Computer Networks 75 (2014) 99–112

Contents lists available at ScienceDirect

Computer Networks

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

ERSS-RLNC: Efficient and robust secure scheme for random linear network coding

Hassan Noura [a,*], Steven Martin [a], Khaldoun Al Agha [a], Khaled Chahine [b]

[a] LRI, Université Paris-Sud, CNRS, Orsay, France
[b] Lebanese International University, Department of Electrical and Electronics Engineering, Signals and Systems Group, Lebanon

ARTICLE INFO

Article history:
Received 29 October 2013
Received in revised form 5 July 2014
Accepted 29 September 2014
Available online 17 October 2014

Keywords:
Random linear network coding
Authentication and encryption algorithm
Homomorphic encryption
Invertible integer and binary
global encoding matrix

ABSTRACT

Random Linear Network Coding (RLNC) is a promising technology of Network Coding (NC) that has been proved to be both sufficient and efficient. To enable the deployment of RLNC in real networks, this paper first introduces a new efficient and flexible authentication–encryption scheme that is immune to Byzantine and eavesdropping attacks. The proposed scheme achieves simultaneously information confidentiality, packet integrity and source authentication with minimum computational complexity and memory consumption. It also presents a new technique for constructing an integer Global Encoding Matrix (GEM) that satisfies the inversion property in a dynamic manner. In addition, the proposed scheme uses dynamic keys to ensure robustness against attacks. Secondly, an efficient implementation of Binary RLNC, suitable for battery constrained mobile devices with low computational capabilities such as mobile phones and sensors, is defined. The effectiveness of the coding process is proved by modifying the Galois field of calculation from integer (int8, int16) to binary. Not only does this ensure low computational requirements, high throughput and low energy consumption, but also reduces the statistical characteristics of the coding process. The obtained theoretical and experimental results show that the new scheme is secure and efficient compared with many recent works in this field.

1. Introduction

In the last few years, NC became an attractive research topic due to its wide range of applications. It allows intermediate nodes to mix input packets and forward the resulting coded packets. The theory of NC promises significant benefits in network performances, especially in lossy networks and in multicast and multipath scenarios. It favors the maximum flow of information shown theoretically in [1] and experimentally in [2], affords lower energy consumption and enhances robustness for reliable communications over networks.

A well known method of NC is Random Linear NC (RLNC) [3], where the destinations perform Gaussian elimination on the set of received coded packets to retrieve the original ones. RLNC is a distributed NC scheme and it was proposed to overcome the centralized code allocation overhead. But due to the unreliable multi-hop transmission and willful intermediate packet mixing, RLNC is also susceptible to various types of security threats such as eavesdropping attacks and Byzantine modifications. The former can seriously impair the confidentiality while the latter can damage the authentication of network coded systems. This makes confidentiality and authentication the top security concerns, which should be ensured by all means and at all times [4]. Hence, the practical benefits

* Corresponding author.
E-mail addresses: hassan.noura@lri.fr (H. Noura), steven.martin@lri.fr (S. Martin), khaldoun.alagha@lri.fr (K. Al Agha), khaled.chahine@liu.edu.lb (K. Chahine).

http://dx.doi.org/10.1016/j.comnet.2014.09.013
1389-1286/

of RLNC can be compromised without proper security, especially when used for banking and military systems where sensitive information is communicated.

In the literature, several techniques have been proposed to ensure the authentication and confidentiality of RLNC (e.g. [5–7]). A set of these solutions (e.g. [8–15]) rely on a new kind of encryption called Homomorphic Encryption (HE) [16] to thwart passive attacks. HE ensures that the arithmetic operations taking place on cipher-text are reflected on the plain-text. The use of public HE scheme is so expensive in terms of the calculation time and the required parameters lengths that it cannot be used at the moment. Also, the public HE operations require a heavy-weight computations at each participating node and are not scalable [9]. Other homomorphic ciphers belonging to the symmetric crypto-systems such as AES in mode CTR that can afford a significant computational gains compared to asymmetric one. Moreover, using selective HE allows to protect only the Global Encoding Vector (GEV) of each packet instead of the long payload [17]. Indeed recent cryptographic schemes apply their solution to set of GEV's (noted also as $G_i,\ i = 1, 2, \ldots, h$) that form the GEM (noted also as $G = \{G_1, G_2, \cdots, G_h, \}$), with h representing the size of generation (i.e., the number of packets).

