DOCTORAL THESIS IN ELECTRICAL ENGINEERING
STOCKHOLM, SWEDEN 2014

Cyber-security in Smart Grid Communication and Control

OGNJEN VUKOVIĆ

KTH ROYAL INSTITUTE OF TECHNOLOGY
SCHOOL OF ELECTRICAL ENGINEERING

Cyber-security in Smart Grid Communication and Control

OGNJEN VUKOVIĆ

Doctoral Thesis
Stockholm, Sweden, 2014

TRITA-EE 2014:039
ISSN 1653-5146
ISBN 978-91-7595-250-5

School of Electrical Engineering
KTH, Stockholm, Sweden

Akademisk avhandling som med tillstånd av Kungl Tekniska högskolan framlägges till offentlig granskning för avläggande av doktorsexamen tisdag den 7 Oktober 2014 i Hörsal F3, KTH, Stockholm.

© Ognjen Vuković, October 2014

Tryck: Universitetsservice US AB

Abstract

Society is increasingly dependent on the reliable operation of power systems. Power systems, at the same time, heavily rely on information technologies to achieve efficient and reliable operation. Recent initiatives to upgrade power systems into smart grids target an even tighter integration with information technologies to enable the integration of renewable energy sources, local and bulk generation and demand response. Thus for the reliable operation of smart grids, it is essential that its information infrastructure is secure and reliable in the face of both failures and attacks. This thesis contributes to improving the security of power systems against attacks on their information infrastructures. The contributions lie in three areas: data integrity, data confidentiality, and data availability of power system applications.

We analyze how characteristics of power system applications can be leveraged for detection and mitigation of data integrity attacks. We consider single and multi-area power system state estimation. For single-area state estimation, we look at the integrity of measurement data delivered over a wide area communication network. We define security metrics that quantify the importance of particular components of the communication network, and that allow us to optimize the deployment of network, transport and application layer security solutions. For multi-area state estimation, we look at the integrity of data exchanged between the control centers of neighboring areas in face of a targeted trojan that compromises an endpoint of the secure communication tunnel. We define multiple attack strategies and show that they can significantly disturb the state estimation. Moreover, we propose schemes that could be used for detection, localization, and mitigation of data integrity attacks.

We investigate how to provide data confidentiality for power system applications when they utilize cloud computing. We focus on contingency analysis and propose an approach to obfuscate information regarding power flows and the presence of a contingency violation while allowing the operator to analyze contingencies with the needed accuracy in the cloud. Our empirical evaluation shows that the errors introduced into power flows due to the proposed obfuscation are small, and that the RMS errors introduced grow linearly with the magnitude of obfuscation.

We study how to improve data availability in face of gray hole attacks combined with traffic analysis. We consider two cases: SCADA substation to control center communication using DNP3, and inter-control center communication. In the first case, we propose a support vector machine-based traffic analysis algorithm that uses only the information on timing and direction of three consecutive messages, and show that a gray hole attack can be effectively performed even if the traffic is sent through an encrypted tunnel. We discuss possible mitigation schemes, and show that a minor modification of message timing could help mitigate the attack. In the second case, we study how anonymity networks can be used to improve availability at the price of increased communication overhead and delay. We show that surprisingly availability is not always improved with more overhead and delay. Moreover, we show that it is better to overestimate than to underestimate the attacker's capabilities when configuring anonymity networks.

The progressive development of man is vitally dependent on invention. It is the most important product of his creative brain. Its ultimate purpose is the complete mastery of mind over the material world, the harnessing of the forces of nature to human needs.

Nikola Tesla

Acknowledgments

I would like to thank my main advisor Assoc. Professor 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 am proud to have had him as my advisor. I would also like to thank my second, but originally main advisor, Professor 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 priceless to me. They were always an endless source of energy and inspiration. I want to personally thank: Zargham, for his invaluable friendship, and for always being a source of cheerfulness, motivation and support. Stavros and Sylvia, for being great friends and very supportive. Vladimir, Ljubica, Marin, and Vedran, my Serbian connection at KTH in Stockholm, for going through this journey together. I am happy to thank Elena for her precious support, understanding, patience, for always knowing how to cheer me up, and for always being there for me.

I am greatly thankful to my family: želeo bih da se zahvalim svojoj mnogobrojnoj porodici, čiju sam podršku svakodnevno osećao i koja mi je izuzetno značila. Zahvalan sam na našim okupljanjima u domovini kao i u Stockholmu, koja su mi uvek bila izvor radosti i davala dodatnu snagu. Ceo ovaj period bili su mi neiscrpan izvor energije i pružali osećaj da smo tako blizu, iako u stvarnosti prilično daleko. Posebno bih izdvojio svoju majku Milku i sestru Jovanu i zahvalio im se za njihovu neizmernu podršku, ljubav i razumevanje. Njima dvema posvećujem ovu tezu.

Contents

Chapter 1

Introduction

The electric power system is a network of components that generate, deliver, and consume electrical energy. The power produced by electric generators is delivered to loads through power system transmission and distribution networks. Transmission networks transfer the energy over long distances, and they may contain a large number of substations interconnected by transmission lines. In order to minimize the energy loses, the electrical energy is transmitted at high voltages, typically ranging from 100 kV to 500 kV [62]. 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 [62]. 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 [62].

Traditionally, power systems have been unidirectional hierarchical systems, where the generators ensure energy supply through the transmission and distribution networks to the loads often without any real-time information about the service parameters of the loads [25]. Consequently, generators are dimensioned to withstand anticipated peaks in demand by the loads, and as the peaks rarely occur, the system is inherently inefficient [25]. Furthermore, to meet the rapid increase in demand for the electrical energy, the system will operate closer to its capacity limits, which calls for more intelligent monitoring and control. To address these shortcomings, the new concept of smart grid has emerged with the idea to provide the system operators with remote real-time monitoring and control, and to allow smooth integration of renewable sources of energy, such as wind, solar, and biomass, so that the system is more efficient, stable, and resilient to anomalies [4, 39, 25, 46]. However, due to the size of the existing systems, one can easily see that smart grids cannot be an immediate replacement; instead, they will coexist with the existing power systems, adding more functionalities and capabilities with new technologies, but keeping full backward compatibility with the existing legacy systems.

A key factor in keeping the power system stable and efficient is its information infrastructure. The information infrastructure includes a system for remote monitoring and control, called Supervisory Control And Data Acquisition (SCADA) system, a suit of applications used to operate the power system, called Energy Management System (EMS), power system communication infrastructure, and computational and storage resources. The SCADA system acquires telemetry data and provides control of remote equipment, and therefore, it relies on the power system communication infrastructure to deliver messages over wide area networks [53]. The EMS includes applications such as state estimation, used to estimate the state of the system based on imperfect measurements [55], and contingency analysis, used to evaluate how an outage would affect the system, and it requires reliable and on-time computational and storage resources. The information infrastructure is essential for realization of the smart grid [31]; it is required to enable real-time monitoring and control as well as forecast and planing. The requirements of the smart grid put higher demands on communication and computation resources as a significantly larger amount of data will be generated, e.g., due to increased number of sensors and more frequent reporting, and that data need to be communicated, stored, and further analyzed within a short time frame [31]. Thus, it is important to find suitable communication and computation infrastructure to handle the demands. Some advanced technologies and applications, such as cloud computing, might be adopted [15].

As proper functioning of information infrastructure is crucial for power systems, the information infrastructure should be secure and reliable both in the face of failures and in the face of attacks. Security of information infrastructures has three aspects: data integrity, data confidentiality, and data availability [54]. Data integrity protects the data against unauthorized generation and modification, and it can be achieved by message authentication codes. Data confidentiality protects the privacy (readability) of the data against unauthorized users, and it can be achieved by data encryption or obfuscation. Finally, data availability ensures data accessibility without excessive delay.

Traditionally, security and reliability of power systems have been achieved by isolating the information infrastructure, and by protecting the system design and implementation. However, the power system information infrastructure is becoming more and more integrated with other information infrastructures, such as the public Internet and potentially cloud computing. Moreover, some parts of the system design, e.g., the communication protocols and application algorithms, 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 information infrastructures. However, due to the size of the systems, it may be economically and practically unfeasible to protect the entire system. Furthermore, the integration with other information infrastructures may leave the system open to unforeseen threats. Therefore, it is important to evaluate the security of both the existing power system and the future smart grid.

This thesis addresses a number of problems related to integrity, confidentiality and availability of power system information technologies. The objectives are described as follows.

- Integrity: we investigate how violations of data integrity in the power system communication infrastructure can affect power system applications, in particular power system state estimation.
- Confidentiality: we investigate how to provide data confidentiality for power system applications when they utilize cloud computing, in particular the contingency analysis.
- Availability: we analyze how data availability can be improved using anonymity networks. Furthermore, we analyze susceptibility of encrypted SCADA communications to gray hole attacks, and consider various mitigation schemes.

The structure of this thesis is as follows. In Chapter 2, we discuss power system communication and computation technologies, and elaborate on data integrity, data confidentiality, and data availability provided by the technologies. In Chapter 3, we discuss power system applications and describe in details power system state estimation and contingency analysis. Furthermore, we discuss how a violation of data integrity can affect the state estimation, and how to provide data confidentiality for contingency analysis when the computation is performed in the cloud. Chapter 4 provides a summary of the papers included in this thesis along with the contributions of the author of this thesis to the each paper. Chapter 5 summarizes the main findings and conclusions, and outlines potential directions for future research.

