Exploring the Security Capabilities of Physical Layer Network Coding

Dr. Weichao Wang
SIS Department and CyberDNA Center
UNC Charlotte

In wireless networks, the bandwidth is considered one of the most scarce and valuable resources. The physical layer network coding (PNC) technique encourages strategically picked senders to interfere so that the destination nodes can leverage the network level information to recover the signals. PNC can yield higher capacity than network layer network coding when applied to wireless networks. However, before PNC can be widely deployed so that we can fully capture its advantages, we must have a thorough understanding and evaluation of the safety of the technique. Previous research on physical layer network coding focuses on the separation of the interfered signals [1, 2]. For the network layer coding technique, the research on its security focuses on the prevention of the malicious activities such as pollution attacks [3].

In this research, we propose to investigate the problem from a different perspective. Specifically, we seek to accomplish two research tasks. First, we want to prove that in addition to improving the bandwidth usage efficiency, PNC can be used to detect malicious attacks on wireless networks. Second, we conduct research in both the network layer and physical layer to turn the detection mechanisms into practical use. Solving these problems will bring great benefits to future research and deployment of PNC. For example, for all attacks that can be effectively prevented by PNC at the physical layer, we do not need to design and deploy another detection mechanism in upper layers. This will simplify the overall design of the security architecture of the wireless networks. As another benefit, the security capabilities of PNC will provide a new incentive for future investigation and deployment of the technique in addition to its advantage in bandwidth usage efficiency.

In this presentation, we choose the stealth attacks on wireless network topology as the research topic. Specifically, we study whether or not the physical layer network coding technique can be used to detect the Sybil attack [4]. Several reasons lead us to choose the detection of Sybil attacks in wireless networks as the primary research topic. First, Sybil attacks impose severe threats to wireless network security. If the same physical device can illegitimately act with multiple identities in the network, it can attack the routing protocols and misbehavior detection mechanisms. Second, a Sybil attack is a representation of stealth attacks on wireless networks, where traditional methods such as encryption and authentication cannot defend against such attacks. Therefore, a detection method based on physical layer network coding will allow us to better understand this problem. Finally, although investigators have proposed the Sybil detection methods based on the signal-level signatures [5], these approaches usually depend on some special hardware [6] or the inaccurate signal propagation models [5]. Our approach does not require time synchronization among wireless nodes or depend on any special hardware.

The basic idea of our proposed approach is as follows: when the long sequences of signals from two senders collide at the receiver, the starting point of collision between the sequences is jointly determined by the sending time and the physical distances between the receiver and the senders. For two receivers, their starting points of collision could be different, and this difference is restricted by the physical distance between them. Therefore, through measuring the interfered parts of the received sequences, we can estimate the physical distance between two receivers. Our analysis will show that when the time difference between the starting points of collision is large enough, the receivers can combine the interfered signals to recover the original data packets. On the contrary, if the two receivers are the Sybil nodes attached to the same physical device, they will receive the same interfered sequences and they cannot accomplish the data recovery operation. In this way, we can distinguish two separate nodes from the Sybil identities. Since the proposed approach only measures the starting points of collision in the sequences, we do not need time synchronization among the wireless nodes. Our analysis will also show that the approach does not depend on any special hardware. Therefore, the method can be adopted by existing systems without significant difficulty.

Although the basic idea of the proposed approach is clear, we need to design schemes at both physical layer and network layer to make the approach practical. At the physical layer, we need to carefully select data transmission parameters such as modulation and carrier frequency. Consequently, algorithms are designed to recover the received sequences. At the network layer, we need to determine the senders and their data sequences. Mechanisms must be designed to reconstruct the data packets from the interfered signals. The wireless nodes need to verify the authenticity of the recovered sequences. Analysis will be conducted to study the detection capability of the proposed approach and its relationship to the network parameters.

Compared to previous approaches, our investigation has the following contributions:

- The research will demonstrate that in addition to improving the bandwidth efficiency and data robustness in wireless networks, physical layer network coding can also be used to detect malicious attacks. This research provides a new incentive for further development of this technique.
- The proposed Sybil detection mechanism does not require any special hardware or time synchronization in the wireless network. Therefore, existing systems can adopt the proposed approach without significant difficulty.
- We carefully design schemes in both network layer and physical layer to make the approach practical. Impacts of different factors on the proposed approach are also studied.

References

[1] Sachin Katti, Shyamnath Gollakota, and Dina Katabi. Embracing wireless interference: analog network coding. In ACM SigComm, pages 397–408, 2007.

[2] Shengli Zhang, Soung Chang Liew, and Patrick P. Lam. Physical-layer network coding. In ACM MobiCom, pages 358–365, 2006.

[3] J. Dong, R. Curtmola, and C. Nita-Rotaru. Secure network coding for wireless mesh networks: Threats, challenges, and directions. Elsevier Computer Communications, 32(17), 2009.

[4] W. Wang, D. Pu, and A. Wyglinski. Detecting Sybil Nodes in Wireless Networks with Physical Layer Network Coding, accepted to appear in the IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2010).

[5] M. Demirbas and Y. Song. An rssi-based scheme for sybil attack detection in wireless sensor networks. In Proceedings of WoWMoM, pages 564–570, 2006.

[6] B. Danev and S. Capkun. Transient-based identification of wireless sensor nodes. In Proc. of IPSN, pages 25–36, 2009.