May 2019

Reliability Analysis of Electric Power Systems Considering Cyber Security

Sirui Tang
University of Wisconsin-Milwaukee

RELIABILITY ANALYSIS OF ELECTRIC POWER SYSTEMS

CONSIDERING CYBER SECURITY

by

Sirui Tang

A Thesis Submitted in

Partial Fulfillment of the

Requirements for the Degree of

Master of Science

in Engineering

at

The University of Wisconsin-Milwaukee

May 2019

ABSTRACT

RELIABILITY ANALYSIS OF ELECTRIC POWER SYSTEMS CONSIDERING CYBER SECURITY

by

Sirui Tang

The University of Wisconsin-Milwaukee, 2019
Under the Supervision of Dr. Lingfeng Wang

The new generation of the electric power system is the modern smart grid which is essentially a cyber and physical system (CPS). Supervisory control and data acquisition (SCADA)/energy management system (EMS) is the key component of CPS, which is becoming the main target of both external and insider cyberattacks. Cybersecurity of the SCADA/EMS system is facing big challenges and influences the reliability of the electric power system. Characteristics of cyber threats will impact the system reliability. System reliability can be influenced by various cyber threats with different attack skill levels and attack paths. Additionally, the change of structure of the target system may also result in the change of the system reliability. However, very limited research is related to the reliability analysis of the electric power system considering cybersecurity issue.

A large amount of mathematical methods can be used to quantify the cyber threats and simulation processes can be applied to build the reliability analysis model. For instance, to analyze the vulnerabilities of the SCADA/EMS system in the electric power system, Bayesian Networks (BNs) can be used to model the attack paths of cyberattacks on the exploited vulnerabilities. The mean time-to-compromise (MTTC) and mean time-to-failure (MTTF) based on the Common Vulnerability Scoring System (CVSS) can be applied to characterize the properties of cyberattacks. What’s more, simulation approaches like non-sequential or sequential Monte Carlo Simulation (MCS) is able to simulate the system reliability analysis and calculate the reliability indexes.

In this thesis, reliability of the SCADA/EMS system in the electric power system considering different cybersecurity issues is analyzed. The Bayesian attack path models of cyberattacks on the SCADA/EMS components are built by Bayesian Networks (BNs), and cyberattacks are quantified by its mean time-to-compromise (MTTC) by applying a modified Semi-Markov Process (SMP) and MTTC models. Based on the IEEE Reliability Test System (RTS) 96, the system reliability is analyzed by calculating the electric power system reliability indexes like LOLP and EENS through MCS. What’s more, cyberattacks with different lurking strategies are considered and analyzed.

According to the simulation results, it shows that the system reliability of the SCADA/EMS system in the electric power system considering cyber security is closely related to the MTTC of cyberattacks, which is influenced by the attack paths, attacking skill levels, and the complexity of the target structure. With the increase of the MTTC values of cyberattacks, LOLP values decrease, which means that the reliability of the system is better, and the system is safer. In addition, with the difficulty level of lurking strategies of cyberattacks getting higher and higher, though the LOLP values of scenarios don’t increase a lot, the EENS values of the corresponding scenarios increase dramatically, which indicates that the system reliability is more unpredictable, and the cyber security is worse. Finally, insider attacks are discussed and corresponding LOLP values and EENS values considering lurking behavior are estimated and compared. Both LOLP and EENS values dramatically increase owing to the insider attacks that result in the lower MTTCs. This indicates that insider attacks can lead to worse impact on system reliability than external cyber attacks. The results of this thesis may contribute to the establishment of perfect countermeasures against with cyber attacks on the electric power system.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACKNOWLEDGEMENTS

First of all, I want to express my deepest gratitude to my advisor Dr. Lingfeng Wang. Without his help, it is impossible for me to successfully finish this thesis and gain plenty of knowledge during the study at UW-Milwaukee. Whenever I turned to him, he was always patient. His serious attitude on research incentivized me to be rigorous in the research of this topic. Additionally, he is a humorous person with positive attitude towards both work and life.

Besides, I am also grateful to Dr. Zhaoxi Liu, whose patient guidance and valuable suggestions helped me successfully complete this thesis. His wide knowledge inspired me in academic study. He gave me much help and advice during the whole process of research and thesis writing.

Additionally, my thanks also go to my labmates, Yitong Shen, Rao Rao and Yingqiao He, for their warm help and concerns on my study and life, making my life aboard happy and feel like being at home.

I am also grateful for the financial support for this project. This work was supported in part by the National Science Foundation under Award ECCS1739485, in part by the Research Growth Initiative Program of University of Wisconsin-Milwaukee under Award 101X360, and in part by the National Science Foundation Industry/University Cooperative Research Center on Grid-connected Advanced Power Electronic Systems (GRAPES) under Award GR-18-06.

I want to appreciate my thesis committee, Dr. Weizhong Wang and Dr. Wei Wei, for their time in serving on my MS committee. Their useful comments and suggestion are helpful for me to improve the thesis.

Last but not least, I want to thank my parents far in my homeland. They are the strongest shield behind me. Whatever I meet, my parents are always staying with me with their wise, inclusion, and deep love.

Chapter 1 Introduction

1.1 Background

As the new generation of the electric power system, the smart grid combines the cyber and physical technologies, building the cyber-physical system (CPS) which provides the high capacity, efficiency, and reliability. However, in a sense of the external environment, the scale and complexity of power systems are further increased owing to the real-time integration of both the physical system and the information computing system in CPS [1]. Thus, various of attacks from both physical and cyber sides may occur on the electric power system without effective counterplots. As the 2003 northeast blackout which happened because of the neglect of management on the critical infrastructures (CI) [2], though accidents like this happen often, by result of the increasing complexity of CPS and the uncertain characteristics of the increasingly higher levels of attacks, system reliability assessment is more difficult, and few quantification efforts were done. This brings to the higher requirement of power system reliability analysis.

To increase the cyber-physical system reliability, the impact of both the characteristics of the infrastructure of electric power system and various cyber attacks on the components of CPS is needed to be analyzed. By considering the cyber-to-physical (C2P) bridge approach, components and their corresponding attacks can be modeled for reliability analysis [3]. For instance, components such as the generators, transmission lines, and loads have respective failure probabilities. In addition, failure probabilities may vary with the change of attack characteristics which means that the impact may different when various attacks with different characteristics occur on the same component. In a word, considering the elements of different components and the characteristics of their corresponding attacks, attacking models of reliability analysis can be built and counterplots can be put forward as well [4].

1.2 The SCADA/EMS System of Electric Power System and Its Reliability

1.2.1 The structure of SCADA/EMS system

Increasing research on the reliability analysis has been focused on in recent years, and it is obvious that both physical and cyber attacks impact the system reliability. However, managing the physical components of electric power system is not as difficult as managing the cyber components, so it is much easier for cyber components to be exposed and under attack, that is cyber attacks are the main impact on the electric power system reliability [5]. Therefore, the reliability analysis of power system is approached by mainly considering the cyber attacks on corresponding components.

In CPS, the communicating and computing is based on supervisory control and data acquisition (SCADA) and perform vital operations for controlling the power grid system. Cyber attacks on the SCADA/EMS system should be studied and analyzed [6]. The structure of SCADA/EMS is shown in Figure 1-1.

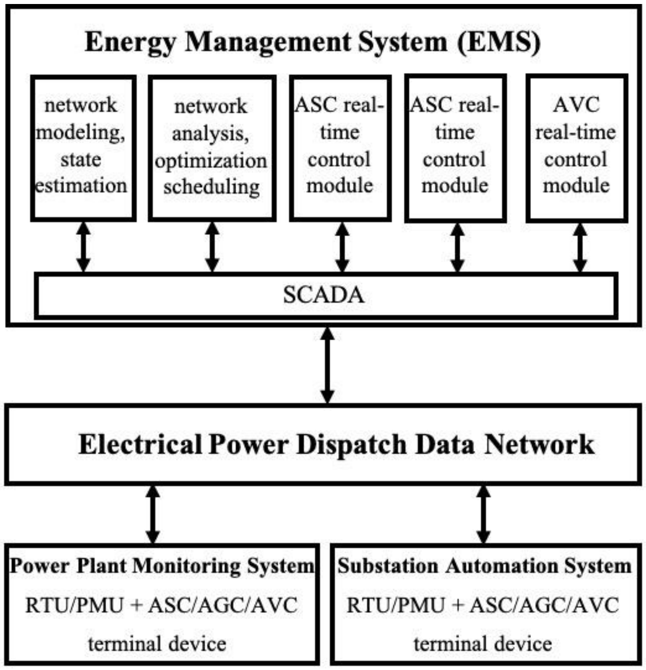

Energy Management System (EMS)
network modeling, state estimation
network analysis, optimization scheduling
ASC real-time control module
ASC real-time control module
AVC real-time control module
SCADA
Electrical Power Dispatch Data Network
Power Plant Monitoring System
RTU/PMU + ASC/AGC/AVC terminal device
Substation Automation System
RTU/PMU + ASC/AGC/AVC terminal device

Figure 1-1 The structure of SCADA/EMS system

EMS is the core part of power dispatch control, and its main goal is to provide the real-time information (including remote measurement information, signal information, etc.) of the electric system operation to power dispatch management personnel and optimize the scheduling and control decisions of the power system operation, so as to ensure that the power system can operate safely, stably and economically. EMS is mainly a closed-loop system consisting of three parts: the control layer, data network and plant station. The basic working process of EMS is: First, data collection such as power running status is performed by terminal devices such as RTU and PMU located at the station floor. Then, the collected data is uploaded to the control layer through the power dispatch data network, and the uploaded data is initially processed by SCADA. According to the uploaded data for network analysis and optimization scheduling, the ASC/AGC/AVC real-time control module is responsible for decision-making control, and control commands are transmitted through the power dispatch data network. Finally, control commands are executed by terminal devices such as ASC/AGC/AVC at the plant station level [7].

Obviously, SCADA is the most widely used information system as the main measurement tool for power systems and it is the most important part of EMS. SCADA is usually used for power system fault analysis, real-time regulation of reactive power compensation devices, information facility monitoring, assistance in creating DTS training programs, power consumption forecasting, actual network loss and loss calculation, dispatcher trend, reactive voltage comprehensive optimization, real-time loss calculation, transformer operation mode research, and intelligent maintenance tickets and operation tickets, in addition to providing steady state information of the grid operation and initial values of the operation mode [8].

1.2.2 Cyber attacks on SCADA/EMS system

The power SCADA/EMS system is vulnerable to different network security threats at different stages and at different levels of data and control command transmission due to different network transmission methods [9]. Figure 1-2 shows the different network security threats of SCADA/EMS at different stages. There are different levels of security threats and risks inside the plant-side information collecting process, RTU controlling process, remote data transmitting process between the plant station and the control center, remote devices of the control center.