Chapter 2

Power System Communication and Computation Technologies

Power systems rely heavily on their communication and computational infrastructures to achieve a secure and reliable operation [56]. The communication infrastructure connects 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 to control the system [6], and a core component of Phasor Networks, where Phasor Data Concentrators aggregate measurements from Phasor Measurement Units (PMUs). Furthermore, the communication infrastructure connects the control centers of interconnected power systems in order to improve operational efficiency and system stability. The connection between control centers 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.

The computational infrastructure enables Energy Management System (EMS), a suit of applications used to securely and to efficiently operate the power system. Examples of such applications are power system state estimation and contingency analysis. Traditionally, the EMS operates centrally within the control center of a power system operator and utilizes the local computational infrastructure in the control center. However, when large amount of acquired data has to be promptly processed for online operation decision support, e.g., on-line contingency analysis, computing resources provided by the computational infrastructure can become the limiting factor, and could impede the execution of computationally heavy algorithms [33]. Furthermore, as the smart grid is expected to increase both the size and the complexity of power systems and to impose stricter latency requirements on EMS applications, the centralized operation and computation will no longer be scalable [42]. Therefore, the computational infrastructure may need to adopt a distributed architecture and may have to embrace new technologies in order to meet the demands [42]. An example of such technologies is cloud computing, which

could provide the ability to occasionally scale computation as needed as well as to make the storage, management and the exchange of data much easier [15].

2.1 SCADA Systems

The SCADA system delivers information from sensors and relays through Remote Terminal Units (RTUs) to SCADA severs, and delivers control messages from SCADA servers through RTUs to relays. Sensors provide measurements of power flows, voltages and currents. Relays control breakers in order to open or to close a line if a fault is detected (protective relays), or to reconfigure a circuit on demand by remote control (control relays). RTUs collect measurements from the sensors, monitor the status of protective relays, and 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.

SCADA WAN

The types of WANs used for the communication between RTUs and SCADA servers can include point-to-point connections over dedicated or shared lines. In the case of dedicated lines, such as serial links, 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 one line per RTU needs to be built or leased. In the case of shared lines, there is a number of RTU to SCADA server connections that utilize the same line. In order to avoid collision between the connections, a telecommunication network based on virtual circuit, packet or cell switching is implemented. Circuit switched networks provide dedicated communication channels (circuits) 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., Public Switched Telephone Network (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, as smart grid technologies, with a growing number of interconnected devices used for monitoring and controlling, impose increasing demands in capacity and in reachability from the communication infrastructure, it may become 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 [13]. 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 [13]. 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 [53]. IEC 60870-5 is the foundation 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 the Americas, South Africa, Asia, and Australia [13].

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 [53]. 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 [53]. 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.

Transmission Modes

IEC 101 supports unbalanced and balanced transmission modes. In the unbalanced mode, only the server can initiate a message exchange. The server polls a remote station, and the station responds with data. In the balanced mode, both the server and the remote stations can initiate data exchange. The remote station can initiate the exchange if, e.g., a measured value has significantly changed since the last reported value.

Addressing

IEC 101 uses the FT1.2 frame format defined in IEC 60870-5-1 [13]. The FT1.2 frame format has three forms: variable-length frame format for bidirectional data transmission, fixed-length frame format for commands or acknowledgments, and a single character frame only for acknowledgments. The structures of the three forms of the FT1.2 frame are given in Figure 2.1 (based on [13]). IEC 101 provides addressing on the data link layer through the link address field in the FT1.2 frame format [13]. 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.

Reliability

The detection of frame losses or duplication is achieved through a Frame count bit that alternates between 0 and 1 for sequential frames, and it is a part of the Link control field. The frame count bit is used only for the direction from the server to remote stations.

IEC 101 provides detection of bit transmission errors through a checksum provided by FT1.2 [13]. FT1.2 uses an 8-bit checksum calculated as the modulo 256 sum of the link layer data [13], 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 indicates a transmission error, the data are discarded and a retransmission is requested. However, it may happen that many bit errors occur so

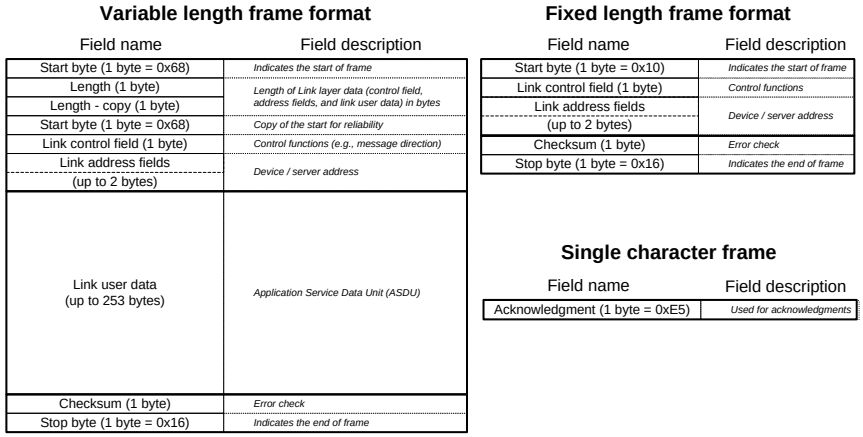

Figure 2.1: Three FT1.2 frame forms used by IEC 101. The figure is based on [13].

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, which is called the Hamming distance. If the number of single bit errors is larger than the Hamming distance of a checksum, the checksum may not detect the errors. The Hamming distance of the checksum used by the IEC 101 frames is equal to 4 [13].

IEC 60870-5-104 (IEC 104)

With the increasing usage of packet switched networks instead of circuit switching networks, IEC 101 needed to be changed to support packet switching. The modification came in the form of the IEC 104 standard, published in 2000 [13, 53]. The application layer of IEC 104 is based on IEC 101, but some data types and functions are no longer used and supported. Consequently, IEC 104 supports the same transmission modes as IEC 101.

Addressing

IEC 104 relies on TCP [35] and IP [34] as transport and network protocols, and it does not impose any limitations on the data link layer and the physical layer protocols. Therefore, IEC 104 does not provide any addressing under the application layer.

Reliability

IEC 104 relies on underlying protocols for detection of bit transmission errors. TCP uses a 16-bit checksum (the bitwise complement of the sum of 16-bit words added using one's complement arithmetic [35]) 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 developed in the early 1990s by Harrison Controls Division based on some early versions of the IEC 60870-5 standard [13, 53]. 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 [21].

Transmission Modes

DNP3 supports only balanced transmission mode (both server and client can initiate the exchange). The server sends polling messages and the client replies immediately with all data. The client can initiate the exchange in case of some sudden changes, e.g., some measured values get significantly changed since the last report. Between the data link layer and the application layer, DPN3 defines the pseudo-transport layer to allow transmission of larger blocks of application data by fragmenting [13].

Addressing

The DNP3 frame format is based on the FT3 frame format defined in IEC 60870-5-1 [13]. FT3 frame format has variable length, and its structure is shown in Figure 2.2 (based on [13]). 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.

Reliability

DNP3 controls the communication flow, and is able to detect lost frames and duplicates through a sequence number located in the control header of link user data. The sequence number can have a value from 0 to 15 for requests, outstation responses, and from 16 to 31 for unsolicited responses and confirmations. Confirmations have the same sequence number as the request or the response.

DNP3 can detect bit transmission errors using 16-bit cyclic redundancy check (CRC-16) checksum [13]. There is one CRC-16 checksum for the frame header, and thereafter one for every block (max 16 bytes) of user data [13] (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 is equal to 6 [13], 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 checksum per every block of 16 bytes of user data.

Secure extensions of IEC 101, IEC 104, and DNP3

IEC 101, IEC 104, and DNP3 do not provide any of the three security aspects: data confidentiality, data integrity, and data availability. With increasing cyber security

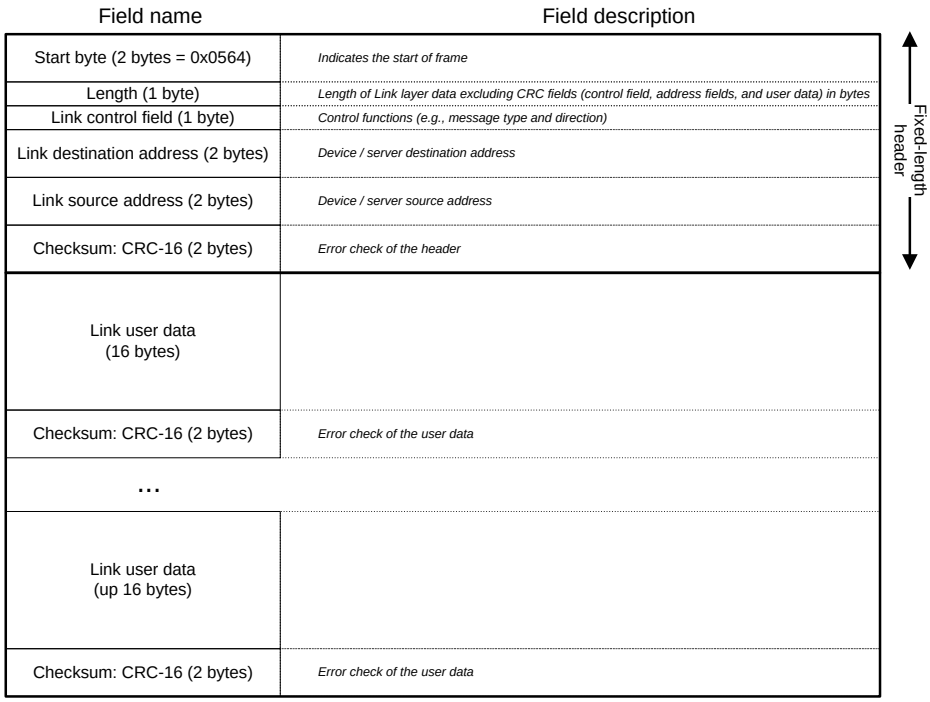

Figure 2.2: DNP3 frame format. The figure is based on [13].

