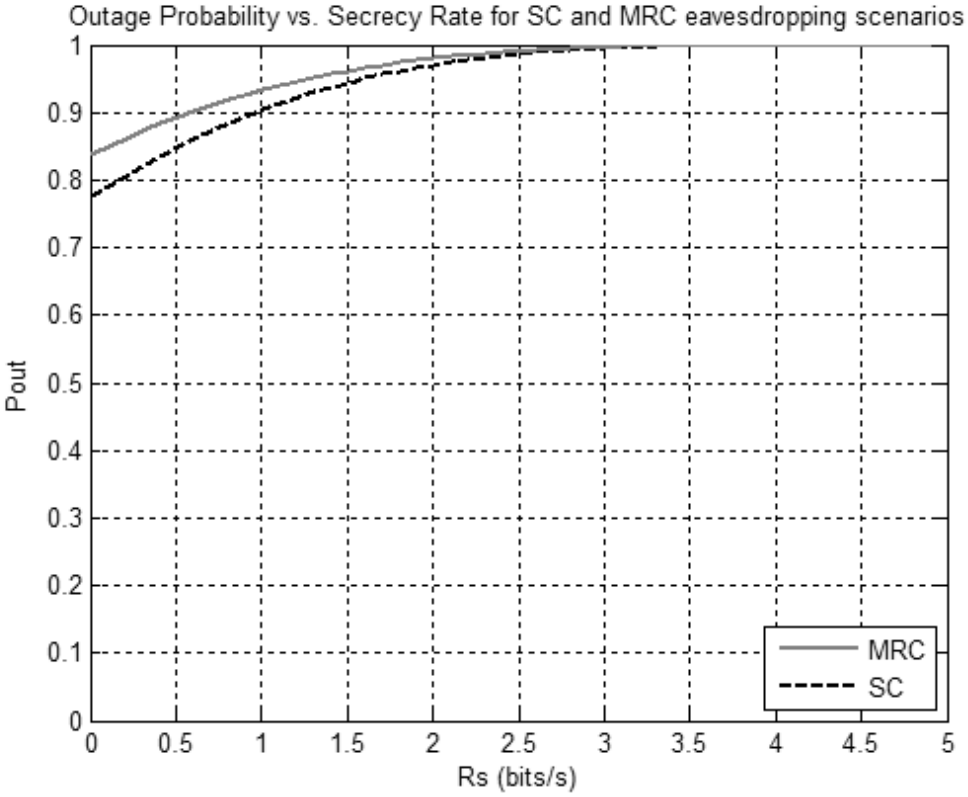

Figure 15: Outage Probability vs. Secrecy Rate for Field Test Trial 4

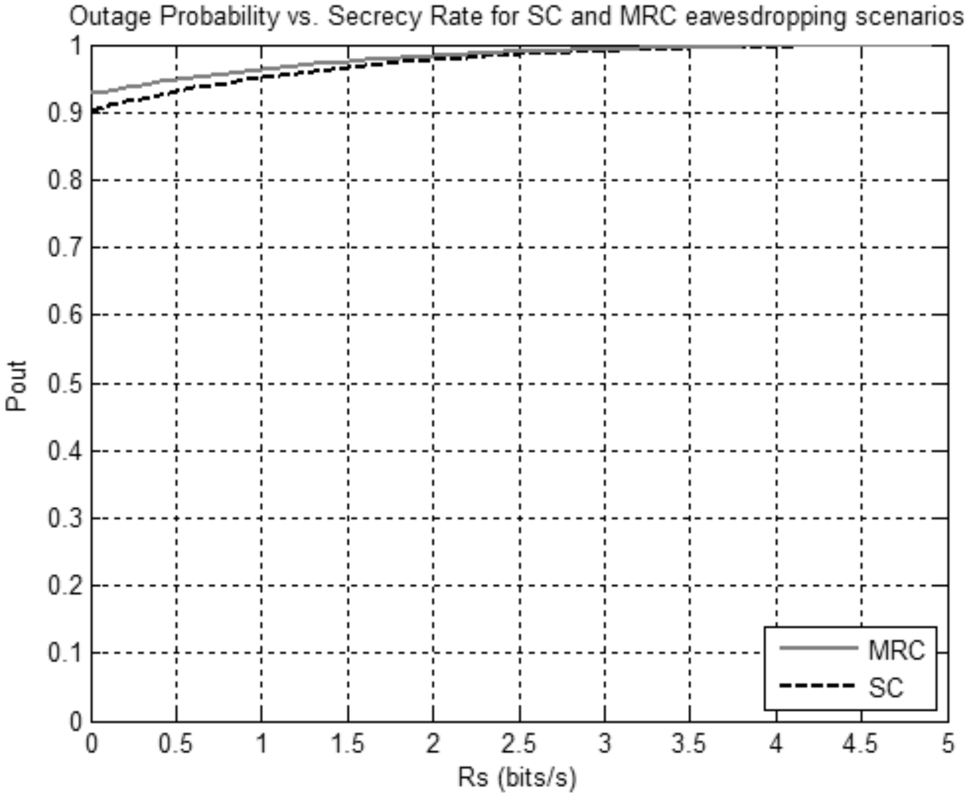

Figure 16: Outage Probability vs. Secrecy Rate for Field Test Trial 6

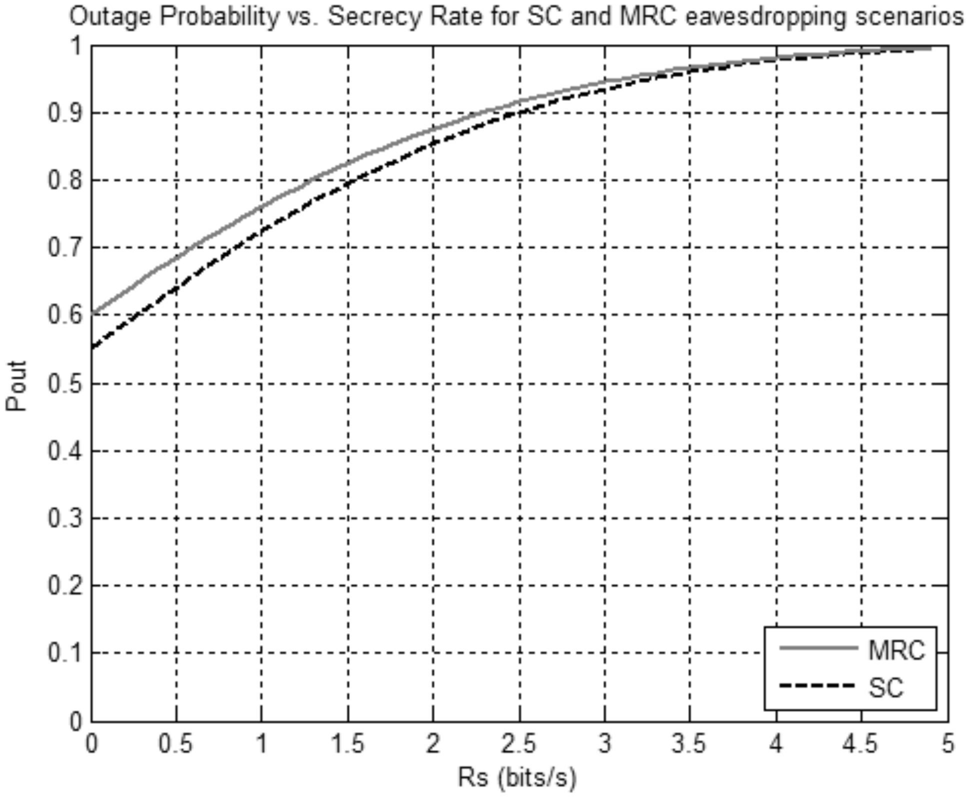

