Security and Privacy in Internet of Things (IoTs)

Models, Algorithms, and Implementations

Edited by **Fei Hu**

CRC Press
Taylor & Francis Group

Security and Privacy in Internet of Things (IoTs)

Models, Algorithms, and Implementations

OTHER BOOKS BY FEI HU

Associate Professor
Department of Electrical and Computer Engineering
The University of Alabama

Cognitive Radio Networks
with Yang Xiao
ISBN 978-1-4200-6420-9

Wireless Sensor Networks: Principles and Practice
with Xiaojun Cao
ISBN 978-1-4200-9215-8

Socio-Technical Networks: Science and Engineering Design
with Ali Mostashari and Jiang Xie
ISBN 978-1-4398-0980-8

Intelligent Sensor Networks: The Integration of Sensor Networks, Signal Processing and Machine Learning
with Qi Hao
ISBN 978-1-4398-9281-7

Network Innovation through OpenFlow and SDN: Principles and Design
ISBN 978-1-4665-7209-6

Cyber-Physical Systems: Integrated Computing and Engineering Design
ISBN 978-1-4665-7700-8

Multimedia over Cognitive Radio Networks: Algorithms, Protocols, and Experiments
with Sunil Kumar
ISBN 978-1-4822-1485-7

Wireless Network Performance Enhancement via Directional Antennas: Models, Protocols, and Systems
with John D. Matyjas and Sunil Kumar
ISBN 978-1-4987-0753-4

Security and Privacy in Internet of Things (IoTs): Models, Algorithms, and Implementations
ISBN 978-1-4987-2318-3

Spectrum Sharing in Wireless Networks: Fairness, Efficiency, and Security
with John D. Matyjas and Sunil Kumar
ISBN 978-1-4987-2635-1

Big Data: Storage, Sharing, and Security
ISBN 978-1-4987-3486-8

Opportunities in 5G Networks: A Research and Development Perspective
ISBN 978-1-4987-3954-2

Security and Privacy in Internet of Things (IoTs)

Models, Algorithms, and Implementations

Edited by **Fei Hu**

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business

CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

Version Date: 20160216

International Standard Book Number-13: 978-1-4987-2319-0 (eBook - PDF)

For Fang, Gloria, Edwin, and Edward . . .

This page intentionally left blank

Contents

This page intentionally left blank

Preface

The Internet of Things (IoT) has attracted strong interest from both academia and industry. The IoT integrates radiofrequency identification (RFID), sensors, smart devices, the Internet, smart grids, cloud computing, vehicle networks, and many other information carriers. Goldman Sachs mentioned that the IoT would bring over 28 billion "things" into the Internet by 2020. Typical "things" include end users, data centers, processing units, smartphones, tablets, Bluetooth, ZigBee, IrDA, UWB, cellular networks, Wi-Fi networks, NFC data centers, RFID, their tags, sensors and chips, household machinery, wristwatches, vehicles, house doors, and many other cyberunits. With the growth of nanodevices, smartphones, 5G, tiny sensors, and distributed networks, the IoT is combining the "factual and virtual" anywhere and anytime, and is attracting the attention of both "maker and hacker."

However, interconnecting many "things" also means the possibility of interconnecting many different threats and attacks. For example, a malware virus can easily propagate through the IoT at an unprecedented rate. In the four design aspects of the IoT system, there may be various threats and attacks: (1) Data perception and collection: In this aspect, typical attacks include data leakage, sovereignty, breach, and authentication. (2) Data storage: The following attacks may occur: denial-of-service attacks (attacks on availability), access control attacks, integrity attacks, impersonation, modification of sensitive data, and so on. (3) Data processing: In this aspect there may exist computational attacks that aim to generate wrong data processing results. (4) Data transmission: Possible attacks include channel attacks, session hijacks, routing attacks, flooding, and so on. Apart from attenuation, theft, loss, breach, and disaster, data can also be fabricated and modified by the compromised sensors.

Therefore, efficient and effective defense mechanisms are of the utmost importance to ensure the security of the IoT. In particular, the U.S. Department of

Energy (DOE) has identified attack resistance to be one of the seven major properties required for the operation of the smart grid, which is an emerging field of the IoT. Then, the question is: how do we use efficient algorithms, models, and implementations to cover the four important aspects of IoT security, that is, confidentiality, authentication, integrity, and availability? Obviously, no single scheme can cover all these four aspects, due to the extreme complexity of IoT attacks.

In this book, we have invited some top IoT security experts from all over the world to contribute their knowledge about different IoT security aspects. We have seamlessly integrated those chapters into a complete book. All chapters have a clear problem statement as well as detailed solutions. More than 100 figures have been provided for graphic understanding.

After reading this book, industrial engineers will have a deep understanding of security and privacy principles in complex IoT systems. They will also be able to launch concrete cryptography schemes based on the detailed algorithms provided in some chapters.

After reading this book, academic researchers will be able to understand all critical issues to be solved in this exciting area. They will get to know some promising solutions to those research problems, and pick up an unsolved, challenging issue for their own research.

After reading this book, policy-makers will have a big picture of IoT security and privacy designs, and get to know the necessary procedures to achieve robust IoT information collection, computation, transmission, and sharing across Internet clouds.

All chapters are written for both researchers and developers. We have tried to avoid much jargon and use plain language to describe profound concepts. In many places, we have also provided step-by-step math models for readers' security test bed implementation purposes.

Overall, this book consists of the following five parts:

Section I. Attacks and Threats: This part introduces all types of IoT attacks and threats. It also demonstrates the principle of countermeasures against those attacks. Moreover, we have given detailed introductions of Sybil attacks, malware propagation, and some other specific attacks.

Section II. Privacy Preservation: Privacy is always one of the top concerns for any network application. The IoT collects data from all the "things" around people. Much data is related to human activities. For example, biomedical data may include patients' health records. How do we distribute those data for Internet sharing while, in the meantime, protecting people's privacy well? In this part, we will discuss privacy preservation issues during data dissemination, participatory sensing, and indoor activities. We will also use smart building as an example to discuss privacy protection solutions.

Section III. Trust and Authentication: The trust model is a critical topic of IoT security design. This part will describe different types of trust models in the

IoT infrastructure. The access control to IoT data is also discussed. A survey of IoT authentication issues is provided in this part.

Section IV. IoT Data Security: This part emphasizes the security issues during IoT data computation. We will introduce computational security issues in IoT data processing, security design in time series data aggregation, key generation for data transmission, as well as concrete security protocols during data access.

Section V. Social Awareness: Any security designs should consider policy and human behavioral features. For example, a security scheme cannot be installed in a real platform without the consent of the users. Many attacks aim to utilize the loopholes of user habits. A security design will have deep impacts on the dissemination of IoT data to each corner of the world. In this part, we will cover social-context-based privacy and trust design in IoT platforms, as well as the policy-based informed consent in the IoT.

We have required each chapter author to provide detailed descriptions of the problems to be solved, the motivations of their proposed solutions, and detailed algorithms and implementations. Our goal is to provide readers with a comprehensive understanding of the security and privacy aspects in the IoT system. A few chapters are written in a survey style. They can be used by beginners to get to know the basic principles of achieving attack-resilient IoT infrastructure.

Due to limitations of time, there may be some points missing in this book. Please contact the publisher if you have any comments for its future improvement.

This page intentionally left blank

Editor

Fei Hu is currently a professor in the Department of Electrical and Computer Engineering at the University of Alabama, Tuscaloosa. He obtained his PhDs at Tongji University (Shanghai, China) in the field of signal processing (in 1999), and at Clarkson University (New York) in electrical and computer engineering (in 2002). He has published over 200 journal/conference papers and books. Dr. Hu's research has been supported by the U.S. National Science Foundation, Cisco, Sprint, and other sources. His research expertise may be summarized as 3S: security, signals, sensors. (1) Security: This concerns how to overcome different cyberattacks in a complex wireless or wired network. Recently he has focused on cyberphysical system security and medical security issues. (2) Signals: This mainly refers to intelligent signal processing, that is, using machine learning algorithms to process sensing signals in a smart way in order to extract patterns (i.e., pattern recognition). (3) Sensors: This includes microsensor design and wireless sensor networking issues.

This page intentionally left blank

Contributors

Krishnashree Achuthan
Center for Cybersecurity Systems and Networks
Amrita Vishwa Vidyapeetham
Kerala, India

Kemal Akkaya
Department of Electrical and Computer Engineering
Florida International University
Miami, Florida

Antonio Marcos Alberti
Instituto Nacional de Telecomunicações
Santa Rita do Sapucaí, Brazil

Gianmarco Baldini
European Commission
Joint Research Centre
Ispra, Italy

Haiyong Bao
School of Electrical and Electronic Engineering
Nanyang Technological University
Singapore

Jorge Bernal Bernabe
Department of Information and Communications Engineering
University of Murcia
Murcia, Spain

Fang Bingxing
School of Computer Science
Beijing University of Posts and Telecommunications and Institute of Information Engineering
Chinese Academy of Sciences
Beijing, China

Abdur Rahim Biswas
CREATE-NET
Trento, Italy

Andreas Brauchli
Department of Information and Computer Sciences
University of Hawaii at Manoa
Honolulu, Hawaii

Kwang-Cheng Chen
Graduate Institute of Communication Engineering
National Taiwan University
Taipei, Taiwan

Pin-Yu Chen
Department of Electrical Engineering and Computer Science
University of Michigan
Ann Arbor, Michigan

Xiang Chen
School of Information Science and Technology
Sun Yat-sen University
Guangzhou, China

Shin-Ming Cheng
Department of Computer Science and Information Engineering
National Taiwan University of Science and Technology
Taipei, Taiwan

Bertrand Copigneaux
Inno-Group
Sophia Antipolis, France

Pablo Cortijo Castilla
OSNA Cyber Security Research Group
National University of Ireland
Galway, Ireland

Edielson Prevato Frigieri
Instituto Nacional de Telecomunicações
Santa Rita do Sapucaí, Brazil

Romeo Giuliano
Department for Innovation Technologies and Processes
Guglielmo Marconi University
Rome, Italy

Jose Luis Hernandez
Department of Information and Communications Engineering
University of Murcia
Murcia, Spain

Cheng Huang
School of Electrical and Electronic Engineering
Nanyang Technological University
Singapore

Xumin Huang
School of Automation
Guangdong University of Technology
Guangzhou, China

Bharat Jayaraman
Department of Computer Science and Engineering
University at Buffalo (SUNY)
Buffalo, New York

Na. Jeyanthi
School of Information Technology and Engineering
Vellore Institute of Technology University
Vellore, India