concerns in SCADA systems, IEC 101, IEC 104, and DNP3 needed to be upgraded to address the security concerns. The highest priority was put on 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 [27, 29]. Researchers and the industry have been proposing different solutions to upgrade the protocols. The most distinguished results are the standard IEC 62351-5 [38] by IEC TC 57 and the standard DNP3 Secure Authentication (DNP3 SA) [21] 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 compatible [29]. Both IEC 62351-5 and DNP3 SA focus on data integrity, while data confidentiality is provided only for the key-exchange messages.

IEC 62351-5 [38] defines the security standards for IEC 60870-5, including IEC 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 rely on 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, which 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 data integrity, and utilize Transport Layer Security (TLS) version 1.0 [19] to provide data confidentiality.

DNP3 SA [59] 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 [21]. To protect data integrity, DNP3 SA uses the challenge-response mechanism described in the IEC 62351-5 standard [38], and utilizes TLS version 1.0 [19] to protect data confidentiality.

Challenge-response mechanism used by IEC 62351-5 and DNP3 SA

The challenge-response mechanism 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 [59]. The challenge-response mechanism can be described as follows [59]. Upon receiving a message, the recipient (challenger) decides whether the data in the message are of critical importance. If not, the message is processed without any verification. However, if the data are of critical importance, 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 sent 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 the 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 management 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 to remotely change the keys [59].

TLS, used by IEC 62351-5 and DNP3 SA to protect data integrity through encryption, relies on digital certificates, encryption, and MAC. IEC 62351-5 and DNP3 SA specify the requirements for the digital certificates, such as application of the certificates, and the procedures for their revocation based on Certificate Revo-

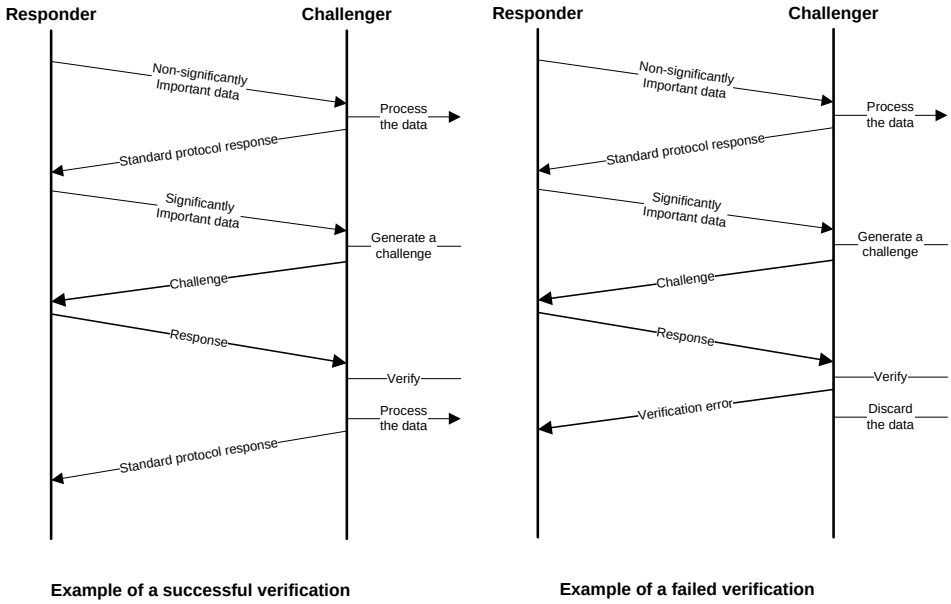

Figure 2.3: Examples of the challenge-response mechanism. The figure is based on [59].

cation Lists (CRL). However, the generation, and provisioning (including the initial distribution) of the certificates remain underspecified [27]. They are acknowledged by IEC as important, and could be a part of future standard extensions [27]. IEC 62351-5 and DNP3 SA manage the keys used by TLS similarly as the keys used by the challenge-response mechanism.

Data Integrity and Availability 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 [22]. 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 [54]. 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 [22].

A cyber attack on the SCADA communication infrastructure may result in manipulation of the data exchanged between RTUs and the SCADA server. If the protocols IEC 101, IEC 104 over TCP/IP, and DNP3 are utilized without any additional cryptographic protection, 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 [49].

Clearly, the communication needs to be cryptographically protected in order to protect the SCADA system against data integrity attacks on the messages exchanged between RTUs and the SCADA server. Cryptographic protection can be provided by encapsulating (or tunneling) the protocols (IEC 101, IEC 104, and DNP3) into a protocol that provides cryptographic protection [22], e.g., IPsec [41] or TLS [19], or by using the recent protocol extensions that provide message authentication: IEC 62351-5 [38] and DNP3 SAv5 [21]. The most important difference between the two is that, unlike IEC 62351-5 and DNP3 SAv5, tunneling appends a MAC to each message and thereby protects the integrity of every message, but at the cost of increased bandwidth and processing requirements. 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, which do not have sufficient processing power, would need to be replaced or supplemented by bump-in-the-wire (BITW) devices [60]. BITW is an approach where a network security mechanism is transparently implemented outside the devices whose communication is being protected. In the case of SCADA system, one hardware module (BITW device) is positioned next to a legacy RTU and it tunnels the communication between the RTU 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, the upgrade 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 in order to help in evaluating and improving data integrity protection. The framework can be used in every stage of the upgrade to prioritize the RTUs to be cryptographically protected. The framework is described in Paper A, which extends our earlier work [65]. We use the framework to evaluate and to improve the security of power systems considering power system state estimation. Our results show that power system state estimation could be secured by upgrading only a small subset of all RTUs in the system.

Once cryptographic protection is applied to protect data integrity and confidentiality, one might expect that it would also make it impossible for an attacker to identify and to drop mission critical measurement and/or control messages without dropping all messages, and thus remain undetected or difficult to be detected. However, the strict timing rules used in the SCADA communication protocols, such as immediate client responses to master station's polling messages, might facilitate traffic analysis attacks and consequently allow the attacker to perform gray hole attacks.

In this thesis, we address the vulnerability of SCADA communication to a gray hole attack when cryptographic protection is applied. The vulnerability to a gray hole attack is investigated in Paper F, where we show through the example of DNP3 that targeted gray hole attacks may be feasible despite sending messages through an encrypted tunnel. We propose a support vector machine based traffic analysis attack, which is computationally simple and is based on the inter-arrival times and directions of consecutive encrypted messages, and show that an attacker would not need exact knowledge of system parameters for a successful attack. We also discuss potential mitigation schemes, and show that the attack can be mitigated by relaxing the strict timing rules, e.g., by introducing a random delay before answering to DNP3 poll messages.

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 the 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 [66]. The exchange of real-time data between control centers is expected to be even more frequent in future power systems [66].

Historically, power system operators relied on proprietary protocols for inter-control center communication [17]. 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 the international IEC 60870-6 standard based on the OSI model, and submitted it to the IEC for standardization [66]. 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 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) [56].

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 bilateral 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 [36] and IEC 62351-4 [37] 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 TLS protocol [20] that should be configured by the operators. It also considers IPsec [41], but TLS is preferred [36]. IEC 62351-4 specifies security measures for protocols that use MMS, and provides application layer security: prevents unauthorized access to information through authentication [37]. 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 [36, 37].

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), also referred to as the control LAN, where all critical applications (e.g., SCADA server and EMS) coexist [51]. 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 [51]). 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 the case of ICCP, the lack of trust typically comes from the fact that the WAN may be insecure and that the other end may be compromised [51].

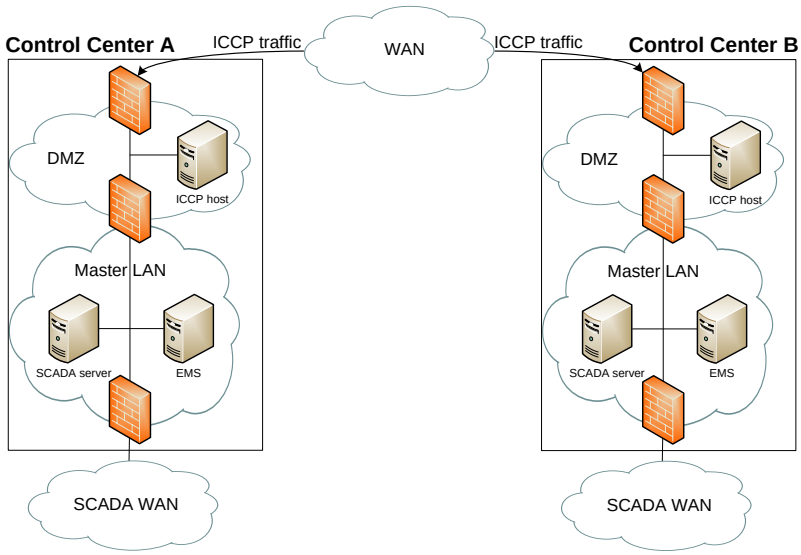

Figure 2.4: Inter-control center communications. The figure is based on [51].