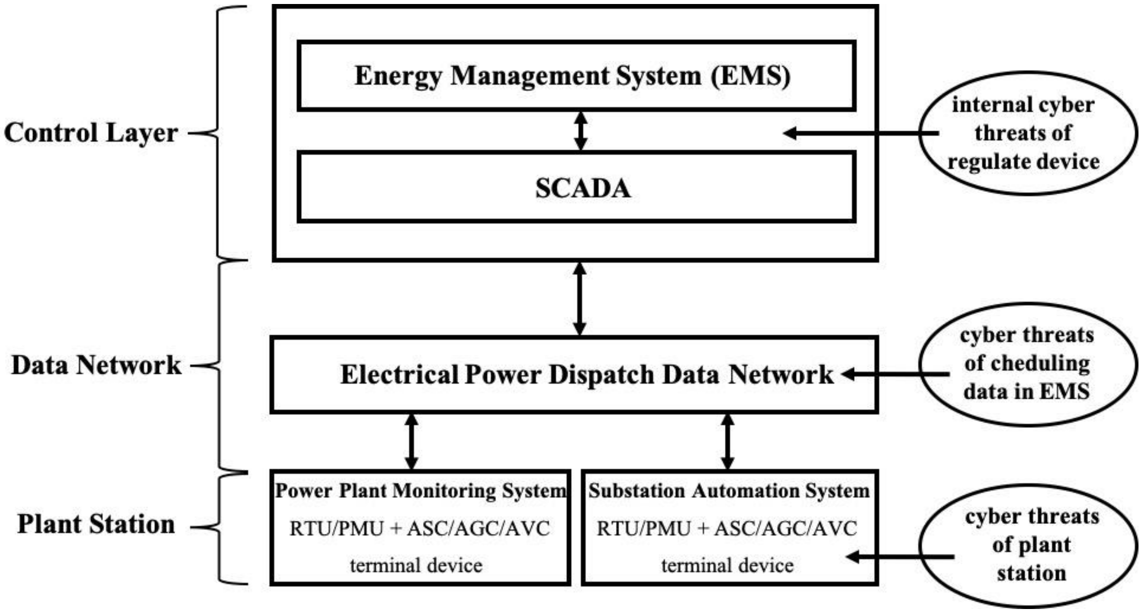

Control Layer
Energy Management System (EMS)
SCADA
internal cyber threats of regulate device
Data Network
Electrical Power Dispatch Data Network
cyber threats of cheduling data in EMS
Plant Station
Power Plant Monitoring System
RTU/PMU + ASC/AGC/AVC terminal device
Substation Automation System
RTU/PMU + ASC/AGC/AVC terminal device
cyber threats of plant station

Figure 1-2 Cyber threats of SCADA/EMS system

In the plant station layer, both sides of the communication are often confirmed by IP address and MAC address. Since TCP/IP is an open protocol, TCP/IP protocol packets are easily captured and tampered during transmission, so once the source IP address and source MAC address are present, critical information such as addresses is maliciously tampering, which will cause important data and resources to flow to illegal nodes. Because IP spoofing, MAC spoofing, and denial of service attacks based on IP spoofing or MAC spoofing which are easy to attack and can quickly stop the service of attack target, the control systems of plant station layer are highly vulnerable to be under attacks.

In the control layer, the transmission of the power system real-time data and control commands mainly relies on communication between SCADA servers and remote terminals such as RTU. However, during the data transmission, there are security vulnerabilities from the communication protocol itself or introduced by TCP/IP, so the control center may receive the forged power system operation data transmitted by the dispatch data network and may also send the forged or falsified control commands to the power dispatch data network. DNP 3.0 over TCP/IP is used for communicating control commands and measurements between control centers and substations. The protocol used in the substation is IEC 61850. Similar to other industry networks, the system environment of SCADA/EMS was relatively closed in the initial design and configuration, that is, the security of system was less considered [10].

To protect the reliability of SCADA/EMS system, the most important thing is to protect the security of SCADA/EMS network systems used to transmit critical power information.

Safeguarding the security of the SCADA/EMS network system can be approached by analyzing and studying the SCADA/EMS network security architecture, combining the universal network security system principle with the characteristics of the SCADA/EMS network, effectively ensuring the integrity and effectiveness of the SCADA/EMS network security strategy and better meeting the security requirements of the power grid system.

1.2.3 Reliability analysis of electric power system and cyber attacks

Reliability analysis of electric power system can be carried out by considering various aspects of components. Compared with the basic components such as the generators, the transmission lines and the loads, SCADA/EMS system faces more serious issue when it is attacked, which may lead to more critical security problem of the power system. In [3], the impact of security attacks which occurred on the generators and transmission lines were estimated. To carry out the security strategy of the generators, the model of evaluation was built, and the loss was evaluated when the generators were out of service. To model the cyber attacks on the generators, the exponential function and the Mean Time to Attack (MTTA) were used. Meanwhile, assuming that the security strategy of the transmission lines is advanced relaying, various Mean Time to Attacks were used to simulate the cyber threats. What’s more, the cyber threats on SCADA system were considered when penetrations entered and affected the status of controls of the generators, transmission lines, and the loads. To simulate the cyber threats of SCADA system, exponentially distributed random variable and a Bernoulli random variable presented by the Average Percentage of Tripped Breakers (APTB) are used. By applying these simulations in the Roy Billinton Test System (RBTS) [11], it is found that cyber attacks on the SCADA system resulted in times more serious impact than on the original components [3], [12].

In [13], Monto Carlo Simulation (MCS) was used to estimate the reliability of an electric service in the SCADA system and the availability of system control. While it is reported that cyber attacks that can be accurately detected is only occupied 30%, and more than half of them have resulted in extremely huge economic losses that may more than 1 million dollars [14]. In other words, evaluating the economic losses of an electric power system caused by the cyber threats is still needed to be studied.

Thus, various reliability analysis of electric power system has called the attention of researchers. In [15], a stateful Intrusion Detection System (IDS) method based on Deep Packet Inspection (DPI) technology was firstly proposed, which can monitor and detect the IEC60870-5-104 traffic in SCADA system to improve the cyber security of SCADA system. And in [16], aiming at the cyber security vulnerabilities of SCADA system in the electric power EMS system, a signature-based and model-based intrusion detection method was proposed. For existing attacks, signature-based intrusion detection was used to generate blacklists. For unknown attacks, communication protocols and intrusion detection of traffic models were used. In [17], by taken both system external and internal cyber attacks into consideration, vulnerabilities of the electric power grid were estimated to collect the various cyber threats and model the respective effects on the corresponding structure.

1.3 Research Objectives and Layout

This thesis is mainly to establish the reliability analysis model of SCADA/EMS system of electric power system considering cyber security issue with different attack strategies. There are two main research objectives taken into consideration in this thesis, which are going to be studied within various scenarios.

- Mathematical modeling of scenarios studies under various cyber attacks on the SCADA/EMS system of electric power system.

- System reliability analysis of the electric power system in view of cyber security issue on the SCADA/EMS system.

It can be divided into four parts. Chapter 1 and Chapter 2 state the necessity of this research and some basic knowledge. Chapter 3 to Chapter 5 focus on the establishment of the mathematical models which can be used to simulate and analysis the system reliability, and various cases considering cyber attacks are studied. In Chapter 3, two modified Bayesian Network (BN) models are introduced and the corresponding attack graph models are built to calculate the failure probabilities of electric power system vulnerabilities caused by cyber threats. By evaluating the Mean Time to Compromise (MTTC) of each scenario and using Monte Carlo Simulation (MCS), the effect of each cyber attack in different attacking skill level on the power system reliability is evaluated. In Chapter 4, luring behavior of each cyber attack is taken into consideration. MCS is used to simulate and analysis the system reliability of different skill level of cyber attacks considering their lurking time with different lurking strategies. Results in Chapter 4 are compared with each other to investigate the system reliability under different kinds of cyber threats. Finally, insider attacks are studied and simulated by MSC in Chapter 5. SMP models are built and MTTCs evaluation are finished based on corresponding SMP models. Results in Chapter 5 are compared with them in Chapter 3 and Chapter 4.

Chapter 2 Cyber Security Issue in the Electric Power System and Its Analyzing Methods

2.1 Cyber Security Issue in Electric Power System

Electric power CPS can obtain more comprehensive and more detailed information of the power grid in real time by means of larger-scale sensing measurement systems and information communication networks which are more complex. Therefore, the dependence of electric power CPS on information systems is getting higher and higher, and the role of cyber security in the operation of the entire power system is becoming more and more important. The network attack against the power system has the characteristics of strong concealment, long latency, and low attack cost [18]. Although it cannot directly damage the primary equipment of power, it can achieve the effect similar to physical attack by weakening or even completely destroying the normal function of the secondary system， which has a serious impact on system reliability, economic operation and social stability [19]. When the power grid is in normal operation, the secondary equipment failure will cause measurement loss or error, affecting the dispatcher's accurate sense of the primary system of the power grid; if the failure occurs on the primary system, provided information interruption, delay, and tampering happen because of the failure or malicious attacks on the communication network of the secondary system such as relay protection device, supervisory control and data acquisition (SCADA)/energy management system (EMS), and wide area measurement system (WAMS), it is very likely to cause the control center to issue faulty commands, as well as the decision unit malfunctions or exit the operation, etc., result in a primary system oscillation and a large-scale blackout [20].

In [21], it states that the three elements of cyber security are confidentiality, integrity, and availability, which is simply referred to as the network “CIA” security goal.

- Confidentiality: Access to information is restricted to authorized users or organizations, and any access through illegal channels should be detected and blocked [22]. The destruction of “confidentiality” will cause leakage of information on the grid, and there are threats that important information (such as user privacy, property rights information, etc.) is used by illegal elements [23].

- Integrity: Maintain and ensure the accuracy and consistency of data or information. The transmission data (including rewriting, deletion, addition, replacement, etc.) cannot be modified and destroyed by any unauthorized organization or data modification [22]. The loss of “completeness” means that data in the network has been modified or destroyed, leading to erroneous power management decisions [23].

- Availability: Any information in the power grid can be 100% authorized by the authorized party to access it at any time [22]. Even if there are sudden events (such as power accidents, attack behaviors, etc.) in the power grid, users, power devices, control centers, etc. can still obtain the required information. Once the “availability” is destroyed, it will lead to problems such as the interruption of data transmission, and the case will have a huge impact on the power transmission under severe circumstances [23].

Cyber attacks broadly refer to any malicious attack that undermines the security objectives of the network “CIA”. While in the electric power system CPS, cyber attacks can be referred as the attacks that for the purpose of destroying or reducing the function of electric power system CPS, track the behavior of communication systems and control systems which contain the various power automation control components that ensure the proper operation of the power system and the operational status of the process control components that collect, monitor, and transmit real-time data [24] without permission, and use the vulnerability and security flaws of the power information communication network (such as operating system vulnerabilities/communication protocol vulnerabilities/application software vulnerabilities) to attack the system itself or resources.

In recent years, attacks on the smart grid through networks and destruction have occurred from time to time. On December 23, 2015, the Ukrainian electric power grid suffered a sudden power outage, causing about 700,000 households in western Ukraine to have power outages for several hours. Afterwards, researchers at iSight Partners, a security company at Dallas, said that this was a destructive event caused by BlackEnergy software/code. BlackEnergy malware was first discovered in 2007. In this attack, its latest version of BlackEnergy Lite was used, and the Kil lDisk component and the SSH (Secure Shell Protocol) backdoor were added. The Kil lDisk component is used to delete data from the computer's hard drive and cause the system to fail to reboot. After obtaining the SSH server access, the SSH backdoor opens the 6789 port of the SSH server, allowing the attacker to permanently access or control the infected SSH server. The blackout was seen as the first real case of malicious behavior against the power supply system [25]. What's more, at the CyberTech 2016 conference, Yuval Steinitz, the head of the Israeli Energy and Hydraulics Department, said that on January 25, 2016, the Israel Electric Authority suffered a serious cyber attack. In this attack, the attacker sent a phishing email containing ransomware to the power bureau staff, tricking the power bureau staff to execute the malicious code, and encrypting the relevant content on the computer, requiring the electric bureau staff to pay to unlock [26]. This is another example of a cyber attack on an electric power infrastructure.

In response to cyber attacks and ensuring cyber security, actions are carried out in several aspects of the related components. In 2003, the US Department of Energy (DOE) proposed 21 elements to protect the information security of SCADA systems [27]. The US Department of Defense's Advanced Research Projects Agency (DARPA) recently launched a program called "Rapid Attack Detection, Isolation, and Characterization," with the goal of developing an automated system that could restore electric power supply within 7 days against a set of devastating attacks on the grid that are targeted at information networks or infrastructure [28].

For researchers, researches about cyber security and system protection are focused. In [29], a model of the control system in SCADA was built to recognize cyber attacks by detecting abnormal state. By using three mathematical methods to model the intruding of the control system in SCADA, a number of impacts from integrity cyber attacks to SCADA are found. Reference [30] pointed out a risky assessment model with Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) to modify different levels of cyber attacks and corresponding vulnerabilities exposed in the control system of SCADA. Cases about possible cyber attacks on the substations were studied in [31], and a logical model was stated as the approach to realize the immediate action against the attacks.

