Data Integrity and Availability in Power System Communication Infrastructures

OGNJEN VUKOVIĆ

Licentiate Thesis
Stockholm, Sweden 2013
Data Integrity and Availability in Power System Communication Infrastructures

OGNJEN VUKOVIĆ

Licentiate thesis
Stockholm, Sweden, 2013
Akademisk avhandling som med tillstånd av Kungl Tekniska högskolan framlägges till offentlig granskning för avläggande av licentiatexamen torsdagen den 30 Maj 2013 i Hörsal F3, KTH, Stockholm.

© Ognjen Vuković, Maj 2013

Tryck: Universitetsservice US AB
Abstract

Society is increasingly dependent on the proper functioning of electric power systems. Today’s electric power systems rely heavily on information and networking technology in order to achieve efficient and secure operation. Recent initiatives to upgrade power systems into smart grids target an even tighter integration with information and communication technologies in order to enable the integration of renewable energy sources, local and bulk generation and demand response. Therefore for a proper functioning of smart grids, it is essential that the communication network is secure and reliable both in the face of network failures and in the face of attacks. This thesis contributes to improving the security of power system applications against attacks on the communication infrastructure. The contributions lie in two areas.

The first area is the interaction of network and transport layer protocols with power system application layer security. We consider single and multi-area power system state estimation based on redundant telemetry measurements. The state estimation is a basis for a set of applications used for information support in the control center, and therefore its security is an important concern. For the case of single-area state estimation, we look at the security of measurement aggregation over a wide area communication network. Due to the size and complexity of power systems, it can be prohibitively expensive to introduce cryptographic security in every component of the communication infrastructure. Therefore, we investigate how the application layer logic can be leveraged to optimize the deployment of network, transport and application layer security solutions. We define security metrics that quantify the importance of particular components of the network infrastructure. We provide efficient algorithms to calculate the metrics, and that allow identification of the weakest points in the infrastructure that have to be secured. For the case of multi-area state estimation, we look at the security of data exchange between the control centers of neighboring areas. Although the data exchange is typically cryptographically secure, the communication infrastructure of a control center may get compromised by a targeted trojan that could attack the data before the cryptographic protection is applied or after it is removed. We define multiple attack strategies for which we show that they can significantly disturb the state estimation. We also show a possible way to detect and to mitigate the attack.

The second area is a study of the communication availability at the application layer. Communication availability in power systems has to be achieved in the case of network failures as well as in the case of attacks. Availability is not necessarily achieved by cryptography, since traffic analysis attacks combined with targeted denial-of-service attacks could significantly disturb the communication. Therefore, we study how anonymity networks can be used to improve availability, which comes at the price of increased communication overhead and delay. Because of the way anonymity networks operate, one would expect that availability would be improved with more overhead and delay. We show that surprisingly this is not always the case. Moreover, we show that it is better to overestimate than to underestimate the attacker’s capabilities when configuring anonymity networks.
Acknowledgments

I would like to thank my main advisor Assoc. Prof. György Dán for his guidance, and for his very helpful and continuous feedback. I am deeply grateful for all our insightful discussions that helped me in enhancing my knowledge, and in identifying and addressing exciting research problems. I would also like to thank my second, but originally main advisor, Prof. Gunnar Karlsson, for giving me an opportunity to join this lab, and for introducing me into the world of scientific research. I am thankful for his support and for his comments on my work. Furthermore, I am grateful to all colleagues in the LCN for providing a friendly and stimulating work atmosphere.

I am thankful to all my friends in Stockholm, back home, and abroad, who were always there for me, and whose presence was invaluable to me. Last but not least, I would like to thank to my family for their continuous support. Among them, my special gratitude goes to my mother Milka and my sister Jovana for their love and understanding.
Contents

Contents iii

1 Introduction 1

2 Power System Communication Infrastructures 5
   2.1 SCADA Communication 5
   2.2 Inter-Control Center Communication 14

3 Power System State Estimation 17
   3.1 Transmission Network Model 17
   3.2 Measurement Model 18
   3.3 Single-area State Estimation 19
   3.4 Multi-area State Estimation 22

4 Summary of original work 25

5 Conclusions and Future work 29

Bibliography 33

Paper A: Network-aware Mitigation of Data Integrity Attacks on Power System State Estimation 37

Paper B: On the Security of Distributed Power System State Estimation under Targeted Attacks 61

Paper C: Traffic Analysis Attacks in Anonymity Networks: Relationship Anonymity-Overhead Trade-off 79
Chapter 1

Introduction

The main role of power systems transmission and distribution networks is to supply consumers with the electrical energy produced by electric generators. Transmission networks transfer the energy over long distances, and they may contain a large number of substations interconnected by transmission lines, forming a mesh network topology. In order to minimize the energy loses, the electrical energy is transmitted at high voltages, typically ranging from 100 kV to 500 kV [43]. When close to consumers, step-down transformers are used to decrease the voltage levels before connecting to the distribution networks that transmit the energy at lower voltage levels, typically under 70 kV [43]. Distribution networks transfer the energy between the transmission network and the consumers, and they typically operate in a radial configuration: feeders emanate from substations and form a tree structure with their roots at the substation and branches spreading over the distribution area [43].

A power system operates in one of three possible operating states: normal, emergency and restorative [30]. Normal operating state means that all the loads, i.e., power demanded by the consumers, can be supplied by the active generators through the transmission and distribution network without violating any operating constraints, such as bounds on the transmission line power flows. Normal operating state can be secure or insecure. The normal operating state is secure if the system can reside in the normal operating state after experiencing a contingency from a list of critical contingencies. Typically considered contingencies are outages of transmission lines and generators. Contrary, the normal operating state is insecure if the system may not preserve the normal operating state after the occurrence of some contingency from the list. In this case, some actions must be taken so that the system is moved to the normal operating secure state, and therefore the emergency operating state is avoided. However, the system may still move to the emergency operating state, e.g., in event of a non-considered contingency. Emergency operating state means that some of the operating constraints may be violated. In this state, instant actions are required to avoid the system collapse and to return the system to the normal operating state. The actions may result in disconnecting some
PARTS OF THE SYSTEM, SUCH AS LOADS AND GENERATORS. THIS MAY STABILIZE THE SYSTEM, WHERE ALL OPERATING CONSTRAINTS ARE SATISFIED AGAIN. HOWEVER, THE BALANCE BETWEEN THE GENERATED AND CONSUMED POWER MAY HAVE TO BE RESTORED. THE SYSTEM IS THEN IN THE RESTORATIVE OPERATING STATE.


POWER SYSTEMS ARE HIGHLY DEPENDENT ON PROPER FUNCTIONING OF THEIR COMMUNICATION INFRASTRUCTURES. THE POWER SYSTEM COMMUNICATION INFRASTRUCTURES SHOULD BE SECURE AND RELIABLE BOTH IN THE FACE OF NETWORK FAILURES AND IN THE FACE OF ATTACKS. SECURITY OF COMMUNICATION INFRASTRUCTURES HAS THREE ASPECTS: DATA CONFIDENTIALITY, DATA INTEGRITY, AND DATA AVAILABILITY [36]. DATA CONFIDENTIALITY PROTECTS THE PRIVACY (READABILITY) OF THE DATA AGAINST UNAUTHORIZED USERS, AND IT CAN BE ACHIEVED BY DATA ENCRYPTION. DATA INTEGRITY PROTECTS THE DATA AGAINST UNAUTHORIZED GENERATION AND MODIFICATION, AND IT CAN BE ACHIEVED BY MESSAGE AUTHENTICATION CODES. FINALLY, DATA AVAILABILITY ENSURES DATA ACCESSIBILITY WITHOUT EXCESSIVE DELAY. AMONG THESE THREE ASPECTS, THE EMPHASIS IS ON DATA INTEGRITY AND DATA AVAILABILITY, SINCE INCORRECT OR UNDELIVERED CONTROL ACTIONS AND MEASUREMENTS COULD BE MORE HARMFUL THAN THEIR DISCLOSURE [23, 24, 41].