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 transfered 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 an ICCP host, the ICCP data might be unprotected after the TLS protection is removed and before the data are 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 [57]. The manipulation of ICCP data could disturb the power system applications that rely on the data exchanged by ICCP.

In this thesis, we address this issue. In Paper B, we study how an attack against the integrity of ICCP data can affect 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 on a well established fully distributed multi-area state estimator, that they can disable the state estimation. We also show a possible way to detect the attacks.

In Paper C, which extends our earlier work [63], we show that the attacks can even disable a state of the art fully distributed state estimator. We propose an

attack detection algorithm based on the properties of the state estimator algorithm and based on the exchanged data. Furthermore, we propose an attack localization and mitigation algorithm based on the consensus of the beliefs of the individual regions about the attack location, and show that strong attacks can often be localized and mitigated faster than weak attacks.

Second, TLS protects data integrity and provides confidentiality for the transmitted data, but it does not protect against denial of service attacks [36, 37]. An attacker that obtains access to the WAN may identify some critical low latency data exchange by observing the size, and the sender and the receiver addresses of every message, and it may perform a targeted denial-of-service attack, i.e., a gray hole 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, in Paper E which extends our earlier work [64], we study how anonymity networks could be used to improve the data availability if face of gray hole 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. Furthermore, increased traffic overhead may result in additional costs. 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 before reaching the destination, and the traffic overhead by the number of times the data are relayed in total. Our results show that, surprisingly, the availability does not always get improved with additional delay or traffic overhead. Moreover, we show that it is better to overestimate than to underestimate the attacker's capabilities when dimensioning anonymity networks.

2.3 Cloud Computing in Power Systems

Cloud computing is a new paradigm for computing technology that provides on-demand network access to shared metered computing resources [32, 5]. It provides a flexible mechanism for offering end users a variety of services, from hardware to application level, so that the users can utilize the computing resources in a completely customizable execution environment [61]. There are three common deployment models of Cloud computing: private cloud, public cloud, and hybrid cloud. Private cloud is a cloud infrastructure exclusively operated and utilized by a single user, and it can provide a high level of data security and privacy but at the price of high initial and unpredictable operating costs. Public cloud is, on the other hand, a cloud infrastructure owned and operated by a third party, such as Amazon AWS, Google, and Microsoft, that provides many users with access to comput-

ing resources via Internet. Consequently, users face little to none initial costs and predictable operating costs, but at the price of no guaranteed data security and privacy. Hybrid cloud is a composition of a number of clouds that can include both public and private clouds in order to offer the benefits of both deployment models.

Power systems could greatly benefit from cloud technology, which can provide reliable data storage and meet the computational demands by applications with time-varying computational needs [15]. Power system operators maintain huge databases of past system states in order to enable reconstructions of events in case of system failures, and to improve operational efficiency through data mining. Traditional SCADA systems generate a few thousands data points a few times per minute which results in around 100TB of data per year [15]. With recent implementations of PMUs that can provide data points 30 times per second, the amount of data to be stored increases drastically. Furthermore for reliability reasons, the stored data are replicated at various locations. Cloud-based data storage could be a cost-efficient solution for storing such large quantities of data.

Many EMS applications used in planing and operation have time-varying computational needs [15]. They are either used periodically/occasionally with high computational demand, or they are used continuously but the computational demand depends on the actual system state that changes with time. An example of such applications is Contingency Analysis (CA) used to identify whether one or more contingencies (failures of system components) from a set of considered contingencies would render the system unstable. A set of considered contingencies depends on the instantaneous load of the power system, the higher the load the more contingencies might need to be considered, and is in practice limited by the capacity of the computational infrastructure in the control center. CA involves solving a non-linear weighted least squares (WLS) estimation problem using an iterative algorithm, and is performed every time the system state is recalculated, which can be as often as once a minute. CA that utilizes cloud computing could allow a power system operator to freely scale the number of considered contingencies based on the system state.

Data Security Issues and Proposed Solutions

Perhaps the most significant issue for utilizing cloud computing in power systems is the fact that for a certain amount of time the control over data and data processing leaves the physical and the electronic security perimeter of the power system operator [3]. To overcome the issue, all three aspects of data security (availability, integrity, and confidentiality) must be preserved while the data is out of the security perimeter.

The security aspects must be preserved while data are being communicated to the cloud infrastructure as well as while data are being stored and processed in the cloud infrastructure. Data availability of real-time applications might be altered by the communication network connecting the security perimeter and the cloud infrastructure if the network is unreliable or introduces large delay. Furthermore, the

response time of the cloud infrastructure must fit in an acceptable time span so that the functionality of real-time applications is not hampered. While it may be acceptable to leave data in the clear when they are stored within the security perimeter, the data have to be cryptographically protected while being communicated to and stored at the cloud infrastructure so that data integrity and confidentiality are guaranteed. However, if the data need to be processed within the cloud infrastructure, e.g., by a power system application that utilizes cloud computing, cryptography is typically not applicable without affecting the outcome of the processing. In such a case, data integrity and confidentiality might be at risk to get compromised by other users utilizing the same cloud computing infrastructure.

One potential approach to protect data confidentiality is to use homomorphic encryption [11, 10], which is a form of encryption that allows specific types of computations to be carried out on encrypted data and generate an encrypted result which, when decrypted, matches the result of operations performed on the original data. However, finding an encryption algorithm that would support the required computations is far from trivial for many power system applications as they require solving non-linear optimization problems. Another approach could be to obfuscate the data enough that a potential adversary cannot infer any sensitive system information while keeping any introduced computational errors to the minimum [9].

In this thesis, we address the issue of providing data confidentiality for power system applications that utilize cloud computing. In Paper E, we consider cloud-based contingency analysis and propose an approach to obfuscate system information, including the presence of a contingency violation, while allowing the operator to analyze contingencies with the needed accuracy in the cloud.

Chapter 3

Power System Applications

A power system operates in one of three possible operating states: normal, emergency and restorative [47]. 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 the 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, so that 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.

The state of the power system can be described by a network model and the voltage phasors at power system buses [1]. The voltage phasors are called state variables, and the set of voltage phasors is called the static state of the system [1]. If the collected measurements are the voltage phasors of all buses, then the static state of the system can be directly obtained. However, typically collected measurements are power injections and power flows. Such measurements need to be processed so that the static state of the system can be determined. Moreover, the measurements are prone to errors, and it may not be economically or technically feasible to provide

the measurements of every power flow and power injection in the system. Therefore, the idea of estimating the system state based on the network model and the collected imperfect measurements was proposed in [55]. The ability to estimate the state of the system provides the foundation for the establishment of Energy Management Systems (EMS). EMS is a suit of applications used to operate the power system, and includes applications such as state estimator, used to estimate the state of the system, contingency analysis, used to evaluate how an outage would affect the system, and optimal power flow, used to estimate the optimal power flows based on particular criteria, e.g., minimization of the cost of generation or minimization of transmission line losses.

3.1 Transmission Network Model

Let us 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 [62]. Branches include transmission lines, transformers and phase shifters [1].

The admittance matrix $\mathbf{Y}$ of the entire transmission network can be built from scratch by introducing components one at a time (their models) of the system, and updating the corresponding entries in $\mathbf{Y}$ [1]. The components include transmission lines, loads, generators, transformers, shunt capacitors and reactors. The matrix $\mathbf{Y}$ is complex in general, and can be written as $\mathbf{G} + j\mathbf{B}$, where $\mathbf{G}$ is the conductance matrix and $\mathbf{B}$ is susceptance matrix. For more information about the components and their models, and how the matrix $\mathbf{Y}$ is built, we refer to [1].

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 [1, 52]. Let us denote the vector of bus voltage phasors by $\mathbf{V}$, and the vector of bus current injections by $\mathbf{I}$. Then, in a network of n buses, the nodal equations can be expressed with the following matrix equation,

$$\mathbf{I} = \mathbf{Y} \cdot \mathbf{V}; \quad \begin{bmatrix} I_1 \\ I_2 \\ \dots \\ I_n \end{bmatrix} = \begin{bmatrix} y_{11} & y_{12} & \dots & y_{1n} \\ y_{21} & y_{22} & \dots & y_{2n} \\ \dots & \dots & \dots & \dots \\ y_{n1} & y_{n2} & \dots & y_{nn} \end{bmatrix} \cdot \begin{bmatrix} \mathcal{V}_1 \\ \mathcal{V}_2 \\ \dots \\ \mathcal{V}_n \end{bmatrix}. \tag{3.1}$$

Power injections at any bus can be derived by multiplying the vector $\mathbf{V}$ with the conjugate of the vector $\mathbf{I}$ from (3.1) [62]. Active and reactive power injections can be further derived by considering the real and the imaginary part of equation $\mathbf{V} \cdot \mathbf{I}^*$. The active power injection P_{b_i} and reactive power injection Q_{b_i} at bus b_i

can expressed as

$$\begin{aligned} P_{b_i} &= V_{b_i} \sum_{b_j \in \mathcal{N}(b_i)} V_{b_j}(g_{ij}cos(\theta_{ij}) + b_{ij}sin(\theta_{ij})), \\ Q_{b_i} &= V_{b_i} \sum_{b_j \in \mathcal{N}(b_i)} V_{b_j}(g_{ij}sin(\theta_{ij}) - b_{ij}cos(\theta_{ij})), \end{aligned} \tag{3.2}$$

where V_{b_i} is the voltage amplitude at bus b_i, θ_{ij} is the difference of phase angles between bus b_i and bus b_j, g_{ij} and b_{ij} are the corresponding entries in matrices $\mathbf{G}$ and $\mathbf{B}$, respectively, and $\mathcal{N}(b_i)$ is the set of adjacent buses to bus b_i [1, 62].

