Int. J. Electron. Commun. (AEÜ) 69 (2015) 467–472

Contents lists available at ScienceDirect

International Journal of Electronics and Communications (AEÜ)

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

SHORT COMMUNICATION

Secure random linear network coding on a wiretap network

Zhanghua Cao[a,*], Shibing Zhang[a], Xiaodong Ji[a], Lai Zhang[b]

[a] School of Electronics and Information, Nantong University at Nantong, Jiangsu Province 226019, PR China
[b] Department of Mathematics and Mathematical Statistics, Umeå University, Umeå SE-90187, Sweden

ARTICLE INFO

Article history:
Received 30 April 2014
Accepted 20 October 2014

Keywords:
Wiretap networks
Information theoretic security
Random linear network coding
Secret sharing
One-time pad

ABSTRACT

We develop a secure random linear network coding scheme on wiretap networks where a wiretapper can only eavesdrop on a limited number of channels. On one hand, by refining Lima's "locked coefficients" method and applying the approach of one-time pad, our scheme can well protect message packets without decreasing network throughput. On the other hand, by treating ciphertext as noisy symbols, inspired by the physical layer technique, and applying Shamir's secret sharing scheme, our scheme can successfully protect secret random seed without any forms of key exchange or secret channels. Compared to existing schemes, our scheme has minimum information overhead, independency of hash functions, and no restriction on global encoding kernel. Finally, we analyze the computational complexity of our proposed scheme and rigorously prove that our scheme can achieve secure network communication.

1. Introduction

Network coding is a generalization of traditional store and forward routing scheme [1]. While network coding greatly advances data transmission and network reliability [2,3], it brings forward new security challenges to the emergent network coded systems [4]. There are basically four groups of secure network coding schemes against external wiretappers.

The first group is the schemes of information theoretic security. Cai and Yeung [5] developed a secure linear network code based on the assumption that an external wiretapper can access only a limited number of channels. Wang and Guo [6] considered the perfect security in linear network coding using well-designed precoding matrix. The construction of precoding matrix is equivalent to finding proper encoding vectors that realize perfectly secure transmission of secret message. Rouayheb [8] proposed a secure protocol by combining the Ozarow–Wyner approach [7] of coset coding at the source with inherent security. A secure network coding with nonuniform or restricted wiretap sets was studied in [9]. A common drawback of these schemes is the linear reduction in communication rate with increasing number of channels obtained by wiretappers.

The second group is the weakly securing network coding. This type of coding schemes can maximize network throughput while ensuring that eavesdropper gets no information about each packet [10–13]. Wei et al. [11] developed a weakly secure network coding scheme by using a random permutation function which enables them to map every element in the code field to another element in the same field. By assuming that all intermediate nodes are potential wiretappers, Du et al. [12] proposed a secure scheme that relies only on network topology and showed that eavesdroppers cannot acquire any information from secure message packets. A probabilistic weak security for linear network coding was investigated in [13]. Although network throughput can be maximized, the weak security of network code is realized at the expense of restricting the selection of global encoding kernel.

The third group is the secure network coding schemes that built on cryptographic hash functions. Adeli and Liu [14] developed a secure linear network coding scheme with hash functions by imposing a restriction on the global encoding kernel, and their scheme can successfully minimize information overhead. This scheme was improved by removing the restriction on the coding kernel [15]. However, this type of schemes requires computation of the hash values of each packet, thereby burdening network communication.

The last group is the schemes that employ secret key exchanges or secret channels [16,17]. This type of schemes first generates locked coefficients randomly, then encrypts them with the keys shared with the destinations, and finally adds locked coefficients to packet header. A nonlinear secret key agreement was considered in [17]. This type of schemes increases not only communication delay but also algorithm complexity.

To overcome the limitations of above schemes, we propose here a secure random linear network coding scheme by improving

[*] Corresponding author. Tel.: +86 13815211319.
E-mail address: cryptocaozhanghua@126.com (Z. Cao).

http://dx.doi.org/10.1016/j.aeue.2014.10.018
1434-8411/© 2014 Elsevier GmbH. All rights reserved.