TRADITIONALLY, SECURITY AND RELIABILITY OF POWER SYSTEM COMMUNICATION INFRASTRUCTURES HAVE BEEN ACHIEVED BY ISOLATING THE COMMUNICATION INFRASTRUCTURE, AND BY PROTECTING THE SYSTEM DESIGN AND IMPLEMENTATION. HOWEVER, POWER SYSTEM COMMUNICATION INFRASTRUCTURES ARE BECOMING MORE AND MORE INTEGRATED WITH OTHER COMMUNICATION INFRASTRUCTURES, INCLUDING PUBLIC ONES. MOREOVER, SOME PARTS OF THE
system design, e.g., the communication protocols, have been standardized, and are therefore known. Due to concerns about the cyber security of their systems, power system operators have started applying commercial security solutions, such as cryptographic protection, in their communication infrastructures. However, due to the size of the systems, it may be economically and practically unfeasible to protect the entire system. Therefore, it is important to understand how secure is the system. One could start by identifying potential consequences for power systems, if any security aspect of the communication infrastructure gets violated. Then, the security of a power system communication infrastructure could be evaluated as how well the infrastructure prevents the consequences based on applied security solutions. Finally, one could identify how to efficiently deploy commercial security solutions in order to minimize the consequences. If, however, the commercial security solutions cannot mitigate the consequences, additional solutions need be explored.

The objectives of this thesis are to:

- Investigate how violations of data integrity in the power system communication infrastructure can affect power system applications, in particular the power system state estimation.
- Define security metrics that can be used to evaluate the security of power system infrastructures, considering the power system state estimation.
- Analyze how data availability can be improved using anonymity networks.

The structure of this thesis is as follows. In Chapter 2, we discuss protocols and architectures used in power system communication infrastructures, and elaborate on data integrity and data availability provided by the infrastructures. In Chapter 3, we describe power system state estimation, and discuss how a violation of data integrity can affect the state estimation. Chapter 4 provides a summary of the papers included in this thesis along with the thesis’ author contributions to each paper. Chapter 5 summarizes the main findings and conclusions, and outlines potential directions for future research.
Chapter 2

Power System Communication Infrastructures

Power systems rely heavily on their communication infrastructure for secure and reliable operation [38]. The communication infrastructure serves two main roles. The first role is to connect the control center with field devices so that measurements can be acquired and remote control can be performed. This is the basis for Supervisory Control and Data Acquisition (SCADA) systems, used by an operator to monitor and control the system [3], and a core component of Phasor Networks, where Phasor Data Concentrators aggregates measurements from Phasor Measurement Units (PMUs). The second role is to connect the control centers of interconnected power systems in order to improve operational efficiency and system stability. This enables the secure operation of large and highly inter-connected systems such as Western Interconnect (WECC) in the U.S. and ENTSO-E in Europe.

2.1 SCADA Communication

SCADA system delivers information from sensors and relays through Remote Terminal Units (RTUs) to SCADA servers, and delivers control messages from SCADA servers through RTUs to relays. Sensors provide various measurements including power flows, voltages and currents. Relays control electrical circuits in order to automatically reconfigure a circuit if a fault is detected (protective relays), or to reconfigure a circuit on demand by remote control (control relays). An RTU is a programmable device located at a substation, and is used to collect measurements from the sensors, to monitor the status of protective relays, and to deliver commands to the control relays. RTUs deliver the measurements and the status information to a SCADA server over a Wide-Area Network (WAN), and receive commands for the control relays from the SCADA server over the WAN. The SCADA server is the central processor of the SCADA system located at the control center, and usually provides a human interface for monitoring and control.
CHAPTER 2. POWER SYSTEM COMMUNICATION INFRASTRUCTURES

SCADA WAN

The types of WANs used for the communication between RTUs and SCADA servers can include point-to-point connections over dedicated lines, circuit switched networks, packet switched networks, and cell switched networks. In the case of point-to-point connections over dedicated lines, there is a separate line for every RTU to a SCADA server connection. The advantage of this solution is that it can provide the best quality of service, but the main disadvantage is the cost, since a line per RTU needs to be built or leased. Circuit switched networks provide dedicated communication channels between RTUs and SCADA servers. Unlike for the case of dedicated lines, communication channels in circuit switched networks are not always active, they are established and used when needed so the network resources can be shared among many pairs of end points. Examples of technologies used are Frequency Division Multiplexing (FDM), where each communication channel gets a non-overlapping frequency range, and Time Division Multiplexing (TDM), where each communication channel gets recurrent fixed-length time slot. In packet switched networks, one communication channel may be shared by many participants, who communicate by exchanging variable-length packets. Examples of such technologies are X.25, Frame relay, GPRS, and Ethernet. Finally, cell switched networks are similar to packet switched networks, but they use fixed, instead of variable, length packets (cells). Prior transporting, data is divided into fixed-length cells. An example of such technology is Asynchronous Transfer Mode (ATM).

In principle, the communication infrastructure used for the WAN can be owned by the operator, e.g., optical ground wires (OPGW) that run between the tops of high-voltage transmission towers, or leased, e.g., PSTN, Public Land Mobile Networks (PLMN), and satellite networks. In practice, the infrastructure is mostly owned by the power system operator for reliability reasons. However, the increasing demands imposed on the communication infrastructure by smart grid technologies may make it more economically efficient for the operators to lease commercial networks than to deploy their own.

SCADA/RTU communication protocols

Historically, the SCADA communication protocols were independently designed by different SCADA equipment manufacturers. Each manufacturer developed the protocols to be a part of its proprietary system, and to meet its specific needs [6]. These proprietary protocols had disadvantages for the user, the user could not combine equipment produced by different manufacturers. With the increasing use of SCADA systems, these disadvantages were becoming more prominent, and the need for open standards was recognized [6]. To address the issues, standards organizations were working on defining open protocols that would provide interoperability between systems. One of the arising standards was the IEC 60870-5 standard, created and progressively published from 1990 by the International Electro-technical Commission (IEC) Technical Committee (TC) 57 [35]. IEC 60870-5 is a foundation
2.1. SCADA COMMUNICATION

for today’s most commonly used protocols for the communication between RTUs and SCADA servers: IEC 60870-5-104 (including its predecessor IEC 60870-5-101), and Distributed Network Protocol 3 (DNP3). IEC 60870-5-101 and IEC 60870-5-104 are predominantly used in Europe, while DNP3 is predominantly used in North and South America, South Africa, Asia, and Australia [6].

IEC 60870-5

IEC 60870-5 is a part of the IEC 60870 standard, that defines operating conditions, electrical interfaces, performance requirements, and data transmission protocols. IEC 60870-5 defines communication protocols used for sending basic telecontrol messages between two systems. IEC 60870-5 is based on the Enhanced Performance Architecture (EPA) model, which is a simplified version of the International Standards Organization (ISO) Open Systems Interconnection (OSI) model [35]. EPA is designed to provide optimum performance for telecontrol applications, and it defines only three layers: physical layer, link layer, and application layer. The physical layer is defined by IEC 60870-5-1, in particular, coding, formatting, bit error check, and synchronization of data frames of variable and fixed lengths. It includes the specification of four frame formats. IEC 60870-5-2 defines the link layer: link transmission procedures using a control field and address field. IEC 60870-5-3 defines how the application data units are structured in transmission frames. IEC 60870-5-4 provides rules for defining information data elements, such as process variables that are frequently used by the applications. Finally, IEC 60870-5-5 specifies standard services (functions) of the application layer which serve as basic guidelines when creating application profiles for specific tasks. Each application profile uses a specific set of functions. If there is a function needed by the application but not specified in the standards, it should be specified within the profile.