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

$$\begin{aligned} P_{b_i b_j} &= V_{b_i}^2(g_{si} + g_{ij}) - V_{b_i}V_{b_j}(g_{ij}cos(\theta_{ij}) + b_{ij}sin(\theta_{ij})), \\ Q_{b_i b_j} &= -V_{b_i}^2(b_{si} + b_{ij}) - V_{b_i}V_{b_j}(g_{ij}sin(\theta_{ij}) - b_{ij}cos(\theta_{ij})), \end{aligned} \tag{3.3}$$

where $g_{si} + jb_{si}$ is the admittance of the shunt branch connected at bus b_i [1].

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 [1]. 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 M measurements that are given by the vector

$$\mathbf{Z} = \begin{bmatrix} z_1 \\ z_2 \\ ... \\ z_M \end{bmatrix} = \begin{bmatrix} f_{z_1}(x) \\ f_{z_2}(x) \\ ... \\ f_{z_M}(x) \end{bmatrix} + \begin{bmatrix} e_{z_1} \\ e_{z_2} \\ ... \\ e_{z_M} \end{bmatrix} = F(x) + e, \tag{3.4}$$

where x is the state vector constructed from the vector $\mathbf{V}$ 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 $\mathbf{W} = E(ee^T)$ is diagonal [1, 52, 62].

3.3 State Estimation

State estimation can be centralized (single-area) or distributed (multi-area). 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 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. 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 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.

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 [1]

$$l_M(\mathbf{Z}) = l(z_1)l(z_2)\cdots l(z_M). \tag{3.5}$$

The function $l_M(\mathbf{Z})$ is referred to as the likelihood function, and it represents the probability of measuring the measurements in $\mathbf{Z}$. It will obtain its peak value when the unknown parameters are chosen to be the closest to the actual values [1]. 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. In order to simplify the maximization problem, the likelihood function is replaced by

its logarithm, the so called Log-Likelihood function, and it can be expressed as

$$\mathcal{L} = \log(l_M(\mathbf{Z})) = \sum_{i=1}^{M} \log(l(z_i)) = -\frac{1}{2}\sum_{i=1}^{M}(\frac{z_i - E(z_i)}{\sigma_i})^2 - \frac{M}{2}\log(2\pi) - \sum_{i=1}^{M}\log(\sigma_i), \tag{3.6}$$

where the measurement error probability distributions are assumed to be Gaussian distributions with the mean value $E(z_i)$ and standard deviation σ_i for the measurement z_i [1]. The expected value $E(z_i)$ can be expressed as $f_{z_i}(x)$, and σ_i is assumed to be known (it equals to the square root of diagonal entry w_{ii} of the covariance matrix $\mathbf{W}$) [1]. Finally, the state vector x can be found by solving the MLE problem defined as

$$\max_x \quad \log(l_M(\mathbf{Z})), \tag{3.7}$$

which is equivalent to

$$J(x) = \min_x \quad \sum_{i=1}^{M}(\frac{z_i - E(z_i)}{w_{ii}})^2 = \min_x \quad [\mathbf{Z} - F(x)]^T\mathbf{W}^{-1}[\mathbf{Z} - F(x)]. \tag{3.8}$$

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:

$$g(x) = \frac{\partial J(x)}{\partial x} = -H^T(x)\mathbf{W}^{-1}[\mathbf{Z} - F(x)] = 0, \tag{3.9}$$

where $H = [\partial F(x)/\partial x]$ is the Jacobian of $F(x)$ [1]. 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,

$$x^{(k+1)} = x^{(k)} + [H^T(x^{(k)})\mathbf{W}^{-1}H(x^{(k)})]^{(-1)}H^T(x)\mathbf{W}^{-1}[\mathbf{Z} - F(x)], \tag{3.10}$$

known as the Gauss-Newton method [1]. 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

$$\Delta x^{(k)} = [H^T(x^{(k)})\mathbf{W}^{-1}H(x^{(k)})]^{(-1)}H^T(x)\mathbf{W}^{-1}[\mathbf{Z} - F(x)], \tag{3.11}$$

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 $|\Delta x^{(k)}|_\infty \not\leq \epsilon$, 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 $k^* = x^{(k)}$, after $k^* = k$ iterations (*convergence time*). ϵ is the convergence threshold and $|\cdot|_\infty$ denotes the maximum norm of a vector.

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 eliminated. Such errors may occur when the meters have bias, drift, and wrong physical connections [1]. 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) [1].

After the WLSE obtains a solution, the BDD is done by processing the resulting measurement residuals, i.e., $\Delta\mathbf{Z}^{(k^*)} = \mathbf{Z} - F(x^*)$. The most commonly used BDD algorithm is the Largest Normalized Residual Test (LNRT) [1, 52]. LNRT identifies the largest element in the normalized residual vector $(\Delta\mathbf{Z}^{(k^*)}/||\Delta\mathbf{Z}^{(k^*)}||_2)$, and if that element is larger than a statistical threshold, then the corresponding measurement as 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 performed again.

Data Integrity Issues and Proposed Solutions for Single-area State Estimation

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 has 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 be ensured (Section 2.1), which leaves the measurements vulnerable to cyber attacks [28].

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 way that the BDD does not detect the manipulation [8, 16, 50]. 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 $\mathbf{Z}$, i.e.,

$$\mathbf{Z}_a = \mathbf{Z} + a, \tag{3.12}$$

where $\mathbf{Z}_a$ denotes the measurements after the manipulation. If the attack vector satisfies

$$a = Hc, \quad \text{for some } c \in \mathbb{R}^n, \tag{3.13}$$

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 [50, 8, 58, 45, 16, 43]. 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 [16], 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 the 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 which extends [65], we develop quantitative metrics to assess the importance of substations and communication equipment with respect to stealth attacks against the state estimation. We use the metrics to evaluate the potential of various mitigation schemes, such as single-path routing, multi-path routing, and data authentication. We consider data authentication achieved either by encapsulating (or tunneling) the communication through bump-in-the-wire (BITW) devices adjacent to legacy RTUs [60], 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 stealth attacks, and to evaluate the efficiency of different mitigation schemes to protect their systems against the attacks.

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., [14, 44, 24, 23, 2, 55, 12, 48, 56, 40]. Typically, the algorithms use the normal equations (3.11), or their modifications, to perform updates within the areas before the coordination [14, 44, 23, 2, 55, 12, 48, 56, 40]. The algorithms can be categorized based on a number of criteria [30]. First, they may differ in the way the coordination is done: in a hierarchical manner, e.g., in [14, 44, 24, 23, 2], or in a distributed manner, e.g., in [55, 12, 48, 56, 40]. 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 [44, 24, 12, 48, 56, 40], or after a number of iterations, e.g., in [14, 23, 2]. Third, they may differ in the assumption on the shared buses and transmission lines between areas. Some assume that areas share only transmission lines [44, 24, 2, 12, 56, 40], while others assume that the areas share only buses [14, 23, 55, 48], or both transmission lines and buses. For a detailed overview of multi-area state estimation algorithms and their categorization, we refer to [30].

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 [56, 40]. The exchanged values are later used when the first step is repeated [56, 40]. The exchange may be synchronous, in which case the steps are synchronized among the areas, or asynchronous [56]. In the asynchronous case, it might be hard to guarantee that a solution will be found [56].

Data Integrity Issues and Proposed Solutions for Multi-Area State Estimation

Measurements used as input to a multi-area state estimator are provided by the SCADA infrastructure, similar to the case of single-area state estimator. An attacker that is able to manipulate the measurements sent from RTUs to the control center could perform attacks similar to the stealth attacks described in Section 3.3 so that the BDD of a multi-area state estimator does not detect the manipulation [26]. Moreover, by denying the delivery of a set of particular measurements, the attacker could make a multi-area state estimator unable to estimate some entries in the state vector x [26].

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 affect fully distributed multi-area state estimation. We consider an attacker that compromises a single computing entity and manipulates with the data sent from and to the entity. We define various attack strategies that differ in the attacker's knowledge of the system, and show on the example of a well-established fully distributed state estimator [56] that they 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 where each area performs independent estimation upon detecting the attacks. Note that such independent estimates can result in high estimation errors on any line connecting two different areas, regardless of whether these areas are compromised or not.

