Fifteenth International Workshop on Algebraic and Combinatorial Coding Theory
June 18-24, 2016, Albena, Bulgaria *pp. 278–283*

Anonymous Coherent Network Coding Against Active Adversary [1]

O. Trushina oksana.trushina@gmail.com
Moscow Institute of Physics and Technology (State University)

Abstract. This paper considers a problem of anonymous transmission against eavesdropping and jamming in coherent network coding. A message of n packets is transmitted between some source-receiver pair. An adversary can eavesdrop arbitrary μ packets and inject no more then t malicious packets. The goal is to achieve a communication in such a manner that the adversary can not determine who communicates with whom. The scheme is based on coset coding for network coding and property of sum of uniform variables over a finite field. The scheme is simple but has requirement for network topology.

1 Introduction

Network coding is a data transmission concept allowing the relay nodes to perform operations on input packets. The most widely studied kind of network coding is linear network coding. The main point of it is to transmit linear combinations of input packets. The two sorts of linear network coding are considered. Namely, *coherent network coding* when the coefficients of linear combinations are known in advance and *random network coding* when the ones are chosen by the relay nodes in real time.

This transmission strategy causes the tasks concerning security, since traditional security methods can not be applied due to the operations performed by the relay nodes that forces the packets to modify.

This paper considers the problem of anonymous transmission against adversary who can inject the malicious packets into the network and eavesdrop the packets. Anonymous transmission means that using obtained information the adversary can not determine who communicates with whom. This work is an extension of the work [1], where a passive adversary who can only eavesdrop packets is considered. The previous works on this problem either focus on random network coding [2] or use cryptography [3, 4]. Proposed approach based on secure error-correcting coding scheme [5] and properties of a sum of the uniformly distributed variables in a finite field. We show that simple modification on this scheme allows to guarantee not only security against aforementioned adversary but also anonymity.

[1]The research is supported in part by Russian Foundation for Basic Research, project №15-07-08480

2 Problem Statement

Security of transmitted message is a necessary condition of anonymity in coherent network coding. Indeed, if the adversary can see incoming and outgoing packets of some relay node it is easy to map incoming packets to outgoing packets by checking possible linear combinations of incoming packets. It means that the adversary has the opportunity to trace the message of some source and compromise anonymity.

Secure error-correcting scheme [5] and proposed approach based on coset coding concept [6]. The key point of the concept is to provide security by mapping initial message not to particular code word but to entire coset of this code. Then random word of this coset is transmitted to the network. Perfect security can be guarantee if an adversary eavesdrops an amount of message symbols or packets not more then given number which depends on the parameters of the code. Maximum security rate is known to be reached in case of the code to be maximum distance code.

In error free case the whole space is filled by the cosets of the code. Adversary packets injecting can be considered as transmission with errors. In this case the distance between cosets is insufficient to correct the errors. To increase distance the density of cosets must be reduced. So not the whole space but subspace must be filled by the cosets. In other words two nested codes $C_2 \subset C_1$ must be chosen and fine code C_1 is filled by the cosets of coarse code C_2.

We consider a network implementing coherent network coding. There are multiple source nodes and multiple receiver nodes. It is worth mentioning that the anonymity task is sensible only in presence of multiple source and multiple receiver nodes. Network coding scheme for this scenario hasn't been clear enough yet. But it is widely studied and existing results allows to use this scenario.

Any source-receiver pair is supposed to has a route established in such a way that any relay node of the route can receive entire message of a previous route node. This requirement imposes constrains on a network topology. A network nodes and links density must be sufficient for either physical network topology to meet the requirement itself or it is possible to construct a logical network topology to meet the requirement.

The sources transmit to network the packets. A packet is a vector of length m with coordinates being the elements of finite field $\mathbb{F}_q$. In order to transmit k packets, i.e. a matrix S of size $k \times m$ over $\mathbb{F}_q$, the source transmits a matrix X of size $n \times m$, $n \leq m$ over $\mathbb{F}_q$. Some node of the route receives

$$Y = AX + DZ$$

where $A \in \mathbb{F}_q^{N \times n}$ is a matrix of coding vectors or transfer matrix which is known, $Z \in \mathbb{F}_q^{t \times m}$ is a matrix of error packets injected by the adversary and $D \in \mathbb{F}_q^{N \times t}$

is a matrix of coding vectors of links where the error packets were injected. Let this node transmits further some Y'. Let $B \in \mathbb{F}_q^{\mu \times n}$ is a matrix of coding vectors of links eavesdropped by the adversary. So the following conditions must be satisfied:

- decoding condition: $H(S|Y) = 0 \; \forall A : \; rankA = n$;
- security condition: eavesdropped $W = BX$, i.e. μ packets of X, $I(S;W) = 0 \; \forall B \in \mathbb{F}_q^{\mu \times n}$;
- anonymity condition: $I(Y;Y') = 0$.

