Ad Hoc Networks 21 (2014) 123–133

Contents lists available at ScienceDirect

Ad Hoc Networks

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

Secrecy transmission capacity in noisy wireless ad hoc networks

Jinxiao Zhu [a,b,*], Yin Chen [a], Yulong Shen [b], Osamu Takahashi [a], Xiaohong Jiang [a], Norio Shiratori [c,d]

[a] School of Systems Information Science, Future University Hakodate, Hakodate 041-8655, Japan
[b] State Key Laboratory of Integrated Services Networks (ISN), Xidian University, Xi'an 710071, PR China
[c] GITS, Waseda University, Tokyo 169-0051, Japan
[d] RIEC, Tohoku University, Sendai-shi 980-8579, Japan

ARTICLE INFO

Article history:
Received 20 December 2013
Received in revised form 22 March 2014
Accepted 18 May 2014
Available online 24 May 2014

Keywords:
Physical layer security
Transmission capacity
Wireless networks
Secrecy outage probability

ABSTRACT

This paper considers the transmission of confidential messages over noisy wireless ad hoc networks, where both background noise and interference from concurrent transmitters affect the received signals. For the random networks where the legitimate nodes and the eavesdroppers are distributed as Poisson point processes, we study the secrecy transmission capacity (STC), as well as the connection outage probability and secrecy outage probability, based on the physical layer security. We first consider the basic fixed transmission distance model, and establish a theoretical model of the STC. We then extend the above results to a more realistic random distance transmission model, namely nearest receiver transmission. Finally, extensive simulation and numerical results are provided to validate the efficiency of our theoretical results and illustrate how the STC is affected by noise, connection and secrecy outage probabilities, transmitter and eavesdropper densities, and other system parameters. Remarkably, our results reveal that a proper amount of noise is helpful to increase the secrecy transmission capacity.

1. Introduction

The inherent openness of wireless medium makes information security one of the most important and difficult problems in wireless networks. Traditionally, information security is ensured by applying cryptography which encrypts a plain message into a ciphertext that is computationally infeasible for any adversary without the key to break (decrypt). However, due to the improvement in computing technology and complication in cryptographic key management, there is an increasing concern that the cryptography no longer suffices, especially in sensitive applications requiring everlasting secrecy. Recently, the physical layer security has been widely demonstrated as a promising approach to providing everlasting secrecy. Unlike the traditional cryptography that ignores the difference between transmitting channels, the recent physical layer security achieves information-theoretic security by properly designing wiretap channel code according to the channel capacities [1,2] such that the original data can be hardly recovered by the eavesdropper regardless of how strong the eavesdropper's computing power is.

Considerable research efforts have been devoted to understand the performance of physical layer security. Wyner initially studied the maximum secret information rate, namely secrecy capacity, for a discrete memoryless wire-tap channel, where only three nodes are involved

[*] Corresponding author at: State Key Laboratory of Integrated Services Networks (ISN), Xidian University, Xi'an 710071, PR China. Tel.: +81 0138 34 6226.

E-mail addresses: jxzhu1986@gmail.com (J. Zhu), ychen1986@gmail.com (Y. Chen), ylshen@mail.xidian.edu.cn (Y. Shen), Osamu@fun.ac.jp (O. Takahashi), jiang@fun.ac.jp (X. Jiang), norio@shiratori.riec.tohoku.ac.jp (N. Shiratori).

http://dx.doi.org/10.1016/j.adhoc.2014.05.014
1570-8705/© 2014 Elsevier B.V. All rights reserved.

(one transmitter, one legitimate receiver and one eavesdropper), and showed the existence of channel codes to ensure the message is reliably delivered to the legitimate receiver while secured at the eavesdropper [1]. Wyner's work was then extended to other channel models, such as Gaussian wire-tap channel [2], fading wire-tap channel with or without channel correlations [3–6], broadcast channels with confidential messages [7]. Based on these pioneering works on the basic point-to-point wire-tap channels, many recent research efforts have been conducted to understand the performances of physical layer security in large-scale wireless networks, where lots of legitimate nodes and eavesdroppers are involved, in terms of secrecy throughput capacity [8–11], secrecy coverage [12], connectivity [13–16] and percolation phenomenon [10,17,18] under secrecy constraints, etc.

