Intrusion Detection in Wireless Ad-Hoc Networks

Edited by
Nabendu Chaki • Rituparna Chaki
# Contents

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preface</td>
<td></td>
<td>ix</td>
</tr>
<tr>
<td>About the Editors</td>
<td></td>
<td>xi</td>
</tr>
<tr>
<td>Contributors</td>
<td></td>
<td>xiii</td>
</tr>
<tr>
<td><strong>Chapter 1</strong></td>
<td><strong>Introduction</strong></td>
<td>1</td>
</tr>
<tr>
<td>NOVARUN DEB, MANALI CHAKRABORTY, AND NABENDU CHAKI</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Chapter 2</strong></td>
<td><strong>Architecture and Organization Issues</strong></td>
<td>43</td>
</tr>
<tr>
<td>MANALI CHAKRABORTY, NOVARUN DEB, DEBDUTTA BARMAN ROY, AND RITUPARNA CHAKI</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Chapter 3</strong></td>
<td><strong>Routing for Ad-Hoc Networks</strong></td>
<td>73</td>
</tr>
<tr>
<td>DEBDUTTA BARMAN ROY AND RITUPARNA CHAKI</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Chapter 4</strong></td>
<td><strong>Different Types of Attacks for WANs</strong></td>
<td>95</td>
</tr>
<tr>
<td>DEBDUTTA BARMAN ROY AND RITUPARNA CHAKI</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Chapter 5</strong></td>
<td><strong>Honesty and Trust-Based IDS Solutions</strong></td>
<td>111</td>
</tr>
<tr>
<td>NOVARUN DEB, MANALI CHAKRABORTY, AND NABENDU CHAKI</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Chapter 6</strong></td>
<td><strong>Blackhole Attack Detection Technique</strong></td>
<td>147</td>
</tr>
<tr>
<td>DEBDUTTA BARMAN ROY AND RITUPARNA CHAKI</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
VIII

CONTENTS

Chapter 7  Intrusion Detection for Wireless Mesh Networks  171
NOVARUN DEB, MANALI CHAKRABORTY, AND NABENDU CHAKI

Chapter 8  Future Trends in WAN Security  201
TAPALINA BHATTASALI, MANALI CHAKRABORTY, AND NABENDU CHAKI

Index  231
Preface

It’s a great pleasure to introduce this book on intrusion detection systems (IDSs) for wireless ad-hoc networks. The book aims to ease the job of future researchers working in the field of network security.

This book covers the security aspects for all the basic categories of wireless ad-hoc networks and related application areas, with a focus on IDSs. The categories included are mobile ad-hoc networks (MANETs), wireless mesh networks (WMNs), and wireless sensor networks (WSNs). In the book’s eight chapters, the state-of-the-art IDSs for these variants of wireless ad-hoc networks have been reviewed and analyzed. The book also presents advanced topics, such as security in the smart power grid, securing cloud services, and energy-efficient IDSs.

It has been organized in the form of an edited volume with eight chapters, each coauthored by one or more of our senior research scholars and ourselves. We thank and appreciate Novarun Deb, Manali Chakraborty, Debdutta Barman Roy, and Tapalina Bhattasali not only for their chapter contributions, but also for their hard work and innovative suggestions in preparing the manuscript. We especially mention Novarun and Manali for going through the drafts of all the chapters again and again toward improving the quality and content. This has gone a long way toward making this a comprehensive research title in the area of intrusion detection for wireless ad-hoc networks.
We express our sincere thanks to Richard O’Hanley for his continual support and positive influence right from the point of offering us to work on a book on this topic. We are grateful to the publisher for extending us the opportunity to be CRC Press authors. It has been a nice experience to work with Stephanie Morkert and Judith Simon of Taylor & Francis Group during the project and its production process.

Lastly, we must mention and thank every member of our family for their support. We are lucky to have kids like Rikayan and little Nandini, who spared us and sacrificed their valuable time to let us concentrate on the book.

We are sure that all these sacrifices will turn into delight when this book helps budding scholars to explore the area of network security and inspires them to go beyond the covers of this book to craft even better contributions.

Nabendu Chaki
Rituparna Chaki
Kolkata, India
About the Editors

Nabendu Chaki is a senior member of the Institute of Electrical and Electronics Engineers (IEEE) and an associate professor in the Department of Computer Science and Engineering, University of Calcutta, India. Besides editing several volumes for Springer in the Lecture Notes in Computer Science (LNCS) and other series, Nabendu has authored two textbooks and more than 100 refereed research papers in journals and international conferences. His areas of research interests include distributed systems and network security.

Dr. Chaki has also served as a research assistant professor in the Ph.D. program in software engineering in the U.S. Naval Postgraduate School, Monterey, California. He is a visiting faculty member for many universities, including the University of Ca’Foscari, Venice, Italy. Dr. Chaki is a knowledge area editor in mathematical foundation for the SWEBOK project of the IEEE Computer Society. In addition to being on the editorial board for Springer Verlag and many international journals, he has also served on the committees of more than 50 international conferences.
Rituparna Chaki has been an associate professor in the A.K. Choudhury School of Information Technology, University of Calcutta, India, since June 2013. She joined academia as a faculty member at the West Bengal University of Technology in 2005. Before that, she served under the government of India in maintaining its industrial production database.