The first two conditions are achieved by secure error correcting scheme [5]. A coding process from S to X is as follows. Convert the matrices S and X to column vectors $\mathcal{S}$ and $\mathcal{X}$ over a field $\mathbb{F}_{q^m}$ using some basis Ω. So $\mathcal{S} \in \mathbb{F}_{q^m}^k$ and $\mathcal{X} \in \mathbb{F}_{q^m}^n$. Let C_1 be $[n, k+\mu]$ maximum rank distance (MRD) code with generator matrix $G_1 \in \mathbb{F}_{q^m}^{(k+\mu)\times n}$. Let

$$\mathcal{U} = \begin{pmatrix} \mathcal{S} \\ \mathcal{V} \end{pmatrix}$$

where $\mathcal{V} \in \mathbb{F}_{q^m}^{\mu}$ is uniformly distributed and independent of $\mathcal{S}$.

$$\mathcal{X} = G_1^\top \mathcal{U}. \tag{1}$$

The t errors may be corrected iff rank distance of C_1 meets $d_R(C_1) \geq 2t+1$.

To reveal security condition meeting it is convenient to introduce invertible matrix $T \in \mathbb{F}_{q^m}^{n\times n}$ so that the last $k+\mu$ rows of $T^\top$ form matrix G_1, i.e. $T^\top = \begin{pmatrix} \Delta G_1 \\ G_1 \end{pmatrix}$. Rewrite eq. 1 as

$$\mathcal{X} = G_1^\top \mathcal{U} = T \begin{pmatrix} 0 \\ \mathcal{U} \end{pmatrix} = T \begin{pmatrix} \mathcal{S}' \\ \mathcal{U} \end{pmatrix}$$

where $\mathcal{S}' = \begin{pmatrix} 0 \\ \mathcal{S} \end{pmatrix}$. The $\mathcal{S}'$ is secure under μ observations if the last μ rows of $T^\top$ form generator matrix G_2 of $[n, \mu]$ MRD code C_2. This is consistent with coset coding idea. Indeed, we have $G_1 = \begin{pmatrix} \Delta G_2 \\ G_2 \end{pmatrix}$, then $H_2 = \begin{pmatrix} H_1 \\ \Delta H \end{pmatrix}$, where H_1 and H_2 are parity-check matrix of codes C_1 and C_2 correspondingly. So $C_2 \subset C_1$.

$$\begin{aligned} &\mathcal{S}_1 = H_1 \mathcal{X} \\ &\mathcal{S}' = H_2 \mathcal{X} \qquad\qquad \text{and } \mathcal{S}' = \begin{pmatrix} \mathcal{S}_1 \\ \mathcal{S} \end{pmatrix} \\ &\mathcal{S} = \Delta H \mathcal{X} - \text{relative syndrome} \end{aligned}$$

Since $\mathcal{X} \in C_1$, then $\mathcal{S}_1 = 0$ and $\mathcal{S}' = \begin{pmatrix} 0 \\ \mathcal{S} \end{pmatrix}$. In that case, the code C_1 can be filled in $(q^m)^{k+\mu-\mu} = (q^m)^k$ cosets of the code C_2. In other words, a message of size k can be sent in secrecy. So the message $\mathcal{S} \in \mathbb{F}_{q^m}^k$ can be sent in secrecy.

3 Proposed Scheme

To meet the last anonymity condition consider

$$\mathcal{X} = G_1^\top \mathcal{U} = T \begin{pmatrix} 0 \\ \mathcal{U} \end{pmatrix} = \begin{pmatrix} \Delta G_1^\top & \Delta G_2^\top & G_2^\top \end{pmatrix} \begin{pmatrix} 0 \\ \mathcal{S} \\ \mathcal{V} \end{pmatrix} = \begin{pmatrix} \Delta G_1^\top & \Delta G_2^\top \end{pmatrix} \begin{pmatrix} 0 \\ \mathcal{S} \end{pmatrix} + G_2^\top \mathcal{V}.$$

$\mathcal{X}$ is a random vector of a coset defined by syndrome $\begin{pmatrix} 0 \\ \mathcal{S} \end{pmatrix}$ of the code C_2. The vector

$$\mathcal{X}' = \begin{pmatrix} \Delta G_1^\top & \Delta G_2^\top \end{pmatrix} \begin{pmatrix} 0 \\ \mathcal{S} \end{pmatrix} + G_2^\top (\mathcal{V} + \mathcal{V}') = \mathcal{X} + G_2^\top \mathcal{V}'$$

is the vector of the same coset. If the vector $\mathcal{V}'$ is uniform over $\mathbb{F}_{q^m}^\mu$, then $G_2^\top \mathcal{V}'$ is uniform over $\mathbb{F}_{q^m}^\mu$. According to

