Computer Networks 54 (2010) 28–40

Contents lists available at ScienceDirect

Computer Networks

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

An efficient dynamic-identity based signature scheme for secure network coding

Yixin Jiang [a,b], Haojin Zhu [a], Minghui Shi [a], Xuemin (Sherman) Shen [a,*], Chuang Lin [b]

[a] Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Ontario, Canada N2L 3G1
[b] Department of Computer Science and Technology, Tsinghua University, Beijing 100084, China

ARTICLE INFO

Article history:
Received 3 February 2009
Received in revised form 15 May 2009
Accepted 7 August 2009
Available online 13 August 2009
Responsible Editor: W. Wang

Keywords:
Network coding
Identity-based cryptography
Signature
Pollution attacks

ABSTRACT

The network coding based applications are vulnerable to possible malicious pollution attacks. Signature schemes have been well-recognized as the most effective approach to address this security issue. However, existing homomorphic signature schemes for network coding either incur high transmission/computation overhead, or are vulnerable to random forgery attacks. In this paper, we propose a novel *dynamic-identity based signature scheme* for network coding by signing linear vector subspaces. The scheme can rapidly detect/drop the packets that are generated from pollution attacks, and efficiently thwart random forgery attack. By employing fast packet-based and generation-based batch verification approaches, a forwarding node can verify multiple received packets synchronously with dramatically reduced total verification cost. In addition, the proposed scheme provides one-way identity authentication without requiring any extra secure channels or separate certificates, so that the transmission cost can be significantly reduced. Simulation results demonstrate the practicality and efficiency of the proposed schemes.

1. Introduction

Network coding, as an efficient means of information dissemination, is a promising approach in many practical network applications, such as traditional multicast or broadcast networks [1], wireless sensor networks [2,3], and peer-to-peer content distribution networks [4–7]. Network coding was first introduced in [8] as an alternative to the traditional routing networks, and it has been shown that random linear coding can achieve the optimal throughput for multicast [1,9] and even unicast transmissions [10,11].

Unlike the traditional forwarding approach which requires duplicating every input message, network coding allows each intermediate node to encode packets en-route. Therefore, each output message sent to the downlink can be linear combination of input messages received from the uplinks, as illustrated in Fig. 1 [16]. Generally, network coding system consists of the transmission, encoding, and re-encoding of messages at intermediate nodes, such that the encoded messages can be decoded at their final destinations.

A primary benefit of network coding is that it can improve throughput and minimize the transmission delay of a network. Another compelling benefit is its robustness and adaptability. Practical network coding techniques, such as random linear coding, packet tagging, and buffering, allow the encoding and decoding to proceed in a distributed manner, even if asynchronous packets arrive and depart in arbitrarily varying rate, delay, and loss. Thus, network coding is well suited for dynamic network scenarios, where nodes only have partial information about the global network topology. In addition, network coding can minimize the amount of energy required per packet multicast in wireless networks.

[*] Corresponding author. Tel.: +1 519 888 4567 32691; fax: +1 519 746 3077.

E-mail addresses: yixin@bbcr.uwaterloo.ca (Y. Jiang), h9zhu@bbcr.uwaterloo.ca (H. Zhu), mshi@bbcr.uwaterloo.ca (M. Shi), xshen@bbcr.uwaterloo.ca (X. (Sherman) Shen), clin@csnet1.cs.tsinghua.edu.cn (C. Lin).

1389-1286/$ - see front matter © 2009 Elsevier B.V. All rights reserved.
doi:10.1016/j.comnet.2009.08.006

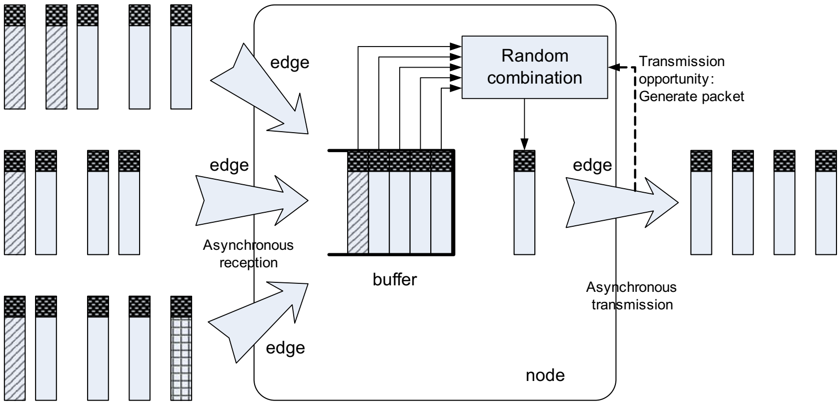
edge
edge
edge
edge
Random combination
Transmission opportunity: Generate packet
Asynchronous reception
buffer
Asynchronous transmission
node

Fig. 1. Coding at network node.

