

WOJCIECH MAZURCZYK, STEFFEN WENDZEL,  
SEBASTIAN ZANDER, AMIR HOUMANSADR,  
AND KRZYSZTOF SZCZYPIORSKI

# INFORMATION HIDING IN COMMUNICATION NETWORKS

Fundamentals, Mechanisms,  
Applications, and Countermeasures

 **IEEE**  
IEEE PRESS

  
IEEE Press Series on  
Information & Communication  
Networks Security  
Stamatis Kartalopoulos, Series Editor

**WILEY**

BIBLIOTHEQUE DU CERIST

# CONTENTS IN BRIEF

---

<b>1</b>	<b>INTRODUCTION</b>	<b>1</b>
<b>2</b>	<b>BACKGROUND CONCEPTS, DEFINITIONS, AND CLASSIFICATION</b>	<b>39</b>
<b>3</b>	<b>NETWORK STEGANOGRAPHY</b>	<b>59</b>
<b>4</b>	<b>CONTROL PROTOCOLS FOR RELIABLE NETWORK STEGANOGRAPHY</b>	<b>89</b>
<b>5</b>	<b>TRAFFIC TYPE OBFUSCATION</b>	<b>117</b>
<b>6</b>	<b>NETWORK FLOW WATERMARKING</b>	<b>139</b>
<b>7</b>	<b>EXAMPLES OF INFORMATION HIDING METHODS FOR POPULAR INTERNET SERVICES</b>	<b>163</b>
<b>8</b>	<b>NETWORK STEGANOGRAPHY COUNTERMEASURES</b>	<b>207</b>
<b>9</b>	<b>CLOSING REMARKS</b>	<b>243</b>

---

# CONTENTS

---

<b>List of Figures</b>	<b>xv</b>
<b>List of Tables</b>	<b>xxi</b>
<b>Foreword</b>	<b>xxiii</b>
<b>Preface</b>	<b>xxv</b>
<b>Acknowledgments</b>	<b>xxix</b>
<b>Acronyms</b>	<b>xxxii</b>
<b>1 INTRODUCTION</b>	<b>1</b>
1.1 Information Hiding Inspired by Nature	1
1.2 Information Hiding Basics	5
1.3 Information Hiding Throughout the History	8
1.4 Evolution of Modern Information Hiding	11
1.4.1 Information Hiding in Digital Content	13
1.4.2 File System Steganography	14
1.4.3 Network Steganography	15
1.4.4 Traffic Type Obfuscation	17
1.5 Emerging Trends in Information Hiding	18
1.5.1 Network Steganography	18
1.5.2 Traffic Type Obfuscation	22
1.6 Applications of Information Hiding and Recent Use Cases	23
1.6.1 Benign Applications of Information Hiding	23
1.6.2 Malicious Applications of Information Hiding	24
1.7 Countermeasures for Information Hiding Techniques	28
1.8 Potential Future Trends in Information Hiding	29
1.9 Summary	30
1.10 Organization of the Book	31
References	32

<b>2</b>	<b>BACKGROUND CONCEPTS, DEFINITIONS, AND CLASSIFICATION</b>	<b>39</b>
2.1	Classification of Information Hiding in Communication Networks	40
2.2	Evolution of Information Hiding Terminology	41
2.3	Network Steganography: Definitions, Classification and Characteristic Features	44
2.4	Traffic Type Obfuscation: Definitions, Classification and Characteristic Features	50
2.5	Hidden Communication Model and Communication Scenarios	52
2.6	Information Hiding Countermeasures Models	54
2.7	Summary	56
	References	57
<b>3</b>	<b>NETWORK STEGANOGRAPHY</b>	<b>59</b>
3.1	Hiding Information in Protocol Modifications	60
3.1.1	Size Modulation of Protocol Data Units	61
3.1.2	Sequence Modulation in PDUs	61
3.1.3	Add Redundancy to PDUs	62
3.1.4	Random Values in PDUs	62
3.1.5	Value Modulation in PDUs	62
3.1.6	Reserved/Unused Bits in PDUs	63
3.2	Hiding Information in the Timing of Protocol Messages	64
3.2.1	Rate or Throughput of Network Traffic	64
3.2.2	Interpacket Times	66
3.2.3	Message Sequence Timing	67
3.2.4	Artificial Message/Packet Loss	68
3.2.5	Artificial Retransmissions	69
3.2.6	Manipulated Message Ordering	69
3.2.7	Collision and Timing of Frames	70
3.2.8	Temperature-Based Covert Channels	71
3.2.9	Indirect Timing Channels	72
3.2.10	Covert Sender Location	72
3.3	Hybrid Methods	73
3.3.1	Lost Audio Packets Steganography	74
3.3.2	Retransmission Steganography	80
3.4	Summary	84
	References	84