Roger Piqueras Jover
AT & T Security Research Center
New York, New York

Jiawen Kang
School of Automation
Guangdong University of Technology
Guangzhou, China

Jinesh M. Kannimoola
Center for Cybersecurity Systems and Networks
Amrita Vishwa Vidyapeetham
Kerala, India

Chin-Fu Kuo
Department of Computer Science and Information Engineering
National University of Kaohsiung
Kaohsiung, Taiwan

Depeng Li
Department of Information and Computer Sciences
University of Hawaii at Manoa
Honolulu, Hawaii

Liu Licai
School of Computer Science
Beijing University of Posts and Telecommunications and Institute of Information Engineering
Chinese Academy of Sciences
Beijing, China

Yin Lihua
Institute of Information Engineering
Chinese Academy of Sciences
Beijing, China

Xiaodong Lin
Faculty of Business and Information Technology
University of Ontario Institute of Technology
Oshawa, Canada

Hong Liu
Department of Electrical and Computer Engineering
University of Massachusetts Dartmouth
North Dartmouth, Massachusetts

Pavel Loskot
College of Engineering
Swansea University
Swansea, United Kingdom

Rongxing Lu
School of Electrical and Electronic Engineering
Nanyang Technological University
Singapore

Yung-Feng Lu
Department of Computer Science and Information Engineering
National Taichung University of Science and Technology
Taichung, Taiwan

Liangli Ma
School of Electronic Engineering
Naval University of Engineering
Wuhan, China

Franco Mazzenga
Department of Enterprise Engineering
University of Rome Tor Vergata
Rome, Italy

Hugh Melvin
OSNA Cyber Security Research Group
National University of Ireland
Galway, Ireland

Klaus Moessner
Centre for Communications Systems Research
University of Surrey
Surrey, United Kingdom

Mara Victoria Moreno
Department of Information and Communications Engineering
University of Murcia
Murcia, Spain

Michele Nati
Centre for Communications Systems Research
University of Surrey
Surrey, United Kingdom

Ricardo Neisse
European Commission
Joint Research Centre
Ispra, Italy

Alessandro Neri
Department of Engineering
Roma Tre University
Rome, Italy

Jason M. O'Kane
Department of Computer Science and Engineering
University of South Carolina
Columbia, South Carolina

Niklas Palaghias
Centre for Communications Systems Research
University of Surrey
Surrey, United Kingdom

Ranga Rao Venkatesha Prasad
Mathematics and Computer Science Department
Delft University
Delft, the Netherlands

Wei Ren
School of Computer Science
China University of Geosciences
Wuhan, China

Yi Ren
Department of Computer Science
National Chiao Tung University
Hsinchu, Taiwan

Rodrigo da Rosa Righi
Interdisciplinary Program
Universidade do Vale do Rio dos Sinos
São Leopoldo, Brazil

Nico Saputro
Department of Electrical and Computer Engineering
Florida International University
Miami, Florida

Michael Schukat
OSNA Cyber Security Research Group
National University of Ireland
Galway, Ireland

Antonio Skarmeta
Department of Information and Communications Engineering
University of Murcia
Murcia, Spain

Arif Selcuk Uluagac
Department of Electrical and Computer Engineering
Florida International University
Miami, Florida

Anna Maria Vegni
Department of Engineering
Roma Tre University
Rome, Italy

Miao Xu
Department of Computer Science and Engineering
University of South Carolina
South Carolina, Columbia

Wenyuan Xu
Department of Computer Science and Engineering
University of South Carolina
Columbia, South Carolina

Rong Yu
School of Automation
Guangdong University of Technology
Guangzhou, China

Guo Yunchuan
Institute of Information Engineering
Chinese Academy of Sciences
Beijing, China

Ali Ihsan Yurekli
Department of Electrical and Computer Engineering
Florida International University
Miami, Florida

I THREATS AND ATTACKS

This page intentionally left blank

Chapter 1

Internet of Things (IoT) as Interconnection of Threats (IoT)

N. Jeyanthi

CONTENTS

1.1 Introduction

People worldwide are now ready to enjoy the benefits of the Internet of Things (IoT). The IoT incorporates everything from the body sensor to the recent cloud computing. It comprises major types of networks, such as distributed, grid, ubiquitous, and vehicular; these have conquered the world of IT over a decade. From parking vehicles to tracking vehicles, from entering patient details to observing postsurgery, from child care to elder care, from smart cards to near field cards, sensors are making their presence felt. Sensors play a vital role in the IoT as well. The IoT works across heterogeneous networks and standards. Exceptionally, no network is free from security threats and vulnerabilities. Each of the IoT layers is exposed to different types of threats. This chapter focuses on possible threats to be addressed and mitigated to achieve secure communication over the IoT.

The concept of the IoT was proposed in 1999 by the Auto-ID laboratory of the Massachusetts Institute of Technology (MIT). ITU released it in 2005, beginning in China. The IoT can be defined as "data and devices continually available through the Internet." Interconnection of things (objects) that can be addressed

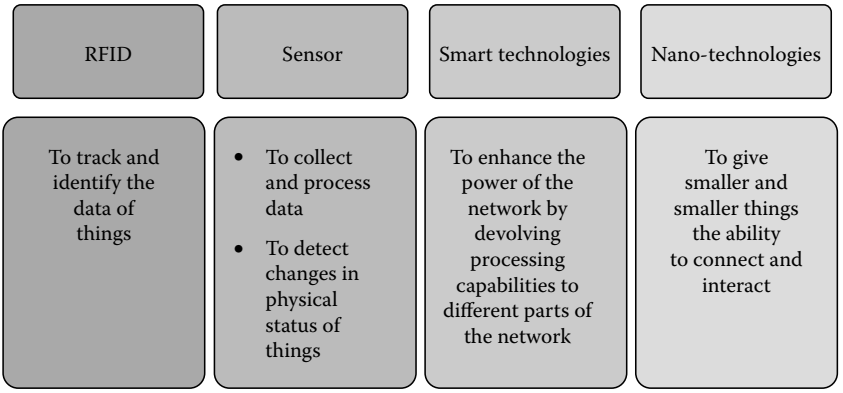

Figure 1.1: IoT underlying technologies.

unambiguously and heterogeneous networks constitute the IoT. Radiofrequency identification (RFID), sensors, smart technologies, and nanotechnologies are the major contributors to the IoT for a variety of services, as shown in Figure 1.1. Goldman Sachs quoted that there are 28 billion reasons to care about the IoT. They also added that in the 1990s, the fixed Internet could connect one billion end users, while in the 2000s, the mobile Internet could connect another two billion. With this growth rate, the IoT will bring as many as 28 billion "things" to the Internet by 2020. With the drastic reduction in the cost of things, sensors, bandwidth, processing, smartphones, and the migration toward IPv6, 5G could make the IoT easier to adopt than expected. Every "thing" comes under one umbrella encompassing all the things.

The IoT also views everything as the same, not even discriminating between humans and machines. Things include end users, data centers (DCs), processing units, smartphones, tablets, Bluetooth, ZigBee, the Infrared Data Association (IrDA), ultra-wideband (UWB), cellular networks, Wi-Fi networks, near field communication (NFC) DCs, RFID and their tags, sensors and chips, household equipment, wristwatches, vehicles, and house doors; in other words, IoT combines "factual and virtual" anywhere and anytime, attracting the attention of both "maker and hacker." Inevitably, leaving devices without human intervention for a long period could lead to theft. IoT incorporates many such things. Protection was a major issue when just two devices were coupled. Protection for the IoT would be unimaginably complex.

1.2 Phases of IoT System

The IoT requires five phases, from data collection to data delivery to the end users on or off demand, as shown in Figure 1.2.

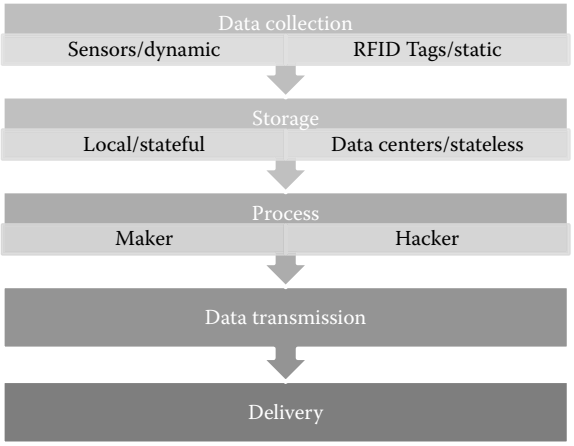

Figure 1.2: Phases of IoT system.

1.2.1 Phase I: Data collection, acquisition, perception

Be it a telemedicine application or vehicle tracking system, the foremost step is to collect or acquire data from the devices or things. Based on the characteristics of the thing, different types of data collectors are used. The thing may be a static body (body sensors or RFID tags) or a dynamic vehicle (sensors and chips).

1.2.2 Phase II: Storage

The data collected in phase I should be stored. If the thing has its own local memory, data can be stored. Generally, IoT components are installed with low memory and low processing capabilities. The cloud takes over the responsibility for storing the data in the case of stateless devices.

1.2.3 Phase III: Intelligent processing

The IoT analyzes the data stored in the cloud DCs and provides intelligent services for work and life in hard real time. As well as analyzing and responding to queries, the IoT also controls things. There is no discrimination between a boot and a bot; the IoT offers intelligent processing and control services to all things equally.

1.2.4 Phase IV: Data transmission

Data transmission occurs in all phases:

- From sensors, RFID tags, or chips to DCs
- From DCs to processing units
- From processors to controllers, devices, or end users

1.2.5 Phase V: Delivery

Delivery of processed data to things on time without errors or alteration is a sensitive task that must always be carried out.

1.3 Internet of Things as Interconnections of Threats (IoT vs. IoT)

In the future, maybe around the year 2020 with IPv6 and the 5G network, millions of heterogeneous things will be part of the IoT. Privacy and security will be the major factors of concern at that time. The IoT can be viewed in different dimensions by the different sections of academia and industry; whatever the viewpoint, the IoT has not yet reached maturity and is vulnerable to all sorts of threats and attacks. The prevention or recovery systems used in the traditional network and Internet cannot be used in the IoT due to its connectivity.

Change is the only thing that is constant, and end users strive to develop technology to suit their needs. The evolution of threats has caused an increase in the security measures that need to be taken into consideration. This chapter presents security issues in three dimensions, based on phase, architecture, and components. Figures 1.3 through 1.6 show all possible types of attacks in these three different views, thus depicting the IoT as the Interconnection of Threats.

1.3.1 Phase attacks

Figure 1.3 demonstrates the variety of attacks on the five phases of IoT. Data leakage, sovereignty, breach, and authentication are the major concerns in the data perception phase.

