Available online at www.sciencedirect.com

ScienceDirect

Electronic Notes in DISCRETE MATHEMATICS

Electronic Notes in Discrete Mathematics 57 (2017) 199–204 www.elsevier.com/locate/endm

Anonymous Coherent Network Coding Against Eavesdropping and Jamming

Oksana Trushina [1,2] Ernst Gabidulin [1,3]

Department of Radio Engineering and Cybernetics
Moscow Institute of Physics and Technology
Moscow, Russian Federation

Abstract

This paper considers a problem of anonymous transmission against eavesdropping and jamming in coherent network coding. We propose an information-theoretical message unlinkability scheme based on coset coding. We show that if an incoming message is transformed to another message of the same coset by adding a random codeword then the incoming and outgoing messages are statistically independent and consequently, unlinkable.

Keywords: Anonymity, Network Coding, Coset Coding.

1 Introduction

An anonymous coherent network coding method against eavesdropping was described in the paper [6]. This work addresses the problem of anonymity guarantee in coherent network coding system against both eavesdropping and jamming.

[1] Supported in part by the Russian Foundation for Basic Research, project № 15-07-08480
[2] Email: oksana.trushina@gmail.com
[3] Email: ernst_gabidulin@yahoo.com

http://dx.doi.org/10.1016/j.endm.2017.02.033

Network coding [1] is a new idea of information transmission. Different network coding scenarios and network coding schemes providing secrecy of message content are widely studied. The other important information security issue is anonymity. In this work, we say that the transmission is anonymous if an adversary can not determine who communicates with whom. The task is to guarantee a message forwarding to be untraceable. A primary goal is to provide *bitwise unlinkability* or simply *unlinkability*. Unlinkability guarantees that incoming and outgoing messages "look" different, so an adversary can not correlate incoming and outgoing messages just by comparing symbols composing them.

We consider linear coherent network coding. The relay nodes transmit linear combination of incoming packets with coefficients being specified in advance. This coefficients form *coding vector*. The linear dependence between incoming and outgoing packets may be used by an adversary to determine who sends message to whom. Consider a toy example (Fig. 1). There are two source nodes S_1 and S_2 and two sink nodes D_1 and D_2. Node S_1 sends message containing two packets $a,\ b$ to node D_1, while node S_2 sends packets $c,\ d$ to node D_2. The coding vectors and corresponding linear combinations are pictured in the figure. An adversary may eavesdrop all incoming links of node r obtaining packets $a+b,\ a+2b$ from S_1 and $c+3d,\ 2c+d$ from S_2. On eavesdropping link $r \to D_1$ an adversary obtains a message $5a+7b$. The link $r \to D_1$ has coding vector $(3,2)$. An adversary can see that $3(c+3d)+2(2c+d) \neq 5a+7b$, while $3(a+b)+2(a+2b) = 5a+7b$. This provides an adversary with convincing evidence that node D_1 is a sink node for node S_1.

The most straightforward way to provide unlinkability is encryption. The pioneer work on anonymous transmission [2] having evolved into famous Onion Routing is based on encryption. We propose scheme to provide unlinkability based on the coset coding idea. Coset coding allows us to change an incoming message in a very simple and elegant way so that an outgoing message "looks" very differently. Particularly, incoming and outgoing messages are statistically independent. So we propose information-theoretical model of anonymity in contrast to computational model based on encryption.

2 Preliminaries

2.1 Network Model

A network is represented by a directed multigraph with error free unit capacity edges. There are several source nodes and several destination nodes. Data is