Figure 17: Outage Probability vs. Secrecy Rate for Field Test Trial 7

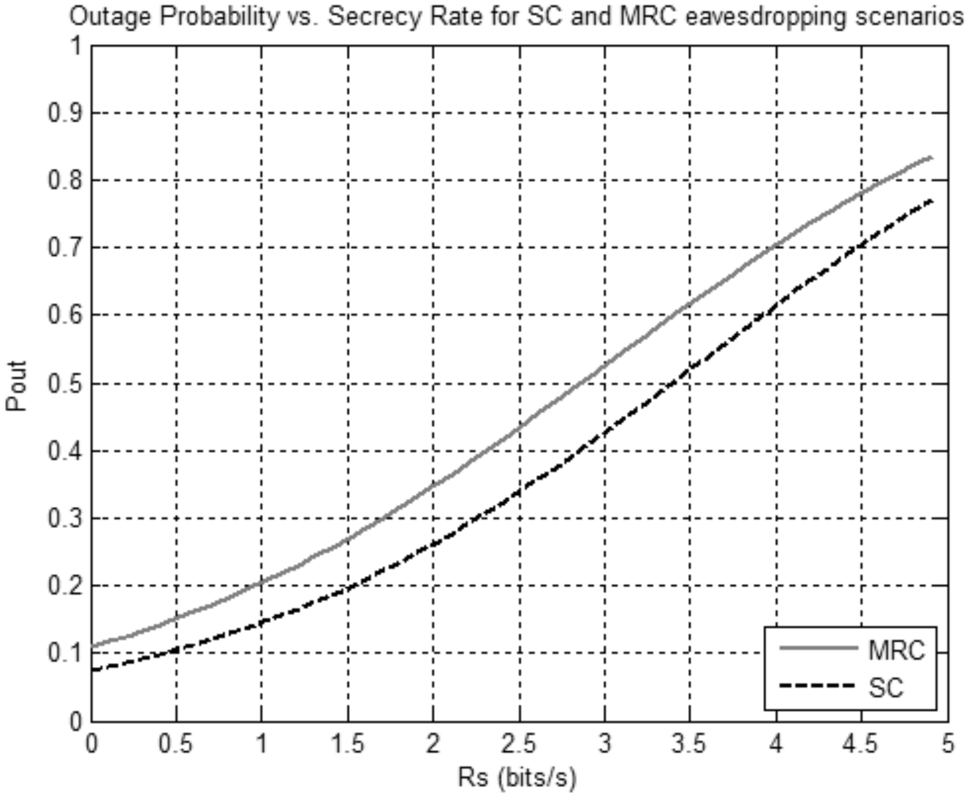

Figure 18: Outage Probability vs. Secrecy Rate for Field Test Trial 8

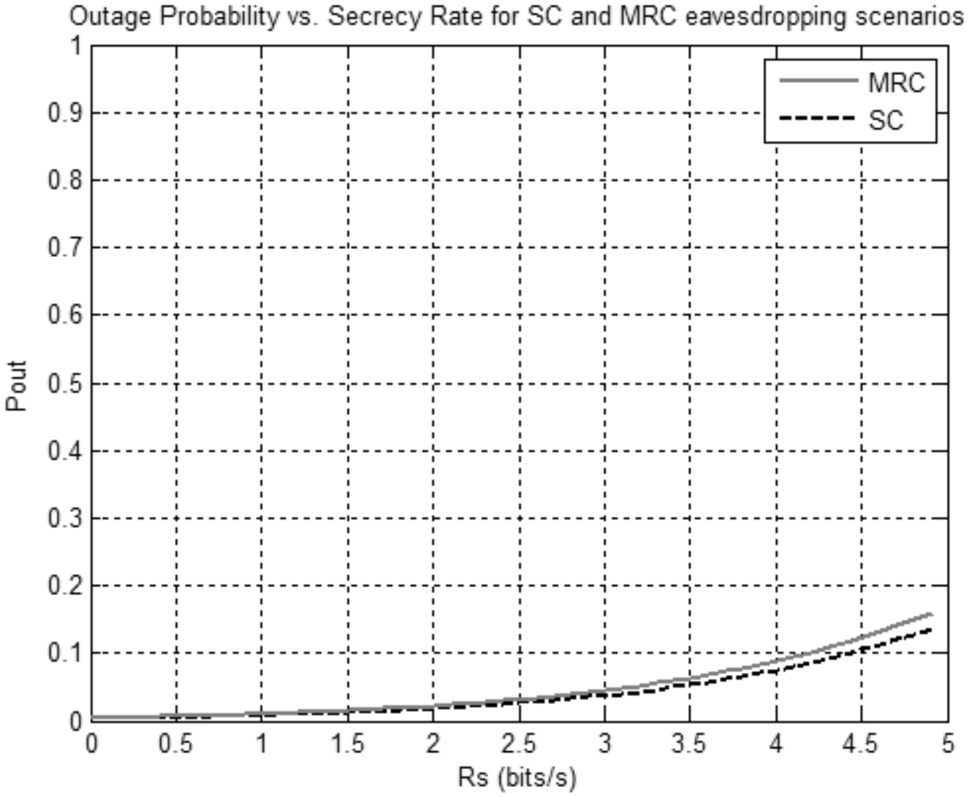

Figure 19: Outage Probability vs. Secrecy Rate for Field Test Trial 10