1.3.1.1 Data leakage or breach

Data leakage can be internal or external, intentional or unintentional, authorized or malicious, involving hardware or software. Export of unauthorized data or information to an unintended destination is data leakage. Generally, this is done by a dishonest or dissatisfied employee of an organization. Data leakage is a serious threat to reliability. As the cloud data move from one tenant to several other tenants of the cloud, there is a serious risk of data leakage. The severity of data leakage can be reduced by the use of DLP (data leakage prevention).

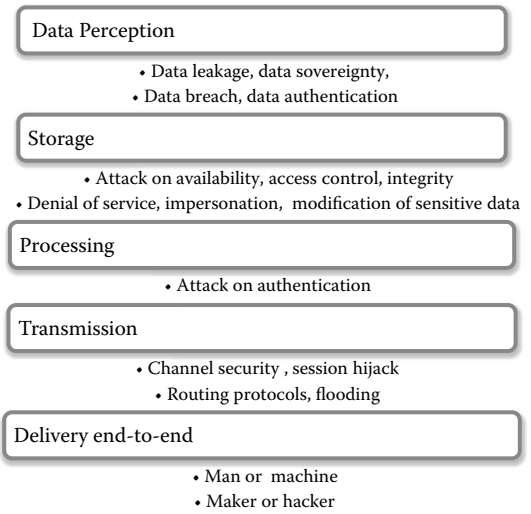

Figure 1.3: Attacks on phases.

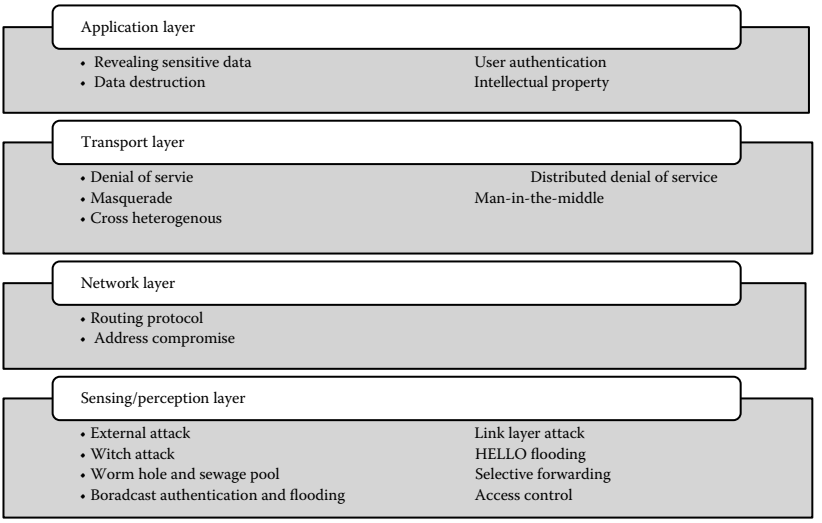

Figure 1.4: Possible attacks based on architecture.

1.3.1.2 Data sovereignty

Data sovereignty means that information stored in digital form is subject to the laws of the country. The IoT encompasses all things across the globe and is hence liable to sovereignty.

1.3.1.3 Data loss

Data loss differs from data leakage in that the latter is a sort of revenge-taking activity on the employer or administrator. Data loss is losing the work accidentally due to hardware or software failure and natural disasters.

1.3.1.4 Data authentication

Data can be perceived from any device at any time. They can be forged by intruders. It must be ensured that perceived data are received from intended or legitimate users only. Also, it is mandatory to verify that the data have not been altered during transit. Data authentication could provide integrity and originality.

1.3.1.5 Attack on availability

Availability is one of the primary securities for the intended clients. Distributed denial of service (DDoS) is an overload condition that is caused by a huge number of distributed attackers. But this not the only overload condition that makes the DCs unavailable to their intended clients. The varieties of overload threat occurrence that cause DCs to freeze at malicious traffic are analyzed here:

- Flooding by attackers
- Flooding by legitimates (flash crowd)
- Flooding by spoofing
- Flooding by aggressive legitimates

1.3.1.5.1 Flooding by attackers

DDoS is flooding of malicious or incompatible packets by attackers toward the DCs. This kind of overload threat can be easily detected by Matchboard Profiler. If the attacker characteristic is found, the user can be filtered at the firewall.

1.3.1.5.2 Flooding by legitimates (flash crowd)

Flash crowd is an overload condition caused by huge numbers of legitimate users requesting the DC resources simultaneously. This can be solved by buffering an excess number of requests so that this overload condition remains live only for a certain period of time.

1.3.1.5.3 Flooding by spoofing attackers

This is caused by impersonation which can be detected by acknowledging each request and by maintaining the sequence number of the requests and requesters' Internet protocol (IP) address.

1.3.1.5.4 Flooding by aggressive legitimates

Aggressive legitimates are users who are restless and repeatedly initiate similar requests within a short time span. This leads to an overload condition, where the legitimate users flood the server with requests that slow down the DC performance. These attacks are difficult to detect because of their legitimate characteristics. By analyzing the inter-arrival time between data packets as well as the values of the back-off timers, those attacks can be detected.

1.3.1.6 Modification of sensitive data

During transit from sensors, the data can be captured, modified, and forwarded to the intended node. Complete data need not be modified; part of the message is sufficient to fulfill the intention.

Modification takes place in three ways: (1) content modification, in which part of the information has been altered; (2) sequence modification, in which the data delivery has been disordered, making the message meaningless; and (3) time modification, which could result in replay attack.

For example, if an ECG report has been altered during a telemedicine diagnosis, the patient may lose his or her life. Similarly, in road traffic, if the congestion or accident has not been notified to following traffic, it could result in another disaster.

1.3.2 Attacks as per architecture

The IoT has not yet been confined to a particular architecture. Different vendors and applications adopt their own layers. In general, the IoT is assumed to have four layers: the lowest-level perception layer or sensing layer, the network layer, the transmission layer, and the application layer. Figure 1.4 depicts the layers and the possible threats to each layer.

1.3.2.1 External attack

In order to make full use of the benefits of the IoT, security issues need to be addressed first. Trustworthiness of the cloud service provider is the key concern. Organizations deliberately offload both sensitive and insensitive data to obtain the services. But they are unaware of the location where their data will be processed or stored. It is possible that the provider may share this information with others, or the provider itself may use it for malicious actions.

1.3.2.2 Wormhole attack

Wormhole attack is very popular in ad hoc networks. IoT connects both stationary and dynamic objects, ranging from wristwatches and refrigerators to vehicles. The link that binds these objects is also heterogeneous, may be wired or wireless,

and depends on the geographical location. Here, the intruder need not compromise any hosts in the network. The intruder just captures the data, forwards them to another node, and retransmits them from that node. Wormhole attack is very strange and difficult to identify.

1.3.2.3 Selective forwarding attack

Malicious nodes choose the packets and drop them out; that is, they selectively filter certain packets and allow the rest. Dropped packets may carry necessary sensitive data for further processing.

1.3.2.4 Sinkhole attack

Sensors, which are left unattended in the network for long periods, are mainly susceptible to sinkhole attack. The compromised node attracts the information from all the surrounding nodes. Thereby, the intruder posts other attacks, such as selective forward, fabrication, and modification.

1.3.2.5 Sewage pool attack

In a sewage pool attack, the malicious user's objective is to attract all the messages of a selected region toward it and then interchange the base station node in order to make selective attacks less effective.

1.3.2.6 Witch attack

The malicious node takes advantage of failure of a legitimate node. When the legitimate node fails, the factual link takes a diversion through the malicious node for all its future communication, resulting in data loss.

1.3.2.7 HELLO flood attacks

In HELLO flood news attacks, every object will introduce itself with HELLO messages to all the neighbors that are reachable at its frequency level. A malicious node will cover a wide frequency area, and hence it becomes a neighbor to all the nodes in the network. Subsequently, this malicious node will also broadcast a HELLO message to all it neighbors, affecting the availability. Flooding attacks cause nonavailability of resources to legitimate users by distributing a huge number of nonsense requests to a certain service.

1.3.2.8 Addressing all things in IoT

Spoofing the IP address of virtual machines (VMs) is another serious security challenge. Malicious users obtain the IP address of the VMs and implant malicious machines to attack the users of these VMs. This enables hacking, and the attackers can access users' confidential data and use it for malicious purposes.

Since the cloud provides on-demand service and supports multitenancy, it is also more prone to DDoS attack. As the attacker goes on flooding the target, the target will invest more and more resources into processing the flood request. After a certain time, the provider will run out of resources and will be unable to service even legitimate users. Unless DLP agents are embedded in the cloud, due to multitenancy and the movement of data from users' control into the cloud environment, the problem of data leakage will also exist.

The Internet has been expanding since its inception, and with it, threats to users and service providers. Security has been a major aspect of the Internet. Many organizations provide services through the Internet that involve banking transactions, registrations, and so on. As a consequence, these websites need to be protected from malicious attacks.

1.3.2.9 Distributed denial of service (DDoS)

DDoS, an attack initiated and continued by some hundreds or even thousands of attackers, starts by populating unwanted traffic packets with enormous size in order to capture and completely deplete memory resources. At the same time, the traffic disallows legitimate requests from reaching the DC and also depletes the bandwidth of the DC. This eventually leads to unresponsiveness to legitimate requests. A denial of service (DoS) or DDoS attack can overwhelm the target's resources, so that authorized users are unable to access the normal services of the cloud. This attack is a cause of failure of availability. Table 1.1 shows the various types of DDoS attacks, the tools used, and the year of origination.

1.3.2.10 Flash crowd

A flash crowd is basically a sudden increase in the overall traffic to any specific web page or website on the Internet and the sudden occurrence of any event that triggers that particular massive traffic of people accessing that web page or website.

Less robust sites are unable to cope with the huge increase in traffic and become unavailable. Common causes of flash crowd are lack of sufficient data bandwidth, servers that fail to cope with the high number of requests, and traffic quotas.

1.3.2.11 IP spoof attack

Spoofing is a type of attack in which the attacker pretends to be someone else in order to gain access to restricted resources or steal information. This type of attack can take a variety of different forms; for instance, an attacker can impersonate the IP address of a legitimate user to get into their accounts. IP address spoofing, or IP spoofing, refers to the creation of IP packets with a forged source IP address, called spoofing, with the purpose of concealing the identity of the sender or impersonating another computing system.

