Computer Networks 81 (2015) 258–271

Contents lists available at ScienceDirect

Computer Networks

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

Optimal power allocation for protective jamming in wireless networks: A flow based model

Siddhartha Sarma *, Joy Kuri

Department of Electronic Systems Engineering, Indian Institute of Science, Bangalore, Karnataka 560012, India

ARTICLE INFO

Article history:
Received 30 June 2014
Received in revised form 22 November 2014
Accepted 14 February 2015
Available online 21 February 2015

Keywords:
Wireless network
Optimal power allocation
Friendly jamming
Eavesdroppers
Scheduling
Vulnerability region

ABSTRACT

We address the problem of *passive eavesdroppers* in multi-hop wireless networks using the technique of *friendly jamming*. The network is assumed to employ *Decode and Forward* (DF) relaying. Assuming the availability of perfect channel state information (CSI) of legitimate nodes and eavesdroppers, we consider a *scheduling* and *power allocation* (PA) problem for a multiple-source multiple-sink scenario so that eavesdroppers are jammed, and source–destination throughput targets are met while minimizing the overall transmitted power. We propose *activation sets* (AS-es) for scheduling, and formulate an optimization problem for PA. Several methods for finding AS-es are discussed and compared. We present an approximate linear program for the original nonlinear, non-convex PA optimization problem, and argue that under certain conditions, both the formulations produce identical results. In the absence of eavesdroppers' CSI, we utilize the notion of *Vulnerability Region* (VR), and formulate an optimization problem with the objective of minimizing the VR. Our results show that the proposed solution can achieve power-efficient operation while defeating eavesdroppers and achieving desired source–destination throughputs simultaneously.

1. Introduction

Though the open access nature of wireless transmission makes the deployment of ad hoc networks easier, it also facilitates eavesdropping in such networks. An adversary with an appropriate receiver can easily intercept radio transmissions. In many application scenarios (*e.g.* battlefield, rescue operations in the presence of malicious adversary), ensuring data secrecy is crucial to successful operation.

Though *frequency hopping* can be used to avoid eavesdropping, such schemes can be jeopardized if the adversary uses a wideband scanner; this can indicate the channel where transmission is taking place, and the adversary can switch to that channel. Cryptographic measures, the well-accepted and current trend in network security, are only effective if the adversary is unaware of the secret keys. To retrieve those keys, an adversary can either capture a node and probe it, or run some computation intensive programs on intercepted packets. With advances in VLSI technology, devices with superior computational capabilities are now feasible. Hence, cryptographic measures may not be able to guard against such adversaries for long [1]. Generating and distributing pairwise keys on a regular basis is an alternate but cumbersome solution. In addition to that, due to hardware and power constraints, it might be impractical to implement sophisticated cryptographic schemes in low power sensor networks [2].

Another characteristic of wireless networks is *interference*. Concurrent transmissions from multiple wireless

* Corresponding author.
E-mail addresses: siddharth@dese.iisc.ernet.in (S. Sarma), kuri@dese.iisc.ernet.in (J. Kuri).

http://dx.doi.org/10.1016/j.comnet.2015.02.011
1389-1286/© 2015 Elsevier B.V. All rights reserved.

devices over the same frequency can not only interfere at the receiver but also make reception completely unintelligible. We use this intrinsic property of wireless networks to ensure data security.

The *information theoretic* study of secure communication was initiated by Wyner in his seminal paper "*The Wiretap Channel*" [3]. Wyner considered a degraded channel for the eavesdropper and showed that a non-zero *secrecy rate* is achievable. Following his work, several authors [4–11] have proposed schemes to ensure secure communication for different network configurations. The basic idea remains same: ensure a better channel between source 'S' and destination 'D' as compared to source to eavesdropper 'E' channel either by improving the S–D channel with the help of relays or by degrading S–E channel using jammers or both. While the motivation behind those papers was to understand the fundamental limits of secure communication, their analyses do not fit in many scenarios involving practical wireless networks. For example, all the works mentioned above were limited to simple one-hop or two-hop networks, whereas, a real world network can have multiple sources, sinks and communicate via multiple hops, as shown in Fig. 1. We, therefore, propose a novel and pragmatic framework to address the issue of secure communication in multi-hop networks with multiple sources and sinks.