It is showed that the cyber security of the whole electric power grid which affects the system reliability, is closely related with the effects of cyber attacks and corresponding vulnerabilities exposed in the SCADA/EMS system. Therefore，the reliability of the electric power system considering cyber security highly requires for attention, and the corresponding counterplots need to be stated.

2.2 Mathematical Methods of the System Reliability Analysis Considering Cyber Security

To model the cyber attacks and analysis their impacts on the SCADA/EMS system of electric power grid, mathematical approaches are helpful and effective. Bayesian network (BN) and attack graph model, Semi-Markov Processes (SMP) and Mean Time-to-Compromise (MTTC) are used in the modeling processes.

2.2.1 Bayesian Networks (BNs) and attack graph models

There are a lot of uncertainties which need to be represented, reasoned and learned by expert systems, decision support, and data mining in the real world. Probability model is a powerful tool for dealing with random phenomena. Long-term and persistent researches have been conducted by people on how to use probability theory to effectively deal with uncertainty information and knowledge, proposing and implementing many probability-based intelligent information processing models and methods. The Bayesian network (BN) is one of the most representative intelligent information processing models.

The foundational work of the Bayesian network is a philosophical paper by mathematician Bayes [32]. Jeffreys' book [33] marks the formation of the Bayesian school. For the uninformed distribution of information, Jeffreys proposed the important ‘Jeffrey Criterion’. Based on an in-depth study of the relationship between the topological structure of the graph and the conditional independence between the variables, Pearl first proposed the Bayesian network model in 1988 [34]. This network is based on probability theory and graph theory, which has both a solid mathematical foundation and an intuitive visual semantics. It is one of the most effective theoretical models in the field of uncertain knowledge representation and reasoning. Bayesian networks not only have powerful modeling functions, but also have perfect reasoning mechanism, to complete various queries by effectively combining prior knowledge and current observations.

As for attack graph model, the dependences among weak components and possible series of attacks are represented [35]. Combined with BNs, cyber attacks in the electrical power system can be easily model in a probability model and system reliability can be evaluated and analyzed [36].

The Bayesian network is also called the belief network, which is composed of three parts: X, A and N, where <X, A> represents a directed acyclic graph G and N is a set of parameters in the network. X is a collection of nodes in the network, where $X_i \in X$ represents a random variable that limits the domain; A is the set of directed edges in the network, where $a_{ij} \in A$ represents the direct dependency between nodes, and aij represents the directed connection between X_i and X_j, $X_i \leftarrow X_j$; N is the network parameter, where $N_i \in N$ represents the conditional probability distribution function associated with the node X_i. The Bayesian network implies a conditional independence hypothesis. That is, given a node's parent node set, the node is independent of all its non-descendant nodes. Therefore, as shown in equation (2.1), the joint probability of all nodes represented by the Bayesian network can be expressed as the product of the conditional probability of each node.

$$P(a_1, \dots a_n) = \prod_{i=1}^{n} P\big(a_i \big| parents(a_i)\big) \tag{2.1}$$

2.2.2 Semi-Markov Processes (SMP)

The Markov stochastic process based on discrete time is called a discrete-time Markov chain, and its time period of decision-making cannot consider the time factor, so only the moments of priority are considered. Practical problems often require continuous observation of the state of the system. Because of the state transitions that can occur in the system, when decision makers need to make decisions in a timely manner, a continuous model is needed. Semi-Markov Processes are proposed for a half Markov process that takes time factors into account.

Semi-Markov Processes (SMP) are a large set of stochastic processes particularly containing the continuous time Markov chains (CTMC), discrete time Markov chains (DTMC), as well as the ordinary, modified, and alternating renewal processes. Compared with the Markov Process, the state transitions of the SMP are temporary because their corresponding transition rates are only related to the current state. Additionally, the distribution of the inter-arrival times between subsequent states is not exponential cause the transition rate between different states may change during the state duration [37].

An SMP includes six components： $\{\mathrm{S}, \mathrm{A}(i), P_{ij}(a), T(i,a,j), r(u,i,a,j,t), V, i, j \in S, a \in A(i)\}$, where:

- S is assumed to be a countable set, and S is a state set. For the state $i \in S$, $A(i)$ is the set of actions available in state $i. S$ and $A(i)$ have the same meaning as discrete time Markov;

- $P_{ij}(a)$ indicates that the system is in state i at a certain decision time. When action a is taken, the probability that the system is in state j at the next decision point, the time required to move to state j which is the distribution function, are the non-negative random variable of $T(i,a,j)$; When transferring to state j, and considering the condition of the transfer time t, the reward of the system obtained in the time period $[0,u](u \leq t)$ is $r(u,i,a,j,t)$;

- V is a criterion function, which has the same meaning in discrete time Markov, and can be divided into expected total reward criteria and average criteria.

The definition of the SMP is described below in details：

Assuming $S = \{1, \dots, \mathrm{N}\}$ which is the a collection of states in the system, and probability function P as the probability space, a bivariate time-homogeneous Markov chain $(X, T) = \{(X_n, T_n); n \in N = \{0,1,2, ...\}\}$ can be defined, where X_n gets value from S, and T_n states the parameter on the half-real line $R_+ = [0, \infty)$, and constraint is set as $0 = T_0 \leq T_1 \leq ... \leq T_n \leq T_{n+1} \leq \cdots$. Set $U_n = T_n - T_{n-1}$ for all $\mathrm{n} \geq 1$. (X, T) is a Markov Renewal Process (MRP) with the transition function of the semi-Markov kernel:

$$\begin{cases} Q_{ij}(t) = P(X_{n+1} = j, U_n \leq t | X_n = i), (i, j \in S, i \neq j, t \geq 0) \\ Q_{ij}(t) = 0, (i \in S, t \geq 0) \end{cases} \tag{2.2}$$

In (X, T), the component X represents a Markov chain which has the transition function $p(i, j) = Q_{ij}(+\infty)$. In addition, T_n is assumed to equal as $U_1 + ... + U_n$, standing time of the n-th renewal with $N_1 = sup\,\{n: T_n \leq t\}$, which is a counter process of the number of the renewal between 0 and t.

Description above is about MRP, so Semi-Markov Process can be represented as: $Z = \{Z_t; t \in R_+\}$, where $Z_t = X_n$, and $X_n = Z_{T_n}$. The transition probability is represented as $P_{ij}(t) = PZ_t = j|Z_0 = i$, where $j \in S$ is the system occupied state at time $t \geq 0$. Thus, $P_{ij}(t)$ can be estimated by the renewal equation:

$$P_{ij}(t) = h_i(t) \cdot 1_{i=j} + \sum_k \int^t Q_{ik}(dx) \cdot P_{kj}(t-x) \tag{3.3}$$

where $h_i(.) = 1 - \sum_k Q_{ik}(.)$. The transition probabilities can also be evaluated as:

$$\boldsymbol{P}(t) = \boldsymbol{h}(t) + \boldsymbol{P} \times \boldsymbol{Q}(t) \tag{3.4}$$

where $\boldsymbol{P}(.) = P_{ij}(.)$ States a square matrix function and $\boldsymbol{h}(.) = diag\big(h_i(.)\big)$ states a diagonal matrix function [38].

Semi-Markov is a generalization of discrete-time Markov. Similar with all Markov systems, the system can be divided into several states. The current state of the system is independent with the previous state. The extension of Semi-Markov from standard Markov is mainly reflected in the following three characteristics:

- Allowing or requiring the change selected by decision makers in system state when making action decisions;

- Simulating the evolution of the continuous time system;

- Allowing the duration of a particular state to obey a random distribution of probability distributions.

Unlike the Markov Process, the Semi-Markov Process considers the duration of stay for each state. Therefore, devices that are often used in semi-Markov have a limited number of states and each state stays at a specified time or duration. However, similar to other stochastic processes, SMPs are widely used in a range of modeling and simulation problems in computing and engineering like the analysis of attacks on the intrusion tolerant system, and the evaluation and modeling of mean time to failure (MTTF) between different states in a system [39].

2.2.3 Mean Time-to-Compromise (MTTC)

Learned from the physical system, a mean time-to-compromise (MTTC) can be estimated as the time which a particularly skilled attacker will use to successfully attack a system. The attacker levels are divided into Novice, Beginner, Intermediate and Expert, which are depend on capabilities. Figure 2-1 shows the relationship among different skill levels of attackers. Parameter s is set based on learning curves to represent the top of the skills group [40].

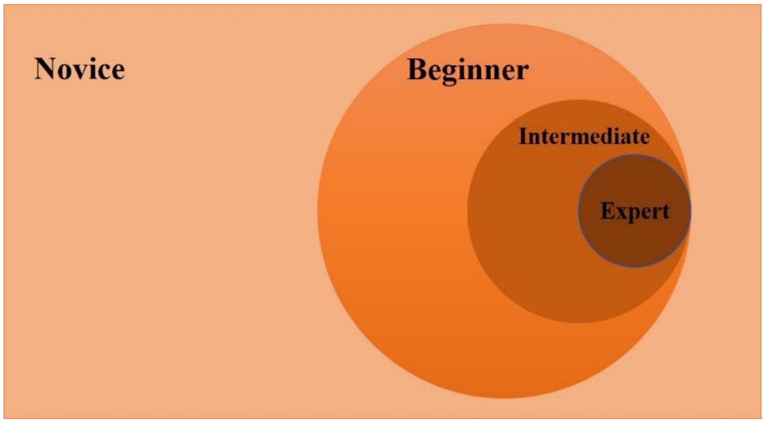


Figure 2-1 Relationship between different skill levels of attackers

Like the mean time-to-failure (MTTF) of the components in the electric power grid, the MTTC also can be estimated. It is used to do quantification evaluation of the average frequency of the cyber attacks on the vulnerabilities of the electric power grid [41]. Considering the idea of the minimal attack order that all the attacks on the components are effective, with the increasing of MTTC of the system, the probability and frequency of the attacks that make efforts will decrease [35]. To evaluate the MTTC of a particular state, the Bayesian Networks (BN) and attack graph are used to analysis the attack approach and its duration from the start of an attack to the end that attacking goal is reached.

In the study of MTTC, a post condition is assumed considering the increased privilege, which means that the system have various exploited vulnerabilities. The overall MTTC is stated as the sum of MTTCs of all exploits in this study. The MTTC may vary with the change between different attack scenarios with different attack paths, structure of attacking target system, vulnerabilities of the components, and skill levels of attackers.

Chapter 3 Power System Reliability Analysis with Intrusion of the SCADA system Considering Cyber Security

3.1 Introduction

In recent years, Cyber Physical System (CPS) has provided new research methods for the reliability analysis of modern electrical power system. However, while CPS is improving the reliability of modern power systems, due to the introduction of information systems, the scale and complexity of power systems are further increased, and system reliability assessment is more difficult. The SCADA system, as the most important and widely used information system, is becoming the main target of cyber threats. Studies on the reliability analysis of the SCADA system of CPS in electric power system require more attention. The reliability assessment for the SCADA systems focuses on the reliability assessment of the information transmission link and the entire network.

In this study, a mean time-to-compromise (MTTC) model [41] is expounded and used to assess the time interval of successful intrusion into network components in the control network. Additionally, to analyze different scenarios, Bayesian Networks (BNs) are described to create the attack graph models of corresponding cyber attacks on the system [42]. According to [35] and [36], BNs can be divided into two categories to model and quantify various cyber attacks of the SCADA system, first of which models the cyber threats on control center LAN, corporation LAN, and substation LANs by evaluating the probabilities that the root privilege of components above has obvious vulnerabilities that are attacked. Another one focuses on the cyber threats on communication links between control center and substation by evaluating the probability respectively. By taking MTTC model and BNs model into consideration at the same time, quantification models of various cyber attacks on the SCADA system are successfully established to realize the quantification process. Finally, Monte Carlo Simulation (MCS) is run to analyze the system reliability and evaluate the cyber security.