Lemma 1 *Let X and Y be two independent statistical variables from finite group. If X is uniformly distributed over the group, then $Z = X + Y$ is uniformly distributed as well and independent of Y.*

$\mathcal{X}'$ is uniform over $\mathbb{F}_{q^m}^\mu$, i.e. within the coset, and independent of $\mathcal{X}$. So

$$I(\mathcal{X}; \mathcal{X}') = 0.$$

Consider some relay node. It receives

$$\mathcal{Y} = A\mathcal{X} + D\mathcal{Z}.$$

If the relay node transmits further a message

$$\mathcal{Y}' = A(\mathcal{X} + G_2^\top \mathcal{V}') + D\mathcal{Z} = A\mathcal{X}' + D\mathcal{Z},$$

then according to lemma 1

$$I(\mathcal{Y}; \mathcal{Y}') = 0$$

regardless of distribution of error packets $\mathcal{Z}$.

On the assumption that there are several source nodes and several receiver nodes, any relay node transmits messages of more than one source-receiver

communication. Then any relay node has several input messages and several output messages. So it is correct that

$$I(\mathcal{Y}_i^{in}; \mathcal{Y}_j^{out}) = 0, \ \forall i, j = 1, 2, 3...$$

It means that the adversary has no idea about correspondence of input and output messages of any relay node.

The proposed scheme doesn't increase decoding complexity. Let a length of a route be p hops. Then

$$\begin{aligned}
\mathcal{X}^{(p)} &= \mathcal{X} + G_2^\top(\mathcal{V}' + \mathcal{V}'' + \ldots + \mathcal{V}^{(p)}) \\
&= G_1^\top \begin{pmatrix} \mathcal{S} \\ \mathcal{V} \end{pmatrix} + G_2^\top(\mathcal{V}' + \mathcal{V}'' + \ldots + \mathcal{V}^{(p)}) \\
&= \begin{pmatrix} \Delta G_2^\top & G_2^\top \end{pmatrix} \begin{pmatrix} \mathcal{S} \\ \mathcal{V} \end{pmatrix} + G_2^\top(\mathcal{V}' + \mathcal{V}'' + \ldots + \mathcal{V}^{(p)}) \\
&= G_1^\top \begin{pmatrix} \mathcal{S} \\ \mathcal{V} + \mathcal{V}' + \mathcal{V}'' + \ldots + \mathcal{V}^{(p)} \end{pmatrix} = G_1^\top \mathcal{U}^{(p)}.
\end{aligned}$$

On getting a message $\mathcal{Y}^{(p)}$ a receiver applies a decoder for C_1 in order to obtain $\mathcal{U}^{(p)} \in \mathbb{F}_{q^m}^{k+\mu}$. Then extracting the first k rows of $\mathcal{U}^{(p)}$ it finds the message $\mathcal{S}$.

4 Conclusion

This work has addressed to the problem of anonymous transmission for coherent network coding subject to eavesdropping and malicious injecting. The simple scheme has been proposed. It based on coset coding and properties of uniform variables over finite field.

A possible future work might be to thoroughly examine network topology constrains and possible malicious patterns of injected packets which can help an adversary to trace a message through its route.

References

[1] O. Trushina, E. Gabidulin, A new method for ensuring anonymity and security in network coding, *Problems of Information Transmission*, 51, 2015, 75 – 81.

[2] Wang J., Wang J., Wu C., Lu K., Gu N., Anonymous Communication with Network Coding against Traffic Analysis Attack, *Proceedings IEEE International Conference on Computer Communications INFOCOM*, 2011, 1008 – 1016.

[3] Fan Y., Jiang Y., Zhu H., Chen J., Shen X., Network Coding Based Privacy Preservation against Traffic Analysis in Multi-Hop Wireless Networks, *IEEE Transactions on Wireless Communication*, 10, 2011, 834 – 843.

[4] Zhang P., Jiang Y., Lin C., Fan Y., Shen X., P-Coding: secure network coding against eavesdropping attacks, *Proceedings of the 29th IEEE International Conference on Computer Communications INFOCOM*, 2010, 1 – 9.

[5] D. Silva, F. R. Kschischang, Universal Secure Erro-Correcting Schemes for Network Coding, *Proceedings of ISIT*, 2010, 2428 – 2432.

[6] L.H. Ozarow, A.D. Wyner, Wire-Tap Channel II, *Advances in Cryptology Lecture Notes in Computer Science*, 209, 1985, 33 – 50.