Rituparna completed her Ph.D. from Jadavpur University in 2002. She has been associated with organizing many conferences in India and abroad as program chair, organizing chair, or member of the Technical Program Committee. She has published more than 60 research papers in reputed journals and peer-reviewed conference proceedings. Her research interest is primarily in ad-hoc networking and its security. She is a professional member of IEEE and ACM.
8

FUTURE TRENDS IN WAN SECURITY

TAPALINA BHATTASALI, MANALI CHAKRABORTY, AND NABENDU CHAKI

Contents

8.2 Securing Cloud Services in Wireless Ad-Hoc Network 204
  8.2.1 Attacks on Cloud Computing Systems 206
  8.2.2 An Architecture for Secured Cloud Service 209
8.3 Smart Grid Security in Wireless Ad-Hoc Networks 210
  8.3.1 Security in Smart Grid 211
  8.3.2 Some Possible Threats for Smart Grid Network 215
  8.3.3 Research Challenges 215
    8.3.3.1 Smart Meter Security 215
    8.3.3.2 Home Area Network Security 216
    8.3.3.3 PCS Security 216
    8.3.3.4 Security in Distribution Systems 217
    8.3.3.5 Cyber Security in Transmission Network 217
    8.3.3.6 Smart Grid Communication Protocol Security 217
  8.3.4 Conclusion 218
8.4 Energy-Efficient Intrusion Detection in WAN 218
  8.4.1 Energy-Efficient Hybrid Intrusion Detection System (EEHIDS) 221
  8.4.2 Intrusion Detection in WAN 223
  8.4.3 Performance Comparison 226
8.5 Summary 227
References 227

This chapter focuses on the future trends in wireless ad-hoc network (WAN) security. It is sometimes very useful to predict the future to get new ideas and visualize the present in a more appropriate context. Future trends are the consequence of today’s activities. There are many open issues related to the future of wireless ad-hoc networks. A scenario of completely unrestricted “anytime, anywhere” communications using this technology seems to be inevitable in the nearest future. Wireless networking can be very well suited for the next-generation communications. Wireless ad-hoc networks have the potential to change how the communication world is seen. One of the major concerns today is the aggressive marketing policies of corporations. The industrial houses are perpetually in the rat race of claiming edges over each other. This remains their prime interest, and the big companies are just fascinated to see themselves the winner at the cost of almost anything. Quite often this thrust of staging eye-catching marketing stunts and promising more flexible and powerful user applications prompts them to market technologies in premature states. Security-related problems are unavoidable in such a scenario where technology is not thoroughly tested and critically analyzed.

Section 8.1 gives a brief overview of future trends in WAN security. Section 8.2 presents the idea of secure cloud services in the wireless ad-hoc network environment. It briefly describes a security architecture of cloud services on WAN to solve the problems associated with an integrated cloud-WAN environment. Section 8.3 includes ideas about secure smart grid architecture in a limited-energy wireless ad-hoc environment. Section 8.4 presents an idea about energy-efficient intrusion detection in WAN having a high probability of being compromised. Finally, Section 8.5 concludes the chapter.

In the next generation of the network, technology needs to be adapted to support the increase in network traffic being driven by an alarming number of devices and enhanced demand of huge bandwidth for big data. It has been seen that the total number of devices grew from 500 million to 1.2 billion in 2012 [26]. There is still space for improvements since the performance of WAN is typically poor compared to that of other wireless technologies. In the field of wireless ad-hoc networks, new application areas are emerging, such as cloud
services, smart grid applications, energy-efficient applications, vehicular ad-hoc networks (VANETs), etc. VANET is based on ad-hoc connections between vehicles to improve safety in transport. With the advent of novel applications, it is expected that VANET will be widely adopted to provide a set of services that can also be used for critical applications efficiently. Sensor network area is also related to ad-hoc networks that move toward the future generation of Internet of Things applications. The wireless mesh network (WMN) is also a related area in this domain.

This chapter focuses mainly on securing cloud services and smart grid architecture on WAN. Another considerable issue is energy-efficient computation in this type of network. The real challenge lies in finding the solutions to handle high volumes of data securely while maintaining quality-of-service requirements. An optimized solution of future WANs can control the Internet to reshape the way we use critical applications. To achieve greater efficiency, we require solutions for network traffic from limited-resource devices, cloud services, new types of IPv6 content, etc. An additional burden is placed on WAN in terms of increased demand for security.

In order to manage network security effectively, one should gain full visibility into how network capacity is being used by the applications. Besides understanding what type of traffic is flowing through the network, bandwidth usage per application should also be measured. The most critical question is how to improve performance without investing in new network infrastructure or upgrading bandwidth. Cloud service has a profound impact in this regard. As more applications are deployed through cloud services, it is more efficient from the cost and latency perspective. This concept reduces network costs and improves performance. The privacy and security challenges are also increasing day by day, which include concern about trust establishment, secure transmission, protecting data privacy, ensuring data integrity, identifying the most dangerous attacks, and designing solutions of intrusion detection.

Smart grid technology also places greater demands for reliability on WAN communications [3]. This will allow prioritized communication—high priority for abnormal events and system control operations and low priority for asset management tasks. Connectivity protection and its data confidentiality in smart grid applications in the WAN.
environment are critical. In this scenario, having a fast and real-time reaction upon an abnormal event is vital. The wireless architecture should aim for high-priority, low-latency alerts when abnormality occurs. In a smart grid almost all the nodes are fixed, so the communication architecture does not consider node mobility explicitly. In this environment, high overhead is created by multiple nodes trying to send the same information and excessive use of control packets. This reduces available bandwidth for data traffic, and can also result in higher latencies for critical alert packets. Therefore, it is necessary to ensure that overhead be kept low.

8.2 Securing Cloud Services in Wireless Ad-Hoc Network

In the last section, a brief overview of the future trends in WAN security was given. A detailed account on securing cloud services on WAN is presented in this section. The boundary between the physical world and the digital world has been dissolved due to advances in the areas of ubiquitous computing. WAN collects data about the physical environment. However, collected data cannot be processed over long periods of time due to lack of storage capacity. In WAN, all the nodes and topology are unstable due to the fact that there is no decentralized location where all the shared information can be stored with knowledge of the network resource. This will also lead to a great challenge in the quality of service (QoS) of this type of network. Cloud computing provides an alternative for data storage and computation. Ubiquitous ad-hoc environments and cloud computing complement each other. Cloud service is used to provide resources in on-demand environments. It makes response time faster and cost lower. The U.S. National Institute of Standards and Technology (NIST) [25] defined cloud computing this way: “Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.”