In this chapter, in 3.2, the structure of the SCADA system and its corresponding attack paths considering cyber security are stated. Bayesian Networks (BNs) are used to build the attack graph models in 3.3, and the estimation method of MTTC are mentioned in 3.4. Finally, in 3.5, MCS is expounded, and based on MCS, combining BNs and MTTC model, the reliability of IEEE Reliability Test System 96 (RTS96) [43] is analyzed by evaluating the reliability factors of electrical power system.

3.2 Cyber Attack Scenarios in the SCADA System of the Electric Power System

3.2.1 Architecture of the SCADA system

With the development of information control technology, the SCADA system with the RTU as the terminal will further improve the monitoring and control capabilities of the power grid. SCADA is the most widely used information system. It is used as the main measurement tool for power systems which is usually used for power system fault analysis, real-time regulation of reactive power compensation devices, information facility monitoring, assistance in creating DTS training programs, power consumption forecasting, and actual network loss. variable loss calculation, dispatcher flow, integrated reactive voltage optimization, real-time loss calculation, transformer operation mode and intelligent maintenance ticket and operation ticket, it can also provide the steady state information of the grid operation and the initial value of the operation mode. Figure 3-1 illustrates general structure of the SCADA system. It is mainly composed by the RTU, the control center, and the communication system.

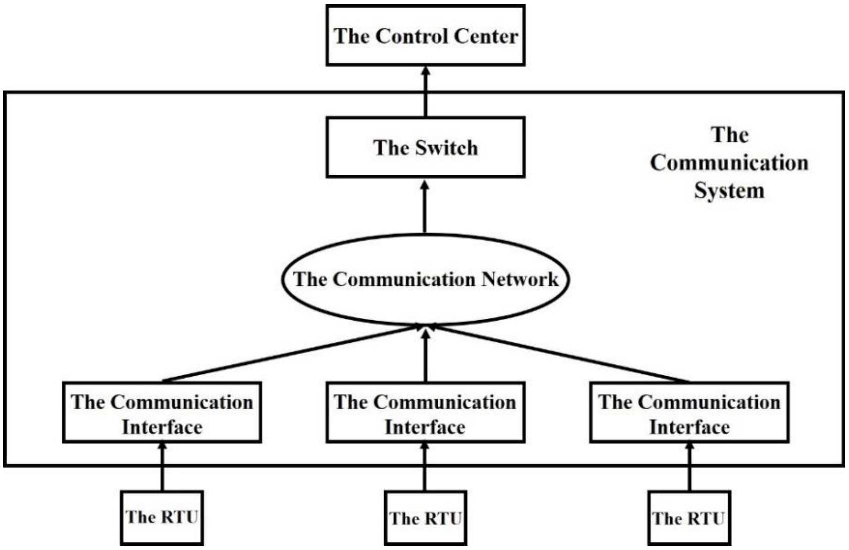

The Control Center
The Switch
The Communication System
The Communication Network
The Communication Interface
The Communication Interface
The Communication Interface
The RTU
The RTU
The RTU

Figure 3-1The general structure of the SCADA system

- The RTU: The RTU is a data acquisition and monitoring terminal unit, which is composed of a power supply part, a control part, a telemetry part, a remote signal part, a remote adjustment part and a modem part. SCADA can continuously monitor the voltage level, line power and current level, generator power and system frequency of each node in the grid operation. The monitoring data is then transmitted to the control center via the communication system. RTU collects data at the same time point based on the specified time and transmits it to the control center.

- The communication system: SCADA has a rich communication system, which is divided into wired communication and wireless communication according to the presence or absence of carriers. Wired communication methods include power line carrier communication, optical fiber communication, and cable line communication, while wireless communication methods include satellite communication, radio wave communication, and radio communication. The communication system is the bridge connecting the RTU to the primary station. An efficient and secure communication system is an important guarantee for fast and secure data transmission. According to the characteristics of data collection and security monitoring, the current SCADA system mainly adopts optical fiber communication technology and transmits measurement data to the main station center through optical fiber to realize data security transmission.

- The control center: The control center is the commander of the entire system. It is responsible for receiving the data transmitted by the communication system and processing the data to realize the operation state analysis of the unit, the alarm of oscillation or disturbance, the monitoring of low frequency oscillation, the control of the load and the generator. The control center is mainly composed of front-end system, database system, workstation, WEB server, etc. As shown in Figure 3-2, the front-end system mainly implements advanced functions such as data reception, storage, and processing. Database systems are usually divided into real-time databases and historical database systems. The real-time database system mainly implements real-time data update, and the historical database system can be used to view historical data. The workstations are divided into engineer workstations, production scheduling workstations, monitoring workstations, and upper application workstations. The engineer workstation is mainly responsible for system graphics production and system maintenance. The production dispatching station is responsible for monitoring the entire power system and user data. Monitoring workstations are typically used in particularly complex and large workstations that divide the system into sections for monitoring. The upper application workstation is based on the monitoring data for power flow calculation, power system stability analysis load forecasting. The WEB server is a user who browses certain data of the grid through the server according to his own authority.

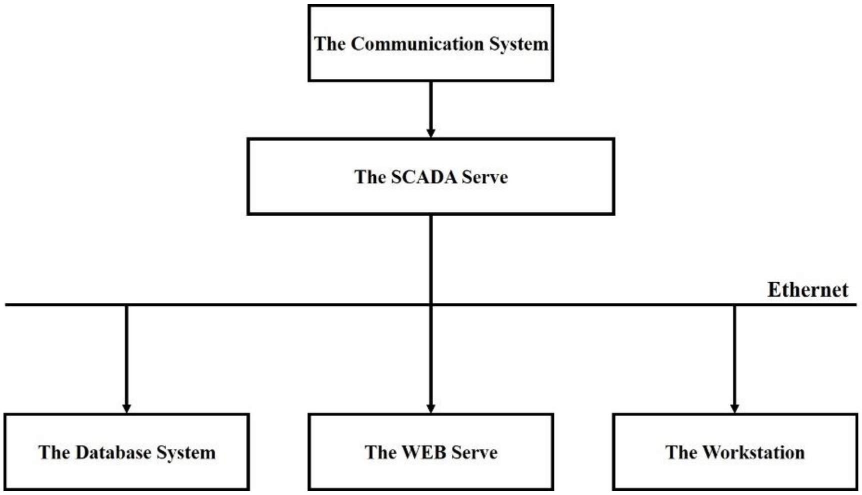


Figure 3-2 The structure of the control center

Figure 3-3 shows the function of the SCADA system in the electric power system. As an information platform, the SCADA system can not only collect grid data for system condition monitoring, but also further analyze the characteristics of grid operation, identify the dangerous state of operation of the system, and take timely control measures to greatly improve the safe operation level of the system.

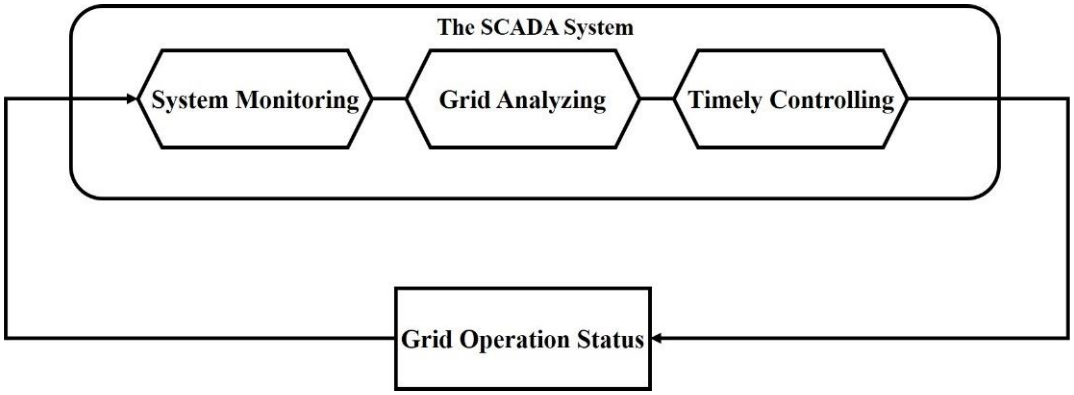


Figure 3-3 The function of the SCADA system in the electric power system

3.2.2 Attack scenarios and corresponding attack paths in the SCADA system

Various LANs of the SCADA system are the targets of the attackers to invade by discovering the vulnerabilities among the components of cyber networks. Thus, there are 4 main ways of intrusion as attack scenarios that the attackers can use to finish various cyber attacks to transmit wrong commands, resulting in the malfunction of generators, transmission lines and loads.

3.2.2.1 Cyber attacks on the control center LAN

Though the control center can be carefully protected by improving the protection mechanism from the physical structure design of the system, it is still possible to be attacked in practical operation. Figure 3-4 states a simple control center LAN. After the attacker bypasses the hardware firewall by using well-planned intrusion strategy, the attacker can access the switch through the port scan method. When an attacker successfully hacks into the control center network, it can scan the network's hosts and servers by invading the history server without calling the attention of the IDS. Because the application server can send commands directly to other devices, it is selected as the target of network intrusion. The application server is used to store data and send updated data to other clients, like the HMI [44]. To obtain the root privilege of the application server, the trip command can be sent directly to the RTU in a substation by the front-end processor.

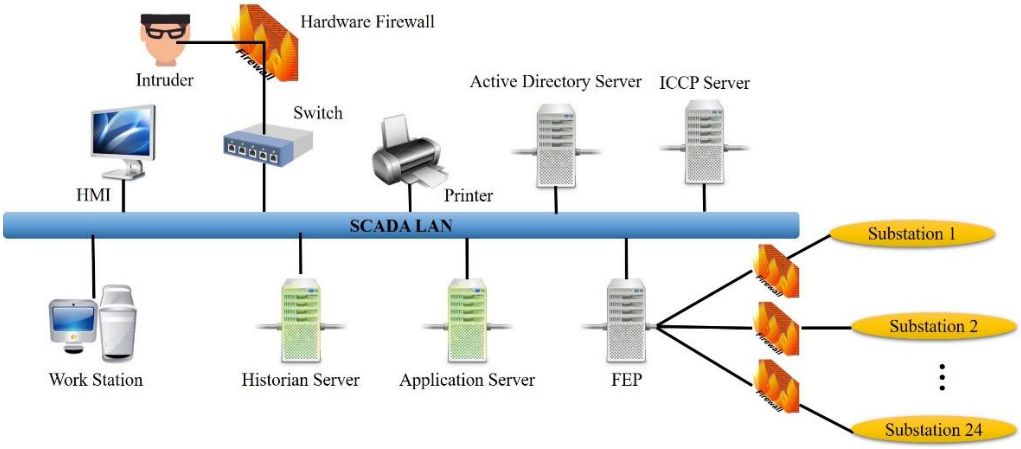


Figure 3-4 Attack paths of the control center LAN

3.2.2.2 Cyber attacks on the corporation LAN

Because of the complex communication network between the attackers and substation networks, it is possible for the attackers firstly access the corporation LAN via the Internet. Figure 3-5 illustrates the possible cyber attacks on the corporation LAN. By accessing the communication network between the control center and the substation, an attacker installs an eavesdropping device on a wired or wireless network. The attacker monitors the traffic, intercepts and captures the measured values or status packets, and replaces some of the normal state data with the manufactured anomaly data, which is sent to the state estimation module. When a false operating condition is ultimately presented to the operator, some operators may be misled and send an incorrect command.