Table 1.1 Origin of DDoS attacks

DDoS Tool	*Possible Attacks*	*Year*
Fapi	UDP, TCP (SYN and ACK), and ICMP floods	June 1998
Trinoo	Distributed SYN DoS attack	June 1999
Tribe Flood Network (TFN)	ICMP flood, SYN flood, UDP flood, and SMURF-style attacks	August 1999
Stacheldraht	ICMP flood, SYN flood, UDP flood, and SMURF attacks	Late summer of 1999
Shaft	Packet flooding attacks	November 1999
Mstream	TCP ACK Flood attacks	April 2000
Trinity	UDP, fragment, SYN, RST, ACK, and other flood attacks	August 2000
Tribe Flood Network 2K (TFN2K)	UDP, TCP, and ICMP Teardrop and LAND attacks	December 2000
Ramen	Uses back chaining model for automatic propagation of attack	January 2001
Code Red and Code Red II	TCP SYN Attacks	July and August 2001
Knight	SYN attacks, UDP flood attacks	July 2001
Nimda	Attacks through e-mail attachments and SMB networking and backdoors attacks	September 2001
SQL slammer	SQL code injection attack	January 2003
DDOSIM (version 0.2)	TCP-based connection attacks	November 2010
Loris	Slowloris attack and its variants, viz. Pyloris	June 2009
Qslowloris	Attacks the websites, e.g., IRC bots, botnets	June 2009
L4D2	Propagation attacks	2009
XerXeS	WikiLeaks attacks, QR code attacks	2010
Saladin	Webservers attacks, Tweet attacks	November 2011
Apachekiller	Apache server attacks, scripting attacks	August 2011
Tor's Hammer	http POST attacks	2011
Anonymous LOIC tool	—	2013

IP spoofing is most frequently used in DoS attacks. In such attacks, the goal is to flood the victim with overwhelming amounts of traffic, and the attacker does not care about receiving responses to the attack packets. They have additional advantages for this purpose—they are more difficult to filter, since each spoofed packet appears to come from a different address, and they hide the true source of the attack.

There are three different types of spoof attacks: impersonation, hiding attack, and reflection attack. Congestion is a threat in any network if the number of incoming packets exceeds the maximum capacity. The factor that is affected at the time of congestion is throughput.

1.3.2.12 Types of spoof attacks

Among the several types of spoofing attacks, the following attacks are addressed, as they are launched on behalf of clients and destroy the DC's resources.

Type I, Hiding attack: Attackers simultaneously send a large number of spoofed packets with random IP address. This creates chaos at the DC regarding which specific packets should be processed as legitimate packets, shown in Figure 1.5.

Type II, Reflection attack: Attackers send spoof packets with the source IP address of the victim to any unknown user. This causes unwanted responses to reach the victim from unknown users and increases the flood rate, shown in Figure 1.6.

Type III, Impersonation attack: Attackers send spoof packets with the source IP address of any unknown legitimate user and acting as a legitimate user. This is equivalent to a man-in-the-middle attack. The spoof attacker receives requests from clients, spoofs IP, and forwards the requests to the DC, acting as a legitimate user. The responses of the DC are again processed intermediately and sent to the clients. This leads to confidentiality issues and data theft or loss at the DC, as shown in Figure 1.7.

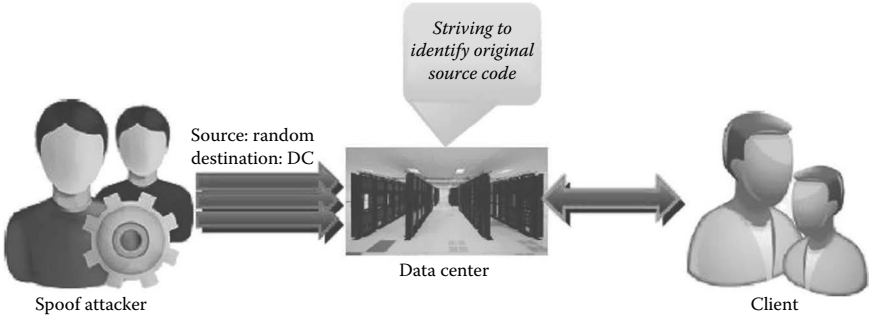

Figure 1.5: Hiding attack.

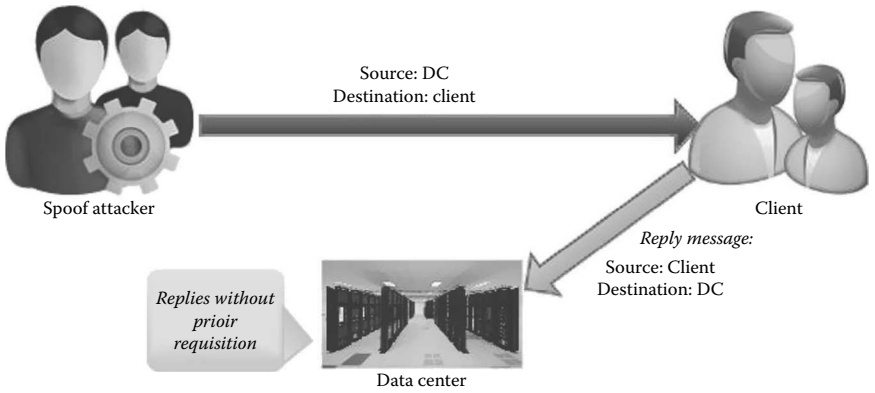

Figure 1.6: Reflection attack.

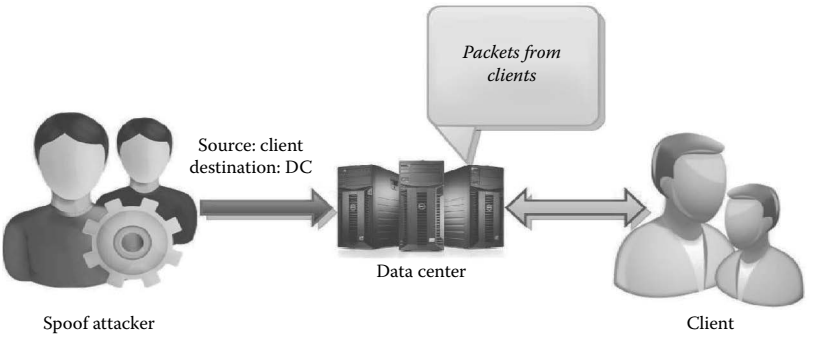

Figure 1.7: Impersonation attack.

If a proper spoof detection mechanism is not in place, the DC could respond badly, leading to a partial shutdown of services.

- In network-level DDoS, the attackers will try to send invalid requests with the aim of flooding the cloud service provider (CSP); for example, requests for a half-open connection.
- In service-level DDoS, the attacker will be sending requests that seem to be legitimate. Their content will be similar to a request made by a legitimate user. Only their intention is malicious.

1.3.2.13 Goodput

Goodput is the application-level throughput, that is, the number of useful information bits, delivered by the network to a certain destination, per unit of time.

The amount of data considered excludes protocol overhead bits as well as retransmitted data packets. The goodput is a ratio between the amount of information delivered and the total delivery time. This delivery time includes interpacket time gaps, overhead in transmission delay, packet queuing delay, packet retransmission time, delayed acknowledge, and processing delay.

1.3.2.14 Data centers (DCs)

A DC is a centralized repository, either physical or virtual, for the storage, management, and dissemination of data and information organized around a particular body of knowledge or pertaining to a particular business.

A DC is a facility used to house computer systems and associated components and huge storage systems. The main purpose of a DC is to run the applications that handle the core business and operational data of the organization. Such systems may be proprietary and developed in house by the organization, or bought from enterprise software vendors. Often, these applications will be composed of multiple hosts, each running a single component. Common components of such applications are databases, file servers, application servers, middleware, and various others.

1.3.2.15 Botnet

A *botnet* is a collection of Internet-connected computers whose security defenses have been breached and control ceded to a malicious party. Each such compromised device, known as a "bot," is created when a computer is penetrated by software from a malware distribution, otherwise known as malicious software. The controller of a botnet is able to direct the activities of these compromised computers through communication channels formed by standards-based network protocols such as Internet Relay Chat (IRC) and hypertext transfer protocol (http).

In DDoS attacks, multiple systems submit as many requests as possible to a single Internet computer or service, overloading it and preventing it from servicing legitimate requests. An example is an attack on a victim's phone number. The victim is bombarded with phone calls by the bots, attempting to connect to the Internet.

1.3.2.16 Confidentiality

All the clients' data are to be transacted in a network channel with greater visibility regarding assurance for the intended clients that data are tamperproof.

1.3.2.17 Physical security

Hardware involved in serving clients must be continuously audited with a safe checkpoint for the sake of hysteresis identification of threats.

1.3.2.18 Software security

Corruption or modification of application software by threats could affect several clients who depend on that particular application programming interface (API) and related software interfaces.

1.3.2.19 Network security

Bandwidth attacks such as DoS and DDoS can cause severe congestion the network and also affect normal operations, resulting in communication failure.

1.3.2.20 Legal service-level agreement (SLA) issues

SLAs between customer and service provider must satisfy legal requirement, as the cyber laws vary for different countries. Incompatibilities may lead to compliance issues.

1.3.2.21 Eavesdropping

Eavesdropping is an interception of network traffic to gain unauthorized access. It can result in failure of confidentiality. The *man in the middle attack* is also a category of eavesdropping.

The attack sets up a connection with both victims involved in a conversation, making them believe that they are talking directly but infecting the conversation between them.

1.3.2.22 Replay attack

The attacker intercepts and saves old messages and then sends them later as one of the participants to gain access to unauthorized resources.

1.3.2.23 Back door

The attacker gains access to the network through bypassing the control mechanisms using a "back door," such as a modem and asynchronous external connection.

1.3.2.24 Sybil attack

Impersonation is a threat in which a malicious node modifies the data flow route and lures the nodes to wrong positions. In *Sybil attack*, a malicious user pretends to be a distinct user after acquiring multiple identities and tries to create a relationship with an honest user. If the malicious user is successful in compromising one of the honest users, the attacker gains unauthorized privileges that help in the attacking process.

1.3.2.25 Byzantine failure

Byzantine failure is a malicious activity that compromises a server or a set of servers to degrade the performance of the cloud.

1.3.2.26 Data protection

Data Protection It is difficult for the cloud customer to efficiently check the behavior of the cloud supplier, and as a result, the customer is confident that data is handled in a legal way. But practically, various data transformations intensify the job of data protection.

1.3.2.27 Incomplete data deletion

Incomplete Data Deletion Accurate data deletion is not possible, because copies of data are stored in the nearest replica but are not available.