<b>4</b>	<b>CONTROL PROTOCOLS FOR RELIABLE NETWORK STEGANOGRAPHY</b>	<b>89</b>
4.1	Steganographic Control Protocols	89
4.1.1	Features of Control Protocols	90
4.1.2	Requirements for Control Protocols	91
4.1.3	Existing Control Protocols	93
4.1.4	Comparison of Existing Control Protocols	96
4.2	Deep Hiding Techniques	97
4.3	Control Protocol Engineering	98
4.3.1	Elementary Aspects for Embedding a Control Protocol	100
4.3.2	Status Updates: Dynamic Control Protocol Headers	100
4.3.3	Design of Conforming Control Protocols	102
4.4	Adaptive and Autonomous Covert Control Channels	106
4.4.1	Optimized Post-NEL Communication	107
4.4.2	Forwarding in Covert Channel Overlays	108
4.4.3	Influence of Steganographic Attributes	110
4.5	Techniques for Timing Methods	110
4.6	Attacks on Control Protocols	111
4.7	Open Research Challenges for Control Protocols	111
4.7.1	Multilayer Control Protocols	111
4.7.2	Protocol Translation for Control Protocols	111
4.7.3	Handling of Fake-Input	112
4.8	Summary	112
	References	113
<b>5</b>	<b>TRAFFIC TYPE OBFUSCATION</b>	<b>117</b>
5.1	Preliminaries	118
5.1.1	Applications	118
5.1.2	Comparison with Network Steganography	118
5.2	Classification Based on the Objective	119
5.2.1	Traffic De-identification	119
5.2.2	Traffic Impersonation	121
5.3	Classification Based on the Implementation Domain	124
5.3.1	Content-Based Schemes	124
5.3.2	Pattern-Based Schemes	126
5.3.3	Protocol-Based Schemes	128
5.3.4	Hybrid Schemes	129

5.4	Countermeasures	130
5.4.1	Content-Based Countermeasures	130
5.4.2	Pattern-Based Countermeasures	131
5.4.3	Protocol-Based Countermeasures	134
5.5	Summary	136
	References	136

## **6 NETWORK FLOW WATERMARKING 139**

6.1	Principles, Definitions, and Properties	140
6.1.1	Network Traffic Analysis	140
6.1.2	Linking Network Flows	141
6.1.3	Building Blocks of Flow Watermarking Systems	142
6.1.4	Features of Flow Watermarks	143
6.2	Applications of Flow Watermarks	144
6.2.1	Detection of Stepping Stone Attacks	145
6.2.2	Compromising Anonymous Communication	145
6.2.3	Detection of Centralized Botnets	146
6.2.4	Mitigating Loopback Attacks in Tor	148
6.3	Example Flow Watermarking Systems	148
6.3.1	Types of Flow Watermarks	149
6.3.2	Interval-Centroid-Based Watermarking (ICBW)	149
6.3.3	RAINBOW System	151
6.3.4	SWIRL System	152
6.3.5	Overview of Other Systems	154
6.4	Watermarking Versus Fingerprinting	155
6.4.1	Compromising Anonymity Systems	155
6.4.2	Stepping Stone Detection	157
6.5	Challenges of Flow Watermarking	158
6.5.1	Natural Network Perturbations	158
6.5.2	Adversarial Countermeasures	158
6.6	Summary	158
	References	159

## **7 EXAMPLES OF INFORMATION HIDING METHODS FOR POPULAR INTERNET SERVICES 163**

7.1	IP Telephony: Basics and Information Hiding Concepts	164
7.1.1	Steganographic Methods Applied to VoIP-specific Protocols	165

7.1.2	Transcoding Steganography as VoIP Steganography Example	167
7.2	Information Hiding in Popular P2P Services	172
7.2.1	Skype	172
7.2.2	BitTorrent	176
7.3	Information Hiding in Modern Mobile Devices	179
7.4	Information Hiding in New Network Protocols	182
7.5	Information Hiding Concepts for Wireless Networks	183
7.5.1	Intentionally Corrupted Checksums	184
7.5.2	Padding at Physical Layer	184
7.5.3	Controlling the Intervals Between OFDM Symbols	185
7.5.4	Proposals Specific to 802.11 Networks	185
7.5.5	Implementations: Rather Modification of a Header	186
7.6	Multiplayer Games and Virtual Worlds	187
7.6.1	First Person Shooter Games	187
7.6.2	In-game Client-Server Message Exchange	188
7.6.3	Encoding and Decoding the Covert Data	190
7.6.4	Channel Noise	192
7.6.5	Reliable Data Transport	192
7.6.6	Achievable Throughput	194
7.7	Social Networks	196
7.8	Internet of Things	196
7.8.1	From Surveillance to Steganographic Data Leakage	197
7.8.2	Steganographic Communications	199
7.9	Summary	200
	References	201

