ELSEVIER
AEÜ
International Journal of Electronics and Communications
Contents
www.elsevier.com/locate/aeue
ISSN 1434-8411
Int. J. Electron. Commun. (AEÜ)
70(2016)2 · pp. 121–210

An Efficient Privacy-preserving Scheme for Secure Network Coding Based on Compressed Sensing

Dong Xie, Haipeng Peng, Lixiang Li, Yixian Yang

PII: S1434-8411(17)31234-7
DOI: http://dx.doi.org/10.1016/j.aeue.2017.05.028
Reference: AEUE 51899

To appear in: *International Journal of Electronics and Communications*

Received Date: 26 December 2015
Accepted Date: 19 May 2017

An Efficient Privacy-preserving Scheme for Secure Network Coding Based on Compressed Sensing

Dong Xie[a,b], Haipeng Peng[a,b,], Lixiang Li[a,b], Yixian Yang[a,b]

[a]*Information Security Center, State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing, 100876 China*

[b]*National Engineering Laboratory for Disaster Backup and Recovery, Beijing University of Posts and Telecommunications, Beijing, 100876 China*

Abstract

Network coding (NC) provides an elegant solution for improving capacity and robustness in computer networks. Different to traditional "store-and-forward" transmission paradigm, each intermediate node linearly combines received data packets, and the original files can be decoded at the sink nodes in NC settings. This brand-new paradigm is vulnerable to pollution attack, which means that some malicious nodes inject fake data packets into the network and this will lead to incorrect decoding. There are some information-theoretical solutions and cryptographic solutions for solving this security issue, and most existing schemes can thwart data pollution attacks. However, the privacy of the original files are vital to some application environments (e.g. military network). To the best of our knowledge, there is not a secure scheme which can thwart pollution attack and can protect the privacy of transmitted data simultaneously. In this paper, we present an efficient privacy-preserving scheme for secure network coding based on compressed sensing (CS), which has attracted considerable research interest in the signal processing community. Specifically, we embed CS into the general NC framework, i.e., the source node needs to compress each original data packet using the sensing matrix before creating the augmented vector and the sink nodes require to perform an additional CS reconstruction algorithm for reconstructing the original file. In addition, we construct a simple key distribution protocol and each intermediate node just needs two secret keys for verifying the integrity of received data packets. Such novel hybrid construction enables the privacy-preserving guarantee, and the performance comparison shows the high-efficiency of our scheme in terms of the computational complexity and

Email address: penghaipeng@bupt.edu.cn (Haipeng Peng)