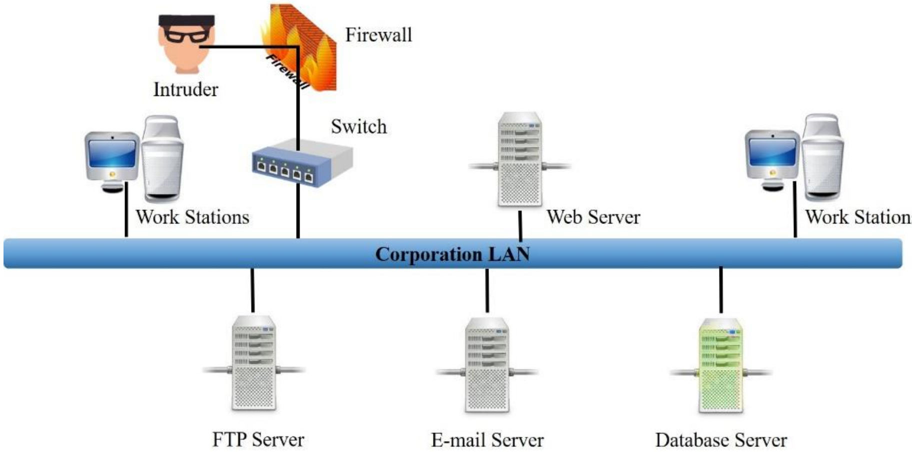


Figure 3-5 Attack paths of the corporation LAN

3.2.2.3 Cyber attacks on the substation LANs

The attacker uses IP and port scanning tools to identify the active system port of a substation and log into one of the routers using a dictionary-based or strong password attack. Since the adversary has access to the substation's network, the IP scanning tool is re-deployed for substation user interface intrusion. The substation HMI is then accessed through the user interface and one or more commands are sent.

In the SCADA system of the electric power system, the substation LANs can be classified into three categories as shown from Figure 3-6 to Figure 3-8. The substation LAN in Figure 3-6 has the basic automation stage and the structure [45], since which only has the basic countermeasure, it is easy for attackers to invade the HMI and immediately send the incorrect commands to the IEDs by intruding into the substation LAN 1.

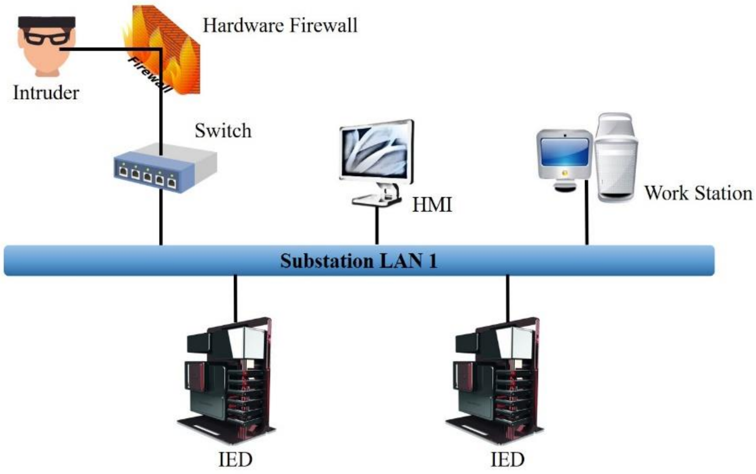


Figure 3-6 Attack paths on the substation LAN 1

Figure 3-7 states the cyber attacks against the substation LAN 2. Compared with the substation LAN 1, the substation LAN 2 is more complex and completed with two networks with Virtual LAN (VLAN). There are corresponding switches which are applied to realize the control of devices' communication, which requires attackers to access the shared server at the same time to intrude the devices of the Bay VLAN. Thus, at least two VLANs need to be intruded by attackers when the substation HMI is under successfully attack. Because of the function that VLANs can stop the unwanted data, the substation LAN 2 is much safer than the substation LAN 1.

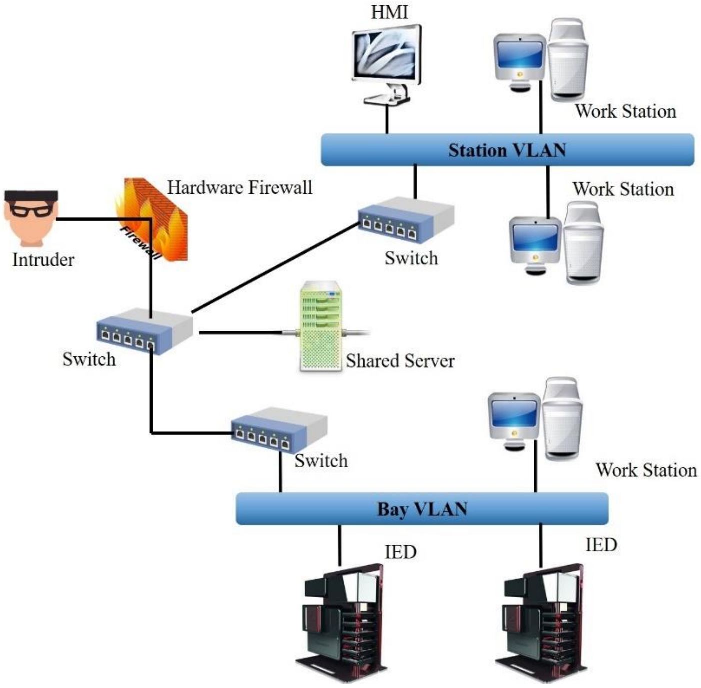


Figure 3-7 Attack paths on the substation LAN 2

Among all three categories of the substation LANs, the substation LAN 3 is the most automatic and safest one because of a local SCADA system which is used to locally and remotely control [45]. The communication and control between components are modular by building the local SCADA system. The licensed action between panels becomes possible due to the particular and standard protocols, such as IEC6185, IEC61870, and Modbus/TCP [46]. As there is only one component, the local SCADA system connected with the external, the HMI can be protected well against the external network. Therefore, if attackers want to successfully invade the HMI, the local SCADA system needs to be attacked firstly.

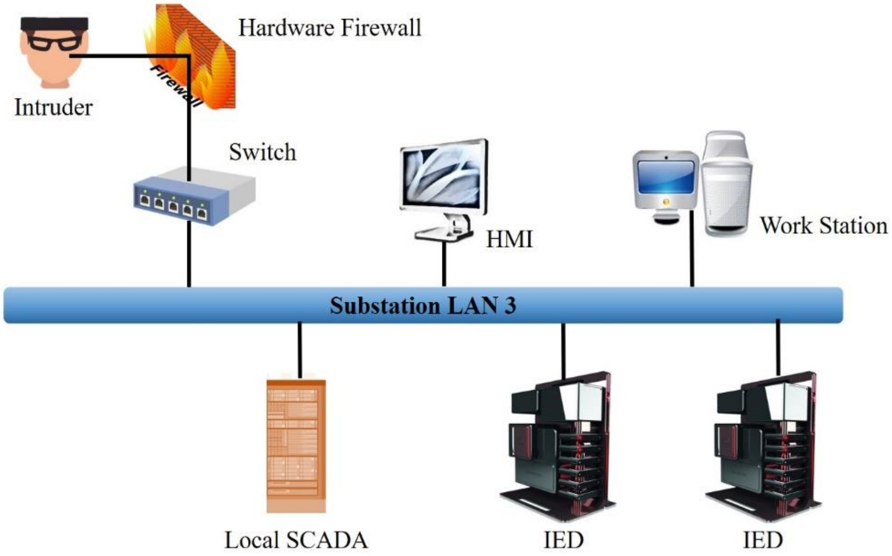


Figure 3-8 Attack paths on the substation LAN 3

3.2.2.4 MITM attacks on the communication links

Wired or wireless network provided the attack targets to attackers to set the bugging devices from the communication links between the control center and the substations [36]. So the entre of accessing is the communication links which may be entered the trip data by the intruder. As messages in the communication links of the SCADA system are too plain even though they are encrypted, it is easy for intruders to understand and decipher the information in messages by setting the bugging devices. This allows intruders to replace the real traffic data with the fabricated one and mislead some operators to take incorrect actions via the intrusion during the transmission.

3.3 Cyber Attack Graph Models in SCADA System of the Electric Power System

Bayesian Networks (BNs) are used to model the cyber attack graph in the SCADA system of the electric power system. Because the vulnerabilities of components in the SCADA system can be divided into LANs of the control center, corporation, substations, and communication links, corresponding attack graph are respectively classified into two models.

The first one models the probability of effective root privilege getting via LANs of the control center, corporation, and substations. Assuming an attack graph $G(V \cup C)$, V represents the vulnerabilities and C stands for component conditions. C is classified as service (S), standing as $\mathrm{service(host)}$; connection (N), which means as $< \mathrm{source\ hos, destiantion\ host} >$; and privilege (L), stated as $\mathrm{privilege(host)}$. Figure 3-9 is an example of a Bayesian attack graph model of vulnerabilities in the control center LAN. As for component conditions, they are satisfied as all pre-conditions are which are assumed to be the initial conditions or post-conditions occurred before [35]. Therefore, the privilege $\mathrm{user}(0)$ and the connection $< 0{,}1 >$ are required to be satisfied, and $\mathrm{Dos}(1)$ and $\mathrm{Exec}(1)$ need to be available to access by intruders. Then, the zero-day vulnerabilities $< \mathrm{Dos}, 0, 1 >$, $< \mathrm{Exec}, 0, 1 >$, $< \mathrm{ssh}, 1, 2 >$, and the known vulnerability $< \mathrm{bof}, 2, 2 >$ will be exploited one by one.

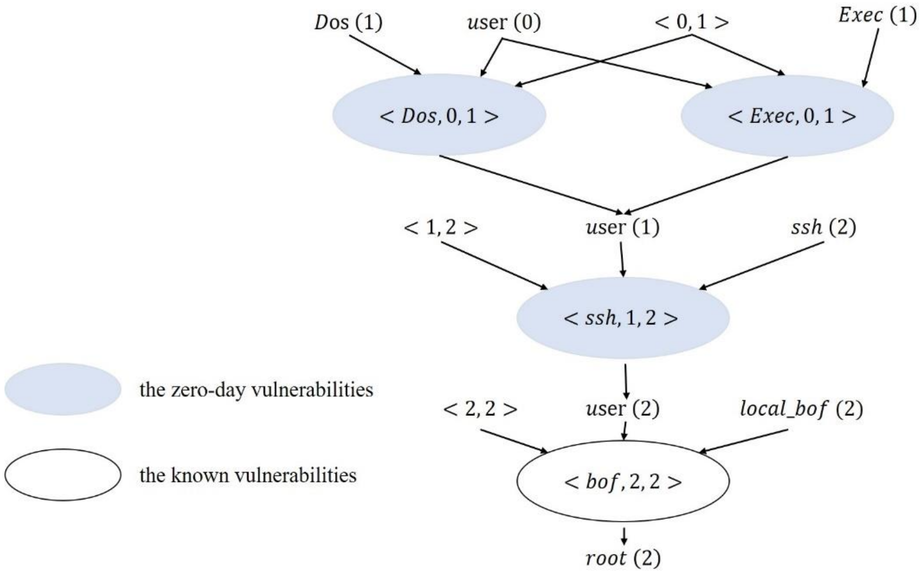


Figure 3-9 Bayesian attack graph model of vulnerabilities in the control center LAN

If any of the vulnerabilities is successfully attacked, the post-condition will be reached, which means the post-condition analysis is the key to evaluate the probabilities of successful attacks against the target components. According to [47], the probability that the vulnerability is exploited is represented as equation (3.1).

$$p(v_i \wedge c) = \begin{cases} p(v_i = T) \times p(c = T|v_i = T), & i = 1 \\ p(v_i = T) \times \prod_{j=1}^{i-1} p(v_j = F) \times p(c = T|v_i = T, v_1 \cdots v_{i-1} = F), & 2 \leq i \leq n \end{cases} \tag{3.1}$$

where i means different numbers of the pre-vulnerabilities which result to the vulnerabilities that are under attack finally. $p(v_i)$ is the probability that pre-conditions are reached and $p(c)$ is the probability that target conditions are reached.

Another attack graph model shows the attack paths in communication links of MIMT attacks. Figure 3-10 is an example with three layers. In Figure 3-10, counterplots are represented as A_j, while B_i is the sub-goals and C_m is overall goals.