IEC 60870-5-101 (IEC 101)

IEC 101, published in 1995, was the first IEC complete working SCADA protocol under IEC 60870-5 [35]. It was designed to provide all necessary application level functions for telecontrol applications that operate over large geographical areas, using low bandwidth point-to-point links.

IEC 101 uses the FT1.2 frame format defined in IEC 60870-5-1 [6]. On the link layer, IEC 101 uses some selected transmission procedures from IEC 60870-5-2 that may be used for reliable transfer, and it supports unbalanced (only server initiated message exchange) and balanced (both server and client can initiate the exchange) transmission modes. IEC 101 defines Application Service Data Units (ASDUs) from a given general structure in IEC 60870-5-3, which are used for structuring transmission frames. The contents and sizes of fields in ASDUs are specified according to IEC 60870-5-4. The basic application functions utilized by IEC 101 include cyclic data transmission, data acquisition by polling, command transmission, acquisition of events, etc., and are defined in IEC 60870-5-5.
## Variable length frame format

<table>
<thead>
<tr>
<th>Field name</th>
<th>Field description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start byte</td>
<td>1 byte = 0x10</td>
</tr>
<tr>
<td>Length (1 byte)</td>
<td>Length of Link layer data (control field, address field, and link user data in bytes)</td>
</tr>
<tr>
<td>Start byte</td>
<td>1 byte = 0x10</td>
</tr>
<tr>
<td>Link control field</td>
<td>Copy of the start for reliability</td>
</tr>
<tr>
<td>Link address fields</td>
<td>(up to 2 bytes)</td>
</tr>
<tr>
<td>Link address fields</td>
<td>Device / server address</td>
</tr>
<tr>
<td>Checksum (1 byte)</td>
<td>Error check</td>
</tr>
<tr>
<td>Stop byte</td>
<td>1 byte = 0x16</td>
</tr>
</tbody>
</table>

## Fixed length frame format

<table>
<thead>
<tr>
<th>Field name</th>
<th>Field description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start byte</td>
<td>1 byte = 0x10</td>
</tr>
<tr>
<td>Link control field</td>
<td>Control functions</td>
</tr>
<tr>
<td>Link address fields</td>
<td>(Up to 2 bytes)</td>
</tr>
<tr>
<td>Checksum (1 byte)</td>
<td>Error check</td>
</tr>
<tr>
<td>Stop byte</td>
<td>1 byte = 0x16</td>
</tr>
</tbody>
</table>

## Single character frame

<table>
<thead>
<tr>
<th>Field name</th>
<th>Field description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acknowledgement byte</td>
<td>1 byte = 0xE5 Used for acknowledgments</td>
</tr>
</tbody>
</table>

Figure 2.1: Three FT1.2 frame forms used by IEC 101. The figure is based on [6].

The FT1.2 frame format has three forms: variable-length frame format, fixed-length frame format, and a single character frame [6]. The variable-length frame is used for bidirectional data transmission between the server and the remote station. The fixed-length frame format is used for commands, and it can be used for acknowledgments. The single character frame consists of just one byte, and it can be only used for acknowledgments. The structures of the three forms of the FT1.2 frame are given in Figure 2.1 (based on [6]). IEC 101 provides addressing on the data link layer through the link address field in the FT1.2 frame format [6]. The link address field can be from 0 to 2 bytes for the balanced transmission mode, or from 1 to 2 for the unbalanced transmission mode. Since the balanced transmission mode may go through a point-to-point link, the link address is redundant. In that case the link address can be omitted.

IEC 101 provides detection of bit transmission errors through checksum provided by FT1.2 [6]. FT1.2 uses an 8-bit checksum calculated as the modulo 256 sum of the link layer data [6], which is the data that starts after the second start field and ends before the checksum field (Figure 2.1). By recalculating the checksum on the receiver side, bit errors due to transmission can be detected but not corrected. If the checksum detects the transmission errors, the data is discarded and a retransmission is requested. However, it may happen that many bit errors occur so that the 8-bit checksum calculation results in the same 8 bits as in the case without errors. The strength of a checksum can be evaluated by the maximum number of single bit errors that will be always detected, or so-called the Hamming distance. If the number of single bit errors is larger than the Hamming distance of a checksum, the checksum may or may not detect the errors. The Hamming distance of the checksum used by the IEC 101 frames is to 4 [6].
2.1. SCADA COMMUNICATION

IEC 60870-5-104 (IEC 104)

With the increasing affinity towards packet switching networks instead of circuit switching networks, IEC 101 needed to be changed to support more network technologies. The modification came in the form of the IEC 104 standard, published in 2000 [6, 35]. The application layer of IEC 104 is based on IEC 101, but some data types and functions are no longer used and supported. IEC 104 relies on TCP [20] and IP [19] as transport and network protocols, and it does not impose any limitations on the data link layer and the physical layer protocols.

IEC 104 does not need to provide any addressing on the layers under the application layer, since it relies on the underlying protocols for that purpose. Moreover, IEC 104 does not provide any detection of bit transmission errors. The bit error check is provided by the underlying protocols: TCP uses a 16-bit checksum (the bitwise complement of the sum of 16-bit words added using one's complement arithmetic [20]) to verify the TCP header together with the IEC 104 data. Moreover, some other underlying protocols (e.g., Ethernet) may have verification algorithms that consider the IEC 104 data (Ethernet uses a 32-bit cyclic redundancy check).

Distributed Network Protocol 3 (DNP3)

The DNP3 protocol was being developed in early 1990s by Harrison Controls Division based on some early versions of the IEC 60870-5 standard [6, 35]. Initially, it was developed as a proprietary protocol for use in the electrical utility industry. However, in 1993, DNP3 was taken over by the DNP Users Group, and it became an open standard that has been used by other industries as well (oil and gas, water supply, etc.). Later on, IEEE adopted DNP3 as standard in [1].

The DNP3 frame format is based on the FT3 frame format defined in IEC 60870-5-1 [6]. On the data link layer, DNP3 supports only balanced transmission mode (both server and client can initiate the exchange). Between the data link layer and the application layer, DNP3 defines the pseudo-transport layer to allow transmission of larger blocks of application data by fragmenting [6].

DNP3 frame format has variable length, and its structure is shown in Figure 2.2 (based on [6]). DNP3 provides addressing on the data link layer through the destination and source address fields in the frame header. The address fields are two bytes each.

DNP3 can detect bit transmission errors using 16-bit cyclic redundancy code (CRC-16) checksum [6]. There is one CRC-16 checksum for the frame header, and thereafter one for every block (max 16 bytes) of user data [6] (Figure 2.2). By recalculating all CRC-16 checksums on the receiver side, bit errors due to transmission can be detected. In the case of DNP3 frames and the CRC-16 checksum, the Hamming distance equals to 6 [6], which is higher than in the case of IEC 101. However, DNP3 has also a higher transmission overhead in terms of the checksum bits: the ratio of checksum bits to the message bits is higher since it includes a CRC-16 code per every block of 16 bytes of user data.
Secure extensions of IEC 101, IEC 104, and DNP3

In their original formats, IEC 101, IEC 104, and DNP3 do not provide any of the three security aspects: data confidentiality, data integrity, and data availability. With the increasing cyber security concerns of SCADA systems, IEC 101, IEC 104, and DNP3 needed to be upgraded to provide the security aspects. The highest priority was put on the data integrity and availability, since it may be more harmful for the power system if control actions and measurements are incorrect or undelivered than if they are disclosed [15, 17]. International standard organizations and researchers have been proposing different standards and solutions to upgrade the protocols. The most distinguished resulting standards are IEC 62351-5 [24] by IEC TC 57 and the DNP3 Secure Authentication (DNP3 SA) [1] by the DNP Users Group. IEC 62351-5 and DNP3 SA have been developed in parallel, and IEC TC 57 and DNP Users Group worked together closely so that IEC 62351-5 and DNP3 SA are compliant [17]. Both IEC 62351-5 and DNP3 SA focus on the data integrity, while data confidentiality is provided only for the key-exchange messages.