Because of the distributed nature, achieving security for cloud environments is consistently raised as a major concern. In the current scenario, where cyber attacks and data leakage incidents are increasing, it must be ensured that data assets are well protected when they
are kept in the hands of a third party. The data stored in the cloud are accessed a large number of times and are often subject to different types of changes. This may comprise bank accounts, passwords, and highly confidential files not to be read by someone other than the owner. Hence, even a small slip may result in loss of data security. Cloud security mainly deals with identity management, encryption, intrusion detection, forensics issues, and risk assessment, along with the responsibility for deciding how and where data are stored and accessed in the cloud. It has been identified that most of the potential risks include malware, data leakage or breach, denial-of-service (DoS) attacks, etc. Figure 8.1 represents the basic threat model in a cloud environment. It mainly categorizes the attacks as denial-of-service attacks, client-side attacks, data leakage, violation of access, application vulnerabilities, physical breaches, data separation, virtual platform attacks, and data storage attacks on the cloud environment that includes infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), software-as-a-service (SaaS).

In order to secure the cloud, security options must be analyzed to make sure data protection is in the right place. Therefore, focus must be on how to balance cloud computing security risks with the convenience in WAN. Before uploading data to a cloud from any of the wireless hosts, security policies need to be included. The information in the cloud database will be used to detect vulnerabilities in the data sent from wireless nodes. This will be done in real time, to ensure...
that information is delivered in a secure manner, when it is needed. A secure cloud service architecture on WAN is presented next to minimize the problems that arise in this scenario. Security issues and attacks in a cloud are different for different layers of the underlying networking infrastructure, such as network layer, application layer, or from the host level. Some of these attacks are listed below.

8.2.1 Attacks on Cloud Computing Systems

Chapter 4 presented a thorough discussion on the different types of attacks for computer networks. As any cloud architecture is built on underlying network connectivity, the common networking threats, like the man-in-the-middle attack or denial of services, are highly relevant for the cloud as well. In this section, we present a few common attacks, typical for the cloud domain:

*SQL injection attacks:* In this type of attack, a hacker can access a cloud database inserting a malicious code in the Structured Query Language (SQL) code for a standard query [17]. This not only allows the attacker to access sensitive data, but also may create confusion by inserting wrong data in the cloud database.

*Cross-site scripting (XSS) attacks:* With this attack, the intruder injects malicious scripts in web contents [18]. Static websites don’t suffer from the XSS attacks. Cross-site attacks are planned for the dynamic websites providing diverse and on-the-fly services to the users. There are two variants of this attack: stored XSS and reflected XSS. In a stored XSS, the attacker stores the malicious code in a resource managed by the web application. The actual attack is triggered at a stage when the victim requests a dynamic page that is constructed from the contents of this resource. However, in case of a reflected XSS, the attack script is not stored in the web application. Such an attack is immediately reflected back to the user.

*Reused IP address attack:* This is a typical network attack. We know that each node of a network is provided an IP address that has a specific range, depending on the type of network. This attack is somewhat analogous to a situation with two
successive bank ATM users, when the second user finds that although the previous user has left, his session is still in use. From the user’s perspective a major difference is that in the case of an ATM user, the security of the first ATM user is at stake. In the reused IP address attack in a network, the privacy of the second user may be compromised.

When a particular user A moves out of a network, then the IP address so far associated with A is assigned to a new user, say B. This sometimes risks the security of the new user, as there is a certain time lag between the change of an IP address in the Domain Name System (DNS) and the clearing of that address in DNS caches [19]. Hence, it may be said that sometimes, though the old IP address is being assigned to a new user, the chances of accessing the data by the old user exists. This is because the address still exists in the DNS cache and the data belonging to B may become accessible to A, violating the privacy of B.

**Sniffer attacks:** Sniffing refers to unauthorized reading of data packets flowing in a network that are not encrypted. Thus, an attacker can capture vital information flowing across the network. A sniffer program works in the promiscuous mode to track all data flowing in the network [20].

**Google hacking:** Google hacking refers to using the Google search engine to find sensitive information that a hacker can use to his benefit toward hacking a user’s account. The hackers find the security loopholes of a cloud infrastructure or a cloud-based system using Google. The attacker may even use Google to find the target with the loopholes and containing the right kind of data or service that is being targeted. After gathering the necessary information, the system is hacked. In a well-known Google hacking event of the recent past, the login details of various gmail users were stolen by a group of hackers [21].

**Account hijacking:** This is one of the most serious threats for any commercial cloud service provider. According to cloud security alliance (CSA) [22], account and service hijacking often occur using credentials stolen from genuine users. With
stolen credentials, attackers can often access critical areas of deployed cloud computing services, allowing them to compromise the confidentiality, integrity, and availability of those services.

*Abuse of cloud services:* More and more paid and unpaid services are being deployed using cloud. Very important government to citizen (G2C) services are increasingly being deployed as cloud services. Hackers are taking advantage of these and often use the immanence power of cloud computing to hack other services. This is abuse of existing cloud services. The impact of such an attack goes far beyond the Google hacking discussed above.

*CAPTCHA breaking:* Internet users are often asked to enter some text displayed in a box where characters are oriented in all possible angels. These are CAPTCHAs. Free mail services like Google, Yahoo, and a large number of other websites use CAPTCHA to prevent usage of internet resources by robots or computers. Even the multiple website registrations, dictionary attacks, etc., by an automated program are prevented by using a CAPTCHA.