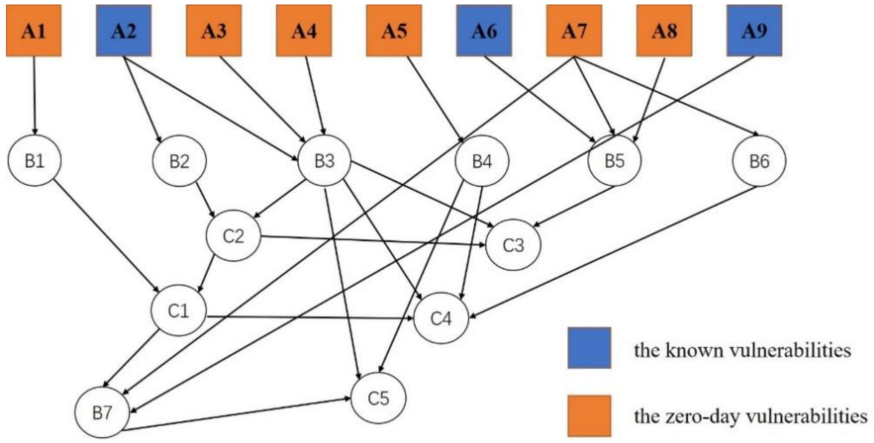


Figure 3-10 Bayesian attack graph model of vulnerabilities in the communication links

C_m can be achieved when all corresponding B_i are reached at the same time. So, the probability of C_m is related to corresponding B_i as shown in equation (3.2), while the probabilities that B_i are realized are related to A_j which can show the security level of countermeasures which are represented as equation (3.3). Additionally, it cannot be neglected that

B_i are not only related with A_j but also with C_m, like the relationship between B_7 and A_7, A_9, and C_1 in Figure 3-10.

$$p(C_m = T) = \prod_{i=1}^{n} p(B_i = T) \tag{3.2}$$

$$p(B_i) = \sum_{j=1}^{n} p\left(B_i = T \middle| A_j\right) \cdot p\left(A_j\right) \tag{3.3}$$

3.4 MTTC Estimation of Cyber Attacks on SCADA System of Electric Power System

3.4.1 Compromise time model of vulnerabilities

To calculate the compromise time of vulnerabilities, three statistical steps are identified to describe the actions of a successful intrusion. Step 1 describes the issue that one or more vulnerabilities are exploited by the intruders. Reference [41] assumes the probability of an attack in step 1 as P_1 which is calculated by the search theory [48] as follows:

$$P_1 = 1 - e^{-V \times E/S} \tag{3.4}$$

where V is the amount of the known vulnerabilities. E represents the quantity of exploits which are related to the attack skill levels. In this study, E are assumed as 50, 150, 250, 360 respectively corresponding to the novice, beginner, intermediate and expert. S is the quantity of all kinds of vulnerabilities of the examined system. In this study, according to the National Vulnerability Database, S is set as 7000. According to [41], the mean time of exploit occurred in step 1 is 1 day. Without the exploit of the known vulnerabilities, the zero-day vulnerabilities will be examined in order to realize the attacks against the target system. S stands for the characteristics of components and database, and V' as well as E' represent the quantities of the zero-day vulnerabilities and exploits. So, like P_1, P'_1 is the probability that the zero-day vulnerability is exploited which can be calculated as equation (3.4), and the mean time of exploit is 1 day, too.

$$P'_1 = 1 - e^{-V' \times E'/S} \tag{3.5}$$

Step 2 indicates that there is no exploit can be attacked by the attackers. Thus, step 2 and step 1 are mutually exclusive, which means the probability of step 2 are $1 - P_1$ and $1 - P'_1$ corresponding to the known vulnerabilities and the zero-day vulnerabilities. And the mean time of each attack on one exploit is 5.8 days [41], so the total mean time of step 2 can be estimated as follows:

$$t_2 = 5.8 \times ET \tag{3.6}$$

where ET represents the frequency expectation of tries on searching for new exploits, and it is denoted as equation (3.7):

$$ET = k \times 1 + \sum_{i=1=2}^{V-AM+1} \left[i \times \prod_{j=2}^{i} \left(\frac{V-AM-j+2}{V-j+1} \right) \right] \tag{3.7}$$

where AM is the average quantity of the vulnerabilities that require for creating or finding, and k is the factor showing the attack skill levels which is $k = AM/V$.

In step 3, both vulnerabilities and exploits can be found after previous steps. The mean time between vulnerabilities (MTBV) is calculated in [41], and as there are different kinds of vulnerabilities, MTBV are set as 30.42 days and 5.8 days when the time intervals of the known vulnerabilities change. As for the zero-day vulnerabilities, more time is needed, so the MTBV is assumed as 65 days and 32 days. Therefore, the lifetime of the known vulnerabilities and the zero-day vulnerabilities are evaluated respectively as equation (3.8) and (3.9).

$$t_3 = \left[\left(\frac{1}{k} - 0.5 \right) \times 30.42 \right] + 5.8 \tag{3.8}$$

$$t_3 = \left[\left(\frac{1}{k} - 0.5 \right) \times 65 \right] + 32 \tag{3.9}$$

where $\frac{1}{k}$ represents the ration of vulnerabilities, which is $\frac{1}{k} = V/AM$ [41].

Therefore, for the known vulnerabilities, the total compromise time is denoted as follows:

$$T = t_1 P_1 + t_2(1 - P_1)(1 - u) + t_3 u(1 - P_1) \tag{3.10}$$

where u is the probability if step 2 is failed. And the total compromise time of the zero-day vulnerabilities is obvious as follows:

$$T' = t_1 P'_1 + t_2(1 - P'_1)(1 - u') + t_3 u'(1 - P'_1) \tag{3.10}$$

3.4.2 MTTC in the SCADA system with cyber attacks

Combining the attack graph models $G(V \cup C)$, the MTTCs of the overall goal conditions can be estimated. As initial conditions are pre-conditions without exploited vulnerabilities, the goal conditions are the post conditions which can be realized by the exploitation of vulnerabilities, so the MTTCs of the overall goal conditions are the MTTCs of all the post-conditions which denoted by the every MTTC of each exploit. Assuming one goal condition is c, its MTTC is:

$$MTTC(c) = \frac{\sum_{v_i \in V} T(v_i) \cdot p(v_i \wedge c)}{p(c)} \tag{3.11}$$

where $T(v_i)$ indicates the MTTC that exploiting the vulnerability v_i takes, and $p(v_i \wedge c)$ represents the probability of the success exploiting of the vulnerabilities. $p(c)$ is the probability showing the reaching of the goal condition [35].

According to two Bayesian attack graph models, the MTTCs of goal conditions can be evaluated. For attack paths in the control center LAN, corporation LAN, and substation LANs, supposing $\mathrm{n}-1$ goal conditions need to be reached before the successful intruding, the overall MTTC is calculated as equation (3.12):

$$MTTC = \sum_{j=1}^{n} MTTC(c_j) \tag{3.12}$$

While for attack paths in the communication links, each exploiting rate aiming at each vulnerability on the counterplots needs to be considered, which represents the process that v_j and c are substituted into A_j and B_i. The MTTC to reach the sub-goal is:

$$MTTC(B_i) = \frac{\sum_{v_i \in V} T(A_j) \cdot p(A_j \wedge B_i)}{p(B_i)} \tag{3.13}$$

where $T(A_j)$ is the MTTC that the known vulnerabilities or the zero-day vulnerabilities on the counterplots A_j are exploited. Additionally, because of the “AND” relationship between the sub-target B_i and the overall goal C_m, the overall MTTC is:

$$MTTC(C_m) = \sum_{j=1}^{n} MTTC\ (B_i) \tag{3.14}$$

3.5 Simulation and Reliability Analysis

3.5.1 Bayesian attack graph models and MTTC evaluation of the SCADA system considering cyber security

3.5.1.1 Bayesian attack graph models and MTTCs of attacks on the control center LAN

In Figure 3-11, the attack path on the control center LAN is illustrated. The path that the root privilege of the application server in the control center LAN is intruded from the attacker $(host(0))$ to the target server $(host(2))$. As the zero-day vulnerabilities are easier to be firstly exploited in the control center, $<\mathrm{Dos},\ 0,\ 1>$ and $<\mathrm{Exec},\ 0,\ 1>$ are two zero-day vulnerabilities used in the historian $(host(1))$, as well as $<\mathrm{ssh},\ 1,\ 2>$ is another one in the application server. The root privilege may be stolen when $<\mathrm{bot},\ 2,\ 2>$ which is assumed as a known vulnerability in exploited.

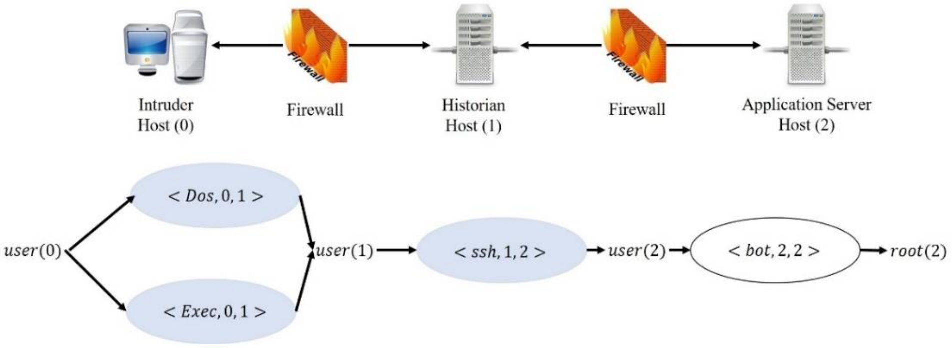


Figure 3-11 The attack path of the control center LAN

The MTTCs of the attack on the control center LAN are showed in the Figure 3-12. Corresponding to different attack levels (novice, beginner, intermediate, and expert), about 1039 days, 401 days, 163.5 days, and 44 days are needed respectively to realize the cyber attacks on the control center. Additionally, it can be seen that the higher attack skill level is, the less MTTC is needed.

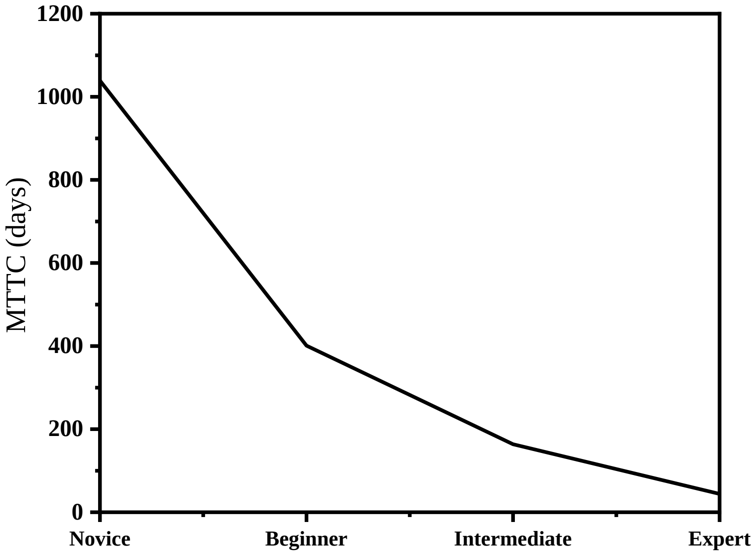


Figure 3-12 The MTTCs of the attack on the control center LAN

3.5.1.2 Bayesian attack graph models and MTTCs of attacks on the corporation LAN

In the corporation LAN, because of two firewalls, the external system can only be connected to the web server $(host(1))$, and if the attackers want to intrude the database server, they need to open the FTP server by using its vulnerability. The attack path of the cyber attack on the corporation LAN are stated in Figure 3-13, and through estimating the probability of hitting each exploit ($<\text{ftp}, 1, 2>$, $<\text{DB}, 2, 3>$, and $<\text{DB}, 1, 3>$), the MTTCs under different attack skill levels can be evaluated as shown in Figure 3-14. 734 days, 289.6 days, 120 days, and 39.3 days are needed to finish a successful intruding. Compared with the MTTCs of the intruding in the control center LAN, even though there are more exploits in the corporation LAN, only one kind of zero-day vulnerability is exploited. Thus, the values of overall MTTCs are less than that of the control center LAN.

