TSINGHUA SCIENCE AND TECHNOLOGY
ISSN 1007-0214 05/09 pp505-519
Volume 16, Number 5, October 2011

Forced Collision: Detecting Wormhole Attacks with Physical Layer Network Coding*

Zhiwei Li, Di Pu†, Weichao Wang**, Alex Wyglinski†

Department of Software & Information Systems, UNC Charlotte, 9201 Univ. City Blvd, Charlotte, NC 28223, USA;
† Department of Electrical & Computer Engineering, Worcester Polytechnic Institute, 100 Institute Road, Worcester, MA 01609, USA

Abstract: Previous research on security of network coding focused on the protection of data dissemination procedures and the detection of malicious activities such as pollution attacks. The capabilities of network coding to detect other attacks have not been fully explored. In this paper, we propose a new mechanism based on physical layer network coding to detect wormhole attacks. When two signal sequences collide at the receiver, the starting point of the collision is determined by the distances between the receiver and the senders. Therefore, by comparing the starting points of the collisions at two receivers, we can estimate the distance between them and detect fake neighbor connections via wormholes. While the basic idea is clear, we have proposed several schemes at both physical and network layers to transform the idea into a practical approach. Simulations using BPSK modulation at the physical layer show that the wireless nodes can effectively detect fake neighbor connections without the adoption of special hardware or time synchronization.

Key words: physical layer network coding; wormhole attacks; cross-layer design

Introduction

Investigators have proposed the physical layer network coding technique[1,2] to fully explore the advantages such as improved throughput, reduced congestion, and strengthened robustness. The technique is especially valuable in wireless networks when we consider the limited bandwidth and power resources of the nodes. Since network coding may allow data errors and/or corrupted packets to propagate widely and ruin the data recovery procedure at the final destination, previous research into network coding security focused on the protection of data dissemination procedures and the detection of malicious activities such as pollution attacks[3,4].

However, the security capabilities of physical layer network coding to detect malicious attacks have not been fully explored. For instance, it is possible that when signals collide at the receiver, we can potentially extract information about the network structure. This information can then be used to detect attacks on network topology. In this paper, we conduct an investigation of this problem. Specifically, we propose a new mechanism to detect wormhole attacks.

Several reasons lead us to choose wormhole attacks as the primary research topic for this investigation. First, wormhole attacks impose severe threats to the correct detection of network topology, which is the foundation of various operations within wireless networks such as routing and data transmission. Second, a wormhole attack is a representation of stealth attacks on wireless networks, where traditional methods such

Received: 2011-06-21; revised: 2011-08-29
* Supported in part by the NSF CNS Award (No. 1143602)

** To whom correspondence should be addressed.
E-mail: weichaowang@uncc.edu

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, previous approaches for detecting wormhole attacks are usually implemented at the network layer. Our proposed approach uses physical layer properties. At the same time, 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 from two senders collide at the receiver, the starting point of the collision between the sequences is jointly determined by the sending time and the physical distances across all the receiver and senders. For two receivers, their starting points of collision will be different, and this difference is restricted by the physical distance between them. Therefore, through measuring and comparing the overlapping parts of the received sequences, we can estimate the physical distance between two wireless nodes and detect the fake connection between them. Since the proposed approach only measures the starting point of the collision in the sequences, we do not need time synchronization among the wireless nodes. Our analysis will also show that the physical distances among the senders and receivers will not impact the detection results. Therefore, we can choose the senders from a large area within the network.

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 network layer, we need to determine the senders and their data sequences. Mechanisms must be designed to prevent the man-in-the-middle attack. At the same time, the receivers need a scheme to verify the authenticity of the recovered sequences from collisions. 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. We will also investigate the impacts of different factors, such as phase shift and carrier frequency jitter, on the proposed approach using both analysis and simulation.

Our investigation has the following contributions:

- We make an attempt to explore the security capabilities of the physical layer network coding technique. 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 wormhole detection mechanism does not require any special hardware or time synchronization in the wireless network. Therefore, existing systems can easily adopt the proposed approach without going through drastic structural and functional changes.
- We carefully design schemes in both network layer and physical layer to make the approach practical. Impacts of different factors in the communication channel are studied through theoretic analysis and simulation.

The remainder of the paper is organized as follows: in Section 1, we introduce the basic idea of the detection mechanism and the role of physical layer network coding in wormhole detection. Section 2 reviews the related work. Sections 3 and 4 design mechanisms in the network layer and in the physical layer to make the approach secure and practical. We perform both an analysis and simulations to investigate the impacts of different factors in the physical layer. In Section 5 we study the security and detection accuracy of the proposed approach. Finally, Section 6 concludes the paper.

1 The Basic Idea

In this part, we introduce the basic idea of using physical layer network coding to detect wormhole attacks. We assume that two wireless nodes are neighbors if and only if the distance between them is shorter than r. However, this assumption does not restrict wireless nodes from transmitting signals at a higher power level in order to reach a longer distance. We assume the attackers are not capable of compromising any wireless nodes within the network. However, they can deploy their own nodes to eavesdrop on the traffic, tunnel the packets, and retransmit the data. In the following analysis, we use d_{MN} to represent the physical distance between two nodes M and N. We use T to represent a specific moment and t to represent a time duration. If the radio signal propagates at the speed of light s, the transmission delay between two nodes M and N will be $\frac{d_{MN}}{s}$. In the following