However, recently it has been found that spammers are able to break the CAPTCHA [23] provided by popular free mail service providers. Various techniques, such as implementing letter overlap, using variable fonts, increasing the string length, and using a background, are being tried to secure CAPTCHAs [24].

Because it is known to all that integrated WAN-cloud communication imposes hard real-time requirements, this architecture must not introduce long delays. To investigate service delay, cloud should collect node and WAN status information and predict appropriate actions to be taken; cloud should serve as a server, i.e., assisting a mobile node to establish trust with another node controlled in different domains; and cloud should emulate the actions of the network for post-event analysis. From the above discussion, it has been seen that cloud service has great potential to bring more application scenarios securely on wireless ad-hoc networks.
8.2.2 An Architecture for Secured Cloud Service

Figure 8.2 shows the conceptual infrastructure to secure cloud services in WAN [2]. This is basically designed to secure data access policy management for protecting users’ data, to monitor WAN status for risk assessments, to detect intrusion and respond accordingly, and to simulate and predict future WAN status for decision making. This also provides trust management and feedback capability to the users. Trust management includes identity management, key management, efficient data access control, risk assessment, etc., to provide security as a service (SeaaS), which can offer security service according to the request from different applications.

This model mainly depends on several components, such as virtual trusted and provisioning domain (VTaPD), software agents (SAs), programmable router, node manager (NM), resource and application manager (RAM), and trust manager server (TMS). VTaPD service is used to isolate information flows from different security domains through programmable routers. Software agents are used to link the cloud services and wireless devices. Each device can have multiple SAs for different services, which are managed by the application manager of the device. The application interface provides interfaces to the VTaPD manager and RAM, which constructs VTaPDs according to
the direction of the VTaPD manager and TMS. The VTaPD manager collects context awareness information and uses it for intrusion detection and risk management. TMS acts as trust authority, which handles attribute-based key distribution and revocation. It provides an identity search for devices belonging to multiple domains and policy checking to provide a unified trust management system. This framework considers time synchronization service on wireless devices and virtual routing domain to emulate the routing behaviors of the WAN and communicate the decisions to the nodes. This integrated framework of secure cloud services in WAN will reduce the uncertainty by functioning as information storage. But there are several issues that need to be addressed in the near future. The first issue is whether this framework can protect users’ data, even if the devices are compromised. To develop an efficient many-to-many secure group communication system, a fine-grained data access control mechanism \( \mu \)VTaPD needs to be constructed, where \( \mu \) is used to specify different types of constraints. The next issue is how to construct and delete \( \mu \)VTaPD.

8.3 Smart Grid Security in Wireless Ad-Hoc Networks

The conventional electrical power grid that has been used for decades has met our needs in the past. However, as our society advances technologically, so do the expectations from various infrastructures surrounding us. Smart grid is an initiative to completely restructure the electrical power grid to meet the current and future requirements of its customers. Updating our electrical power grid could introduce new security vulnerabilities into the system. Therefore, security is one of the important aspects in smart grid technology.

A smart grid is an intelligent electricity network that integrates the actions of all users connected to it and makes use of advanced information, control, and communication technologies to save energy, reduce cost, and increase reliability and transparency. The easiest way to define the smart grid is by its characteristics. The smart grid is an upgrade to the current electrical power system, so it has all of the functionality of our current power system plus several new functionalities. These new functionalities cause more vulnerability to the system [33].

Smart grid is mainly composed of six basic systems: power generation system, distribution system, transmission network, data
management and processing system, smart metering system, and customer information system. The network architecture of smart grid hierarchically consists of three components: home area network (HAN), neighborhood area network (NAN), and wide area network (WAN) [44], as shown in Figure 8.3. The HAN provides the communication between the smart meters in a home and other appliances in that home, while the NAN connects smart meters to the local data management and processing centers, and WAN provides access between the generation plants, distribution points, and transmission networks. The generation system, distribution points, and transmission networks build the core utility system of a smart grid.

Like the characteristics of each tier network, different wireless communication techniques can be adapted, i.e., WiFi or Zigbee for HAN in indoor small areas, WiMAX or WiFi for NAN with wireless mesh topology, and WiMAX, 4G, or cognitive radio for WAN [44, 45].

8.3.1 Security in Smart Grid

As smart grid technology is different from normal power grid technology, the security challenges in smart grid are also different from normal power grid technology. Beyond the application of traditional information technology (IT) security mechanisms, such as proper authentication, secure protocols, intrusion detection/response systems, and proper security engineering processes, security in the smart grid also faces novel challenges. Thus, the existing security solutions need to be upgraded, and also some new security solutions are needed.
for securing smart grid technology. This requires guaranteeing the stability of control systems that are also undergoing malicious disturbances [34, 35]. At the same time, IT security must take into account the real-time and analog nature of the grid and adapt risk management as graceful degradation (i.e., a slower, controlled, safe failure), as opposed to a sudden, disastrous failure when under attack.

A smart grid electric power system delivers electricity from producers to consumers using two-way smart meter technology that can remotely control consumer electricity use. This can help utilities conserve energy, reduce costs, increase reliability and transparency, and make processes more efficient. However, the increasing use of IT-based electric power systems increases cyber security vulnerabilities, and this increases the importance of cyber security. The main objective of providing security in smart grid is to maintain three important qualities in it: availability, integrity, and confidentiality.

Availability is the most important security objective. Smart grid is a critical real-time system and continuously monitors the state of the electrical power grid, and a disruption in communications can cause a loss of power. Thus, availability of the electrical power grid is its most important factor. By extension, the most important security object of most of the electrical power system components is also availability [33].

Integrity is the next important security objective in the smart grid. The smart grid uses data collected by various sensors and agents. These data are used to monitor the current state of the electrical power system. The integrity of these data is very important. Unauthorized modification of the data, or insertion of data from unknown sources, can cause failures or damage in the electrical power system.