Lima's method of "locked coefficients" [16], and utilizing the one-time pad encryption scheme, the Shamir's secret sharing scheme as well as the physical layer technique. Specifically, the improved "locked coefficients" approach and one-time pad encryption scheme are applied to protect source packets, while combination of the Shamir's secret sharing scheme and the idea of physical layer technique enables us to transmit the secret random data to sink nodes securely. In this way, we can obtain a perfectly secure linear network coding scheme with a network utilization $1-1/n$, where n is the network capacity.

The remainder of this paper is organized as follows. In Section 2, we give a brief review on the employed notations and general assumptions. The proposed secure linear network coding is described in Section 3, and a corresponding security analysis is provided in Section 4. The paper is closed with a brief conclusion.

2. Preliminaries

2.1. Network model

A multicast communication network is a collection of directed edges connecting transmitters, switches, and receivers, and usually represented by a directed graph $G=(V, E)$, where V and E are, respectively, the set of network nodes and the set of network edges. In our model, we assume that G is acyclic and delay free, and each directed edge has a unit capacity. The network capacity is defined as $n=\min\{maxflow(s, t_i): t_i\in V_D\}$, where V_D is a collection of destination nodes and $maxflow(s, t_i)$ characterizes the max-flow from a source node s to a destination node $t_i\in V_D$.

A wiretap network means that there is a passive adversary who can access at most $n-1$ channels of a multicast communication network with a capacity n. The wiretap network can be regarded as a generalization of Ozarow and Wyner's model of wiretap channel II [7]. In our model, we assume that a wiretapper knows the proposed encryption and decryption schemes.

Network coding is described as follows. Let $G=(V, E)$ be a multicast communication network with capacity n, which indicates that the source node s sends n packets $x_1, x_2, \ldots, x_n\in(\mathrm{F}_q)^{\lambda}$ to destinations at each time instant. Here F_q is a finite field. The packet transmitted through channel $e\in E$ is denoted by $Y(e)$. For any intermediate node $v\in V$, let $d_1, d_2, \ldots, d_\eta$ be the edges ending at v and e_i an outgoing edge of v. According to linear network coding, $Y(e_i)=\alpha_1 Y(d_1)+\alpha_2 Y(d_2)+\cdots+\alpha_\eta Y(d_\eta)$, where $\alpha_1, \alpha_2, \ldots, \alpha_\eta\in \mathrm{F}_q$. If the coefficients $\alpha_1, \alpha_2, \ldots, \alpha_\eta$ are chosen in a random, independent fashion, then the data transmission technology is called random linear network coding. The random linear coding not only maintains most of the benefits of linear network coding, but also affords a remarkable simplicity of design.

2.2. One-time pad and secret sharing

A cryptosystem consists of three processes: key generation algorithm, encryption algorithm, and decryption algorithm. An encryption scheme is called perfectly secret if for every probability distribution over the message space M, every message $m\in M$, and every ciphertext $c\in C$ with $\Pr\{c\}>0$, it holds that $\Pr\{m|c\}=\Pr\{m\}$. The notation of perfect secrecy was introduced by Shannon [18], who further demonstrated that perfectly secret encryption scheme can be achieved using one-time pad.

The one-time pad scheme reads as follows. Assume that the message space M, key space K, and ciphertext space C are all equal to $\{0, 1\}^N$, where N is an integer. For a given message $m=(m_1, m_2, \ldots, m_N)\in\{0, 1\}^N$, choose a string $k=(k_1, k_2, \ldots, k_N)\in\{0, 1\}^N$ according to the uniform distribution. The encryption and decryption processes are, respectively, $Enc_k(m)=(m_1\oplus k_1, m_2\oplus k_2, \ldots, m_N\oplus k_N)$ and $Dec_k(c)=(c_1\oplus k_1, c_2\oplus k_2, \ldots, c_N\oplus k_N)$.

Now, we introduce the Shamir's (t, ω) threshold scheme [19] which will be used later to construct our secure random linear network coding scheme. Consider that a trusted party T first chooses ω distinct and non-zero elements $y_1, y_2, \ldots, y_\omega$ from a finite field $\mathrm{F}(|\mathrm{F}|>\omega)$. These elements are public. Then T passes on the value y_i to user $P_i(i=1, \ldots, \omega)$. To share a key $k\in \mathrm{F}$ with the users, T securely selects $t-1$ independent elements $a_1, \ldots, a_{t-1}$ at random, and finally transfers securely $f(y_i)$ to user P_i, where $f(y)=k+\sum_{j=1}^{t-1}a_j y^j$ is a polynomial defined over F. This scheme is a perfect secret sharing scheme, and makes an unauthorized subset of participants impossible to access the value k.