In Paper C which extends [63], we show that the attacks can even disable a state of the art state estimator [40]. We propose an attack detection algorithm based on the convergence properties of the state estimator algorithm and based on the evolution of the exchanged state variables. Furthermore, we propose an attack mitigation algorithm based on the consensus of the beliefs of the individual regions about the attack location, formulated as the stationary distribution of a random walk on a graph. We establish existence, uniqueness, and convergence of the stationary distribution. Upon localizing the compromised area, other areas can neglect the data received only from this area and continue performing fully distributed state estimation among non-compromised areas. Our simulation results on an IEEE benchmark power system show that strong attacks can often be localized and mitigated faster than weak attacks.

3.4 Contingency Analysis

Contingency analysis provides the operator of a power system with an indication of the system operating state in case one or more contingency occur, i.e., it determines whether the system is normal secure operating state or normal insecure operating state [7]. Typical considered contingencies are outages such as disconnection of generators or transmission lines. Therefore, the contingency analysis informs the operator of a dangerous contingency that would move the system to the emergency state. Given the information, the operator should take certain actions to avoid a possible system collapse if the contingency occurs, and thus, to move the system to the normal secure operating state. Contingency analysis is performed every time a new state estimate becomes available as a result of state estimation, and it can happen as often as every few minutes.

Contingency analysis uses a model of the transmission network, described in Section 3.1, and a list of considered contingencies to calculate the output that

consists of estimated voltage phasors at power system buses and power flows on transmission lines. In the following we outline AC load-flow based contingency analysis, which is widely used.

AC Load-flow based Contingency Analysis

Let us denote by P_I the vector of power injections, by c a contingency, and by f^c the function that describes the power flows under contingency c as a function of the system state, i.e., $P^c = f^c(x)$. If a contingency concerns a disconnection of a transmission line, then the system topology is changed and thus $f^c(.) \neq f(.)$. Similarly, if a contingency concerns the disconnection of a generator, then the vector of power injections $P_I^c \neq P_I$. To capture the relationship between the power injections before and after the contingency we introduce the matrix F^c such that $P_I^c = F_I^c P_I$. If contingency c does not affect the power injections then F_I^c is the identity matrix.

Given the vector of power injections P_I^c under contingency c, contingency analysis requires the solution of the load-flow problem, i.e., finding the state vector x^c that solves $P_I^c = f_I^c(x^c)$. The state vector is obtained through solving the power balance equations,

$$\Delta P_b \stackrel{d}{=} -P_b + \sum_m P_{bm} = 0. \tag{3.14}$$

Since the sum of the injections over all buses is zero, there are in total $n-1$ power balance equations and $N-1$ unknowns, as the phase angle of the reference bus is set to zero.

The equations (3.3) are non-linear, thus the solution to (3.14) is obtained using an iterative numerical method, typically the Newton-Raphson method. Starting from an initial guess $x^c(0)$, the Newton-Raphson method obtains an updated estimate at iteration k by computing

$$\Delta x^c(k+1) = -J_k^{-1} \Delta P_I(k), \tag{3.15}$$

where $J_k = \frac{\partial P_I}{\partial x}|_{x=x^c(k)}$ is the Jacobian evaluated at the most recent guess $x^c(k)$, and then letting $x^c(k+1) = x^c(k) + \Delta x^c(k+1)$. Observe that the Jacobian is a non-singular square matrix of size $(n-1) \times (n-1)$. The algorithm terminates when the power mismatch ΔP_I is below a certain threshold. Let x^c be the computed system state under contingency c.

Given the system state x^c under the contingency, the power flows can be calculated as $P^c = f^c(x^c)$. If any of the power flows exceeds the capacity limit (e.g., thermal capacity) of the transmission line then the system is said to be in an insecure state, and a corrective action must be taken by the operator to move the system to a state in which no contingency results in a capacity violation.

Data Confidentiality Issues and Proposed Solutions for Cloud-based Contingency Analysis

The number of contingencies that needs to be considered depends on the instantaneous load of the power system, the higher the load the more contingencies might have to be considered. The number of contingencies considered in practice is limited by the computational power available in the control center, and is often constrained to considering the loss of a single components known as N-1 security. Cloud-based contingency analysis could allow an operator to scale the number of considered contingencies freely as a function of the instantaneous system state and enable N-x security that is considered desirable, but it could expose the current system state and possible critical contingencies, thereby facilitating targeted attacks.

In this thesis we address this issue; in Paper D, we propose an algorithm to obfuscate information regarding power flows and the presence of a contingency violation while allowing the operator to analyze contingencies with the needed accuracy in the cloud. Our empirical evaluation shows that the error introduced by the approach when using an AC model is quite small and that the RMS error grows linearly with the magnitude of obfuscation applied.

Chapter 4

Summary of original work

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

Ognjen Vuković, Kin Cheong Sou, György Dán, Henrik Sandberg.
In IEEE Journal on Selected Areas in Communications (JSAC), vol. 30, no. 6, July 2012.

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 co-authors.

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

Ognjen Vuković and György Dán.
In Proceedings of ACM Symposium on Applied Computing (SAC), March 2013.

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: Security of Fully Distributed Power System State Estimation: Detection and Mitigation of Data Integrity Attacks

Ognjen Vuković and György Dán.
In IEEE Journal on Selected Areas in Communications (JSAC), vol. 32, no. 7, July 2014.

Summary: In this paper we address the vulnerability of fully distributed state estimation to data integrity attacks. We consider an attacker that compromises the communication infrastructure of a single control center and can manipulate the state variables exchanged between the control center and its neighbors. We show that a denial of service attack can be launched against a state of the art state estimator this way. We propose an attack detection algorithm based on the convergence properties of the distributed state estimation algorithm and based on the evolution of the exchanged state variables. Furthermore, we propose an attack mitigation algorithm based on the consensus of the beliefs of the individual regions about the attack location, formulated as the stationary distribution of a

random walk on a graph. We establish existence, uniqueness, and convergence of the stationary distribution. We show the efficiency of the attack detection and mitigation algorithms via simulations on an IEEE benchmark power system, and we use the simulations to illustrate the trade-off between localization speed and localization accuracy. Our numerical results also show that strong attacks can often be localized and mitigated faster than weak attacks.

Contribution: The author of this thesis defined the detection algorithm and the mitigation algorithm as well as provided the corresponding analytical results 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 D: Confidentiality-preserving Obfuscation for Cloud-based Power System Contingency Analysis

Ognjen Vuković, György Dán, and Rakesh B. Bobba.
In Proceedings of IEEE SmartGridComm, October 2013.

Summary: In this paper we propose an approach to obfuscate information regarding power flows and the presence of a contingency violation to enable Contingency Analysis in the cloud while allowing the operator to obtain accurate post contingency flows. Our approach doesn't introduce any error for CA using a DC model and our numerical results show that the error introduced when using AC models is tolerable, and that the RMS errors introduced grow linearly with the magnitude of obfuscation.

Contribution: The author of this thesis implemented and carried out the simulations, and analyzed the resulting data. The article was written in collaboration with the co-authors.

Paper E: Mitigating Gray Hole Attacks in Industrial Communications using Anonymity Networks: Relationship Anonymity-Communication Overhead Trade-off

Ognjen Vuković, György Dán, and Gunnar Karlsson.
Submitted to IEEE Transactions on Parallel and Distributed Systems.

Summary: In this paper we consider the problem of mitigating gray hole attacks by providing relationship anonymity among a fixed set of nodes. We describe two anonymity networks, MCrowds and Minstrels. MCrowds is an extension of Crowds, and provides unbounded path length, while Minstrels provides bounded path length. We consider two attack methods the Bayesian inference method and the Maximum posteriori method. We show that MCrowds provides better relationship anonymity than Crowds, but in order to provide anonymity to the receiver

the sender is more exposed than in Crowds. Moreover, we show that Minstrels provides better relationship anonymity than MCrowds. We use the two anonymity systems to study the trade-off between relationship anonymity and communication overhead, and show that increased overhead does not always lead to improved relationship anonymity. When comparing the two traffic analysis methods, we show that the Maximum posteriori method performs always better. We study the way relationship anonymity scales with the number of nodes, and show that relationship anonymity improves with the number of nodes but at the price of higher overhead. Our results also indicate that in practice anonymity systems should be optimized for a higher number of attackers than expected.

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.

Paper F: Peekaboo: A Gray Hole Attack on Encrypted SCADA Communication using Traffic Analysis

Nunzio Marco Torrisi, Ognjen Vuković, György Dán, and Stefan Hagdahl.
In Proceedings of IEEE SmartGridComm, November 2014.

Summary: In this paper we address the vulnerability of SCADA communication to a gray hole attack, in which an attacker drops unsolicited reports sent by an outstation to a SCADA master, while letting through solicited reports in order to avoid detection. We show that such a gray hole attack is possible even if messages are sent through an encrypted tunnel, because due to the strict timing rules used in SCADA protocols traffic analysis can effectively be used to classify protocol messages. We propose a support vector machine based traffic analysis algorithm, used trace-based simulations to evaluate the attack, and show that an attacker would not need exact knowledge of system parameters for a successful attack. We quantified the impact of the attack in terms on monitoring accuracy, and showed that the operator's observation can be up to 10% off on average, and up to 20% off in 5% of the time. Finally, we discuss potential mitigation schemes, and show that the attack can be mitigated by introducing a random delay before answering to poll messages.