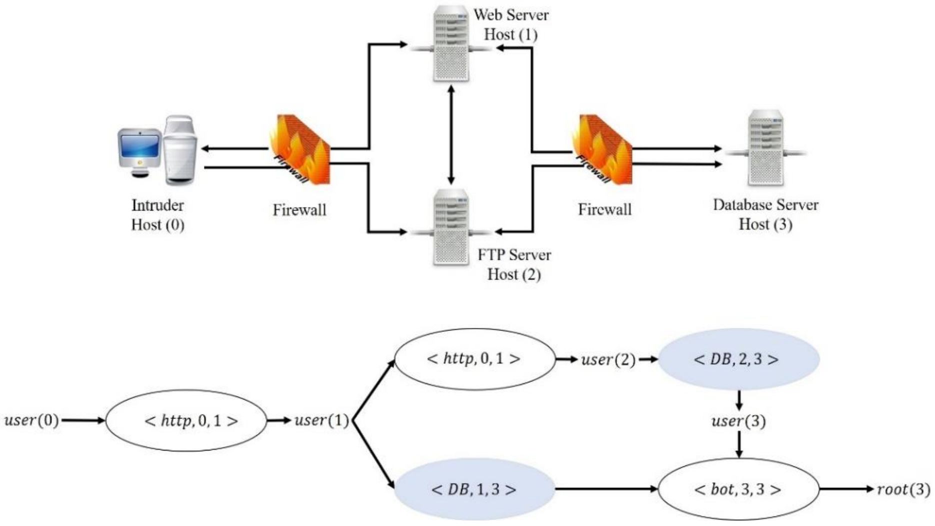


Figure 3-13 The attack path of the corporation LAN

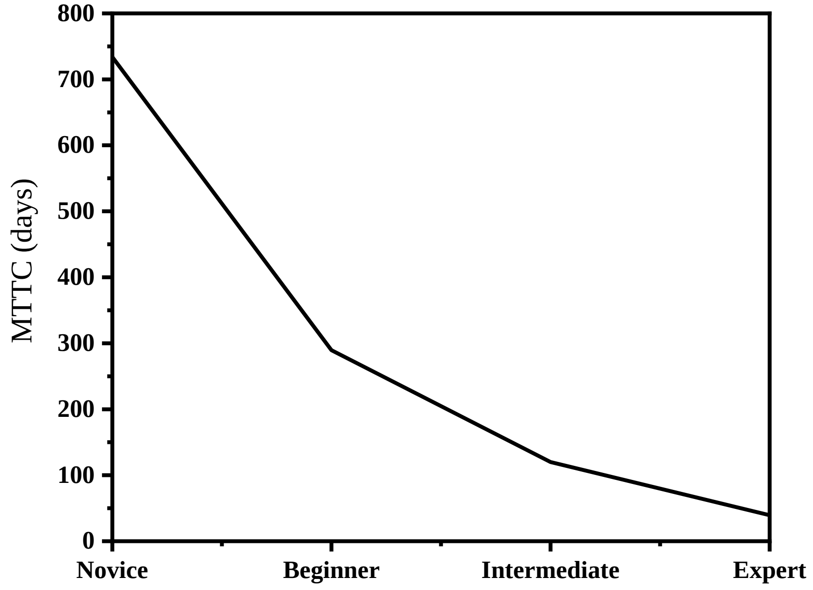


Figure 3-14 The MTTCs of the attack on the corporation LAN

3.5.1.3 Bayesian attack graph models and MTTCs of attacks on the substation LANs

As there are three kinds of substation LANs in the SCADA system of electric power system, the Bayesian attack graph are classified into 3 models as well. For the simplest substation LAN (the substation LAN 1), once the only one firewall and two exploits in HMI are accessed, the root privileged will be stolen. The attack path is shown in Figure 3-15 (a). For the substation LAN 2, VLAN and the Bay VLAN are equipped to increase the security level, resulting in the finding of the known vulnerabilities by the fast communication between them. In Figure 3-15 (b), one path is that $< \text{ftp},\ 1,\ 2 >$ and $< \text{ssh},\ 1,\ 2 >$ are two vulnerabilities in the HML and can be exploited by hitting the exploit $< \text{DB},\ 0,\ 1 >$. The root privilege will be obtained then. Another path is that attackers can steal the root privilege by hitting $< \text{ssh},\ 0,\ 2 >$ and $< \text{ftp},\ 0,\ 2 >$ in the HMI straightforwardly. As for the substation LAN 3 in Figure 3-15 (c), like the attack path of the corporation LAN, as the local SCADA is the only component that is able to be externally controlled, once one known vulnerability $< \text{http},\ 0,\ 1 >$ of the local SCADA is used, the HMI will be reached.

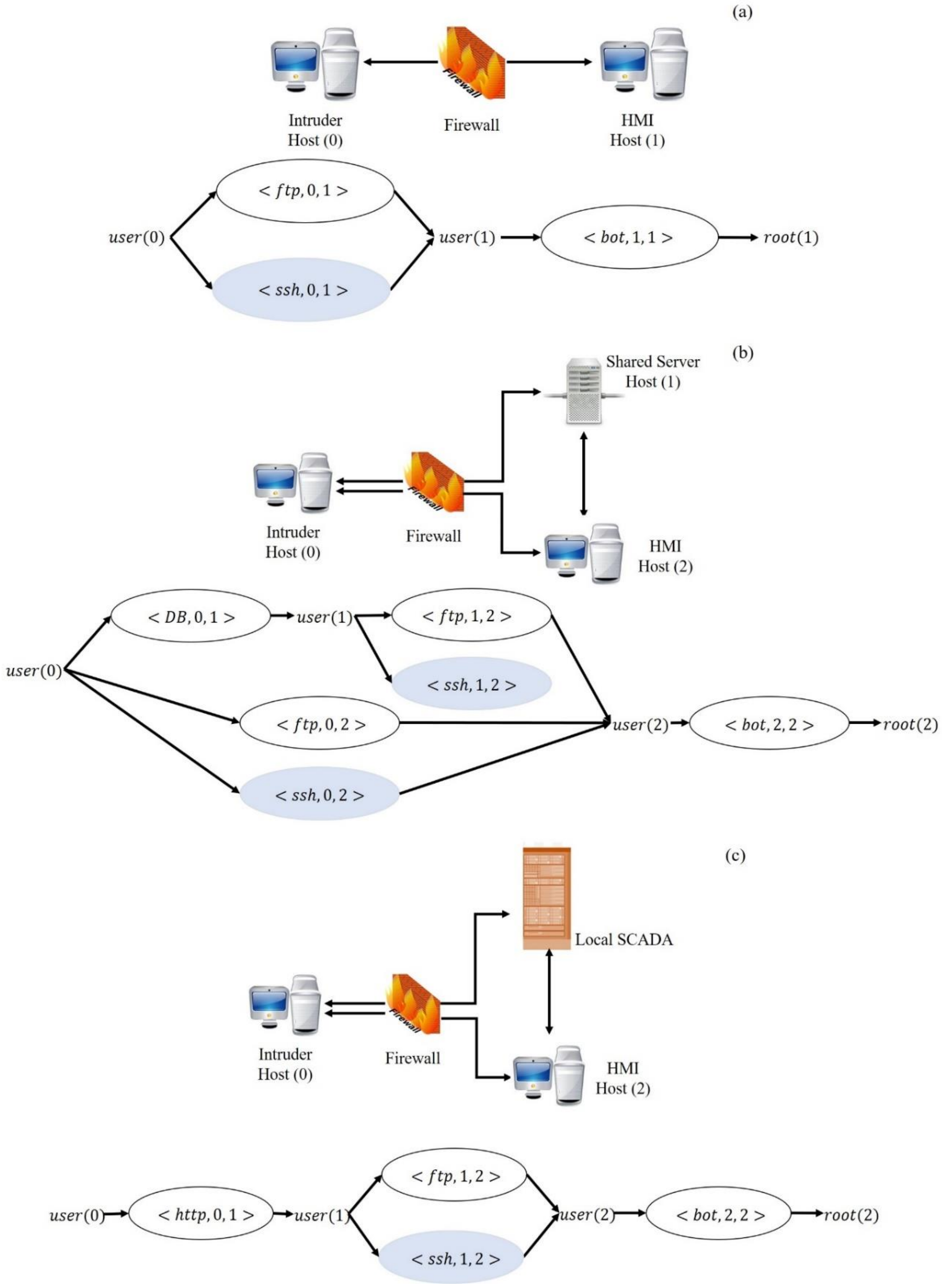


Figure 3-15 The attack path of the substation LANs: (a) LAN 1 (b) LAN 2 (c) LAN 3

Figure 3-16 shows the MTTCs values of reaching the attack targets in three kinds of substation LANs. Assuming that there are totally 24 substations in the studied SCADA system, 12 substations, 8 substations and 4 substations use the substation LAN 1, LAN 2, LAN 3 respectively. It shows that the network of the substation LAN 1 is the weakest one because of the lowest MTTCs compared with the substation LAN 2 and LAN 3. It may spend about half month to realize the attack aim for an expert. The MTTCs of the substation LAN 2 are about 1.1 times higher than the substation LAN 1, and the MTTCs of the substation LAN 3 are the highest because the network of LAN 3 is the most separate one due to the local SCADA system, which are more than 1.5 times higher than the MTTCs of the substation LAN 1.

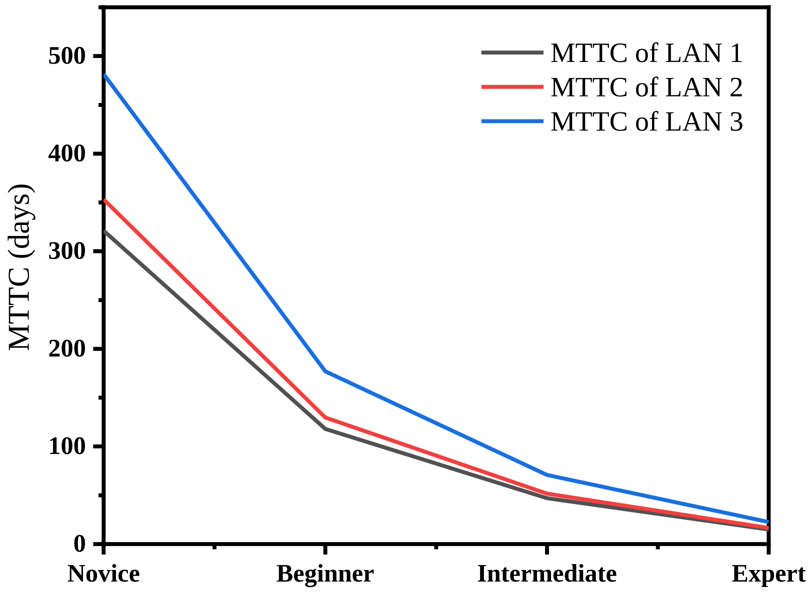


Figure 3-16 The MTTCs of the attack on the substation LANs

3.5.1.4 MTTCs of attacks on the communication links

24 links are investigated in this study, and according to equation (3.13) and equation (3.14), the MTTCs that need to take to realize a successful intruding in the communication links are shown in Figure 3-17. With the increase of the attack skill levels, the MTTC values still decrease.