1.3.3 Attacks based on components

The IoT connects "everything" through the Internet. These things are heterogeneous in nature, communicating sensitive data over a distance. Apart from attenuation, theft, loss, breach, and disaster, data can also be fabricated and modified by compromised sensors. Figure 1.8 shows the possible types of attacks at the component level.

Verification of the end user at the entry level is mandatory; distinguishing between humans and machines is extremely important. Different types of Completely Automated Public Turing test to tell Computers and Humans

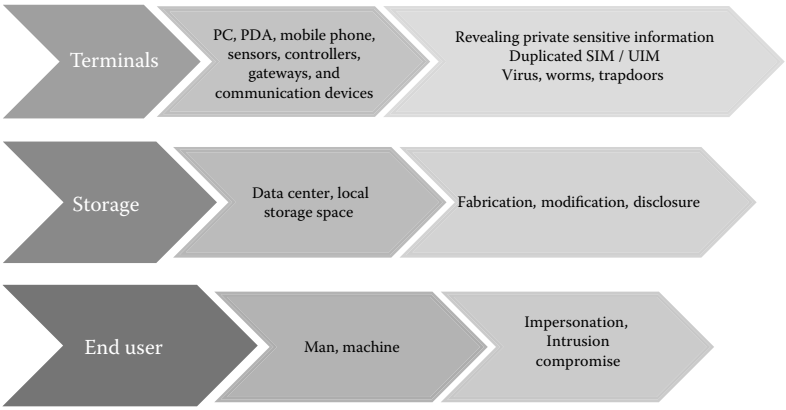

Figure 1.8: Possible attacks based on components.

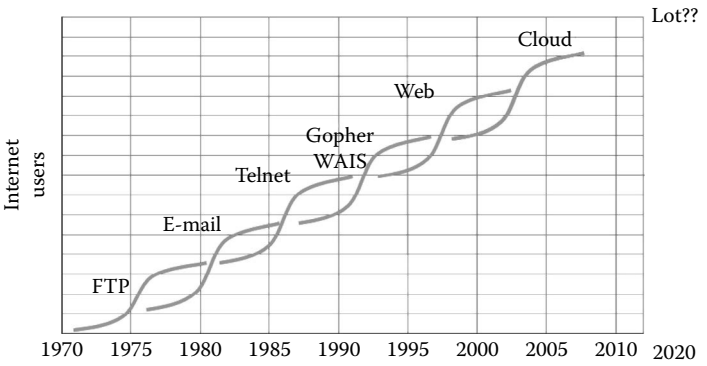

Figure 1.9: Growth of IoT. (*Courtesy of Forrester*.)

Apart (CAPTCHA) help in this fundamental discrimination. With its exponential growth, the IoT will soon dominate the IT industry, as shown in Figure 1.9.

Bibliography

[1] Chuankun, Wu. A preliminary investigation on the security architecture of the Internet of Things. *Strategy and Policy Decision Research*, 2010, 25(4): 411–419.

[2] Goldman Sachs. *IoT Primer, The Internet of Things: Making Sense of the Next Mega-Trend*. September 3, 2014.

[3] International Telecommunication Union. ITU Internet reports 2005: The Internet of Things. 2005.

[4] Ibrahim Mashal, Osama Alsaryrah, Tein-Yaw Chung, Cheng-Zen Yang, Wen-Hsing Kuo, Dharma P. Agrawal. Choices for interaction with things on internet and underlying issues. *Ad Hoc Networks*, 2015, 28: 68–90.

[5] Jeyanthi, N., N.Ch.S.N. Iyengar. Escape-on-sight: An efficient and scalable mechanism for escaping DDoS attacks in cloud computing environment. *Cybernetics and Information Technologies*, 2013, 13(1): 46–60.

[6] Kang Kai, Pang Zhi-bo, Wang Cong. Security and privacy mechanism for health Internet of Things. *The Journal of China Universities of Posts and Telecommunications*, 2013, 20(Suppl. 2): 64–68.

[7] Kim Thuat Nguyen, Maryline Laurent, Nouha Oualha. Survey on secure communication protocols for the Internet of Things. *Ad Hoc Networks*, 2015, 32: 17–31.

[8] Lan Li. Study on security architecture in the Internet of Things. *Measurement, International Conference on Information and Control (MIC)*, 2012, pp. 374–377.

[9] Peng, Xi, Zheng Wu, Debao Xiao, Yang Yu. Study on security management architecture for sensor network based on intrusion detection. *2009 International Conference on Networks Security, Wireless Communications and Trusted Computing*, IEEE, New York.

[10] Prabadevi, B., N. Jeyanthi. Distributed denial of service attacks and its effects on cloud environment: A survey. *The 2014 International Symposium on Networks, Computer and Communications*, June 17–19, 2014, Hammamet, Tunisia, IEEE.

[11] Qazi Mamoon Ashraf, Mohamed Hadi Habaebi. Autonomic schemes for threat mitigation in Internet of Things. *Journal of Network and Computer Applications*, 2015, 49: 112–127.

[12] Qinglin, Cao. Review of research on the Internet of Things. *Software Guide*, 2010, 9(5): 6–7.

[13] Rodrigo Roman, Jianying Zhou, Javier Lopez. On the features and challenges of security and privacy in distributed Internet of Things. *Computer Networks*, 2013, 57: 2266–2279.

[14] Rolf H. Weber. Internet of Things—New security and privacy challenges. *Computer Law and Security Review*, 2010, 26: 23–30.

[15] Sicari, S., Rizzardi, A., Grieco, L.A., Coen-Porisini, A. Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*, 2015, 76: 146–164.

[16] Wang, Y.F., Lin, W.M., Zhang, T., Ma, Y.Y. Research on application and security protection of Internet of Things in smart grid, *Information IET International Conference on Science and Control Engineering 2012 (ICISCE 2012)*, 2012, pp. 1–5, Shenzhen, China.

[17] Xingmei, Xu, Zhou Jing, Wang He. Research on the basic characteristics, the key technologies, the network architecture and security problems of the Internet of Things. *3rd International Conference on Computer Science and Network Technology (ICCSNT)*, 2013, pp. 825–828.

[18] Yang Guang, Geng Guining, Du Jing, Liu Zhaohui, Han He. Security threats and measures for the Internet of Things. *Tsinghua University (Science and Technology)*, 2011, 51(10): 19–25.

[19] Yang Yongzhi, Gao Jianhua. A study on the "Internet of Things" and its scientific development in China. *China's Circulation Economy*, 2010, 2: 46–49.

[20] Yang Geng, Xu Jian, Chen Wei, Qi Zheng-hua, Wang Hai-yong. Security characteristic and technology in the Internet of Things. *Journal of Nanjing University of Posts and Telecommunications (Natural Science)*, 2010, 30(4): 21–28.

[21] Zhang Fu-Sheng. *Internet of Things: Open a New Life of Intelligent Era*. ShanXi People's Publishing House. 2010, pp. 175–184.

This page intentionally left blank

Chapter 2

Attack, Defense, and Network Robustness of Internet of Things

Pin-Yu Chen

CONTENTS

2.1 Introduction

The Internet of Things (IoT) [3] enables ubiquitous communication among different devices. However, the functionality and operations of the IoT heavily depend on the underlying network connectivity structure. Despite the fact that the IoT features ubiquitous communication among all kinds of electronic devices, it inevitably raises security concerns due to seamless penetration and automated integration among all sorts of applications. For example, an adversary may leverage the interconnected devices for malware propagation [7, 16–19]. Therefore, efficient and effective defense mechanisms are of the utmost importance to ensure the reliability of the IoT [9, 12]. In particular, the U.S. Department of Energy (DOE) has identified attack resistance to be one of the seven major properties required for the operation of the smart grid [1], which is an emerging field of the IoT.

By representing the intricate connections of the IoT as a graph, we can investigate the network vulnerability of the IoT to various attack schemes. Three defense schemes are investigated to counter fatal attacks: the intrinsic topological defense scheme, the fusion-based defense scheme, and the sequential defense scheme. Furthermore, by formulating the interplay between an adversary and a defender as a two-player zero-sum game, in which they aim to maximize their own payoffs in terms of network connectivity, we can use the game equilibrium to evaluate network robustness. A sequential defense scheme is also introduced to defend against fatal attacks in the IoT. The results are demonstrated via real-world network data.

Throughout this chapter, we use the undirected and unweighted graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ to characterize the network connectivity structure of the IoT, where $\mathcal{V}$ is the set of nodes (devices) with size n, and $\mathcal{E}$ is the set of edges (connections) with size m. Equivalently, the graph can be represented by an n-by-n binary symmetric adjacency matrix $\mathbf{A}$, where $\mathbf{A}_{ij} = 1$ if there is an edge between nodes i and j; otherwise, $\mathbf{A}_{ij} = 0$. For the following sections, we use the fraction of the largest connected graph as a measure of network resilience to node or edge removals in the IoT. Node or edge removals can be viewed as temporal device or connection failures or targeted attacks in the IoT setting. For instance, node or edge removals in a graph can be caused by denial of service (DoS) or jamming attacks, or by natural occurrences.

2.2 Centrality Attacks, Network Resilience, and Topological Defense Scheme

2.2.1 Centrality attacks

A node centrality measure is a quantity that measures the level of importance of a node in a network. The utility of centrality measures is that they can break the combinatorial bottleneck of searching through all the possible permutations

and combinations of nodes that might reduce largest component size. An attack that removes nodes according to a measure of centrality will be referred to as a *centrality attack* [14]. For example, the authors of [2, 6, 11, 28] study the effectiveness of degree centrality attacks, that is, removing the largest hub nodes, as a way to reduce the size of the largest component of the network. However, it has been shown in [13] that node degree is not the most effective centrality measure for minimizing largest component size. For different network topologies, investigating resilience of network connectivity to centrality attacks provides a unified metric for evaluating network vulnerabilities.

Let $\mathcal{N}_i$ denote the set of nodes connecting to node i (i.e., the set of neighbors of node i), and let $|\mathcal{N}_i|$ denote the set size. The degree of node i is the number of edges connected to it, that is, $d_i = \sum_{j=1}^{|\mathcal{V}|} \mathbf{A}_{ij} = |\mathcal{N}_i|$. The degree matrix $\mathbf{D}$ is defined as $\mathbf{D} = \text{diag}\left(d_1, d_2, \ldots, d_{|\mathcal{V}|}\right)$, where $\mathbf{D}$ is a diagonal matrix with degree information on its main diagonal, the rest of the entries being 0. The graph Laplacian matrix $\mathbf{L}$ is defined as $\mathbf{L} = \mathbf{D} - \mathbf{A}$, and therefore it encodes degree information and connectivity structure of a graph. $\mathbf{L}$ is a positive semidefinite matrix, all its eigenvalues are nonnegative, and $\text{trace}(\mathbf{L}) = 2|\mathcal{E}|$, where $\text{trace}(\mathbf{L})$ is the sum of eigenvalues of $\mathbf{L}$, and $|\mathcal{E}|$ is the number of edges in $\mathcal{G}$. Moreover, the smallest eigenvalue of $\mathbf{L}$ is always 0, and the eigenvector of the smallest eigenvalue is a constant vector. The second smallest eigenvalue of $\mathbf{L}$, denoted by $\mu(\mathbf{L})$, is also known as the algebraic connectivity [21]. It has been proved in [21] that $\mu(\mathbf{L})$ is a lower bound on node and edge connectivity for any noncomplete graph. That is, algebraic connectivity $\leq$ node connectivity $\leq$ edge connectivity.