IEC 62351-5 [24] defines the security standards for IEC 60870-5, including IEC

<table>
<thead>
<tr>
<th>Field name</th>
<th>Field description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start byte (2 bytes = 0x0564)</td>
<td>Indicates the start of frame</td>
</tr>
<tr>
<td>Length (1 byte)</td>
<td>Length of Link layer data excluding CRC fields (control field, address fields, and user data) in bytes</td>
</tr>
<tr>
<td>Link control field (1 byte)</td>
<td>Control functions (e.g., message type and direction)</td>
</tr>
<tr>
<td>Link destination address (2 bytes)</td>
<td>Device / server destination address</td>
</tr>
<tr>
<td>Link source address (2 bytes)</td>
<td>Device / server source address</td>
</tr>
<tr>
<td>Checksum: CRC-16 (2 bytes)</td>
<td>Error check of the header</td>
</tr>
<tr>
<td>Link user data (16 bytes)</td>
<td></td>
</tr>
<tr>
<td>Checksum: CRC-16 (2 bytes)</td>
<td>Error check of the user data</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Checksum: CRC-16 (2 bytes)</td>
<td>Error check of the user data</td>
</tr>
</tbody>
</table>

Figure 2.2: DNP3 frame format. The figure is based on [6].
2.1. SCADA COMMUNICATION

101 and IEC 104, and for IEC 60870-5 derivatives, such as DNP3. The security standards can be divided into two categories: one for the protocols that utilize low bandwidth point-to-point links (IEC 101), and the other for the protocols that can go over the TCP/IP protocol stack (IEC 104 and DNP3). The protocols in the first category, e.g., IEC 101, are supplemented with additional security measures, that involve cryptographic algorithms, to primarily protect the data integrity. The protocols in the second category, e.g., IEC 104 and DNP3, rely on a challenge-response mechanism combined with a Message Authentication Code (MAC) to protect the data integrity, and utilize the Transport Layer Security (TLS) version 1.0 [9] to protect the data confidentiality.

DNP3 SA [41] has been developed in parallel with IEC 62351-5 by the DNP User Group, as a secure extension of DNP. DNP3 SA is compliant with IEC 62351-5, and is a part of the IEEE standard [1]. To protect the data integrity, DNP3 SA uses the challenge-response mechanism described in the IEC 62351-5 standard [24], and utilizes TLS version 1.0 [9] to protect the data confidentiality.

The challenge-response mechanism, used by IEC 62351-5 and DNP3 SA, is applied at the application layer, assuming that the underlying layers do not provide any security. The main motivation behind this approach is that it permits that some data exchange can be left unprotected, if desired, which reduces bandwidth and processing requirements [41]. Moreover, it is more practicals in diverse networks found in power systems. The challenge-response mechanism can be described as follows [41]. Upon receiving a message, the recipient (challenger) decides whether the data in the message are of significant importance, i.e., if the data should be protected. If not, the message is processed without any verification. However, if the data should be protected, the challenger initiates the verification of data integrity by sending a challenge message to the sender (responder). The challenge message contains information about the MAC algorithm that the responder should use in the reply, and some randomly generated number to be send back in the reply (used as a protection against replay attacks). The challenge message also specifies if the data from the received message should be contained in the reply: if not, the challenger only verifies the identity of responder, if yes, the challenger also verifies the data. The responder generates the reply message that includes the responder identification, the randomly generated number sent by the challenger, and, if requested, the data to be verified. Before sending the reply message, the responder performs the specified MAC algorithm on the message using a pre-shared session key, and adds the resulting MAC value to the reply message. Upon receiving the reply, the challenger performs the same MAC algorithm, and if the resulting MAC values match, the verification of the data integrity is successful. Examples of the challenge-response mechanism are shown in Figure 2.3.

The MAC algorithms that can be used for the challenge-response mechanism are specified in IEC 62351-5 and DNP3 SA. The keys for the MAC algorithms are pre-shared by default. However, the need for more sophisticated managing of the keys is recognized by IEC and the DNP User Group, and is a subject of future standard releases. Some recent releases, e.g., DNP SA version 5, provide methods...
CHAPTER 2. POWER SYSTEM COMMUNICATION INFRASTRUCTURES

![Diagram of challenge-response mechanism]

Figure 2.3: Examples of the challenge-response mechanism. The figure is based on [41].

Example of a successful verification

Example of a failed verification

The SCADA infrastructure has been traditionally designed to operate in an isolated environment in order to achieve secure and reliable operation. Cyber security has been provided through isolation: it was assumed that no attacker had detailed knowledge of the system design and implementation, including the used proprietary protocols [11]. This security principle is called security through obscurity, and it has been widely criticized as it provides a very fragile security: the system is

Data Integrity Issues and Proposed Solutions

The SCADA infrastructure has been traditionally designed to operate in an isolated environment in order to achieve secure and reliable operation. Cyber security has been provided through isolation: it was assumed that no attacker had detailed knowledge of the system design and implementation, including the used proprietary protocols [11]. This security principle is called security through obscurity, and it has been widely criticized as it provides a very fragile security: the system is
secure as long as the details remain secret, but quickly breaks once the details are released [36]. Moreover, SCADA infrastructures are becoming more and more integrated with the other corporate infrastructures, and components and protocols have been standardized and are available to practically anyone. This may leave the SCADA systems vulnerable to cyber attacks [11].

A cyber attack on the SCADA communication infrastructure may result in manipulation of the data exchanged between RTUs and the SCADA server. Since the most commonly used protocols (IEC 101, IEC 104 over TCP/IP, and DNP3) can provide only the detection of random bit errors and no protection of data integrity, the attack could remain undetected if the checksums are recalculated after the modification. The attack could result in intentionally wrong control signals and modified (incorrect) measurements, and it could significantly disturb the power system applications that rely on these signals and measurements.

In order to protect the SCADA system against the data integrity attacks on the messages exchanged between RTUs and the SCADA server, the communication needs to be cryptographically protected. Cryptographic protection can be provided by encapsulating (or tunneling) the protocols (IEC 101, IEC 104, and DNP3) into a protocol that provides the cryptographic protection [11], e.g., IPsec [26] or TLS [9], or by using the recent protocol extensions that provide message authentication: IEC 62351-5 [24] and DNP3 SA.v5 [1]. The cryptographic protection requires an upgrade of all RTUs in the system so they can support the computationally intensive cryptographic operations, and the key management. Some RTUs could be reprogrammed, while other legacy RTUs, that do not have sufficient processing power, would need to be replaced or supplemented by bump-in-the-wire (BITW) devices [42]. The BITW devices are positioned next to legacy RTUs and tunnels the communication between the RTUs and the SCADA server. The communication between BITWs and SCADA servers is protected while the communication between BITWs and RTUs remains vulnerable. Due to the size of power systems, it may be practically and economically unfeasible to perform the upgrades in a short amount of time, and therefore, it is expected to go in stages. In every stage of the upgrade, it is challenging to evaluate the system security and to optimally select RTUs that will maximally improve the security by upgrading. On the other hand, the complexity of key management increases with the number of upgraded RTUs. Therefore, it is important to keep the number of upgraded RTUs low while achieving a desirable level of system security.

In this thesis, we propose a framework that captures the characteristics of the SCADA communication infrastructure, and that can help in evaluating and improving the system security. Furthermore, the framework can be used in every stage of the upgrade to prioritize the RTUs to be protected. The framework is described in Paper A, where we also use the framework to evaluate and to improve the security of power systems considering the power system state estimation. Our results show that the power system state estimation could be secured by upgrading only a subset of all RTUs in the system.
CHAPTER 2. POWER SYSTEM COMMUNICATION INFRASTRUCTURES

2.2 Inter-Control Center Communication

Modern power systems have become increasingly inter-connected in order to improve operational efficiency, e.g., the Western Interconnect (WECC) in the U.S. and the ENTSO-E in Europe. The proper operation of an inter-connected system depends on proper operation of its constituent control regions. Therefore, neighboring control regions need to exchange some information about their systems in real-time, so that they can detect disturbances and quickly restore the system to a secure state in case of outages [44]. The exchange of real-time data between control centers is expected to be even more frequent in future power systems [44].