In our paper, we consider an SINR based model, where the decodability of an encoded message depends on the SINR at the receiving node. This is indeed true for several modulation schemes, as manifested by the observation that bit error rate (BER) increases with decreasing SINR [12]. Therefore, if we bring down the SINR at the eavesdropper below a certain threshold, then we can ensure a significant BER at the eavesdropper, thereby ensuring that the message cannot be decoded correctly. On the contrary, we want the SINR at the receiver to be above a certain threshold, thereby ensuring secure transmission with high probability. In fact, a stricter form of this approach is known as "zero-forcing" [7] in the *physical layer security* literature, where the eavesdropper SNR is brought down to zero.

To motivate our work, we give two simple examples which are the building blocks of our model and related analysis. In Fig. 2(a), two transmitters are sending messages simultaneously to their respective receivers, causing interference at the eavesdropper and consequent deterioration of its SINR. On the other hand, in Fig. 2(b), a dedicated friendly jammer is interfering with the eavesdropper's reception.

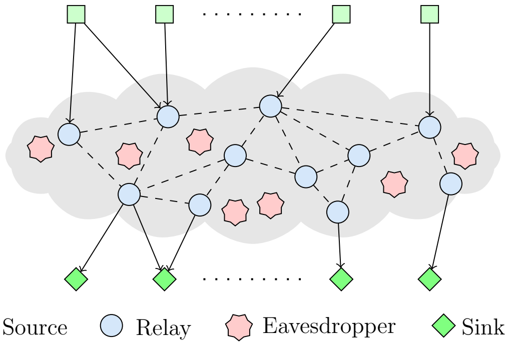

Fig. 1. A general multi-hop network with multiple sources, multiple sinks and multiple eavesdroppers.

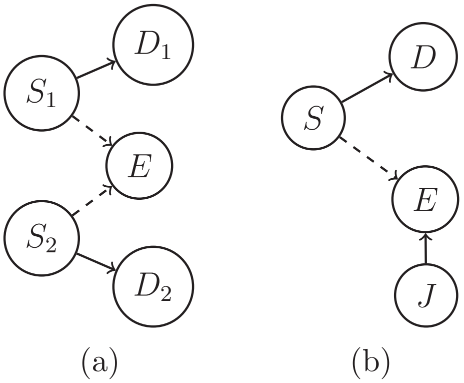

Fig. 2. (a) Simultaneous transmissions cause interference at the eavesdropper. (b) Use of a dedicated jammer to introduce interference at the eavesdropper.

In our previous work [13], we have shown that by exploiting the above mentioned structures present in a network, one can provide end-to-end secure transmission for a single source, single sink multi-hop network. In [13], we considered a weighted function of total power and throughput to circumvent the nonlinearity of the objective function. In the current work, not only have we extended the framework from a single source-sink scenario to multi source-sink scenario, but also approximated the power allocation problem by a linear program, without changing the objective function. As in our previous work, we have assumed the Decode and Forward (DF) relaying strategy, *i.e.*, every transmission is decoded at an intermediate relay node and then it is re-encoded before transmission. Eavesdropping nodes are spread across this network and are trying to eavesdrop on every transmission within their hearing range. For initial analysis, we assume that all the channel gains (including those of the channels to the eavesdroppers) are known. Later, we relax the assumption regarding eavesdroppers' CSI. We use the notion of *Vulnerability Region (VR)* [14] in this context and formulate an optimization problem for optimal power allocation.

In an interference-prone wireless network, if we allow the nodes to transmit arbitrarily, then barely any transmission will be successful. To resolve this, we adopt the idea of *Maximal Independent Set (MIS)*, with necessary modifications. We name these modified sets as *Activation Sets (AS-es)* and address power allocation (PA) for them with a twofold motive: (1) reducing interference at each legitimate receiver, and (2) increasing interference at each eavesdropper. We formulate an optimization problem for power allocation, which turns out to be nonlinear and non-convex. So, we reformulate it as an approximate linear program, which yields the same objective function value as the original optimization problem under certain conditions.

Throughout our paper, we assume a centrally coordinated and highly synchronous data transmission process.