Contribution: The author of this thesis participated in designing the traffic analysis algorithm, defined the metric to quantify the attack impact, designed the mitigation algorithm in collaboration with the co-authors, implemented and carried out the simulations, and analyzed the resulting data. The article was written in collaboration with the third co-author.

Publications not included in the thesis:

- Ognjen Vuković and György Dán, "Detection and Localization of Targeted Attacks on Fully Distributed Power System State Estimation", *in Proc. of IEEE SmartGridComm, October 2013.*
- György Dán and Ognjen Vuković, "Utility-based PMU Data Rate Allocation under End-to-end Delay Constraints", *IEEE COMSOC MMTC E-Letter, vol.7, no.8, November 2012.*
- Ognjen Vuković, Kin Cheong Sou, György Dán, and Henrik Sandberg, "Network-layer Protection Schemes against Stealth Attacks on State Estimators in Power Systems", *in Proc. of IEEE SmartGridComm, October 2011.*
- Ognjen Vuković, György Dán, and Gunnar Karlsson, "Traffic Analysis Attacks in Anonymity Networks: Relationship Anonymity-Overhead Trade-off", *n Proc. of 7th Swedish National Computer Networking Workshop (SNCNW), Jun 2011.*
- Ognjen Vuković, György Dán, and Gunnar Karlsson, "On the Trade-off between Relationship Anonymity and Communication Overhead in Anonymity Networks", *in Proc. of IEEE International Conference on Communications (ICC), Jun 2011.*
- Ognjen Vuković, György Dán, and Gunnar Karlsson, "Minstrels: Improving Communications Availability via Increased Relationship Anonymity", *Euro-NF Workshop on Traffic Engineering and Dependability in the Network of the Future, April 2010.*

Chapter 5

Conclusions and Future work

This thesis addresses data integrity, confidentiality, and availability issues in power system information technologies. 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 addressed the vulnerability of fully distributed state estimation to data integrity attacks. We considered an attacker that compromises the communication infrastructure of a single control center and can manipulate the state variables exchanged between the control center and its neighbors. We showed that a denial of service attack can be launched against a state of the art state estimator this way. We proposed an attack detection algorithm based on the convergence properties of the distributed state estimation algorithm and based on the evolution of the exchanged state variables. Furthermore, we proposed an attack mitigation algorithm based on the consensus of the beliefs of the individual regions about the attack location, formulated as the stationary distribution of a random walk on a graph. We established existence, uniqueness, and convergence of the stationary distribution. We showed the efficiency of the attack detection and mitigation algorithms via simulations on an IEEE benchmark power system, and we used the simulations to illustrate the trade-off between localization speed and localization accuracy. Our numerical results also show that strong attacks can often be localized and mitigated faster than weak attacks.

We proposed an approach to obfuscate information regarding power flows to enable contingency analysis in the cloud while allowing the operator to obtain accurate post contingency flows. Our approach does not introduce any error for contingency analysis using a DC model and our numerical results show that the error introduced when using AC models is tolerable.

We studied how data availability in power system communication infrastructures could be improved by anonymity networks. Since anonymity networks 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.

Finally, we addressed the vulnerability of SCADA communication to gray hole attacks, in which an attacker drops unsolicited reports sent by an outstation to a SCADA master, while letting through solicited reports in order to avoid detection. We showed that such a gray hole attack is possible even if messages are sent through an encrypted tunnel and the attacker does not know exact system parameters, because due to the strict timing rules used in SCADA protocols traffic analysis can effectively be used to classify protocol messages. We discussed potential mitigation schemes, and showed that the attack can be mitigated by introducing a random delay before answering to poll messages.

Future Work

There are a number of different possibilities for future work. Some of them are complementary studies to the studies included in this thesis, while other studies could address some aspects of data integrity, confidentiality, and availability in power system information technologies 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 complementary 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, attacks on data integrity of ICCP data could be targeted against data used by other power system applications. It is an open question if such attacks could also disturb those applications.

Data confidentiality

We proposed a scheme to obfuscate information regarding power flows to enable contingency analysis in the cloud, and showed that our scheme introduces tolerable error for AC models of contingency analysis. A complementary study could analytically bound the introduced error. Moreover, similar schemes could be developed to obfuscate sensitive information for other power system applications that utilize cloud computing.

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 adjustable, 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 [18].

Bibliography

[1] A. Abur and A.G. Exposito. *Power System State Estimation: Theory and Implementation*. Marcel Dekker, Inc., 2004.

[2] Ali Abur. Distributed state estimation for mega grids. In *Proc. of the 15th PSCC Liege*, pages 22–26, Aug. 2006.

[3] B. Akyol. Cyber security challenges in using cloud computing in the electric utility industry. Research report, Pacific Nortwest National Laboratory, September 2012.

[4] S.M. Amin and B.F. Wollenberg. Toward a smart grid: power delivery for the 21st century. *IEEE Power and Energy Magazine*, 3(5):34–41, September 2005.

[5] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia. Above the clouds: A berkeley view of cloud computing. Research report, University of California at Berkeley, Februar 2009.

[6] D. Bailey and E. Wright. *Practical SCADA for Industry*. Newnes, 2003.

[7] N. Balu, T. Bertram, A. Bose, V. Brandwajn, G. Cauley, D. Curtice, A. Fouad L. Fink, M. G. Lauby, B. I. Wollenberg, and J. N. Wrjbel. Online power system security analysis. *Proceedings of the IEEE*, 80(2), February 1992.

[8] R.B. Bobba, K.M. Rogers, Q. Wang, H. Khurana, K. Nahrstedt, and T.J. Overbye. Detecting false data injection attacks on DC state estimation. In *Preprints of the First Workshop on Secure Control Systems, CPSWEEK*, Stockholm, Sweden, April 2010.

[9] A.R. Borde, D.K. Molzahn, P. Ramanathan, and B.C. Lesieutre. Confidentiality-preserving optimal power flow for cloud computing. In *Proceedings of Allerton Conference on Communication, Control, and Computing*, pages 1300–1307, October 2012.

[10] M. Brenner, H. Perl, and M. Smith. How practical is homomorphically encrypted program execution? an implementation and performance evaluation. In *Proceddings of IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, pages 375–382, June 2012.

[11] M. Brenner, J. Wiebelitz, G. von Voigt, and M. Smith. Secret program execution in the cloud applying homomorphic encryption. In *Proceedings of IEEE International Conference on Digital Ecosystems and Technologies Conference (DEST)*, pages 114–119, May 2011.

[12] C.W. Brice and R.K. Cavin. Multiprocessor static state estimation. *IEEE Transactions on Power Apparatus Systems*, pages 302–308, February 1982.

[13] G. Clarke and D. Reynders. *Practical Modern SCADA Protocols: DNP3, 60870.5 and Related Systems*. Newnes, 2004.

[14] K.A. Clements, O.J. Denison, and R.J. Ringlee. A multi-area approach to state estimation in power system networks. In *IEEE PES Summer Meeting*, July 1972.

[15] G. Dán, R. B. Bobba, G. Gross, and R. H. Campbell. Cloud computing for the power grid: From service composition to assured clouds. In *Proc. of USENIX HotCloud'13*, Jun 2013.

[16] G. Dán and H. Sandberg. Stealth attacks and protection schemes for state estimators in power systems. In *Proc. of IEEE SmartGridComm*, Oct. 2010.

[17] G. Dán, H. Sandberg, M. Ekstedt, and G. Björkman. Challenges in power system information security. *IEEE Security & Privacy*, 10(4):62–70, July 2012.

[18] G. Dán and O. Vuković. Utility-based pmu data rate allocation under end-to-end delay constraints. *IEEE COMSOC MMTC E-Letter*, 7(8), November 2012.

[19] T. Dierks and C. Allen. The tls protocol version 1.0. RFC 2246, IETF, January 1999. URL `http://www.ietf.org/rfc/rfc2246.txt`.

[20] T. Dierks and E. Rescorla. The Transport Layer Security (TLS) Protocol, Version 1.2. RFC 5246, IETF, August 2008. URL `http://www.ietf.org/rfc/rfc5246.txt`.

[21] DNP3 IEEE WG. IEEE Standard for Electric Power Systems Communications-Distributed Network Protocol (DNP3). *IEEE Std 1815-2012 (Revision of IEEE Std 1815-2010)*, pages 1–821, 2012.

[22] D. Dzung, M. Naedele, T.P. Von Hoff, and M. Crevatin. Security for industrial communication systems. *Proceedings of the IEEE*, 93(6):1152–1177, 2005.

[23] R. Ebrahimian and R. Baldick. State estimation distributed processing. *IEEE Trans. on Power Systems*, 4:1240–1246, Nov. 2000.

[24] A.A. El-Keib, J. Nieplocha, H. Singh, and D.J. Maratukulam. A decomposed state estimation technique suitable for parallel processor implementation. *IEEE Trans. on Power Systems*, 3:1088–1097, Aug. 1992.

[25] H. Farhangi. The path of the smart grid. *IEEE Power and Energy Magazine*, 8(1):18–28, January 2010.

[26] Y. Feng, C. Foglietta, A. Baiocco, S. Panzieri, and S.D. Wolthusen. Malicious false data injection in hierarchical electric power grid state estimation systems. In *Proceedings of the Fourth International Conference on Future Energy Systems*, e-Energy '13, pages 183–192, New York, NY, USA, 2013. ACM. URL `http://doi.acm.org/10.1145/2487166.2487187`.