## **8 NETWORK STEGANOGRAPHY COUNTERMEASURES 207**

8.1	Overview of Countermeasures	208
8.1.1	General Strategy to Deal with Covert Channels	209
8.1.2	Countermeasures Exploiting Control Protocols	210
8.2	Identification and Prevention During Protocol Design	211
8.3	Elimination of Covert Channels	212
8.3.1	Securing Hosts and Networks	212
8.3.2	Traffic Normalization	213
8.3.3	Elimination Attacks Against Control Protocols	215
8.3.4	Covert Channel Prevention for the Internet of Things	217
8.3.5	Removal Attacks on Network Flow Watermarking	218

8.4	Limiting the Channel Capacity	218
8.4.1	Channel Capacity	218
8.4.2	Limiting Address and Length Field Channels	219
8.4.3	Limiting Timing Channels	219
8.4.4	Limiting Acknowledgment Message Timing Channels	220
8.4.5	Limiting Protocol Switching Channels	221
8.4.6	Limiting RTP Covert Channels	222
8.5	General Detection Techniques and Metrics	222
8.5.1	Machine Learning	223
8.5.2	Statistical Tests and Metrics	226
8.6	Detection Techniques for Covert Channels	228
8.6.1	General Detection Approaches	229
8.6.2	Header Field Channels	229
8.6.3	Timestamp Channels	230
8.6.4	Packet Rate and Timing Channels	231
8.6.5	Payload Tunneling	232
8.6.6	Channels in Multiplayer Games	232
8.6.7	Protocol Switching Channels	233
8.6.8	VoIP-Based Channels	233
8.6.9	Passive Attacks Against Control Protocols	235
8.6.10	Passive Detection of Watermarks	235
8.7	Future Work	236
8.8	Summary	236
	References	237

## **9 CLOSING REMARKS** **243**

### **Glossary** **247**

### **Index** **253**



Describes information hiding in communication networks, and highlights its important issues, challenges, trends, and applications.

This book provides the fundamental concepts, terminology, and classifications of information hiding in communication networks along with its historical background. *Information Hiding In Communication Networks: Fundamentals, Mechanisms, Applications, and Countermeasures* begins with introducing data concealment methods and their evolution. Chapter two discusses the existing terminology, introduces a new classification and describes the model for hidden communication and related communication scenarios. Chapters three to six present the main classes of information hiding in communication networks accompanied by a discussion of their robustness and undetectability. Chapter seven reviews hiding methods for popular Internet services. The book concludes with a discussion of potential countermeasures against information hiding techniques, which includes different types of mechanisms for the detection, and prevention of covert communication channels.

- Highlights development trends and potential future directions of information hiding
- Introduces a new classification and taxonomy for modern data hiding techniques
- Explains the different types of network steganography mechanisms
- Covers several example applications of information hiding in communication networks including recent techniques in popular Internet services

This book is intended for academics, graduate students, professionals, and researchers working in the fields of network security, networking, and communications.

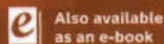
**WOJCIECH MAZURCZYK** is an Associate Professor at the Institute of Telecommunications, Faculty of Electronics and Information Technology, Warsaw University, Poland. He is also a senior member of IEEE.

**STEFFEN WENZEL** is Head of a research team on Secure Building Automation at the Fraunhofer Institute for Communication, Information Processing, and Ergonomics (FKIE) in Bonn, Germany.

**SEBASTIAN ZANDER** is a Lecturer at the School of Engineering and Information Technology, Murdoch University, Australia.

**AMIR HOUMANSADR** is an Assistant Professor within the College of Information and Computer Sciences at the University of Massachusetts Amherst.

**KRZYSZTOF SZCZYPIORSKI** is a Professor of Telecommunications at the Institute of Telecommunications, Faculty of Electronics and Information Technology at Warsaw University of Technology, Poland.



Subscribe to our free Engineering eNewsletter at  
[wiley.com/enewsletters](http://wiley.com/enewsletters)  
[www.wiley.com/ieee](http://www.wiley.com/ieee)

WILEY

 **IEEE**  
IEEE PRESS