This paper focuses on the study of secrecy transmission capacity (STC) in large-scale wireless networks, which is defined as the achievable rate of successful transmission of confidential messages per unit area of a network, subject to constraints on both connection outage probability and secrecy outage probability. It is notable that the STC indicates the area spectral efficiency (ASE) of wireless networks under the given constraints on the levels of reliability and security, and hence it is of fundamental importance and can serve as a guideline for the design and development of wireless networks. Besides, compared with the aforementioned studies on the *secrecy throughput capacity* of large-scale wireless networks that only provide scaling law results [8–11], exact results can be obtained from STC study, which can lead to a finer optimization on network performance.

Some prior works on STC have been done by Zhou et al. in [19,20], where the authors calculated the secrecy transmission capacity for decentralized wireless networks with a fixed distance transmission scheme under the signal-to-interference ratio (SIR) model that neglects the impact of background noise. It is noticed that the background noise is a ubiquitous natural phenomenon and ignoring it may cause inaccuracy in the performance estimation. Moreover, it is also noticed that the additional noise on one hand is harmful to the reliability of a transmission since it makes the signal received at the intended receiver worse, on the other hand is helpful to the security performance since it makes the signal received at eavesdroppers worse. Hence, a natural question to ask is what is the overall impact of the noise on the STC. Accordingly, a new study is still required to investigate the exact STC in wireless networks under the impact of background noise.

In this work, we focus on the secrecy transmission capacity in noisy wireless ad hoc networks where interference from concurrent transmitters and background noise from natural and sometimes man-made sources affect the received signals. The main contributions of this paper are as follows.

- Based on the tools from stochastic geometry, we start the analysis from a basic fixed transmission distance scenario where each transmitter has an intended receiver at a fixed distance which is the same for all transmitters. We establish a general theoretical model of the STC, as well as the connection outage probability and secrecy outage probability, under the signal-to-interference-noise ratio (SINR) model. Furthermore, for the special scenario when the path-loss exponent $\alpha = 4$ and noise power is the same across space and time slots, we derive a closed-form STC and then propose a condition to achieve a positive STC.
- We then extend the analysis of STC to a more realistic random transmission scenario, nearest receiver transmission in particular, and present the corresponding connection outage probability and STC. It is noticed that the transmission distance has no impact on the secrecy outage probability.
- Finally, we provide extensive simulation and numerical results to validate the efficiency of our theoretical models and also to illustrate our theoretical findings. Remarkably, our results indicate that a proper amount of noise can be helpful to increase the secrecy transmission capacity.

The remainder of this paper is organized as follows. Section 2 presents the system model and performance metrics based on the physical layer security. In Section 3, we obtain analytical results on the secrecy transmission capacity for the fixed transmission distance scenario. Then, Section 4 extends the analysis to the nearest receiver transmission scenario. In Section 5, we validate the theoretical models by simulations and analyze the tradeoff between the system parameters. Finally, concluding remarks are given in Section 6.

2. System model and performance metrics

In this section, we introduce the basic system model of this paper and the performance metrics based on the physical layer security. The notation and symbols used throughout the paper are summarized in Table 1. Random variables are denoted by upper-case Roman letters throughout the paper, e.g., W, H and I.

2.1. System model

We consider an ad hoc wireless network consisting of both legitimate nodes and eavesdroppers over a two-dimensional Euclidean space $\mathbb{R}^2$. For each time snapshot, locations of legitimate nodes are modeled as a homogeneous Poisson point process (PPP) Φ with density λ, denoted by $\Phi = \{X_i\}$, where $X_i \in \mathbb{R}^2$ is the location of the legitimate node i, and locations of eavesdroppers are modeled as a PPP Φ_e with density λ_e, denoted by $\Phi_e = \{X_e\}$, where $X_e \in \mathbb{R}^2$ is the location of the eavesdropper node e. The PPP model for node locations is suitable when the nodes are independently and uniformly distributed over the network area, which is often reasonable for networks with indiscriminate node placement or substantial mobility [21]. The slotted ALOHA is employed at legitimate nodes as the medium access control (MAC) protocol. That is, in each time slot, each legitimate node independently decides to transmit with probability p or act as a potential receiver otherwise. Hence, in each time slot, the set of all transmitters forms a PPP Φ_T with density $\lambda_\mathrm{T} = p\lambda$ and the set of all receivers forms a PPP Φ_R with density $\lambda_\mathrm{R} = (1-p)\lambda$. Notice that $\Phi = \Phi_\mathrm{T} \cup \Phi_\mathrm{R}$.