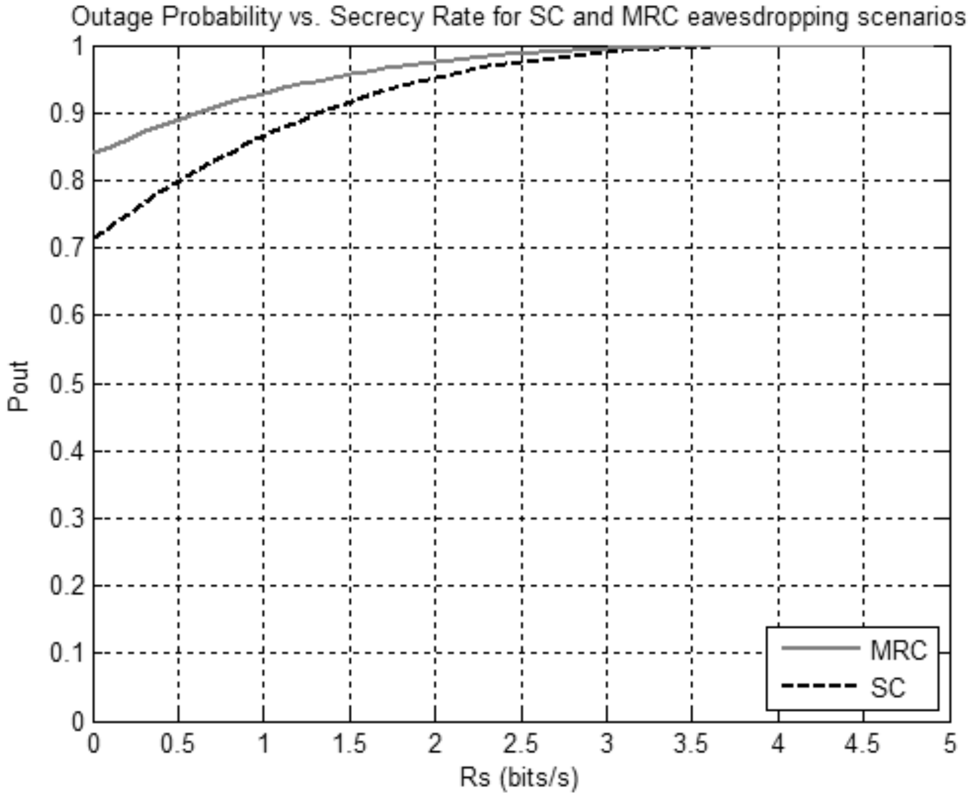

Figure 20: Outage Probability vs. Secrecy Rate for Field Test Trial 11

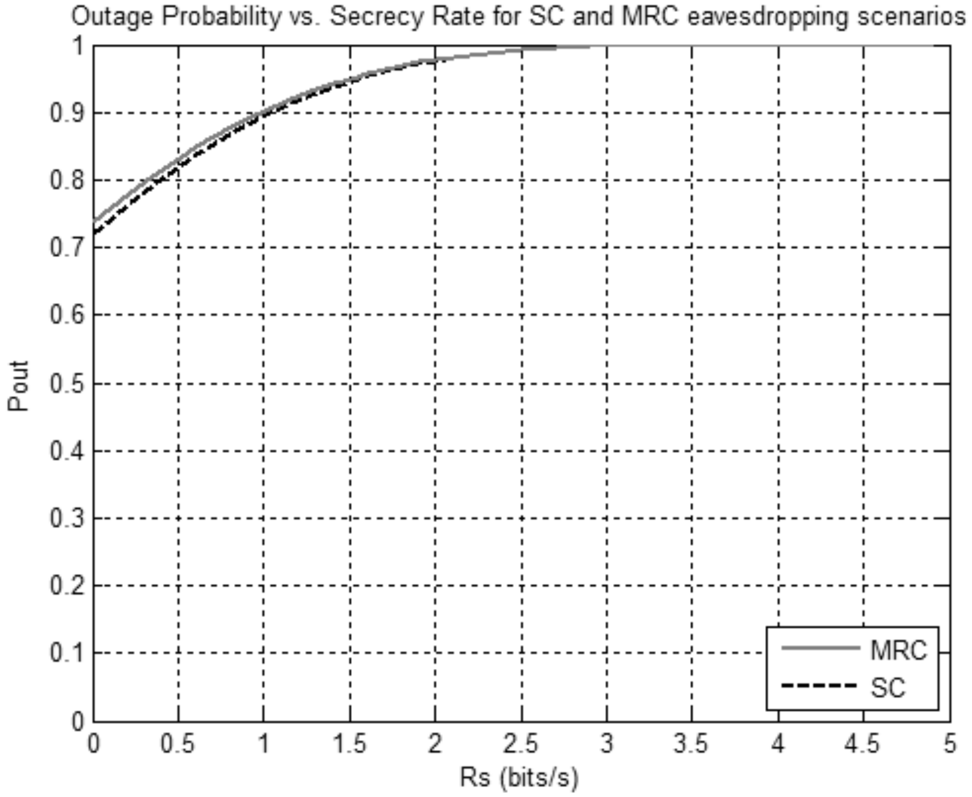

Figure 21: Outage Probability vs. Secrecy Rate for Field Test Trial 12

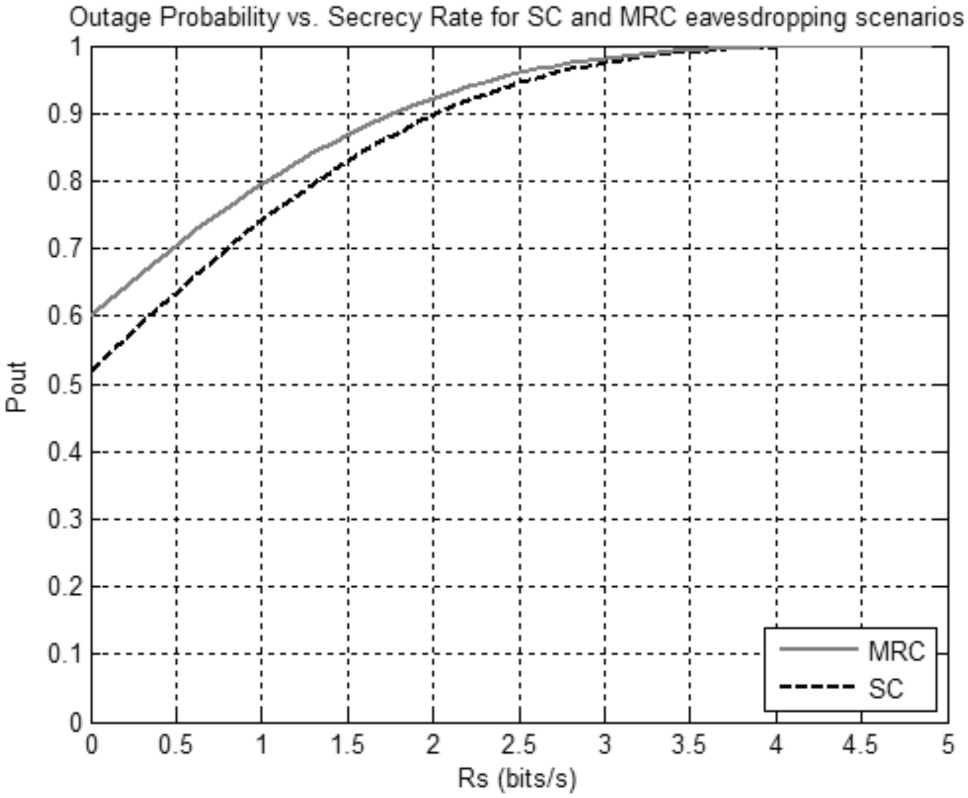

Figure 22: Outage Probability vs. Secrecy Rate for Field Test Trial 15

The results presented in these Figures confirm the findings from the calculation of the Probability of Non-Zero Secrecy Capacity: field test trials 1, 2, 4, 6, 11, 12 are deemed as worst-case scenarios where the WITS solution is severely compromised, field test trials 8, 10 represent scenarios where perfect secrecy is achieved, and field test trials 7 and 15 are middle-of-the-road cases. However, these figures provide analytical information as to the achievable non-zero secrecy capacity in terms of a target secrecy rate (bits/s).

