A MAC-based Scheme for Multi-Generation Content Distribution with Network Coding

Yu Zhang*

*Shanghai Key Laboratory of Intelligent Information Processing
School of Computer Science, Fudan University, Shanghai, China
11210240041@fudan.edu.cn

***Abstract*—The system that uses network coding is highly susceptible to pollution attacks, where a malicious node may pollute a small number of packets with the purpose of preventing the recipient nodes from reconstructing the original messages properly. Some schemes that use Message Authentication Code (MAC) have been proposed for resisting this attack. However, these schemes could be broken with probability 1=q, where q is the size of the underlying field. Although the trace function has already been used for constructing MACs for a higher security, it can only be used for single-generation distribution. This paper proposes a novel MAC-based scheme that also employs trace function. However, different from prior work, our scheme can be immediately used for secure multi-generation distribution.**

***Keyword*—Homomorphic MAC, Pollution Attacks, Network Coding, Authentication, Repetitive Attacks**

Yu Zhang. Yu Zhang received the B.S degree in Computer Science from Fudan University, Shanghai, China, in 2010. He is now a graduate student in the School of Computer Science, Fudan University. His major/interests are Information Security and Network Coding, Computational Complexity and the defense against Pollution Attacks.