[27] S. Fries, H.J Hof, and M. Seewald. Enhancing IEC 62351 to improve security for energy automation in smart grid environments. In *Proc. of the fifth International Conference on Internet and Web Applications and Services (ICIW)*, pages 135–142, 2010.

[28] A. Giani, S.S. Sastry, K.H. Johansson, and H. Sandberg. The VIKING project: An initiative on resilient control of power networks. In *Proc. of the 2nd International Symposium on Resilient Control Systems*, 2009.

[29] G. Gilchrist. Secure authentication for dnp3. In *IEEE Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century*, pages 1–3, 2008.

[30] A. Gómez-Expósito, A. de la Villa Jaén, C. Gómez-Quiles, P. Rousseaux, and T. Van Cutsem. A taxonomy of multi-area state estimation methods. *Electric Power Systems Research*, 81:1060–1069, 2011.

[31] V.C. Gungor, D. Sahin, T. Kocak, S. Ergut, C. Buccella, C. Cecati, and G.P. Hancke. Smart grid technologies: Communication technologies and standards. *IEEE Transactions on Industrial Informatics*, 7(4):529–539, November 2011.

[32] B. Hayes. Cloud computing. *Communications of the ACM*, 51(7):9–11, July 2008.

[33] Q. Huang, M. Zhou, Y. Zhang, and Z. Wu. Exploiting cloud computing for power system analysis. In *Proc. of International Conference on Power System Technology (POWERCON)*, pages 1–6, October 2010.

[34] University of Southern California Information Sciences Institute. Internet Protocol. RFC 791, IETF, September 1981. URL `http://www.ietf.org/rfc/rfc791.txt`.

[35] University of Southern California Information Sciences Institute. Transmission Control Protocol. RFC 793, IETF, September 1981. URL `http://www.ietf.org/rfc/rfc793.txt`.

[36] International Electro-technical Commission (IEC) Technical Committee 57. IEC62351 Power systems management and associated information exchange - Data and communications security - Part 3: Communication network and system security - Profiles including TCP/IP. Technical report, IEC Technical Committee 57, Jun 2007.

[37] International Electro-technical Commission (IEC) Technical Committee 57. IEC62351 Power systems management and associated information exchange - Data and communications security - Part 4: Profiles including MMS. Technical report, IEC Technical Committee 57, Jun 2007.

[38] International Electro-technical Commission (IEC) Technical Committee 57. IEC62351 Power systems management and associated information exchange - Data and communications security - Part 5: Security for IEC 60870-5 and derivatives. Technical report, IEC Technical Committee 57, August 2009.

[39] A. Ipakchi and F. Albuyeh. Grid of the future. *IEEE Power and Energy Magazine*, 7(2):52–62, March 2009.

[40] V. Kekatos and G.B. Giannakis. Distributed robust power system state estimation. *IEEE Transactions on Power Systems*, 28(2):1617–1626, 2013.

[41] S. Kent and R. Atkinson. Security architecture for the internet protocol. RFC 2401, IETF, November 1998. URL `http://www.ietf.org/rfc/rfc2401.txt`.

[42] M. Kezunovic, G. Gurrala, A. Bose, P. Yemula, P. Kansal, and Y. Wang. The next generation energy management system design: Final project report. PSERC Publication 13-40, PSERC, September 2013.

[43] T.T. Kim and H.V. Poor. Strategic protection against data injection attacks on power grids. *IEEE Trans. on Smart Grid*, 2:326–333, Jun. 2011.

[44] H. Kobayashi, S. Narita, and M.S.A.A. Hamman. Model coordination method applied to power system control and estimation problems. In *Proc. of the IFAC/IFIP 4th Int. Conf. on Digital Computer Appl. to Process Control*, 1974.

[45] O. Kosut, L. Jia, R. Thomas, and L. Tong. Malicious data attacks on smart grid state estimation: Attack strategies and countermeasures. In *Proc. of IEEE SmartGridComm*, Oct. 2010.

[46] F. Li, W. Qiao, H. Sun, H. Wan, J. Wang, Y. Xia, Z. Xu, and P. Zhang. Smart transmission grid: Vision and framework. *IEEE Transactions on Smart Grid*, 1(2):168–177, September 2010.

[47] T.E. Dy Liacco. Real-time computer control of power systems. *In Proc. of IEEE*, 62(7):884–891, July 1974.

[48] S.Y. Lin and C.H. Lin. An implementable distributed state estimator and distributed bad data processing schemes for electric power systems. *IEEE Transactions on Power Systems*, pages 1277–1284, August 1994.

[49] S. Liu, B. Chen, T. Zourntos, D. Kundur, and K. Butler-Purry. A coordinated multi-switch attack for cascading failures in smart grid. *IEEE Transactions on Smart Grid*, 5(3):1183–1195, May 2014.

[50] Y. Liu, P. Ning, and M. Reiter. False data injection attacks against state estimation in electric power grids. In *Proc. of the 16th ACM conference on Computer and Communications Security (CCS)*, pages 21–32, 2009.

[51] J.T. Michalski, A. Lanzone, J. Trent, and S. Smith. Secure ICCP Integration Considerations and Recommendations. Technical report, Sandia National Laboratories, Jun 2007.

[52] A. Monticelli. Electric power system state estimation. *Proc. of the IEEE*, 88 (2):262–282, 2000.

[53] D. Reynders, S. Mackay, and E. Wright. *Practical Industrial Data Communications*. Newnes, 2005.

[54] B. Schneier. *Secret and Lies: Digital Security in a Networked World*. Wiley Publishing, Inc., January 2004.

[55] F.C. Schweppe, J. Wildes, and D.B. Rom. Power system static-state estimation, Part I, II, III. *IEEE Transactions on Power Apparatus and Systems*, 89: 120–135, January 1970.

[56] M. Shahidehpour and Y. Wang. *Communication and Control in Electric Power Systems*. John Wiley and Sons, Inc., 2003.

[57] Symantec Security Response. W32.duq: The precursor to the next stuxnet, November 2011.

[58] A. Teixeira, S. Amin, H. Sandberg, K.H. Johansson, and S.S. Sastry. Cybersecurity analysis of state estimators in electric power systems. In *Proc. of IEEE Conf. on Decision and Control (CDC)*, Dec. 2010.

[59] The DNP User Group. DNP Secure Authentication v5. Technical report, The DNP User Group, November 2011.

[60] P.P. Tsang and S.W. Smith. YASIR: A low-latency, high-integrity security retrofit for legacy scada systems. In *Proc. of IFIP/TC11 International Information Security Conference*, 2008.

[61] C. Vecchiola, S. Pandey, and R. Buyya. High-performance cloud computing: A view of scientific applications. In *Proc. of International Symposium on Pervasive Systems, Algorithms, and Networks (ISPAN)*, pages 4–16, December 2009.

[62] A. von Meier. *Electric Power Systems: A Conceptual Introduction*. John Wiley and Sons, Inc., 2006.

[63] O. Vuković and G. Dán. Detection and localization of targeted attacks on fully distributed power system state estimation. In *Proceedings of IEEE SmartGridComm*, pages 390–395, October 2013.

[64] O. Vuković, G. Dán, and G. Karlsson. On the trade-off between relationship anonymity and communication overhead in anonymity networks. In *Proceedings of IEEE International Conference on Communications (ICC)*, June 2011.

[65] O. Vuković, K. C. Sou, G. Dán, and H. Sandberg. Network-layer protection schemes against stealth attacks on state estimators in power systems. In *Proceedings of IEEE SmartGridComm*, pages 184–189, October 2011.

[66] F.F. Wu, K. Moslehi, and A. Bose. Power System Control Centers: Past, Present, and Future. *Proceedings of the IEEE*, 93(11):1890–1908, 2005.

Paper A

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

Ognjen Vuković, Kin Cheong Sou, György Dán, Henrik Sandberg.

in IEEE Journal on Selected Areas in Communications (JSAC), vol. 30, no. 6, July 2012.

Paper B

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

Ognjen Vuković and György Dán.

in Proc. of ACM Symposium on Applied Computing (SAC), March 2013.

Paper C

Security of Fully Distributed Power System State Estimation: Detection and Mitigation of Data Integrity Attacks

Ognjen Vuković and György Dán.

in IEEE Journal on Selected Areas in Communications (JSAC), vol. 32, no. 7, July 2014.

Paper D

Confidentiality-preserving Obfuscation for Cloud-based Power System Contingency Analysis

Ognjen Vuković, György Dán, and Rakesh B. Bobba.

in Proc. of IEEE SmartGridComm, October 2013.

Paper E

Mitigating Gray Hole Attacks in Industrial Communications using Anonymity Networks: Relationship Anonymity-Communication Overhead Trade-off

Ognjen Vuković, György Dán, and Gunnar Karlsson.

Submitted to IEEE Transactions on Parallel and Distributed Systems.

Paper F

Peekaboo: A Gray Hole Attack on Encrypted SCADA Communication using Traffic Analysis

Nunzio Marco Torrisi, Ognjen Vuković, György Dán, and Stefan Hagdahl.

In Proc. of IEEE SmartGridComm, November 2014.

TRITA-EE 2014:039
ISSN 1653-5146
ISBN 978-91-7595-250-5