Again, while MRC provides slightly better services to the eavesdropping activity, both SC and MRC techniques offer overall converging results: in field test trials 2, 6, 10, 12. In all other field test trials, the MRC technique offers slightly higher values of Outage Probability, without, however, significant deviations from the respective values provided by the SC scheme.

6 Conclusions

In this work, a theoretical and experimental investigation of the key parameters of WITS in the presence of multiple (k>1) passive malicious users (eavesdroppers) has been studied. Following a previously conducted measurement scenario for a single eavesdropper, the theoretical values for these key parameters are provided for the single eavesdropper case study, and the comparison is being discussed using both SC and MRC schemes.

For the multiple eavesdroppers' case study, a total of 4 malicious users have been considered. We assume that eavesdroppers, as potential technologically-aware terrorists in an urban environment, have knowledge of the topology characteristics, can acquire information about the channel state and are able to cooperate to enhance the eavesdropping before or after an attempted attack or sabotage or bombing (obstacles may either be buildings full standing or destroyed buildings and materials after a terrorist action).

Theoretical analysis in terms of PDF and CDF of P(Cs>0) values have been presented. For the experimental measurements, an 802.11n ad-hoc network consisting of low-speed moving nodes was implemented. The channel was considered interference-bound with a threshold of -85 dBm for all scenarios. The NetStumbler software was used for measuring local-mean received power levels and for the subsequent calculation of SNR values for all nodes. The exact derivation of the eavesdropping SNR is obviously modified for each cooperative scheme and the results provide the boundaries of secure communication while pointing out the importance of the strongest eavesdropper.

The field test trials, i.e. the set of node routes that formed each experimental trial, have been produced via simulation of human movement. The development and software implementation of the HUMO mobility model allowed for a production of 125 total node routes that were realized among buildings and obstacles in the campus of the University of Patras, in the premises of the Department of Electrical and Computer Engineering. In some cases, 1 or 2 nodes were discarded from the eavesdropping cooperative scheme, since in those paths the received power was below the node's sensitivity level. We had, therefore, a variable number of eavesdroppers, ensuring however a minimum of 2 active malicious users (mean value of 2.93≈3 eavesdroppers), in order to guarantee the multiple eavesdropping in each case study. According to this methodology and empirical observation, it is redundant to insert more eavesdroppers in our test-bed: the randomness of the paths employed for each test trial, the obstacles (surrounding buildings) and the intrinsic limitations in EIRP levels and the receiver sensitivity, as well as the fact that the channel is interference-bound at 2.4 GHz, ensure that even if more eavesdroppers are introduced, the average number of 'active' eavesdroppers in each field test trial will not increase significantly.

The calculation of the Probability of Non-Zero Secrecy Capacity was accomplished for two different cooperative techniques for the multiple eavesdroppers: Selection Combining and Maximal-Ratio Combining. Results demonstrated that MRC enhances the eavesdropping performance, with a mean value of 16.73% for the reduction in the values of the Probability of Non-Zero Secrecy Capacity. It was also proven that in 20% of the cases, $P\left(C_s > 0\right) \cong 1$. In 13.33% of the trials, $P\left(C_s > 0\right) \cong 0.5$, whereas in the majority of the cases, 66.67% (2/3 of the field test trials), $P\left(C_s > 0\right) < 0.3$. In order to further investigate if this range of values for the Probability of Non-Zero Secrecy Capacity compromises the physical-layer solution scheme, the Outage Probability is calculated for an upper bound value of a (target) Secrecy Rate. It is interesting to note, however that the reduction caused by the presence of multiple eavesdroppers (MRC scheme) strongly suggests that the combined activity of all active eavesdroppers per field test trial does not strongly exceed the impact of the 'better-listening' eavesdropper.

