Introduction to Secure Network Coding

Elke Franz, Technische Universität Dresden

Network Coding [1] is a promising approach for increasing throughput, energy efficiency, and robustness of data transmission. However, mere network coding is vulnerable to passive as well as active attacks. Even if network coding already provides a certain level of security against eavesdropping (passive attacks), this inherent security is not sufficient against a stronger attacker who may observe more links or even intermediate nodes in the network. Moreover, network coding is especially vulnerable to pollution attacks (active attacks). Even one single packet can influence the whole subsequent downstream processing of the packets.

Because of the vulnerability of network coding to attacks, there has been a lot of research into security of network coding in the past few years. The approaches we will discuss in this short course are based on Practical Network Coding (PNC) introduced by Chou et al. in [2]. PNC provides a decentralized implementation of Random Linear Network Coding. All receiving nodes are able to decode the combined data packets they receive without the knowledge of coefficients randomly chosen by forwarding nodes for the computation of linear combinations.

Confidentiality of transmitted data can also be enforced by means of end-to-end encryption of the data before network coding is applied. However, network coding schemes providing confidentiality are more efficient than end-to-end encryption. Approaches suggested in the literature include, e.g., the encryption of the encoding coefficients [6] and the use of a permutation function [8].

Due to the damaging influence of pollution attacks, the majority of the suggested secure network coding schemes deals with that threat. Known approaches are based on information theory, network error correction, or cryptography. We will especially focus on the latter. Common cryptographic approaches for authentication like digital signatures or Message Authentication Codes (MACs) cannot be directly applied to network coding since the packets are modified by forwarding nodes. Consequently, MACs as well as digital signatures would become invalid after one hop. To overcome this problem, authenticated checksums, homomorphic hashes, homomorphic MACs, and homomorphic signatures have been suggested for the detection of pollution attacks in network coding. Examples for these different approaches will be introduced [3, 5, 7, 4].

Schedule of the course:

1. Practical Network Coding
2. Security Requirements for Network Coding
3. Excursus: Cryptography
4. Network Coding Schemes Providing Confidentiality
5. Detection of Pollution Attacks

References

[1] R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung. Network information flow. *IEEE Trans. on Information Theory*, 46(4):1204–1216, 2000.

[2] P. A. Chou, Y. Wu, and K. Jain. Practical network coding. In *Proc. Annual Allerton Conference on Communication, Control, and Computing*, 2003.

[3] J. Dong, R. Curtmola, and C. Nita-Rotaru. Practical Defenses Against Pollution Attacks in Intra-Flow Network Coding for Wireless Mesh Networks. In *Proc. WiSec*, 2009.

[4] R. Gennaro, J. Katz, H. Krawczyk, and T. Rabin. Secure Network Coding over the Integers. In *Proc. PKC 2010*, pages 142–160, 2010.

[5] C. Gkantsidis and P. R. Rodriguez. Cooperative Security for Network Coding File Distribution. In *Proc. IEEE Int. Conf. on Computer Communications*, 2006.

[6] J. P. Vilela, L. Lima, and J. Barros. Lightweight security for network coding. In *Proc. IEEE Int. Conf. on Communications*, 2008.

[7] Y. Wang. Insecure "Provably Secure Network Coding" and Homomorphic Authentication Schemes for Network Coding. IACR Eprint archive, 2010.

[8] P. Zhang, Y. Jiang, C. Lin, Y. Fan, and X. Shen. P-Coding: Secure network coding against eavesdropping attacks. In *Proc. IEEE INFOCOMM*, 2010.