The centrality of a node is a measure of the node's importance to the network. Centrality measures can be classified into two categories: *global* and *local* measures. Global centrality measures require complete topological information for their computation, whereas local centrality measures require only partial topological information from neighboring nodes. For instance, acquiring shortest path information between every node pair is a global method required for the betweenness centrality measure, and acquiring degree information of every node is a local method. Some commonly used centrality measures are

- *Betweenness* [22]: Betweenness is the fraction of shortest paths passing through a node relative to the total number of shortest paths in the network. Specifically, it is a global measure defined as betweenness $(i) =$

$$\sum_{k \neq i} \sum_{j \neq i, j > k} \frac{\sigma_{kj}(i)}{\sigma_{kj}},$$

  where σ_{kj} is the total number of shortest paths from k to j, and $\sigma_{kj}(i)$ is the number of such shortest paths passing through i.

- *Closeness* [25]: Closeness is a global measure of shortest path distance of a node to all other nodes. A node is said to have higher closeness if

the sum of its shortest path distance to all other nodes is smaller. Let $\rho(i,j)$ denote the shortest path distance between node i and node j in a connected graph; then closeness$(i) = 1/\sum_{j\in\mathcal{V}, j\neq i}\rho(i,j)$.

- *Eigenvector centrality* (eigen centrality): Eigenvector centrality depends on the ith entry of the eigenvector associated with the largest eigenvalue of the adjacency matrix $\mathbf{A}$. It is defined as eigen$(i) = \lambda_{\max}^{-1}\sum_{j\in\mathcal{V}}\mathbf{A}_{ij}\xi_j$, where $\lambda_{\max}$ is the largest eigenvalue of $\mathbf{A}$, and ξ is the eigenvector associated with $\lambda_{\max}$. It is a global measure, since the eigenvalue decomposition of $\mathbf{A}$ requires complete topological information of the entire network.

- *Degree* (d_i): Degree is the simplest local centrality measure, which is simply the number of neighboring nodes.

- *Ego centrality* [20]: Consider the (d_i+1)-by-(d_i+1) local adjacency matrix of node i, denoted by $\mathbf{A}(i)$, and let $\mathbf{I}$ be an identity matrix. Ego centrality can be viewed as a local version of betweenness that computes the shortest paths between its neighboring nodes. Since $[\mathbf{A}^2(i)]_{kj}$ is the number of two-hop walks between k and j, and $\left[\mathbf{A}^2(i)\circ(\mathbf{I}-\mathbf{A}(i))\right]_{kj}$ is the total number of two-hop shortest paths between k and j for all $k\neq j$, where $\circ$ denotes entrywise matrix product, ego centrality is defined as ego$(i) = \sum_k\sum_{j>k} 1/\left[\mathbf{A}^2(i)\circ(\mathbf{I}-\mathbf{A}(i))\right]_{kj}$.

- *Local Fiedler Vector Centrality* (LFVC) [15]: LFVC is a measure that characterizes vulnerability to node removals. A node with higher LFVC is more important for network connectivity structure. Let $\mathbf{y}$ (the Fiedler vector) denote the eigenvector associated with the second smallest eigenvalue $\mu(L)$ of the graph Laplacian matrix $\mathbf{L}$. LFVC is defined as LFVC$(i) = \sum_{j\in\mathcal{N}_i}(y_i - y_j)^2$. Although LFVC is a global centrality measure, it can be accurately approximated by local computations and message passing using the distributed power iteration method of [5] to compute the Fiedler vector $\mathbf{y}$.

Note that the edge centrality measure can be defined in a similar fashion.

2.2.2 Network resilience

When evaluating network resilience to different centrality attacks, we often compare the number of node removals needed by a centrality attack to reduce the largest component size to a certain amount, say, the number of nodes required to reduce the largest component size to 10% of its original size. For illustration, Figure 2.1 shows the network resilience of the Europe Internet backbone network topology (GTS-CE dataset) [23]. This network contains 149 nodes

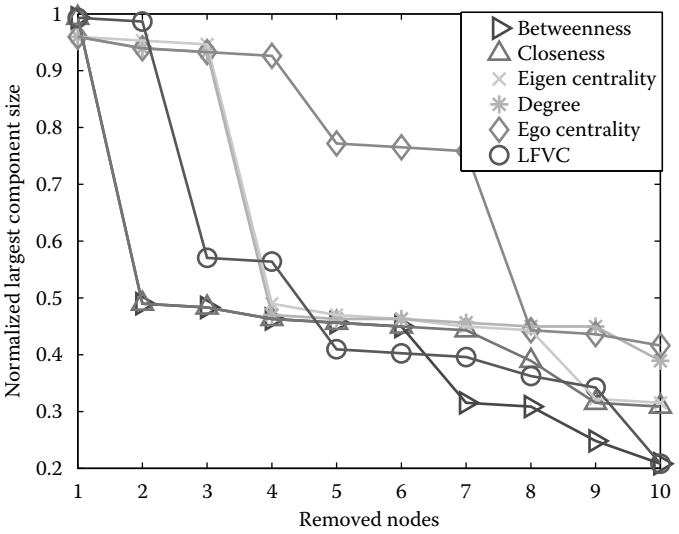

Figure 2.1: Resilience of network connectivity to different centrality attacks on the Europe Internet backbone network topology (GTS-CE dataset). The largest component size can be reduced to 20% of its original size by removing 10 nodes based on LFVC or betweenness attacks. (Data from S. Knight, H.X. Nguyen, N. Falkner, R. Bowden, and M. Roughan. The Internet topology zoo. *IEEE J. Sel. Areas Commun.*, 29(9), 1765–1775, 2011.)

(routers) and 193 edges (physical connections). In this network, betweenness and LFVC attacks have comparable performance that results in 20% reduction of the largest component size by removing 10 nodes from the network. The topological information needed to compute the centrality measures are updated when a node is removed from the graph (i.e., a greedy removal approach). The network resilience of a Western U.S. power grid can be found in [14].

2.2.3 Topological defense scheme

A topological defense scheme allows change of network topology to enhance network resilience. It has been found in [14] that by swapping a small number of edges in the network topology, one is able to greatly improve network resilience without including additional edges. As shown in Figure 2.2, the Europe Internet backbone network can be secured by swapping 20 edges, such that the rewired network is more robust to centrality attacks. Moreover, the proposed edge rewiring method in [14] can be implemented in a distributed fashion, which is particularly preferable for the IoT due to scalability.

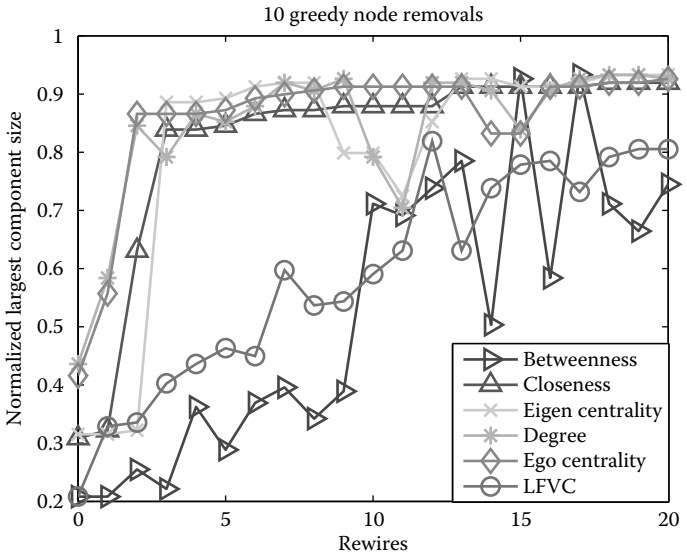

Figure 2.2: Network connectivity of the edge rewiring method when restricted to 10 greedy node removals on the Europe Internet backbone network topology (GTS-CE dataset) [23]. The edge rewiring method can greatly improve network resilience without introducing additional edges into the network. (Data from S. Knight, H.X. Nguyen, N. Falkner, R. Bowden, and M. Roughan. The Internet topology zoo. *IEEE J. Sel. Areas Commun.*, 29(9):17651775, 2011; edge rewiring method proposed by Pin-Yu Chen and Alfred O. Hero. Assessing and safeguarding network resilience to nodal attacks. *IEEE Commun. Mag.*, 52(11):138–143, 2014.)

2.3 Game-Theoretic Analysis of Network Robustness and Fusion-Based Defense Scheme

In many cases, edge rewire is not permitted in the IoT due to circumstances such as protocol confinement, geolocation constraint, and so on. In this scenario, one seeks to use the nodal detectability to infer the presence of an attack [6, 8, 11]. A fusion-based defense mechanism is proposed [6, 8, 11] to infer the presence of an attack based on the feedbacks from each node. The feedback information can be as simple as a binary status report reflecting that each node is, or is not, under attack, based on the node-level detection capabilities. Then, a network-level attack inference scheme is carried out at the fusion center.