The theoretical and the empirical CDF of P(Cs>0) values provide similar results, whereas the respective PDF graphs are in generic agreement. The more detailed investigation of the histograms of P(Cs>0) values for each technique confirm that the fluctuation of the P(Cs>0) values are similar to that of the average (local-mean) received power values, described by log-normal large-scale fading. The Gamma distribution however, provides a smoother fit than the Log-normal distribution.

The Outage Probability graphs confirmed these findings and provided analytical values of the achievable Secrecy Capacity in terms of an upper bound (non-zero target Secrecy Rate). The compromise of the WITS scheme is dependent on the Outage Probability for the said target Secrecy Rate. If the Outage Probability assumes a pre-defined fixed value, then the Secrecy Rate will be a variable under investigation and the bounds of accepted values will determine the robustness of the proposed solution. This is part of immediate future work, which consists of calculating the Outage Secrecy Capacity on the basis of the closed-form expression provided in [18], employing the measured SNR values from this work (multiple eavesdroppers scheme).

Acknowledgment.
The authors would like to acknowledge Dr. Christos Papageorgiou, Mr Giannis Georgopoulos, and Mr. Christos Tselios for their assistance during the experimental work.

References

1. Shannon, C. E.: Communication theory of secrecy systems. Bell Tech. J. 29, 656--715, (1949)
2. Wyner, A. D.: The wire-tap channel. Bell Tech. J. 54, 1355--1387, (1975)
3. Csiszar, I., Korner, J.: Broadcast channels with confidential messages. IEEE Trans. Inf. Th. vol. 24, no. 3, 339--348 (1978)

4. Leung-Yan-Cheong, S. K., Hellman, M. E.: The Gaussian wiretap channel, IEEE Trans. Inf. Th. vol. 24, no. 4, 451--456 (1978)

5. Maurer, U. M.: Secret key agreement by public discussion from common information. IEEE Trans. Inf. Th. vol. 39, no. 3, 733--742 (1993)

6. Maurer, U. M.: Information-theoretically secure secret-key agreement by NOT authenticated public discussion. In: Advances in Cryptology - EUROCRYPT '97, LNCS, vol. 1233, pp. 209--225, Springer-Verlag, Heidelberg (1997)

7. Maurer, U. M., Wolf S.: Information-theoretic key agreement: from weak to strong secrecy for free. In: Advances in Cryptology - EUROCRYPT 2000, LNCS, vol. 1807, pp. 351--368, Springer-Verlag, Heidelberg (2000)

8. Barros, J., Rodrigues, M. R. D.: Secrecy capacity of wireless channels. In: 2006 IEEE International Symposium on Information Theory, pp. 356--360. IEEE Press, New York (2006)

9. Bloch, M., Barros, J., Rodrigues, M. R. D., McLaughlin, S.W.: Wireless Information-Theoretic Security. IEEE Trans. Inf. Th. vol. 54, no. 6, 2515--2534 (2008)

10. Bloch, M., Thangaraj, A., McLaughlin, S. W., Merolla, J. M.: LDPC-based Gaussian key reconciliation. In: 2006 IEEE Information Theory Workshop, pp.116--120. IEEE Press, New York (2006)

11. Richardson, T. J., Shokrollahi, M. A., Urbanke, R. L.: Design of capacity-approaching irregular low-density parity-check codes. IEEE Trans. Inf. Th. vol. 47, no. 2, 619--637 (2001)

12.Prabhu, V. U., Rodrigues, M. R. D.: On Wireless Channels with M-Antenna Eavesdroppers: Characterization of the Outage Probability and Outage Secrecy Capacity. IEEE Trans. Inf. For. & Sec., vol. 6, no.3, 853--860 (2011)

13. Rappaport, T.: Wireless Communications: Principles and Practice. Prentice Hall, Upper Saddle River (2001)

14. Parsons, J. D.: The Mobile Radio Propagation Channel. Wiley Interscience, Hoboken (2000)

15. Ozgur, A., Leveque, O., Preissmann, E.: Scaling laws for one and two dimensional random wireless networks in the low attenuation regime. IEEE Trans. Inf. Th. vol. 53, no. 10, 3573--3585 (2006)