Historically, power system operators relied on proprietary protocols for inter-control center communication. However, with the increasing interconnectivity between independent operators, the inability of proprietary protocols to provide interoperability has become a problem. To address the problem, the power industry jointly developed an international IEC 60870-6 standard based on the OSI model, and submitted it to the IEC for standardization [44]. IEC 60870-6 is a part of the IEC 60870, and it defines protocols for data exchange between control centers over a WAN. There are two protocol versions used for the data exchange: Tele-control Application Service Element-1 (TASE.1) and TASE.2. One of the differences between the two versions is in the specification of mechanisms for message control and interpretation. TASE.2 specifies uses the Manufacturing Message Specification (MMS) for the specification, and it appears to be the prevalent version used. TASE.2 is usually referred to as the Inter-control Center Communication Protocol (ICCP) [38].

ICCP (IEC 60870-6/TASE.2)

ICCP specifies only the application layer of the OSI model, and it relies on other protocols for the underlying layers. ICCP specifies the use of MMS for the message control and interpretation, and it specifies the data object formats and the methods for data request and reporting. ICCP also specifies how the data can be shared among applications at different control centers.

ICCP is realized through logical connections, called associations. A control center may establish associations with more than one control center. Moreover, it may establish more than one association with the same control center that could be used to separate data transfers by priority.

ICCP defines data access control through bilateral tables. Bilateral tables specify for every association which data elements can be accessed. However, ICCP does not provide any security of the data during transport.

Secure ICCP

Since ICCP does not protect the data during transport, IEC Technical Committee 57 specified in the standards IEC 62351-3 [21] and IEC 62351-4 [22] how lower
layer protocols can protect the data. IEC 62351-3 specifies security measures for end-to-end security for protocols that go over TCP/IP. In particular, it describes the parameters and settings for the Transport Layer Security (TLS) protocol [10] that should be configured by the operators. It also considers IPsec [26], but TLS is preferred [21]. IEC 62351-4 specifies security measures for protocols that use MMS, and provides the application layer security: prevents unauthorized access to information through authentication [22]. The authentication is achieved through the use of TLS.

Applied together, IEC 62351-3 and IEC 62351-4 protect the data integrity and confidentiality while transported over ICCP, thanks to TLS. However, TLS does not protect against denial-of-service attacks, and such protection should be applied through implementation-specific measures [21, 22].

The end-to-end security provided by IEC 62351-3 and IEC 62351-4 protects ICCP data transfer between two ICCP hosts, one per control center. These hosts, including databases that contain the data shared over ICCP, should be separated from the Master Local Area Network (LAN), where all critical applications (e.g., SCADA server and EMS) coexist [33]. ICCP hosts should be in a LAN which is separated by a firewall from the Master LAN on one side, and on the other side separated by another firewall from the WAN used to transfer the ICCP data, as shown in Figure 2.4 (based on [33]). Such separation is a common security practice when some network services should be accessible from outside of the network but connections or hosts cannot be fully trusted. The separated segment of the network that contains the services accessible from outside, is commonly referred to as the demilitarized zone (DMZ). In case of the ICCP, the lack of trust typically comes from the fact that the WAN may be insecure [33].

Data Integrity and Availability Issues and Proposed Solutions

By following the standards IEC 62351-3 and IEC 62351-4, the integrity of ICCP data can be protected when transferred between two ICCP hosts in DMZs. However, the ICCP data integrity may not be always protected, and IEC 62351-3 and IEC 62351-4 may not always provide high communication availability, as explained in the following.

First, within a ICCP host, the ICCP data might be unprotected after the TLS protection is removed and before the data is stored in a database (and the other way around), which leaves a potential security threat. Moreover, the threat is aggravated by the fact that the ICCP hosts are in DMZs. They could be victims of sophisticated targeted trojans, whose goal is to manipulate the ICCP data. Examples of recent sophisticated targeted trojans that were targeting industrial control systems are Stuxnet and Duqu [39]. The manipulation of ICCP data could significantly disturb the power system applications that rely on the data exchanged by the ICCP.

Second, TLS provides data integrity and confidentiality of the transmitted data, but it does not protect against denial of service attacks [21, 22]. An attacker that obtains access to the WAN may identify some critical low latency data exchange by
observing the size, and sender and receiver addresses of every message, and it may perform a targeted denial-of-service attack against such data exchange. Such an attack might be misinterpreted as packet loss due to a congestion, and therefore be undetected. As a consequence, the attack may disturb power system applications that rely on timely delivery of exchanged data.

In this thesis, we address both issues. First, in Paper B, we study how an attack against the integrity of ICCP data can affect the fully distributed multi-area power system state estimation, which requires timely data exchange between control centers of neighboring regions. We define attack strategies for sophisticated manipulation of the exchanged data and show that they can disable the state estimation. However, we also show a possible way to detect and to mitigate such attacks. Second, in Paper C, we study how anonymity networks could be used to improve the data availability if faced with targeted denial-of-service attacks. Anonymity networks disguise the sender and the receiver of every message through message relaying, which increases the communication overhead and delay. However, the delay may be a concern for some power system applications, such as distributed state estimation. Therefore, we analyze how much the availability can be improved for a given delay. We quantify the availability by the provided anonymity, i.e., the difficulty of the attacker to correctly identify the origin and the destination of the data. We quantify the delay by the number of times the data are relayed. Our results show that, surprisingly, the availability does not always get improved with additional delay. Moreover, we show that it is better to overestimate than to underestimate the attacker’s capabilities when designing anonymity networks.
Chapter 3

Power System State Estimation

Power system state estimator obtains an estimate of the state of the system by processing redundant measurements [2, 34]. Besides the measurements, the state estimator uses a model of the transmission network as input.

The state estimation can be centralized (single-area) or distributed (multi-area). The single-area state estimation obtains the estimate of an entire power system, or a single-area power system, performed by a single computing entity. An example of the single-area state estimation is the state estimation of a power system controlled by an independent power system operator, where the estimation is performed in the operator’s control center. The multi-area state estimation obtains the estimate of a power system that consists of multiple interconnected areas, where the estimation of each area is performed by an independent computing entity. To obtain a consistent state estimate of the entire multi-area power system, the computing entities need to cooperate and exchange some data used as input to the state estimator in every computing entity. An example of the multi-area state estimation is the state estimation of an interconnected power system that consists of a multiple areas controlled by independent operators. The state estimation of an area is performed in the control center of the operator that controls the area.

3.1 Transmission Network Model

We consider a transmission network that consists of buses that are interconnected by branches. The term bus is derived from the Latin omnibus, which means "for all", and it is a bar of metal to which all incoming and outgoing conductors, i.e., wires through which the electric current can flow, are connected [43]. Branches include transmission lines, transformers and phase shifters [2].

The admittance matrix $Y$ of the entire transmission network can be built from scratch by introducing one-by-one components (their models) of the system, and updating the corresponding entries in $Y$ [2]. The components include transmission lines, loads, generators, transformers, shunt capacitors and reactors. The matrix $Y$
is complex in general, and can be written as \( G + jB \), where \( G \) is the conductance matrix and \( B \) is susceptance matrix. For more information about the components and their models, and how the matrix \( Y \) is built, we refer to [2].