However, network coding may face potential security threats due to open multi-hop communications and the packet encoding at intermediate forwarders. Since network coding involves mixing of packet inside the network, several primary types of attacks, *pollution attacks, random forgery attacks* [38], and *entropy attacks* [5], are particularly relevant to network coding. The *pollution attack* is originated from any malicious behaviors of un-trusted forwarders or adversaries, such as injecting polluted information, modifying and replaying the disseminated messages, which could be fatal to the whole networks. Although this may also occur in a traditional network system without network coding, its effect is far more serious with network coding. If a junk message is mixed by a forwarder, the output messages of the forwarder will be contaminated. Such polluted messages should be detected and filtered as early as possible, since they may spread to all downstream nodes by re-encoding junk messages. The *random forgery attack is* related to homomorphic signature function itself. Jognson et al. [38] conclude that for an additive homomorphic signature function defined on the lattice $L = (\mathbb{Z}/m\mathbb{Z})^d$, if an adversary can derive signature $Sig(x_1), \ldots, Sig(x_d)$, where $x_1, \ldots, x_d$ are a basis for L, then it can launch successful random forgery attacks to the additive homomorphic signature function. The *entropy attack* can be considered as a special replay attack, where an adversary may use “stale” encoded packet vectors to forge non-innovative packets that are trivial linear combinations of existing packets at the forwarders. Although entropy attack does not destroy the linear algebraic constraint conditions between the original packet and the appended encoding vector, it reduces the decoding opportunities at sinks and the overall throughput rate. How to thwart entropy attacks exceeds the scope of this paper, which we have explored at length in [36].

For secure network coding, it is prerequisite to achieve efficient message integrity and validity. The non-cryptography based schemes [14,15] can only detect or filter out polluted messages at the sinks, but not at the forwarders. A well-recognized cryptography-based solution is to sign each message with a signature. However, the traditional hash function based signature schemes may be unsuitable for network coding, since the original source signatures can be destroyed by the subsequent encoding process, which is performed at each forwarder. The basic idea in existing cryptography-based schemes is to detect each packet before it gets mixed into the buffer, including a homomorphic hash scheme [5], a homomorphic signature scheme [12], and a secure random checksum scheme [5]. These solutions either require an extra secure channel [5], incur high computation overhead due to not supporting batch verification [12], suffer from relatively high extra transmission overhead [5,39], endure weak scalability [12,39], or are vulnerable to the random forgery attack [12,13], by which an adversary may arbitrarily forge signatures for a given message if sufficient signatures of “stale” messages are collected [38]. Recently, Yu et al. [13] propose an efficient homomorphic signature scheme based on the RSA signature scheme, with which the forwarders can achieve efficient verification at the expense of increased transmission overhead, since the size of a RSA signature is typically very large in the order of hundreds of bytes. Zhao et al. [39] also present a novel signature scheme for network coding by authenticating the vector sub-space. The significant drawback in this scheme is that the size of both the public signature information and public keys is at least the square root of the file size. Moreover, the scheme is not efficient for distributing multiple files with the same public key, which significantly impairs the system scalability. Finally, to calculate the public signature information, the scheme requires the source to buffer the entire file in advance. Therefore the scheme is not suitable for streaming live data, which are generated on-the-fly. These aforementioned deficiencies motivate us to explore a more efficient and scalable scheme for securing network coding.

In this paper, we propose an efficient *dynamic-identity based signature* scheme for secure network coding, which features the following notable properties: (1) **Efficiency**: The proposed signature scheme can support fast identity-based batch verification, and rapid signature generation for the output packets. By employing two optimized verification techniques, packet-based and generation-based batch verification methods, a node can quickly verify mul-