The final security objective is confidentiality. There are certain areas in the smart grid where confidentiality is more important. Examples include the privacy of customer information, general corporation information, and electric market information.

Security of the smart grid can be divided into three categories: physical security, data security, and cyber security [39]. Physical security relates to protection of the smart grid’s physical infrastructure, including advanced meter interface (AMI) hardware, such as smart meters, transmission lines, generating equipment, and control rooms, from damage. Such damage can be the result of intentional attacks using electromagnetic pulses or other weapons, or unintentional as...
the result of damage from electric storms. Data security refers to the privacy of the information that is transferred over the smart grid; it relates to customer information such as personal details, financial information, and energy usage patterns that can be misappropriated by hackers to do damage to individuals. Cyber security relates to the vulnerability of the grid to intentional infiltration by hackers using the Internet or other digital information management systems with the intention of disrupting the normal operation of the power delivery system.

The backbone of the smart grid will be its network. This network will connect the different components of the smart grid together, and allow two-way communication between them. Networking the components together will introduce security risks into the system. Two-way communication has the potential to create a new avenue for cyber attacks to reach the bulk power system and cause serious damage to this critical infrastructure by way of a customer’s smart meters and other grid-connected smart technology. An attacker who gained access to the communication channels could order metering devices to disconnect customers, order previously shed loads to come back online prematurely, or order dispersed generation sources to turn off during periods when a load is approaching generation capacity, causing instability and outages on the bulk power system. Thus, to prevent these kinds of attacks, we need to secure the routing protocols in smart grid networks and also implement some robust intrusion detection system for a second line of defense [37].

Also, the smart meters are one of the weakest links in the smart grid security chain. Smart meters may be used by hackers as entry points into the broader power system. Hackers could hack into smart meters to take command and control of the advanced metering infrastructure, allowing a mass manipulation of services to homes and businesses [36, 41].

Cyber security must address not only deliberate attacks launched by disgruntled employees, agents of industrial espionage, and terrorists, but also inadvertent compromises of the information infrastructure due to user errors, equipment failures, and natural disasters. Vulnerabilities might allow an attacker to penetrate a network, gain access to control software, and alter load conditions to destabilize the grid in unpredictable ways [42].
However, already there exist a lot of secure routing protocols and intrusion detection systems for ad-hoc networks. Then why do we need some extra effort to secure the smart grid? The answer is because of the unique characteristics of smart grid technology, which differ from those of both traditional power grid systems and traditional ad-hoc networks.

We can also imagine the smart grid network as an ad-hoc network. Then it also implies that the existing security solutions for an ad-hoc network can be used for providing security in smart grid. However, there are some problems.

First, the nature of the network of smart grid is extremely large. For instance, it could be the case where 100,000 nodes (meters) generate meter traffic data every 10 min. And then this huge amount of data is analyzed to generate bills and to monitor the whole network. As a result, we have to incorporate scalability and reliability in the existing solutions so that this data can be delivered to the central utility control safely and in a timely manner [39].

Second, the traffic in a smart grid network will be traversing different types of networks, using a variety of media, ranging from fiber optics/broadband (e.g., for meters to base control center networking) to Zigbee/wireless local area network (WLAN) (e.g., for home networking). So interoperability is another key issue. It can be envisaged that in a complex system such as smart grid, heterogeneous communication technologies are required to meet the diverse needs of the system. Therefore, in contrast to conventional security solutions, the standardization of communications for smart grid means making interfaces, messages, and workflows interoperable. Thus, we can construct a totally new architecture for this kind of network, or we can combine different architectures for different layers, and build some interfaces to connect them with each other, so that they can communicate within themselves [36].

Besides, the traffic that will be generated by e-energy type applications in smart grid will likely be quite different from the traditional browsing/downloading/streaming applications that are in use today, with a mix of both real-time and non-real-time traffic being generated and distributed across different parts of a smart grid. Thus, the traditional security solutions may need to be revisited. The existing
routing policies will also need to be changed to route real-time and non-real-time data simultaneously, with improved QoS [43].

8.3.2 Some Possible Threats for Smart Grid Network

There are some basic security threats [45] for the smart grid network:

- Bill manipulation/energy theft: An attack initiated by a consumer with the goal of manipulating billing information to obtain free energy.
- Unauthorized access from the customer endpoint: Compromising smart meters and other customer end devices to gain unauthorized access to the network.
- Interference with utility telecommunication: Unauthorized access to the core utility system, i.e., generation, distribution, and transmission system, causing mass power disruption.
- Mass load manipulation: Unauthorized access to distribution points and transmission networks, causing havoc in load manipulation.
- Denial of service: Jamming the network channels, requesting false demands, causing denial of service, etc.

8.3.3 Research Challenges

The smart grid is a large and complex system. Because of this complexity, research work typically only focuses on a single component. The different categories are listed below [33, 40, 46]:

- Security in smart meters
- Home area network security
- PCS security
- Security in distribution systems
- Cyber security in transmission network
- Smart grid communication protocol security

8.3.3.1 Smart Meter Security  Smart metering is considered the first point where smart grid begins. The primary mission of a meter is to monitor power consumption. Smart meters are an electronic version
of the power meters that are currently used. The electrical power readings are sent back to the power suppliers at regular intervals [41].

The security of smart meters is important because altered readings from the device can lead to incorrect billing and false power usage approximations. Altering smart meters can provide attackers with monetary gains, and since the device is installed at a customer’s site, access to these devices is readily available.

8.3.3.2 Home Area Network Security The home area network (HAN) [46] is where the smart grid connects with the consumer. It is the part inside the home or place of business, and it is the part over which a utility or other service provider has the least control.

HAN security is clearly an important approach because the use cases and architectures are still new and evolving. Without understanding the architecture and the type of security vulnerabilities, it is difficult to build security systems. Additionally, the HAN security solution must take into account the scalability factor of the network and also the cost of implementation, because every home and business organization would potentially use the solution.