16. Seybold, J.: Introduction to RF Propagation. Wiley Interscience, Hoboken (2005)

17. Chrysikos, T., Kotsopoulos, S.: Impact of channel-dependent variation of path loss exponent on Wireless Information-Theoretic Security. In: Wireless Telecommunications Symposium 2009, pp. 1--7. IEEE Press, New York (2009)

18. Chrysikos, T., Dagiuklas, T., Kotsopoulos, S.: A Closed-Form expression for Outage Secrecy Capacity in Wireless Information-Theoretic Security. In: Security in Emerging Wireless Communication and Networking Systems – SEWCN 2009, LNCS, vol. 42, pp. 3--12, Springer, Heidelberg (2010)

19. Atsan, E. and Ozkasap, O.: A classification and performance comparison of mobility models for ad hoc networks. In ADHOC-NOW, pp. 444–457, 2006.

20. Aschenbruck, N., Gerhards-Padilla, E., Martini, P.: Modeling mobility in disaster area scenarios. In Perform. Eval., Vol. 66, No.12, pp. 773–790, 2009.

21. Johnson, D. and Maltz. D., "Dynamic source routing in ad hoc wireless networks, Mobile Computing, pp. 153–181. Kluwer Academic Publishers, 1996.

22. Royer, E., Melliar-Smith, P. and Moser, L., ".An analysis of the optimum node density for ad hoc mobile networks. In Proc.of the IEEE Int'l Conf. on Communications, pp. 857–861, 2001.

23. Kamal, A. and Al-Karaki, J., "A new realistic mobility model for mobile ad hoc networks. In IEEE Int'l Conf. on Communicatons, pp. 3370–3375, 2007.

24. Papageorgiou, C., Birkos, K., Dagiuklas, T., Kotsopoulos. S., "An obstacle-aware human mobility model for ad hoc networks", In Proc. of the 17th IEEE/ACM International Symposium on Modelling, Analysis and Simulation of Computer and Telecommunication Systems (MASCOTS), 2009.

25. Papageorgiou, C., Birkos, K., Dagiuklas, T., Kotsopoulos. S., “Simulating mission critical mobile ad hoc networks. In Proc. of the 4th ACM workshop on Performance monitoring and measurement of heterogeneous wireless and wired networks (PM2HW2N), 2009.

26. Papageorgiou, C., Birkos, K., Dagiuklas, T., Kotsopoulos, S., “Modelling Human Mobility in Obstacle-constrained Ad Hoc Networks”, Elsevier Ad-Hoc networks, 2011

27. Pinto, P.C., Barros, J., Win, M.J.: Physical-layer security in stochastic wireless networks. In: 2008 IEEE International Conference on Communication Systems, pp. 974--979. IEEE Press, New York (2008)

28. Pinto, P.C., Barros, J., Win, M.J.: Wireless physical-layer security: the case of colluding eavesdroppers. In: 2009 IEEE International Conference on Symposium on Information Theory, pp. 2442--2446. IEEE Press, New York (2009)

29. Chrysikos, T., Dagiuklas, T., Kotsopoulos, S.: Wireless Information-Theoretic Security for Moving Users in Autonomic Networks. In: IFIP Wireless Days 2010, pp. 1-5. IEEE Press, New York (2010)

30. Chrysikos, T., Dagiuklas, T., Kotsopoulos, S: Wireless Information-Theoretic Security in an Outdoor Topology with Obstacles: Theoretical Analysis & Experimental Measurements. EURASIP Journal on Wireless Communications and Networking, Special Issue on Security and Resilience for Smart Devices and Applications, doi:10.1155/2011/628747 (2011)

31. Jakes, W. C. (Ed.): Microwave mobile communications. Wiley Interscience, New York (1974)

32. http://www.isi.edu/nsnam/ns/

33. http://www.netstumbler.com

34. Chrysikos, T., Georgopoulos, G., Kotsopoulos, S.: Empirical Calculation of Shadowing Deviation for Complex Indoor Propagation Topologies at 2.4 GHz. In: International Conference on Ultra Modern Telecommunications – ICUMT 2009, pp. 1--6. IEEE Press, New York (2009)

35. Chrysikos, T., Dagiuklas, T., Kotsopoulos, S.: Wireless Information-Theoretic Security in MANETs. In: IEEE International Conference on Communications - IEEE ICC 2013, pp. 1--5. IEEE Press, New York (2013)