Physical Communication ▮ (▮▮▮▮) ▮▮▮–▮▮▮

Contents lists available at ScienceDirect

Physical Communication

journal homepage: www.elsevier.com/locate/phycom

Full length article

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

Theofilos Chrysikos [a,*], Konstantinos Birkos [a], Tasos Dagiuklas [b], Stavros Kotsopoulos [a]

[a] Department of Electrical & Computer Engineering, University of Patras, Greece

[b] Division of Computer Science and Informatics, London South Bank University, United Kingdom

ARTICLE INFO

Article history:
Received 18 November 2015
Received in revised form
30 September 2016
Accepted 18 November 2016
Available online xxxx

Keywords:
Wireless security
Rayleigh channels
Ad-hoc networks
Diversity

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, the 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.

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.

Abbreviations: WITS, Wireless Information-Theoretic Security; HUMO, Human Mobility Model; NS-2, Network Simulator - 2.

* Correspondence to: P.O.BOX 1182, Patras, 26223, Greece.
E-mail addresses: txrysiko@ece.upatras.gr (T. Chrysikos), kmpirkos@ece.upatras.gr (K. Birkos), tdagiuklas@lsbu.ac.uk (T. Dagiuklas), kotsop@ece.upatras.gr (S. Kotsopoulos).

http://dx.doi.org/10.1016/j.phycom.2016.11.003
1874-4907/

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 follows: 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 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 $\bar{\gamma}_M$ is less than the wiretap channel SNR $\bar{\gamma}_W$, albeit with a possibility less than 0.5 [8]:

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

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:

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

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, $\bar{\gamma}_M$ and $\bar{\gamma}_W$ respectively [9]:

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

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

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

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 [19].

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 [20,21]. 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 [22]. 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) [23], Realistic Mobility Model (speed and direction follow distributions that yield that mimic node movement) [24].

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 [25,26]. 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 Fig. 1 [27].

4. Wireless Information-Theoretic Security with a single eavesdropper

4.1. Theoretical analysis

In [28,29] 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

Please cite this article in press as: T. Chrysikos, et al., Wireless Information-Theoretic Security: Theoretical analysis & experimental measurements with multiple eavesdroppers in an outdoor obstacle-dense MANET, Physical Communication (2016), http://dx.doi.org/10.1016/j.phycom.2016.11.003