8.3.3.3 PCS Security Process control systems (PCSs) are the components responsible for monitoring and controlling physical properties of the electrical power grid. The PCSs in smart grid will be monitoring large geographical areas of the power grid. This means that there will be many entry points to get into the network. PCSs used in the smart grid will need to address these security issues.

There already exist some works addressing different issues, like smart meter intrusion detection systems (IDSs), redundant readings, and privacy. But they are not sufficient. The IDSs are generally signature based, so they cannot detect new attacks. One method to verify the accuracy of smart meters is to install a separate electrical energy measuring device that compares its reads to the readings that the power supplier received from the smart meter. The problem with this approach is that it introduces confidentiality risks. Attackers can intercept the data used to verify the integrity of the smart meter. So we need to use some kind of encryption system to secure smart meters.
8.3.3.4 Security in Distribution Systems  The primary goal of a distribution system is to improve power delivery system reliability, performance, and quality. The present distribution networks have many visible single points of failures, making service disruption due to cyber or physical attack a serious risk [46].

With smart grid distribution systems, outages are identified and located in real time. This allows rapid deployment of the resources to the right location to resolve problems. Distributed generation, automated switching, and self-healing capabilities are used for better functionalities. But this also makes the distribution system vulnerable to many security threats.

8.3.3.5 Cyber Security in Transmission Network  The power grid connects power through a series of substations. The totality of this represents the transmission network that is used to transmit power. To secure a transmission network, the following qualities have to be maintained [46]:

Self-healing: This will ensure that when transmission is affected, the system will automatically take corrective measures.
Power quality: If the power quality is high, then the transmission system can provide high-quality service. However, if it is low, then there might be a problem.
Energy storage: If generation is taken out, then other stored energy will be available.

8.3.3.6 Smart Grid Communication Protocol Security  The smart grid communication protocols are the next category of smart grid security research. The smart grid relies on communication between its different components in order to function. Each of the components has different communication requirements. The communication requirements range from very low latency to high data throughput, and each has a set of security needs [40].

The smart grid will need several communication protocols to meet the varying connection requirements. The security of smart grid communication protocols is important because the network communication is the backbone of the smart grid. Many of the major smart grid
functionalities cannot take place without communication. The security objectives that are important depend on which components are communicating, and what data they are exchanging.

Smart grid communication protocol security is a challenge because there are many different components communicating, each with their own set of communication requirements. Another issue is that the smart grid technology needs to integrate with legacy power systems, and many of these devices have constraints that must be considered. Legacy devices can typically introduce security vulnerabilities into the system because of a lack of security support.

8.3.4 Conclusion

Therefore, we can see that smart grid is a new frontier for communications and networking research. It poses many unique challenges and opportunities, e.g., interoperability, scalability, and security. The success of future smart grid depends heavily on the communication infrastructure, devices, security and enabling services, and software. Although there has been a lot of work toward the security in smart grid, some issues still need to be addressed. It is required that we build a secure architecture with a secured data analysis system that can sustain a certain level of physical and cyber attacks, besides maintaining the basic characteristics of smart grid, i.e., availability, integrity, and confidentiality.

8.4 Energy-Efficient Intrusion Detection in WAN

The previous section provides a basic idea about smart grid security in the context of WAN. A brief review of energy-efficient intrusion detection [8] in WAN has been presented here. Wireless networks are more vulnerable to attacks than wired networks. In this type of network, malicious nodes will be able to join the network at any time because of its infrastructure-less nature. Ad-hoc wireless networks with their changing topology and distributed nature are more prone to intrusions [15]. Therefore, a need to quickly detect and isolate malicious nodes or networks arises. Securely distributing information about malicious entities in the presence of an intruder is a big challenge. Avoiding malicious entities on top of maintaining connectivity
is another challenge. As the demand for wireless networks grows day by day, intrusion detection becomes of high importance [29]. Wireless ad-hoc networks are more vulnerable to intrusions from any direction. Each node in the network must be aware to deal with the intruders. It is difficult to track a single compromised node in a large network, because attacks from compromised nodes are much harder to detect. Ad-hoc networks may rely on cooperative participation [27] of the members within a decentralized architecture. Intruders can take advantage of this lack of centralized architecture to launch new types of attacks. It is known that building such ad-hoc networks poses significant technical challenges because of the many constraints imposed by the environment. As nodes are generally battery operated, they need to be energy conserving [9]. Therefore, any operation in this field must be lightweight to maximize battery life [30]. Several technologies are being developed to achieve the goal of optimized energy consumption, even in the case of intrusion detection.

Intrusion is defined as any set of actions that generally attempt to compromise availability, integrity, and confidentiality of a network resource. Since prevention techniques may not be sufficient and new intrusions continually emerge, IDS is a necessary component of a security system. An IDS is used to detect possible violations of a security policy by monitoring system activities. In order to identify either an outside intrusion or an inside intrusion [10], IDSs normally perform the following tasks: monitoring the network, analyzing collected data, identifying intruders, generating alarms, and tracking intruders to prevent such attacks in the future. These functionalities are encapsulated in several components, like data collector, data storage, data processor, and detection engine, all of which are controlled by the system configuration components.

It is known that intrusion detection methods are classified into three main techniques: anomaly based, misuse based, and specification based. An anomaly-based technique creates a profile of normal behaviors. It detects anomalies when recorded behavior deviates from normal behaviors. Misuse-based detection compares known attack signatures with current system activities. It is efficient and has a low false positive rate only for known attacks. Both anomaly-based and misuse-based approaches have their strengths and weaknesses. The specification-based technique is introduced as an alternative that

BUY Intrusion Detection in Wireless Ad-Hoc Networks
http://www.crcpress.com/product/isbn/9781466515659
combines the strengths of anomaly-based and misuse-based detection techniques, providing detection of known and unknown attacks with lower false positive rates.