In [8], a scheme was presented in which each G_i used at the source is encrypted, while another set of unencrypted ones is attached to maintain the standard coding processes at intermediates nodes. Obviously, this scheme requires less data to be encrypted, but it actually needs two rounds of decoding processes, which may not be efficient as expected. Moreover, considerable space overhead will be doubled by the addition of an extra GEV for each packet. In [10], a multiplication of complexity $O(h^3)$ between G and a static key matrix K is proposed to protect G. The key matrix is distributed to destination nodes through a secure channel and its length is flexible and depends on h. The same key is used throughout the transmission, and the problem of single generation failure may happen, in which an accidental key disclosure in one generation will compromise the secrecy of the following transmission. These methods are inefficient in either computation or space (communication overhead) and hence the security feature provided by RLNC is not fully exploited. In [4], an authenticated encryption scheme that uses a mapping function to construct GEM was proposed. Its major challenge is to preserve the bit pattern of authentication scheme. Also, this technique cannot provide message authentication at the destination and uses the same key throughout the transmission. In [9], a dynamic permutation cipher scheme of computational complexity $O(h \times l)$ (l is the length of payload) was presented and applied on each packet using the same dynamic key. Indeed, the existing techniques always present a trade-off between security and performance; they design network codes that are Shannon secure at the cost of decreased throughput.

In this paper, an efficient and robust scheme that relies on combining a Hash Message Authentication Code (HMAC) with a selective cipher scheme is proposed to ensure the necessary security services for RLNC. The scheme is shown to be Shannon secure with low computational complexity since the key is dynamic. The second contribution of this work is using the binary field to reduce the computational complexity and the amount of coding needed for RLNC. This is achieved by defining a new approach of generation of dynamic invertible integer and binary matrix.

The rest of this paper is organized as follows. Section 2 reviews current scenarios of RLNC and discusses opportunities to ensure security with RLNC. Section 3 presents the proposed authentication–confidentiality scheme and the proposed technique used to construct the invertible dynamic GEM. Section 4 analyzes the properties of the proposed scheme, especially in terms of security, randomness, computational complexity and flexibility. Finally, Section 5 concludes this work and discusses its prospects.

2. Secure RLNC

RLNC has an overhead of $h \times log_2(q)$ per packet, where h is the size of generation (called also Generation Dimension {GD}) and q is the underlying field [18]. Each GEV is represented as a sequence of independent random numbers from a field. At the destination(s), Gaussian elimination is carried out on the set of received coded packets to retrieve the original packets. Hence, the number N of possible GEV's that forms an $h \times h$ invertible matrix [19] is:

$$N = \prod_{k=1}^{h} (q^h - q^{k-1}) \tag{1}$$

In Fig. 1, the variation of N versus the generation size h for different Galois fields is shown. The invertiblity probability of an $h \times h$ matrix over field q is:

$$p_{inv} = \frac{\prod_{k=1}^{h} (q^h - q^{k-1})}{q^{h^2}} = \prod_{k=1}^{h} (1 - q^{k-1-h}) < 1 - \frac{1}{q} \tag{2}$$

In a real implementation, the invertibility probability (p_{inv}) decreases as h grows. Also, for any fixed h and for $q = 2$ (the case of a binary matrix), the invertibility probability tends to ≈ 0.288788 when $h \to \infty$ [19]. This means that there are much fewer invertible matrices in binary field compared with integer field and thus a high invertibility probability cannot be attained. This result proves that the creation of invertible Binary RLNC at the source has a lower probability, which can cause a degradation in the performance of RLNC.

As shown in (2), if the field size q grows, it does not only reduce the number of operations needed in the process of coding, but also prevents the construction of an efficient implementation of the necessary operations. Moreover, the hardware resources available on such devices as mobile phones and wireless sensors are considerably low. Hence, the practical implementation is limited with the field size q, which creates some challenges such as the high complexity of the decoding algorithms. In order to overcome this problem, we choose to use binary Galois fields for the computation of RLNC as in [20] and in contrast to traditional RLNC. Therefore, a new technique to generate invertible dynamic integer and binary GEM is defined