An illustration of the attack and fusion-based defense model for the IoT is shown in Figure 2.3. A two-player game between the defender (the fusion center) and the attacker is naturally formed, given the critical value of network resilience (e.g., the largest component can be no less than 50% of its original size) and the node-level detection configurations. Intuitively, from the adversary's perspective,

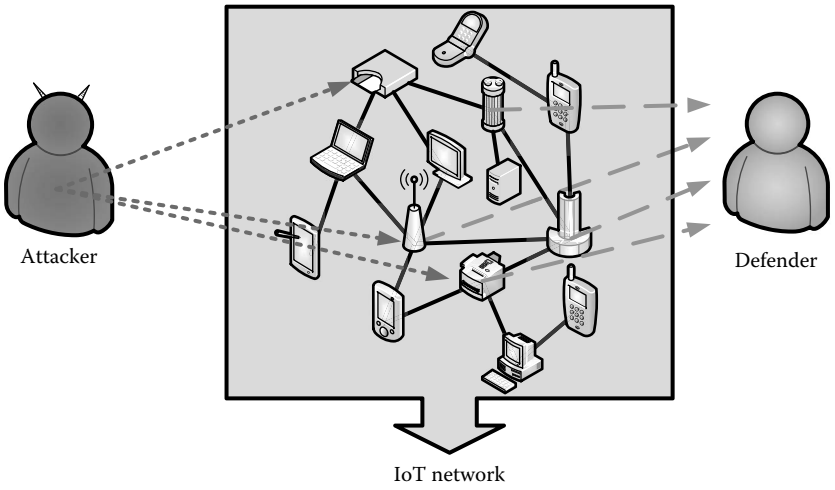

Figure 2.3: Illustration of the attack and fusion-based defense model for the IoT. The adversary attacks a subset of nodes, as indicated by the red dotted arrows. The defender performs attack inference based on the attack status feedbacks from another subset of nodes, as indicated by blue dashed arrows.

too few node removals cause hardly any harm to the network connectivity, while too many node removals are prone to be detected by the fusion center, which means that the attack is eventually in vain. From the defender's perspective, inferring attacks using all feedbacks might treat the topological attack as a false alarm, since only a small subset of nodes are targeted. On the other hand, inferring attacks using only a few feedbacks might suffer from information insufficiency and therefore fail to detect the presence of attacks. Consequently, there exists a balance point at which both attacker and defender are satisfied with their own strategies, which is exactly the notion of Nash equilibrium in game theory [24]. At game equilibrium, no player's payoff can be increased by unilaterally changing strategy. As a result, the game payoff at game equilibrium can be used to study the robustness of a network.

As an illustration, we evaluate the network robustness of the Internet router-level topology [2] and the EU power grid [26] in terms of the payoff of the defender at the game equilibrium in Figure 2.4. The parameter P_D (P_F) denotes the probability of declaring an attack when the attack is actually present (absent). It is observed that the EU power grid is more robust to the Internet router-level topology given the same parameters P_D and P_F, and the network robustness approaches 1 as the detection capability increases, which suggests that the adversary gradually loses its advantage in disrupting the network, and the damage caused by malicious attacks can be alleviated by the fusion-based defense mechanism.

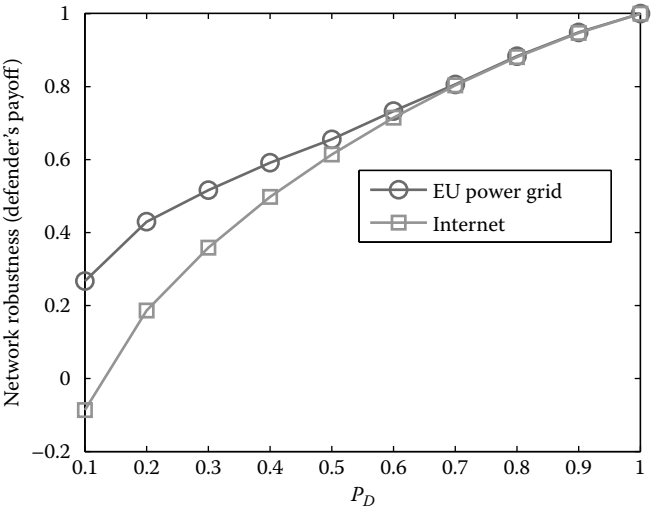

Figure 2.4: Network robustness of the Internet router-level topology and the EU power grid under degree attack when $P_F = 0.01$. The topological map of the Internet contains 6,209 nodes and 12,200 edges, and the EU power grid contains 2,783 nodes and 3,762 edges. (The empirical data are the network parameters collected by Réka Albert, Hawoong Jeong, and Albert-Laszlo Barabási. Error and attack tolerance of complex networks. *Nature*, 406(6794):378–382, 2000; Ricard V. Solé, Martí Rosas-Casals, Bernat Corominas-Murtra, and Sergi Valverde. Robustness of the European power grids under intentional attack. *Phys. Rev. E*, 77:026102, 2008.)

These results suggest that in addition to topological defense approaches (e.g., the edge rewiring method), one can improve network resilience of the IoT by implementing network-level defense mechanisms. However, one main disadvantage of fusion-based defense is the acquisition of feedbacks from all nodes, which may not be applicable to the IoT due to its enormous number of devices. Nonetheless, fusion-based defense can be used in a hierarchical manner for multilayer defense.

2.4 Sequential Defense Scheme

A sequential defense scheme is proposed by [10] that sequentially collects feedbacks from high degree nodes for attack inference. The advantage of sequential defense is that there is no need to acquire feedbacks from all nodes, and it terminates the collection process once sufficient feedbacks have been collected for attack inference. The enormous network size (e.g., Internet routers or sensors in the IoT) renders simultaneous data transmissions infeasible, especially

for wireless networks with scarce radio resources. Moreover, due to the large network size and limited computational power, analyzing the collected information from all nodes incurs tremendous computation overheads, and it may fail to provide timely defense.

It is worth mentioning that the sequential defense scheme is quite distinct from the traditional data fusion scheme [27] due to the fact that the attack may not be a common event to all the nodes in the network. In other words, an intelligent adversary can target some crucial nodes instead of launching attacks on the entire network to efficiently disrupt the network and reduce the risks of being detected, which therefore hinders the precision of attack inference and poses severe threats to the network robustness.

It is proved in [10] that a relatively small fraction of feedbacks is sufficient to detect fatal attacks on the network prior to network disruption. We compare the number of node removals required for a network to break down and the number of feedbacks needed for the sequential defense scheme to detect the attack under three different real-world networks: the webpage links in the World Wide Web (WWW) [4], the Internet router-level topology [2], and the EU power grid [26]. Figure 2.5 shows the number of feedbacks needed for sequential defense under different parameters P_D and P_F. It can be observed that there is a surge in the number of required observations when P_F is large and P_D is small, as intuitively one needs more observations to verify the presence of an attack in the circumstances of low detection capability and high false alarm rate. Comparing the

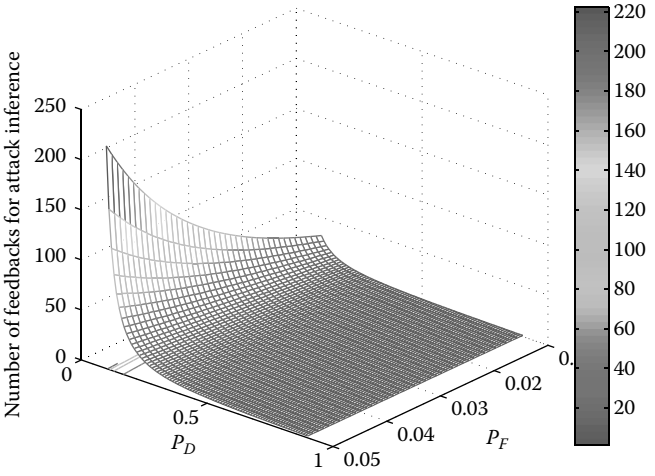

Figure 2.5: Expected number of feedbacks required for the sequential defense scheme to detect a degree attack. The critical values for the WWW, the Internet, and the EU power grid to break down are 21,824, 187, and 766, respectively.

critical number of node removals for network breakdowns, the required numbers of feedbacks for these three networks are less than the critical value for moderate P_D and P_F. These results suggest that sequential defense can effectively detect an attack prior to network breakdown by acquiring only a small number of feedbacks.

2.5 Conclusion

This chapter introduces several centrality attacks that aim to maximally disrupt the connectivity of an IoT network, and three defense schemes to counter these fatal attacks are investigated. The first one is the topological defense scheme, which allows edge swapping to enhance intrinsic network resilience. The second one is the fusion-based defense mechanism and the game-theoretic perspective of network robustness. The third one is the sequential defense scheme, which enables efficient attack inference with only a few feedbacks from the network.

Acknowledgment

The author would like to thank Dr. Alfred Hero at the Department of Electrical Engineering and Computer Science, University of Michigan, Ann Arbor, United States, Dr. Shin-Ming Cheng at the Department of Computer Science and Information Engineering, National Taiwan University of Science and Technology, Taiwan, and Dr. Kwang-Cheng Chen at the Department of Electrical Engineering, National Taiwan University, Taiwan, for their valuable discussion and collaboration.

Bibliography

[1] U.S. Department of Energy (DOE). *A System View of the Modern Grid*. National Energy Technology Laboratory (NETL), U.S. Department of Energy (DOE), 2007.

[2] Réka Albert, Hawoong Jeong, and Albert-Laszlo Barabási. Error and attack tolerance of complex networks. *Nature*, 406(6794):378–382, 2000.

[3] Luigi Atzori, Antonio Iera, and Giacomo Morabito. The internet of things: A survey. *Computer Networks*, 54(15):2787–2805, 2010.

[4] Albert-Laszlo Barabási and Réka Albert. Emergence of scaling in random networks. *Science*, 286(5439):509–512, October 1999.

[5] Alexander Bertrand and Marc Moonen. Distributed computation of the Fiedler vector with application to topology inference in ad hoc networks. *Signal Processing*, 93(5):1106–1117, 2013.

[6] Pin-Yu Chen, Shin-Ming Cheng, and Kwang-Cheng Chen. Smart attacks in smart grid communication networks. *IEEE Commun. Mag.*, 50(8): 24–29, August 2012.

[7] Pin-Yu Chen and Kwang-Cheng Chen. Information epidemics in complex networks with opportunistic links and dynamic topology. In *Proceedings of IEEE Global Telecommunications Conference (GLOBECOM)*, pages 1–6, December 2010.

[8] Pin-Yu Chen and Kwang-Cheng Chen. Intentional attack and fusion-based defense strategy in complex networks. In *Proc. IEEE Global Telecommunications Conference (GLOBECOM)*, pages 1–5, December 2011.

[9] Pin-Yu Chen and Kwang-Cheng Chen. Optimal control of epidemic information dissemination in mobile ad hoc networks. In *IEEE Global Telecommunications Conference (GLOBECOM)*, pages 1–5, December 2011.

[10] Pin-Yu Chen and Shin-Ming Cheng. Sequential defense against random and intentional attacks in complex networks. *Phys. Rev. E*, 91:022805, February 2015.

[11] Pin-Yu Chen, Shin-Ming Cheng, and Kwang-Cheng Chen. Information fusion to defend intentional attack in internet of things. *IEEE IoT-J.*, 1(4):337–348, August 2014.