A transmission network model can be built by deriving a set of nodal equations by using the Kirchhoff’s current law at every bus in the transmission network [2, 34]. Let us denote the vector of bus voltage phasors by \( V \), and the vector of bus current injections by \( I \). Then, in a network of \( n \) buses, the nodal equations can be expressed with the following matrix equation,

\[
I = Y \cdot V;
\]

\[
\begin{bmatrix}
I_1 \\
I_2 \\
\vdots \\
I_n
\end{bmatrix} =
\begin{bmatrix}
y_{11} & y_{12} & \cdots & y_{1n} \\
y_{21} & y_{22} & \cdots & y_{2n} \\
\vdots & \vdots & \ddots & \vdots \\
y_{n1} & y_{n2} & \cdots & y_{nn}
\end{bmatrix}
\begin{bmatrix}
V_1 \\
V_2 \\
\vdots \\
V_n
\end{bmatrix}.
\]

(3.1)

Power injections at any bus can be derived by multiplying the vector \( V \) with the conjugate of the vector \( I \) from (3.1) [43]. Active and reactive power injections can be further derived by considering the real and the imaginary part of equation \( V \cdot I^* \). The active power injection \( P_{bi} \) and reactive power injection \( Q_{bi} \) at bus \( b_i \) can expressed as

\[
P_{bi} = V_{bi} \sum_{b_j \in N(b_i)} V_{bj} (g_{ij} \cos(\theta_{ij}) + b_{ij} \sin(\theta_{ij})),
\]

\[
Q_{bi} = V_{bi} \sum_{b_j \in N(b_i)} V_{bj} (g_{ij} \sin(\theta_{ij}) - b_{ij} \cos(\theta_{ij})),
\]

(3.2)

where \( V_{bi} \) is the voltage amplitude at bus \( b_i \), \( \theta_{ij} \) is the difference of phase angles between bus \( b_i \) and bus \( b_j \), and \( g_{ij} \) and \( b_{ij} \) are the corresponding entries in matrices \( G \) and \( B \), respectively, and \( N(b_i) \) is the set of adjacent buses to bus \( b_i \) [2, 43].

Power flows from bus \( b_i \) to bus \( b_j \) can be derived similarly to (3.2), and expressed as

\[
P_{bi,bj} = V_{bi}^2 (g_{si} + g_{ij}) - V_{bi} V_{bj} (g_{ij} \cos(\theta_{ij}) + b_{ij} \sin(\theta_{ij})),
\]

\[
Q_{bi,bj} = -V_{bi}^2 (b_{si} + b_{ij}) - V_{bi} V_{bj} (g_{ij} \sin(\theta_{ij}) - b_{ij} \cos(\theta_{ij})),
\]

(3.3)

where \( g_{si} + jb_{si} \) is the admittance of the shunt branch connected at bus \( b_i \) [2].

### 3.2 Measurement Model

Based on (3.2) and (3.3), all current and power injections or flows can be determined once we know the voltage phasors. However, we can use the same model to compute the voltage phasors based on the measurements. The most commonly used measurements are power flows, power injections, bus voltage magnitudes and current flow magnitudes [2]. Unfortunately, we cannot just directly use the measured values in (3.2) and (3.3) to get the voltage phasors. The measurements are prone to errors, and typically not all flows and injections are measured in the system.
Therefore, we need to estimate the voltage phasors based on the obtained measurements. In order to perform the estimation, we need a model of measurements, which is described as follows.

Let us consider the set of $M$ measurements that are given by the vector

$$
Z = \begin{bmatrix} z_1 \\ z_2 \\ \vdots \\ z_M \end{bmatrix} = \begin{bmatrix} f_{z_1}(x) \\ f_{z_2}(x) \\ \vdots \\ f_{z_M}(x) \end{bmatrix} + \begin{bmatrix} e_{z_1} \\ e_{z_2} \\ \vdots \\ e_{z_M} \end{bmatrix} = F(x) + e,
$$

(3.4)

where $x$ is the state vector constructed from the vector $V$ by considering the phase angles and the voltage amplitudes separately, $f_{z_i}(x)$ is a function relating measurement $z_i$ to the state vector $x$, and $e$ is the vector of measurement errors. If the measurement $z_i$ is an injection or a flow, then the function $f_{z_i}(x)$ can be expressed based on (3.1), (3.2), or (3.3). However, if the measurement $z_i$ is a voltage amplitude or a phase angle, then the function $f_{z_i}(x)$ equals to the corresponding entry in the vector $x$. Measurement errors are typically assumed to be independent random noise with Gaussian distribution of zero mean, and consequently the covariance matrix $W = E(ee^T)$ is diagonal [2, 34, 43].

### 3.3 Single-area State Estimation

In the case of single-area state estimation, all the measurements and the entire transmission network model are passed to a computing entity that performs the state estimation.

#### Maximum Likelihood Estimation

Maximum Likelihood Estimation (MLE), a method widely used in statistics, can be used to determine the most likely state of the system based on the measurements. The measurement errors are assumed to have a known probability distribution, but with unknown parameters. Let us denote by $l(z_i)$ the probability density function which represents the probability of measuring $z_i$. Assuming that the measurement errors are independent, we can express the joint probability density function of all measurements as the product of individual probability density functions [2]

$$
l_M(Z) = l(z_1)l(z_2) \cdots l(z_M).
$$

(3.5)

The function $l_M(Z)$ is referred to as the likelihood function, and it represents the probability of measuring the measurements in $Z$. It will obtain its peak value when the unknown parameters are chosen to be the closest to the actual values [2]. Therefore, by maximizing (3.5) we will reach the maximum likelihood estimates for the parameters of interest. Typically, the measurement error probability distributions are assumed to be Gaussian distributions, as described in Section 3.2. In that case, the parameters of interest are the mean values and the variances.
order to simplify the maximization problem, the likelihood function is replaced by its logarithm, so called the Log-Likelihood function, and it can be expressed as

$$
\mathcal{L} = \log(l_M(Z)) = \sum_{i=1}^{M} \log(l(z_i)) = -\frac{1}{2} \sum_{i=1}^{M} \left( \frac{z_i - E(z_i)}{\sigma_i} \right)^2 - \frac{M}{2} \log(2\pi) - \sum_{i=1}^{M} \log(\sigma_i),
$$

(3.6)

where the measurement error probability distributions are assumed to be Gaussian distributions with the mean value $E(z_i)$ and standard deviation $\sigma_i$ for the measurement $z_i$ [2]. The expected value $E(z_i)$ can be expressed as $f_{z_i}(x)$, and $\sigma_i$ is assumed to be known (it equals to the square root of diagonal entry $w_{ii}$ of the covariance matrix $W$) [2]. Finally, the MLE problem can be defined as

$$
\max_x \log(l_M(Z)),
$$

(3.7)

which is equivalent to

$$
J(x) = \min_x \sum_{i=1}^{M} \left( \frac{z_i - E(z_i)}{w_{ii}} \right)^2 = \min_x [Z - F(x)]^T W^{-1} [Z - F(x)].
$$

(3.8)

**Weighted Least Squares Estimator (WLSE)**

The optimization problem (3.8) can be solved by using the weighted least squares estimator (WLSE), which can be formulated as follows. At the minimum of (3.8), the first-order optimality conditions have to be satisfied:

$$
g(x) = \frac{\partial J(x)}{\partial x} = -H^T(x)W^{-1}[Z - F(x)] = 0,
$$

(3.9)

where $H = [\partial F(x)/\partial x]$ is the Jacobian of $F(x)$ [2]. By expanding the function $g(x)$ into its Taylor series around $x^{(k)}$, where $k$ is the iteration index, and by considering the first two terms of the series we yield an iterative scheme,

$$
x^{(k+1)} = x^{(k)} + [H^T(x^{(k)})W^{-1}H(x^{(k)})]^{-1}H^T(x)W^{-1}[Z - F(x)],
$$

(3.10)

known as the Gauss-Newton method [2]. Therefore, at each iteration $k$, the update vector $\Delta x^{(k)} = x^{(k+1)} - x^{(k)}$ can be calculated by solving the set of equations

$$
\Delta x^{(k)} = [H^T(x^{(k)})W^{-1}H(x^{(k)})]^{-1}H^T(x)W^{-1}[Z - F(x)],
$$

(3.11)

also known as the Normal Equations.