Due to the decentralized nature of a wireless network, the main focus is on distributed solutions of intrusion detection for the network. Energy-aware design and evaluation of the intrusion detection system [28] for WAN require in-depth practical knowledge of energy consumption behavior of actual wireless devices. But very little practical information is available about the energy consumption behavior. Wireless devices normally operate for a long period of time, depending on their battery energy. Therefore, energy awareness is a major concern in wireless networking. To minimize energy consumption, one consideration should be to minimize the total energy needed for intrusion detection [5], and another consideration should be to look at the methods that extend the battery lifetime of the nodes. The energy consumption of the network interface can be significant, especially for smaller devices. It is sometimes assumed that bandwidth utilization and energy consumption are almost synonymous. In some cases, energy is often treated for purposes of minimizing cost or maximizing time to the network partition. Therefore, to design an energy-efficient intrusion detection system in WAN, issues like accuracy, energy consumption, and real-time response need to be considered.

Several intrusion detection systems have been proposed to deal with the problem of intrusion in wireless networks, some of which are extended versions of IDSs in wired networks. Energy awareness in wireless ad-hoc networks becomes a major issue when considering intrusion detection in larger networks. Monitoring intrusive activity normally occurs from either host-based IDSs or network-based IDSs. Beside this, hybrid intrusion detection systems incorporate multiple features into a single system. These are generally based on agents [11–13] who move throughout the network to provide an effective solution. Energy efficiency is one of the most important considerations in wireless devices due to the limitation of the battery life. Here an energy-efficient hybrid intrusion detection system (EEHIDS) is briefly discussed and compared with existing system power-aware agent-based intrusion detection (SPAID) [4] for performance evaluation.
8.4.1 Energy-Efficient Hybrid Intrusion Detection System (EEHIDS)

A hybrid agent-based intrusion detection system, EEHIDS is used to detect intrusion in an energy-efficient way [14], [16]. It is used to determine the duration for which a particular node can monitor network status. It focuses on the available energy level in each of the nodes to determine the nodes that can monitor the network. Energy awareness in the network results in maintaining energy for network monitoring by determining energy drainage of any node. The advantage of this approach is its inherent flexibility. Only fewer nodes are eligible for becoming candidates of network monitors. EEHIDS is built on an agent-based framework. It includes the following agents to perform its functions.

*Network monitor:* Only a limited number of nodes will have sensor agents for the network packet monitor. The main focus is to preserve the total computational energy and battery energy of hosts.

*Host monitor:* Every node on the network will be monitored internally by a host monitor agent. This includes both system level and application level monitoring.

*Decision maker:* Every node will decide the intrusion threat level. Certain nodes will collect intrusion-related data and make final decisions.

*Actor:* Every node will have an actor that is responsible for solving the intrusion status of a host.

There are three types of major agents categorized as monitor, decision maker, and actor agents. Some of them are present on all hosts, while others are distributed to only a selected group of nodes. In WAN, the elected network monitor nodes will include decision maker and actor modules. Functionalities must be distributed efficiently to save resources. Decision maker agents consider the energy metric, namely, network monitoring energy estimation (NeMEE). It is a node-specific metric to estimate energy consumption per node for running the network monitor agent. The NeMEE metric considers the average number of wireless links, used wireless protocol, remaining battery energy, etc. It can also estimate the duration the
node remains at the same energy level without refreshment. The calculation of the parameter NeMEE involves calculating the duration for which the node can continue as a network monitor, along with its normal operations. NeMEE is calculated as shown in Equation (8.1):

\[ \text{NeMEE'} = \frac{\text{TBER}}{\text{TEC}_{\text{mon}}} \]  

(8.1)

where TBER is the total battery energy remaining at the instant of node selection and TEC_{mon} is the total energy consumption with the network monitor node.

\[ \text{NeMEE'} = \frac{\text{TBER}}{\text{TEC}} \]  

(8.2)

In the absence of measurement for energy consumption of the network monitor, NeMEE is assumed as NeMEE'. The value of NeMEE' is directly available from most distributed wireless networks. TEC is the total energy consumption before the node is selected for network monitoring. Like SPAID, EEHIDS also considers a multihop network for selection of the network monitor within a cluster. The advantage of this type of node selection is that it allows complete coverage of all nodes and links in a network, but it creates redundancy in intrusion detection data collection. EEHIDS is an energy-efficient variation of SPAID. The EEHIDS approach considers each of the initially allocated monitors and the nodes they monitor to be a single tree. The network monitor node is treated as a root, and the nodes being monitored as its child. The root node and its child nodes form individual clusters. As a result, network topology gets divided into clusters in a tree-like fashion, only for intrusion detection purposes. After such cluster formation, when any drainage in energy levels takes place to the monitors, any other child node having higher battery energy is selected as a network monitor of that cluster. Only a limited number of clusters is kept active for a certain period of time. It is feasible that the monitor node gets rearranged within the cluster. The node selection process could be considered for the whole network only when no single node within a cluster has enough potential to monitor the network, or when a new node with a higher NeMEE value enters the existing network. In Figure 8.4, the EEHIDS algorithm is presented in brief.
EEHIDS Algorithm

Step 1: Set a constraint on the NeMEE value of nodes which are allowed to compete for becoming a network monitor node.

Step 2: Organize different nodes in increasing values of NeMEE, for all nodes that satisfy the NeMEE constraint.

Step 3: Initially set hop radius to 1 and increment for each insufficient node selection with the current hop radius.

Step 4: Consider node selection incrementally, starting from the first node having highest NeMEE value to the set of all nodes in the network by incrementing one node each time. This set is known as the working set (WoS) of nodes.

Step 5: Voting for network monitor node selection, considering the limitation that only WoS participants are eligible for being candidates.