[12] Pin-Yu Chen, Shin-Ming Cheng, and Kwang-Cheng Chen. Optimal control of epidemic information dissemination over networks. *IEEE Trans. Cybern.*, 44(12):2316–2328, December 2014.

[13] Pin-Yu Chen and Alfred O. Hero. Node removal vulnerability of the largest component of a network. In *Proceedings of IEEE GlobalSIP*, 2013.

[14] Pin-Yu Chen and Alfred O. Hero. Assessing and safeguarding network resilience to nodal attacks. *IEEE Commun. Mag.*, 52(11):138–143, November 2014.

[15] Pin-Yu Chen and Alfred O. Hero. Local Fiedler vector centrality for detection of deep and overlapping communities in networks. In *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pages 1120–1124, 2014.

[16] Pin-Yu Chen, Han-Feng Lin, Ko-Hsuan Hsu, and Shin-Ming Cheng. Modeling dynamics of malware with incubation period from the view of individual. In *79th IEEE Vehicular Technology Conference (VTC Spring)*, pages 1–5, May 2014.

[17] Shin-Ming Cheng, Weng Chon Ao, Pin-Yu Chen, and Kwang-Cheng Chen. On modeling malware propagation in generalized social networks. *IEEE Commun. Lett.*, 15(1):25–27, January 2011.

[18] Shin-Ming Cheng, Pin-Yu Chen, and Kwang-Cheng Chen. Ecology of cognitive radio ad hoc networks. *IEEE Commun. Lett.*, 15(7):764–766, July 2011.

[19] Shin-Ming Cheng, Vasileios Karyotis, Pin-Yu Chen, Kwang-Cheng Chen, and Symeon Papavassiliou. Diffusion models for information dissemination dynamics in wireless complex communication networks. *Journal of Complex Systems*, Article ID 972352, 2013.

[20] Martin Everett and Stephen P. Borgatti. Ego network betweenness. *Social Networks*, 27(1):31–38, 2005.

[21] Miroslav Fiedler. Algebraic connectivity of graphs. *Czech. Math. J.*, 23(98): 298–305, 1973.

[22] Linton C. Freeman. A set of measures of centrality based on betweenness. *Sociometry*, 40:35–41, 1977.

[23] Simon Knight, Hung X. Nguyen, Nickolas Falkner, Rhys Bowden, and Matthew Roughan. The Internet topology zoo. *IEEE J. Sel. Areas Commun.*, 29(9):1765–1775, October 2011.

[24] Martin Osborne and Ariel Rubinstein. *A Course in Game Theory*. MIT, Cambridge, MA, 1999.

[25] Gert Sabidussi. The centrality index of a graph. *Psychometrika*, 31(4): 581–603, 1966.

[26] Ricard V. Solé, MartíRosas-Casals, Bernat Corominas-Murtra, and Sergi Valverde. Robustness of the European power grids under intentional attack. *Phys. Rev. E*, 77:026102, February 2008.

[27] Pramod K. Varshney. *Distributed Detection and Data Fusion*. Springer, New York, 1996.

[28] Shi Xiao, Gaoxi Xiao, and Tee Hiang Cheng. Tolerance of intentional attacks in complex communication networks. *IEEE Commun. Mag.*, 45(1): 146–152, February 2008.

Chapter 3

Sybil Attack Detection in Vehicular Networks

Bharat Jayaraman

Jinesh M. Kannimoola

Krishnashree Achuthan

CONTENTS

In this chapter, we consider safety issues arising in vehicular ad hoc networks (VANETs) (Figure 3.1). Although vehicular networks originated in the infotainment domain, today they are also used in many safety-critical systems such as in an emergency vehicle grid. Due to the open nature of vehicular networks,

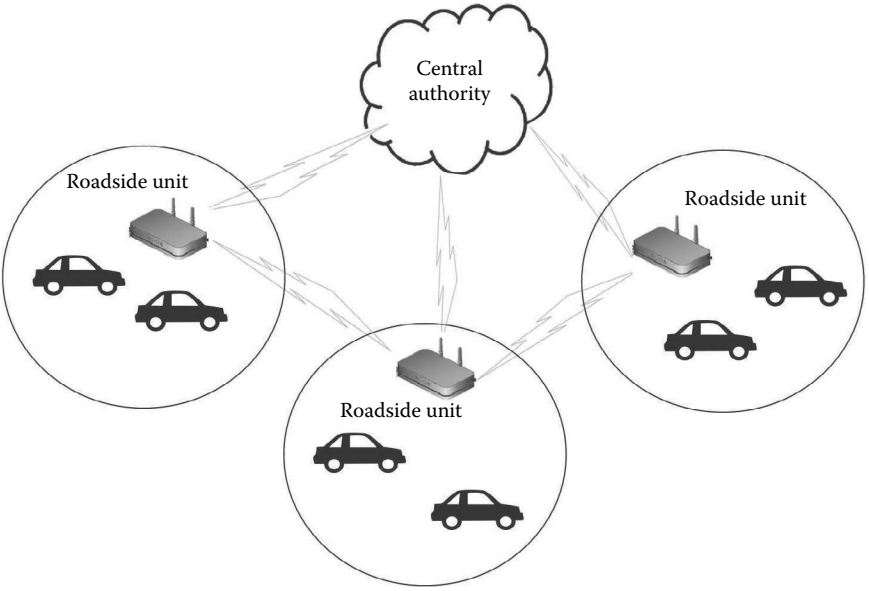

Figure 3.1: Architecture of vehicular ad hoc network

they are more amenable to malicious attacks; and, due to their high mobility and dynamic topology, the detection and prevention of such attacks is also more difficult. We consider one such attack in this chapter, the Sybil attack, in which an attacker tries to violate the unique vehicular ID property by forging or fabricating it and presenting multiple identities. A Sybil attack is a serious threat because it can result in large-scale denial of service or other security risks in the network. This chapter presents a new method to prevent Sybil attacks in a vehicular network based on the traditional cryptographic techniques, as well as the unique features of the network. A key feature of the methodology is the use of fixed roadside units and a central authority. This chapter presents a formal model of the system using the Promela language and shows how the safety property can be verified using the SPIN model checker.

3.1 Introduction

The automobile today has evolved from a complex electromechanical system to a "computer system on wheels" and vehicular networks are pushing the frontier

of the internet of things (IoT) to include the large class of highly mobile entities; namely, vehicles. With the inclusion of vehicles and communication between vehicles, as well as between vehicles and the infrastructure, the "internet of vehicles" can potentially provide real-time connectivity between vehicles around the globe. By further providing connectivity with entities such as traffic lights and RFID devices, we move closer toward the goal of a safe and efficient traffic environment. A vehicle has potentially has more storage, communication, and computing capacity compared to other embedded and mobile devices, and hence, vehicular networks can act as core infrastructure to connect various things.

The vehicular ad hoc network (VANET) facilitates communication between vehicles in the network by sharing road conditions and safety information. The network is especially useful in dense urban regions in promoting greater road safety and efficient traffic control. In contrast with a mobile ad hoc network, a vehicular ad hoc network has a highly dynamic network topology owing to the rapid movement of vehicles, with frequent disconnections in the network and more resource constraints [13]. It uses a combination of networking technologies such as Wi-Fi IEEE 802.11p, WAVE IEEE 1609, WiMAX IEEE 802.16, Bluetooth, IRA, and ZigBee.

There are two types of communication in a vehicular network: (i) vehicle-to-vehicle and (ii) vehicle-to-network-infrastructure. The open nature of VANET communication makes it much more amenable to malicious attacks [11, 18], and the dynamic nature of vehicular movement makes it difficult to protect against these. In this chapter, we consider one such attack, the Sybil attack, in which a single entity can gain control over a substantial fraction of the system by presenting multiple identities [4]. There are mainly two types of Sybil attacks: (i) a single node presents multiple identities; and (ii) a Sybil node uses the identity of another node. Sybil attacks violate the fundamental assumption of one-to-one correspondence of a node with its identity. There are several adverse effects that result from a Sybil attack in a VANET environment [1, 14]:

- Routing: The Sybil attack affects the performance of geographical routing and leads to large-scale denial of service.

- Tampering with voting and reputation systems: Reputation and trust management system crucially depend upon the unique ID and authenticity of the node. A Sybil attack violates this assumption and results in erroneous computation of reputation values.

- Fair resource allocation: A node with multiple identities can exploit the network to its advantage by using more bandwidth and network time.

- Data aggregation: Wireless sensor networks typically aggregate the values from sensor nodes rather than sending individual values. A Sybil node can manipulate these values, resulting in misleading aggregate values.

Our motivation in this chapter is to present an effective approach for Sybil attack detection in the setting a highly dynamic vehicular ad hoc network. Basically, a Sybil attack can be prevented by using public key certificates issued by a central authority (CA) [4]. Such an approach is not scalable because the CA can become a bottleneck in communication. Although methods have been proposed to prevent a Sybil attack in a VANET [2, 10, 15], they fail to capture the dynamic characteristics of the network. Our method makes use of the roadside unit (RSU) along with a cryptographic certificate scheme with position verification to capture the dynamic context of a vehicle in the network. Essentially, in our approach, the RSU acts as an authority to verify the authenticity of a vehicle node by using the information in nearby RSUs. The idea is that an RSU can contact nearby RSUs more quickly compared with the CA.

Thus, the contribution of our work is an effective detection mechanism for Sybil attacks, using a semicentralized approach, by taking advantage of the presence of RSUs in addition to the CA. Essentially, we distribute the function performed by the CA through the RSUs to capture the dynamic nature of the network. A real vehicular network typically contains thousands of vehicular nodes and hundreds of RSUs. Before deploying the system in a real environment, it is desirable to model the key aspects of the technique at an abstract level and check the correctness of the proposed protocol. We therefore develop a formal model of our approach and verify its key properties using a model-checking approach [3], since it supports reasoning over all possible paths of execution.

We develop a specification of the vehicular network using Promela (Process Meta Language) and check its correctness using the open-source model checker SPIN (Simple Promela Interpreter) [6]. Vehicles, RSUs, and the CA are modeled as Promela processes, and the communication between them is represented by Promela channels. Promela supports the dynamic creation of processes as well as channels, the latter being a crucial capability for modeling the mobility of vehicles from one RSU to another. Attack detection is also modeled as a process that continuously observes the network for any violation of the key system properties, including the property that only one vehicle uses a given ID for communication.

The remainder of this chapter is organized as follows: Section 2 presents closely related approaches for Sybil attack detection and their limitations; Section 3 presents the overall design of our Sybil attack detection method; Section 4 gives a formal specification and verification of our method using Promela/SPIN; and Section 5 presents conclusions and areas of further work. The full Promela model is given in the appendices.