WLSE includes the iterative solution to (3.11) and it can be outlined as follows.

1. Set $k = 0$, and assume the starting vector $x^{(0)}$.

2. Calculate the update vector $\Delta x^{(k)}$ using (3.11).

3. If $|\Delta x^{(k)}|_{\infty} \leq \epsilon$, update $x^{(k+1)} = x^{(k)} + \Delta x^{(k)}$ and $k = k + 1$, and go to Step 2.

   Else, stop the estimation: the estimator found the solution vector $x^* = x^{(k)}$, after $k^* = k$ iterations (convergence time). $\epsilon$ is the convergence threshold and $|\cdot|_{\infty}$ denotes the maximum norm of a vector.
3.3. SINGLE-AREA STATE ESTIMATION

Bad Data Detection (BDD)

Large measurement errors may cause the state estimator to find an incorrect solution (a state vector that is far from the actual one), and therefore, should be detected, identified, and to eliminated. Such errors may occur when the meters have bias, drift, and wrong physical connections [2]. Some of the errors are obvious, e.g., negative voltage amplitudes, and can be detected and eliminated a-priori state estimation. Unfortunately, some other errors may not be so easily detectable, and therefore the state estimator needs to be complemented with features that are able to detect and identify any type of bad data. These features depend on the state estimation method, and are referred to as Bad Data Detection (BDD) [2].

After the WLSE obtains a solution, the BDD is done by processing the resulting measurement residuals, i.e., $\Delta Z(k^*) = Z - F(x^*)$. The most commonly used BDD algorithm is the Largest Normalized Residual Test (LNRT) [2, 34]. LNRT identifies the largest element in the normalized residual vector $(\Delta Z(k^*) / ||\Delta Z(k^*)||_2)$, and if that element is larger than a statistical threshold, then the corresponding measurement is assumed as bad data. The threshold can be chosen based on the desired detection sensitivity. After the bad data is identified, the measurement is discarded and the WLSE is started again.

Data Integrity Issues and Proposed Solutions

Measurements used as input to the WLSE are provided by the SCADA infrastructure. The integrity of measurements in face of bit errors is typically provided by an error detection code, e.g., cyclic redundancy check or a cryptographic hash function, calculated at the RTUs, which is sent along with the data. All communication protocols used for the communication with RTUs implement such error detection, as described in Chapter 2, Section 2.1. However, the integrity of measurements in face of malicious manipulation of the data may not been provided (Section 2.1), which leaves the measurements vulnerable to cyber attacks [16].

An attacker that gains access to the SCADA infrastructure could manipulate the measurements sent from the RTUs to the control center. The BDD is supposed to detect inconsistent measurements, but it turns out that the measurements could be manipulated in a such way so that the BDD does not detect it [4, 8, 32]. Such manipulations are usually referred to as stealth attacks on the state estimator.

The manipulation of measurements can be described by an attack vector $a$ added to the actual measurement vector $Z$, i.e.,

$$Z_a = Z + a,$$

where $Z_a$ denotes the measurements after the manipulation. If the attack vector satisfies

$$a = Hc,$$

for some $c \in \mathbb{R}^n$, (3.13)
then BDD will not detect the manipulation, and the vector $a$ is a stealth attack. Hence, if an attacker wants to change a particular measurement $z_i$, it might have to change several other measurements to avoid the BDD.

The difficulty of performing stealth attacks against some measurements has been investigated in [32, 4, 40, 29, 8, 27]. However, a common assumption was that the measurements are delivered directly to the control center, ignoring the actual communication network topology. The characteristics of the SCADA communication infrastructure were considered in [8], where the authors assumed that the measurements are first multiplexed in the substations, and then sent directly to the control center. However, often the measurements visit other substations before they get delivered to the control center due to the topology of SCADA wide area network, described in Section 2.1.

In this thesis, we propose a framework that captures the power system characteristics and the characteristics of the SCADA communication infrastructure in order to estimate the vulnerability of a given system to stealth attacks, and to understand how the stealth attacks can be mitigated using various mitigations schemes. In Paper A, we develop quantitative metrics to assess the importance of substations and communication equipment with the respect to stealth attacks against the state estimation. We use the metrics to evaluate the potential of various mitigations schemes, such as single-path routing, multi-path routing, and data authentication. We consider the data authentication achieved either by encapsulating (or tunneling) the communication through bump-in-the-wire (BITW) devices adjacent to legacy RTUs [42], or by replacing the legacy RTUs with modern RTUs that support message authentication and secure extensions of SCADA/RTU communication protocols (Section 2.1). SCADA system designers and operators can use the framework to evaluate the vulnerability of their systems to the stealth attacks, and to evaluate the efficiency of different mitigation schemes to protect their systems against the attacks.

### 3.4 Multi-area State Estimation

In the case of multi-area state estimation, the power system consists of a number of areas and the state estimation of each area is performed by an independent computing entity. Each entity receives only a subset of all measurements and the part of the transmission network model that correspond to its area. Areas can share buses and transmission lines, so the entities need to coordinate to obtain a consistent state estimate.

There have been many proposed algorithms for multi-area state estimation, e.g., [7, 28, 14, 12, 13, 37, 5, 31, 38, 25]. Typically, the algorithms use the normal equations (3.11), or their modifications, to perform updates within the areas before the coordination [7, 28, 12, 13, 37, 5, 31, 38, 25]. The algorithms can be categorized based on a number of criteria [18]. First, they may differ in the way the coordination is done: in a hierarchical manner, e.g., in [7, 28, 14, 12, 13], or in a distributed
3.4. MULTI-AREA STATE ESTIMATION

manner, e.g., in [37, 5, 31, 38, 25]. Second, they may differ in terms of the time when the coordination is done with the respect to the iterations of the areas’ local state estimators. The coordination can be done after each iteration, e.g., in [28, 14, 5, 31, 38, 25], or after a number of iterations, e.g., in [7, 12, 13]. Third, they may differ in the assumption on the shared buses and transmission lines between areas. Some assume that areas share only transmission lines [28, 14, 13, 5, 38, 25], while others that the areas share only buses [7, 12, 37, 31], or both transmission lines and buses. For a detailed overview of multi-area state estimation algorithms and their categorization, we refer to [18].

Hierarchical Multi-Area State Estimation

In a hierarchical architecture, there exists a central unit that supervises the entities, and subsequently, coordinates the estimates performed by the entities. The entities communicate only with the central unit. The estimation can be considered as a two step process. In the first step, areas perform independent local calculations using their best knowledge of the state estimates of the other areas. In the second step, the central processor coordinates the solutions obtained by areas until a consistent state estimate is found. The steps may be cyclically repeated a number of times before a solution is found.

Fully Distributed Multi-Area State Estimation

In a fully distributed architecture, the areas directly communicate among each other in order to obtain a consistent state estimate. The estimation can be considered as a two step process, similarly to the hierarchical architecture. The only difference is in the second step: the areas coordinate among themselves. They exchange their most recent estimates of the state variables that correspond to the shared buses [38, 25]. The exchanged values are later used when the first step is repeated [38, 25]. The exchange may be synchronous, in which case the steps are synchronized among the areas, or asynchronous [38]. In the asynchronous case, it might be hard to guarantee that a solution will be found [38].

Data Integrity Issues and Proposed Solutions

It is expected that the integrity of the data exchanged between the computing entities is protected. However, in the case of an interconnected power system operated by independent system operators, the integrity of data exchanged between the operators may get violated, as described in Chapter 2, Section 2.2.