Step 6: Check acceptability of nodes. If all are not represented by the set of selected nodes, then WoS is expanded and it is repeated from Step 4. If WoS equals the NeMEE ordered list, then increment the hop radius, and is repeated from Step 3.

Step 7: Create individual tree-structured clusters by considering nodes selected as network monitors as roots and nodes being monitored as child nodes.

Step 8: Changes in energy levels of the root nodes in each cluster will be informed to the child and voting takes place within the cluster to form a new monitor node.

Figure 8.4  Key steps of EEHIDS algorithm.

Steps 1 to 6 are similar to those in SPAID. The difference is that the steps of EEHIDS are also suitable for highly dynamic networks.

8.4.2 Intrusion Detection in WAN

Here, detection of intrusions in the network is done with the help of cellular automata (CA). It could classify a packet transmitted through the network as either normal or compromised. The use of CA is helpful in the identification of well-known intrusions as well as new intrusions.

Intrusion detection using an agent framework depends on both local response and global response. However, individual cells in CA can only communicate locally without the existence of a central control. The main idea behind using a cellular automata framework is
to understand how it is developed using genetic algorithms to perform computational tasks requiring global information processing. Therefore, this framework provides an appropriate approach for intrusion detection where dynamic systems are created to provide local information processing as well as coordinated global information processing.

To solve problems, localized structures are used by cellular automata. Genetic algorithms are normally used to identify populations of candidate hypotheses to a single global optimum [7]. For this reason, a set of rules needs to be considered for designing efficient IDSs. It is not possible to detect whether a network connection is normal or anomalous accurately by using only one rule. Multiple rules are required to detect unrelated anomalies. CA represent a generalized linear classifier looking for the maximum margin hyperplane between two classes in the feature space. The optimal position of the class boundary is obtained as a linear combination of some training samples that are placed near the boundary itself. The hyperplanes are defined by the following set of linear equations [7]:

$$w \cdot x + b = 0, \, w \in R^d, \, b \in R$$  \hspace{1cm} (8.3)

Each input $x$ is subject to the decision function $O(x)$, where

$$O(x) = \text{sign} (w \cdot x + b)$$  \hspace{1cm} (8.4)

Output, $y = +1$, if $w \cdot x + b \geq 1$  \hspace{1cm} (8.5)

Output, $y = -1$, if $w \cdot x + b \leq -1$  \hspace{1cm} (8.6)

The margin width of the hyperplane is calculated by considering the plus plane and minus plane. The plus plane is represented by Equation (8.7):

$$x: w \cdot x + b = +1$$  \hspace{1cm} (8.7)

The minus plane is represented by Equation (8.8):

$$x: w \cdot x + b = -1$$  \hspace{1cm} (8.8)
The perpendicular distance of the plus plane from the classifier boundary is in Equation (8.9):

\[
\frac{|1 - b|}{||w||}
\]  
(8.9)

The perpendicular distance of the minus plane from the classifier boundary is in Equation (8.10):

\[
\frac{|-1 - b|}{||w||}
\]  
(8.10)

The margin width can be calculated by Equation (8.11):

\[
\frac{|1 - b + 1 + b|}{||w||} = \frac{2}{||w||}
\]  
(8.11)

In order to determine the maximum margin between the pair of hyperplanes, the value of w needs to be minimized. The EEHIDS flow is as follows:

Query formation → Intrusion attributes → Presented features → Comparison

Training data → Intrusion attributes → Presented features

If new intrusion is detected after comparison, it is added to the training set; otherwise, necessary steps are taken to prevent intrusion

The two phases in EEHIDS to detect intrusion using cellular automata [31, 32] are:

1. Training phase: In this phase, an intrusion database is populated with sample intrusions and their attributes. Optimal hyperplanes for each of the binary classifiers are constructed based on the training set data. The system is trained with sample intrusions. These form the basis of identifying the pattern of user queries. The attribute vector for each of these intrusions is stored in a feature database. Two classes, namely, affected class and normal class, are considered here. All intrusions recorded in the database are classified into the same affected class. The instances of similar class are grouped into a single category. Two CA need to be built, where each CA is
trained to identify its class by estimating the optimal hyper-plane for each CA.

2. Testing phase: In this phase, the attributes of the instance are used to form a query. The attribute vector is calculated and given as input to the pool of trained CA to identify the class of the instance and to take necessary steps.

8.4.3 Performance Comparison

After performance analysis, it has been seen that EEHIDS results in much better utilization of the available energy than existing SPAID. Figure 8.5 represents the comparative analysis between EEHIDS and existing SPAID. It has been noticed that the percentage of available energy is higher with an increase in node density in EEHIDS than in SPAID.

In EEHIDS, partitioning larger networks to clusters and manipulating energy levels and thresholds provides a more energy-optimal solution than that of SPAID, which considers the entire network. Also, SPAID was considered only for minimum mobility of the networks. EEHIDS with tree-based clusters can be efficient in the case of dynamic wireless networks.

![Figure 8.5](http://www.crcpress.com/product/isbn/9781466515659)  
*Figure 8.5  Comparison between EEHIDS and SPAID.*
8.5 Summary

In this chapter, a brief overview of the future trends in WAN security has been provided. This chapter mainly focuses on the requirement of secure cloud services and smart grid architecture to the limited-resource WAN environment. It also presents a security architecture of cloud in WAN. Finally, it gives an idea about energy-efficient intrusion detection architecture in WAN using cellular automata. It represents the efficient functioning of the EEHIDS algorithm to avoid complete exhaustion of a node or network. The results show that the EEHIDS algorithm gives good results on any type of wireless ad-hoc network. As is evident from the energy utilization performance evaluation, the EEHIDS algorithm proves to be scalable, and even more efficient as the size of the wireless ad-hoc network increases.

References


