

Preface

Network coding is a new transmission paradigm proposed by Ahlswede et al. around the year 2000. It has been recognized as another breakthrough in information theory after Shannon. The key difference of network coding from traditional transmission paradigms is that in-network nodes can perform coding on packets, instead of simple store-and-forward. Benefits of network coding include higher data throughput, lower energy consumption, reduced bandwidth cost, etc. Due to these benefits, network coding has been applied to various kinds of networks, e.g., wireless mesh networks, content distribution networks, distributed storage networks, etc.

However, network coding also introduces new security and privacy challenges at the same time. The most serious problem is that it makes data transmission more vulnerable to *pollution attacks*. A single illegal packet can end up polluting a bunch of good ones through intermediate coding, and causing severe bandwidth waste. Besides data integrity, data confidentiality and user privacy also become quite different in the new context of network coding. On the one hand, we can leverage the intrinsic secrecy property of network coding to provide a lightweight confidentiality. On the other hand, we should redesign privacy-preserving mechanisms (e.g., anonymous routing) to make them compatible with network coding.

This book will first give a brief review of network coding in Chap. 1, including its benefits, applications, and security problems. Then, Chap. 2 will give a detailed review of security issues in network coding, highlighting how the security issues differ from those in traditional settings. In Chaps. 3–5, we will introduce three research works to address these security issues. The first work (Chap. 3) proposes a new method to defeat pollution attacks in network coding. Based on this method, a set of security mechanisms including a private key-based signature, a symmetric key-based MAC, and a hybrid key-based approach are presented and evaluated. The second work (Chap. 4) focuses on data confidentiality in network coding and presents a new encryption scheme named P-Coding. P-Coding recognizes the intrinsic secrecy property of random linear network coding and leverages it to offer a rather lightweight encryption which is very appealing in mobile ad hoc networks (MANETs). The third work (Chap. 5) identifies the problem that existing anonymous routing protocols (e.g., Tor) conflict with wireless network

coding. This work introduces cooperation among wireless nodes in order to resolve such conflict, so that wireless user privacy and network coding benefits can be simultaneously maintained. Finally, in Chap. 6, we will conclude this book and discuss some future directions for the research “security in network coding.”

Xi'an, China
Beijing, China

Peng Zhang
Chuang Lin

Security in Network Coding

Zhang, P.; Lin, C.

2016, XI, 98 p. 34 illus., 18 illus. in color., Hardcover

ISBN: 978-3-319-31082-4