In this thesis, in Paper B, we study how a violation of the integrity of data exchanged between independent computing entities can effect the fully distributed multi-area state estimation. We consider an attacker that compromises a single computing entity and manipulates with the date sent from and to the entity. We define various attack strategies that differ in the attacker’s knowledge of the system.
We show that the attack strategies can significantly disturb the state estimation: they can prevent the state estimator to find a solution, or they can lead the state estimator to an erroneous solution. Moreover, our results emphasize the importance of protecting the confidentiality of the measurements: the attacker can perform significantly stronger attacks if it knows the measurements. We also show a possible way to detect the convergence problems, e.g., caused by the attacks, and a simple mitigation scheme.
Chapter 4

Summary of original work

Paper A: Network-aware Mitigation of Data Integrity Attacks on Power System State Estimation


Summary: In this paper we investigate the vulnerability of single-area power system state estimation to attacks performed against the communication infrastructure used to collect measurement data from the substations. We propose a framework that captures the power system characteristics and the SCADA communication infrastructure, and define security metrics that quantify the importance of individual substations and the cost of attacking individual measurements. We also propose approximations of these metrics, that are based on the communication network topology only, and we compare them to the exact metrics. We provide efficient algorithms to calculate the security metrics. We use the metrics to show how various network layer and application layer mitigation strategies, like single and multi-path routing and data authentication, can be used to decrease the vulnerability of the state estimation. We illustrate the efficiency of the algorithms on the IEEE 118 and 300 bus benchmark power systems.

Contribution: The author of this thesis developed the framework in collaboration with the third co-author, defined the metrics, implemented and carried out the simulations, and analyzed the resulting data. The article was written in collaboration with the third co-author. The second and the forth co-authors developed the efficient algorithms to calculate the security metrics.
CHAPTER 4. SUMMARY OF ORIGINAL WORK

Paper B: On the Security of Distributed Power System State Estimation under Targeted Attacks


Summary: In this paper we investigate the vulnerability of fully distributed multi-area power system state estimation to attacks against data exchange between independent computing entities, e.g., control centers of an interconnected power system. We consider an attacker that compromises a single control center and manipulates the data exchanged between the control center and its neighbors. We describe five attack strategies, and evaluate their impact on the IEEE 118 benchmark power system. We show that even if the state estimation converges despite the attack, the estimate can have up to 30% of error, and bad data detection cannot locate the attack. We also show that if powerful enough, the attack can impede the convergence of the state estimation, and thus it can blind the system operators. Our results show that it is important to provide confidentiality for the measurement data in order to prevent the most powerful attacks. Finally, we discuss a possible way to detect and to mitigate these attacks.

Contribution: The author of this thesis defined the attack strategies and the detection method in collaboration with the second co-author, implemented and carried out the simulations, and analyzed the resulting data. The article was written in collaboration with the second co-author.

Paper C: Traffic Analysis Attacks in Anonymity Networks: Relationship Anonymity-Overhead Trade-off


Summary: In this paper we study how anonymity networks can be used to improve data availability in face of targeted denial-of-service attacks. Anonymity networks conceal the sender and the receiver of every message, i.e., provide relationship anonymity, through message relaying. Higher relationship anonymity implies that it is harder for an attacker to identify the sender and the receiver of a message, and therefore, harder for the attacker to perform targeted denial-of-service attacks. However, provided relationship anonymity comes at the price of increased communication overhead and delay due to the message relaying. Since some applications, e.g., fully distributed multi-area power system state estimation, require timely data delivery, in this work we investigate how to optimize the relationship anonymity for a given overhead and delay. We use two anonymity networks: MCrowds, an extension of Crowds, which provides unbounded communication delay and Minstrels, which provides bounded communication delay. We derive exact and approximate analytical expressions for the relationship anonymity for these networks. Using
MCrowds and Minstrels we show that, contrary to intuition, increased overhead does not always improve anonymity. We investigate the sensitivity of provided relationship anonymity to the mis-estimation of the attacker’s capabilities, and show that it is better to overestimate than to underestimate the attacker’s capabilities when configuring anonymity networks.

**Contribution:** The author of this thesis defined the two anonymity networks in collaboration with the second co-author, derived the analytical expressions for the relationship anonymity for these networks, implemented and carried out the simulations, and analyzed the resulting data. The article was written in collaboration with the second co-author. The work was supervised by the third co-author.

**Publications not included in the thesis:**


Chapter 5

Conclusions and Future work

This thesis addresses data integrity and availability issues in power system communication infrastructures. In the following, we summarize the main contributions of this thesis, and we outline some possible directions for future work.

We developed a framework and proposed security metrics that can be used to evaluate the security of a power system against stealthy attacks on measurements. We provided algorithms to calculate the metrics, and proposed approximations of the metrics, that only consider the communication topology, and therefore, are easier to calculate. We provided an algorithm that could be used to improve the security of the system by applying simpler mitigation strategies, e.g., rerouting, or more involved mitigation strategies, such as multi-path routing and cryptographic protection. Our results emphasized the importance of considering both the communication infrastructure and the power system applications, particularly power system state estimation, when analyzing and improving the security of the system.

We investigated the vulnerability of fully distributed multi-area state estimation (described in Section 3.4) to attacks against the integrity of data exchanged between independent computing entities. We described five attack strategies for sophisticated manipulation of the exchanged data, that differ in the attacker’s knowledge of the system. We showed that the attacks can result in high estimation errors, or disable the state estimation by preventing it from finding a solution. Moreover, our results emphasize the importance of protecting the confidentiality of measurements used for the state estimation, since the attacker can perform more effective attacks by knowing the measurements. We also proposed a detection scheme that could detect such attacks. The detection scheme relies on properties of the algorithm used for the state estimation to detect convergence problems. Based on this detection scheme, we proposed a simple mitigation scheme: upon detecting an attack, the independent entities perform isolated state estimation (without exchanging any data).

Finally, we studied how data availability in power system communication infrastructures could be improved by anonymity networks. Since anonymity net-
works increase message delay, which could be an issue for power system applications that require timely message delivery, we studied the trade-off between the provided anonymity and the message delay. We found that, contrary to intuition, the anonymity is not always improved with more delay. Moreover, we show that it is better to overestimate than to underestimate the attacker’s capabilities when configuring an anonymity network.

Future Work

There are a number of different possibilities for future work. Some of them are complement studies to the studies included in this thesis, while other studies could address some aspects of data integrity and availability in power system communication infrastructures not covered in this thesis. We outline some of the possibilities as follows.

Data integrity

We developed a framework and security metrics that evaluate the security of the power system state estimation against attacks on the data integrity of RTU to SCADA server communication. A complement study could analyze the robustness of the metrics to changes in the power system transmission network topology, as well as to random errors. Moreover, attacks on the data integrity of RTU to SCADA server communication could be also targeted against control messages used to remotely operate control relays. Similar security metrics, and a framework that includes the same model of communication infrastructure complemented with a model of the physical system could be developed to consider such attacks.

We investigated how attacks on data integrity of ICCP data could affect the fully distributed multi-area state estimation. We proposed a detection scheme that could detect such attacks, and outlined a simple mitigation scheme. However, the detection scheme could be improved so that the attack can be localized. Such localization could lead to an improved mitigation scheme. Moreover, attacks on data integrity of ICCP data could be targeted against data used by other power system applications. An open question if such attacks could also disturb those applications.

Data availability

We studied how anonymity networks could be used to improve the data availability against targeted DoS attacks, while keeping message delay low. Studies on how targeted DoS attacks could affect power system applications that require timely data delivery, such as fully distributed multi-area state estimation, could help in finding a good balance between the improved data availability and the increased delay.
Furthermore, a subject of future work could be to address the data availability in communication networks used for the acquisition of PMU measurements. The frequency at which a PMU takes and delivers measurements is selectable, and it may go up to 120Hz. A communication network that acquires measurements from many PMUs at such frequency could experience congestion and losses. Therefore, it is important to understand how congestion could affect the PMU data delivery, and furthermore, to find schemes that would optimally control message generation rate for every PMU in the network so that the losses are minimized.
Bibliography


33