3. The proposed scheme

The proposed secure random linear network coding scheme consists of two parts: encryption algorithm and decryption algorithm. A schematic illustration of our network coding scheme is graphically illustrated in Fig. 1.

3.1. Encryption algorithm

(1) Decompose source message matrix. Assume that there are $n-1$ source message packets $x_1, \ldots, x_{n-1}\in(\mathrm{F}_2)^{2r}$. For a given sufficiently large positive integer Q, choose a divisor l of $2r$ such that $l(n-1)^2\geq Q$ and $2r\geq(n-1)l$. Since the finite field F_{2^l} is isomorphic to $(\mathrm{F}_2)^l$, or alternatively $\mathrm{F}_{2^l}\cong(\mathrm{F}_2)^l$, which indicates that the packets $x_1, \ldots, x_{n-1}\in(\mathrm{F}_2)^{2r}$ can be viewed as vectors of $(\mathrm{F}_{2^l})^{(2r/l)}$. For simplicity, we assume that these vectors are linearly independent in space $(\mathrm{F}_{2^l})^{(2r/l)}$. Then the message packets can be written as a matrix

$$X=\begin{pmatrix} x_{11} & x_{12} & \cdots & x_{1\frac{2r}{l}} \\ \cdots & \cdots & \cdots & \cdots \\ x_{(n-1)1} & x_{(n-1)2} & \cdots & x_{(n-1)\frac{2r}{l}} \end{pmatrix}$$

where $x_{ij}\in\mathrm{F}_{2^l}\quad(i=1, \ldots, n-1; j=1, \ldots, \frac{2r}{l})$.

Pick $n-1$ linearly independent columns from X, and denote the indices of the selected vectors by $N_1<N_2<\cdots<N_{n-1}$. As a result, we construct an $(n-1)\times(n-1)$ matrix $X_L=(x_{LN_1}, \ldots, x_{LN_{n-1}})$ over F_{2^l} such that $\det(X_L-I_{n-1})\neq 0$. The remaining columns of X form a new matrix $X_R=(x_{R1}, \ldots, x_{R((2r/l)-n+1)})$ in accordance with the column ordinal from small to large.

(2) Encrypt the source message. The source generates a secret string $k\in(\mathrm{F}_2)^r$. Select a primitive element g_1 from a finite field $\mathrm{F}_{2^{(n-1)^2 l}}$ and publish it. Take k as an integer and calculate g_1^k. Obviously, g_1^k is a nonzero element of $\mathrm{F}_{2^{(n-1)^2 l}}$ and can be treated as a string of space $(\mathrm{F}_{2^l})^{(n-1)^2}$. Divide the string g_1^k into $n-1$ segments $k_1, \ldots, k_{n-1}\in(\mathrm{F}_{2^l})^{(n-1)}$ that are of equal length. Utilize these vectors $k_1, \ldots, k_{n-1}$ to construct an $(n-1)\times(n-1)$ matrix $\overline{G}$ over F_{2^l}. Due to $\mathrm{F}_{2^l}\cong(\mathrm{F}_2)^l$, $\overline{G}$ and X_L can be treated as $(n-1)\times(n-1)l$ matrices over F_2. Xoring $\overline{G}$ and X_L yields a ciphertext $C_L=\overline{G}\oplus X_L$. Multiplying X_L by X_R gives rise to $Y_R=X_L X_R$. The matrices C_L and Y_R constitute an $(n-1)\times 2r$ matrix $\overline{X}=(C_L|Y_R)$ over the finite field F_2.

(3) Protect the secret random seed k. Denote the row vectors of matrix $\overline{X}$ by $c_1, \ldots, c_{n-1}\in(\mathrm{F}_2)^{2r}$ and half split the vector $c_i(i=1, \ldots, n-1)$, which give rise to two vectors, $c_{iL}=(c_{i1}, \ldots, c_{ir})$ and