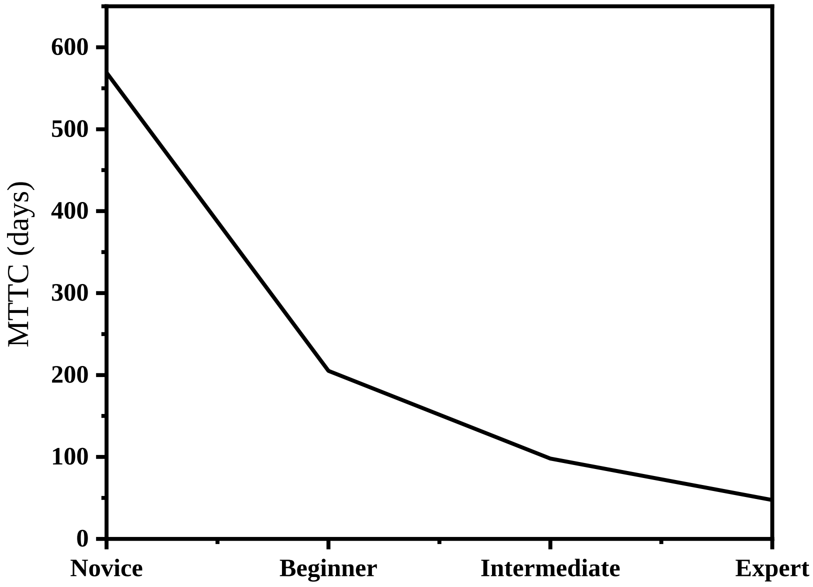


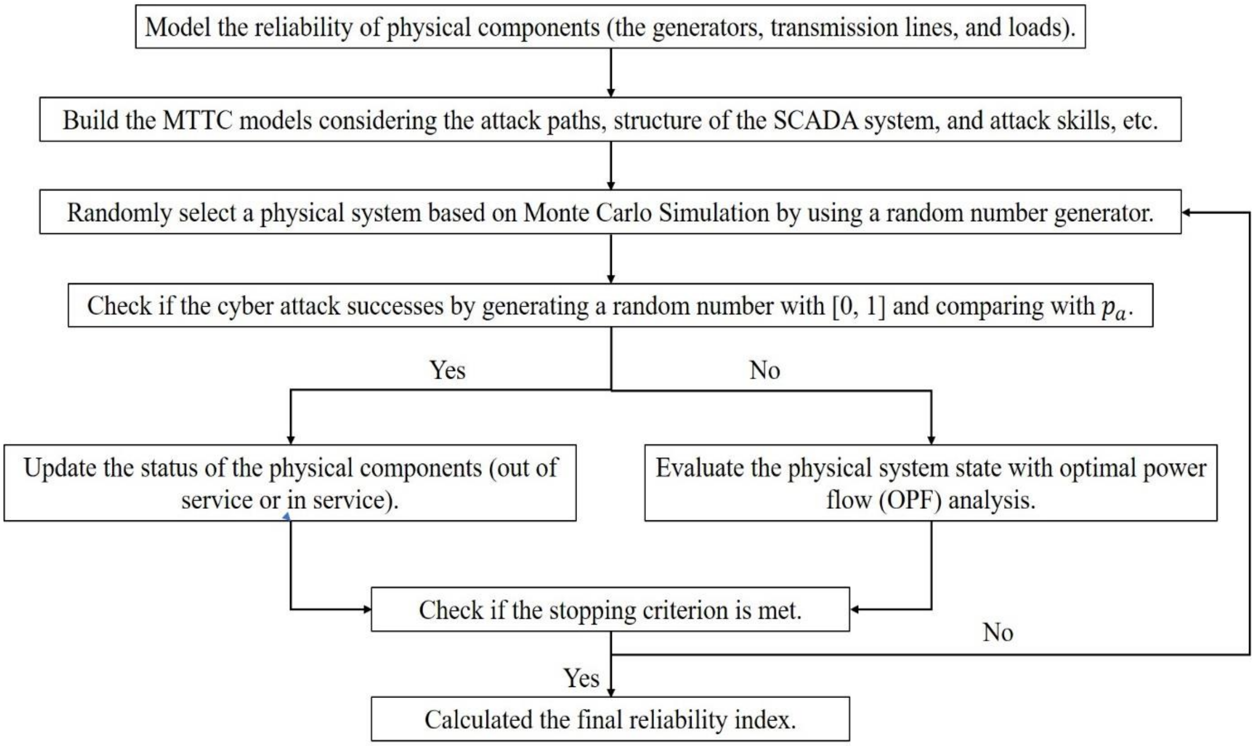
Figure 3-17 The MTTCs of the attack on the communication links

3.5.2 MCS and simulation process

To analyze the reliability of the SCDAD system of the electric power system, Monte Carlo Simulation (MCS) is applied. In the simulation process, it is assumed that all the cyber attacks continually onset. Once the attack reached its goal, the repairing of the system will start. The repair time of the system is related to the process of cyber debating and physical structure restoring, which is represented by the mean time-to-repair (MTTR). Therefore, the probability that a cyber attack is eventually successful in the SCADA system can be evaluated as equation (3.15).

$$p_a = \frac{MTTR}{MTTR + MTTC} \tag{3.15}$$

The simulation process based on MCS is stepped as Figure 3-18. The simulation is taken within 30 years, and the step is 1 hour.



Model the reliability of physical components (the generators, transmission lines, and loads).
Build the MTTC models considering the attack paths, structure of the SCADA system, and attack skills, etc.
Randomly select a physical system based on Monte Carlo Simulation by using a random number generator.
Check if the cyber attack successes by generating a random number with [0, 1] and comparing with p_a.
Yes
No
Update the status of the physical components (out of service or in service).
Evaluate the physical system state with optimal power flow (OPF) analysis.
Check if the stopping criterion is met.
No
Yes
Calculated the final reliability index.

Figure 3-18 The simulation process

3.5.3 Reliability analysis

Based on IEEE Reliability Test System 96 (RTS96), the system reliability of the SCADA system under 14 kinds of cyber attacks is analyzed. LOLP values are evaluated under 14 scenarios with 4 attack skill levels. The MTTR in this study is set as 4 hours. Table 3-1 lists 14 scenarios studied in this chapter, and Figure 3-19 is the LOLP curves of scenarios.

Scenarios	**Target of the cyber attacks**
1	The control center LAN
2	The corporation LAN
3	The communication links
4	The substation LANs
5	control center LAN and corporation LAN
6	control center LAN and communication links
7	corporation LAN and communication links
8	control center LAN and substation LANs
9	corporation LAN and substation LANs
10	communication links and substation LANs
11	control center LAN, corporation LAN, and links
12	control center LAN, corporation LAN, and substation LANs
13	corporation LAN, substation LANs, and links
14	control center LAN, corporation LAN, links, and substation LANs

Table 3-1 14 Scenarios with different targets of the cyber attacks

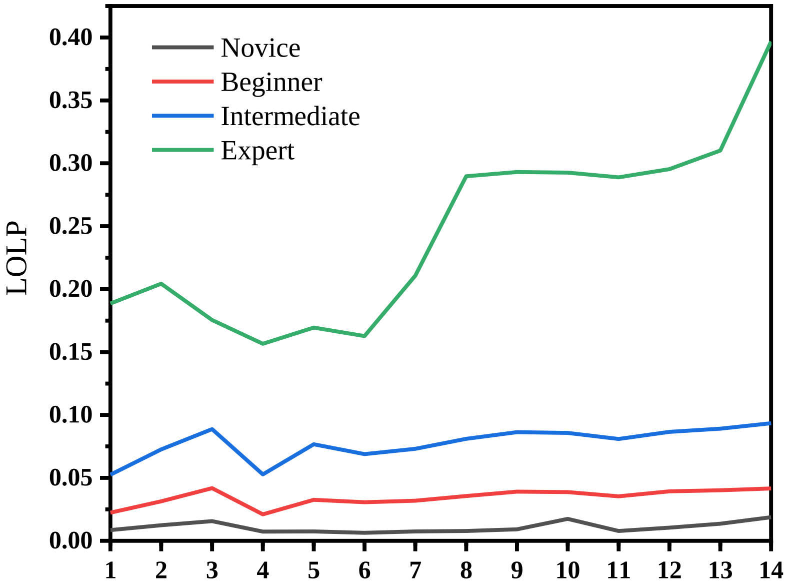


Figure 3-19 LOLP values of 14 scenarios

In Figure 3-19, the value of LOLP is changing with the change of the probability p_a that a caber attack is eventually successful in the SCADA system. This is because p_a is influenced by the MTTC of different systems, and the lower MTTCs are, the higher p_a and LOLP values are. Additionally, corresponding to the different attacking skill levels, LOLP values change as well. The highest LOLP value comes from the cyber attacks by expert, which means the whole system is in the most dangerous condition when experts do the attack.

3.6 Summary

In this chapter, Bayesian Networks are used to model the attack paths in the SCADA system by classifying them into two categories. MTTCs of successful attacks with four attack skill levels on different Bayesian attack graph models are estimated. It is found that the value of MTTC is closely related to the quantity of exploited known vulnerabilities and the attack skill levels. Monte Carlo Simulation is used to simulate the LOLP curves based on IEEE RTS 96. With the shortening of the MTTC, LOLP values increase, which means the whole system is more dangerous with less reliability.

Chapter 4 Reliability Analysis of the SCADA System Considering Cyber Attacks and Their Lurking Strategies

4.1 Introduction

Cyber security is facing the most severe situation now because of the closely relationship between physical structure with the Internet. Various cyber threats in the cyberspace attack the system via kinds of ways. One of the most dangerous way to the system reliability is from the lurking of modern threats [49]. The lurking of the cyber attacks can be also called rootkits, which is harmful to the operating system by inserting malware to tamper the kernel like the jump tables or file system handlers. This kind of cyber attacks can hide their ways on the compromised system without calling the attention of operators and finally successfully intrude the system. On the other hand, as the lurking time of the cyber attacks can be as long as possible, cyber attacks become into the latent persistent cyber threats, hiding the fact that the system is under serious attacked from the user. In other words, although attackers already have reached the root privilege of the system, it is still invisible to the operators, so that latent persistent cyber threats can control the system and tamper the kernel continuously for deeper and longer lurking. Finally, by making operators to think that their system is safe enough and under perfect protection, the system losses control completely [50].

In order to protect the cyber security, it requires users and the intrusion detection system (IDS) to take actions as soon as the cyber attack is found. However, even though there are amount of researches on the system protection of computer hardware and software considering the lurking of cyber threats were finished, studies on the cyber security of the SCADA system in the electric power system considering the lurking of cyber attacks are few. In this study, different lurking strategies of cyber attacks are considered, and their impacts on the reliability of the SCADA system are analyzed. Monte Carlo Simulation (MCS) is used to simulate the reliability analysis by calculating the factors.

In this chapter, in 4.2, the reliability of the SCADA system is analyzed under the lurking strategy 1 that cyber attacks will be lurking is considered, and the reliability factors are compared with that of cases that cyber attacks won't be lurking. With the probabilities that cyber attacks may be detected during their lurking, a limitation of lurking time is set, and corresponding reliabilities of the SCADA system are discussed as the lurking strategy 2 in 4.3. In 4.4, based on the result in 4.3, the lurking strategies are optimized by optimizing the limitation of the lurking time via Hill Climbing (HC) algorithm, to reach the most dangerous situation of the system as the lurking strategy 3, and the system reliability is studied. In 4.5, the detection of cyber attacks during the lurking process is considered, and different probabilities of detection are set to analyze the system reliability considering the optimized limitation of lurking time based on the result in 4.4.

4.2 Reliability Analysis of the SCADA System Considering Lurking Threat

4.2.1 Lurking strategy

In this lurking strategy, only the behavior of lurking that cyber attacks may hide their presence from the operators is considered. Lurking time is chosen to qualify the behavior of lurking. Only generator buses are discussed in this Chapter, so according to the structure, 33 generator buses of IEEE RTS 96 are studied and divided into 9 groups as shown in Table 4-1.

Groups	**Generator Buses Number**
1	101, 102, 107, 113
2	114, 115, 116, 118
3	121, 122, 123
4	201, 202, 207, 213
5	214, 215, 216, 218
6	221, 222, 223
7	301, 302, 307, 313
8	314, 315, 316, 318
9	321, 322, 323

Table 4-1 Classification of 33 generator buses

It is assumed that every attack against on the generator bus is able to lurk, when the maximum of lurking time of each bus in the group is reached, all the generator buses in this group will be under effectively attacks and out of service immediately at the same time. Figure 4-1 illustrates an example of lurking strategy 1.

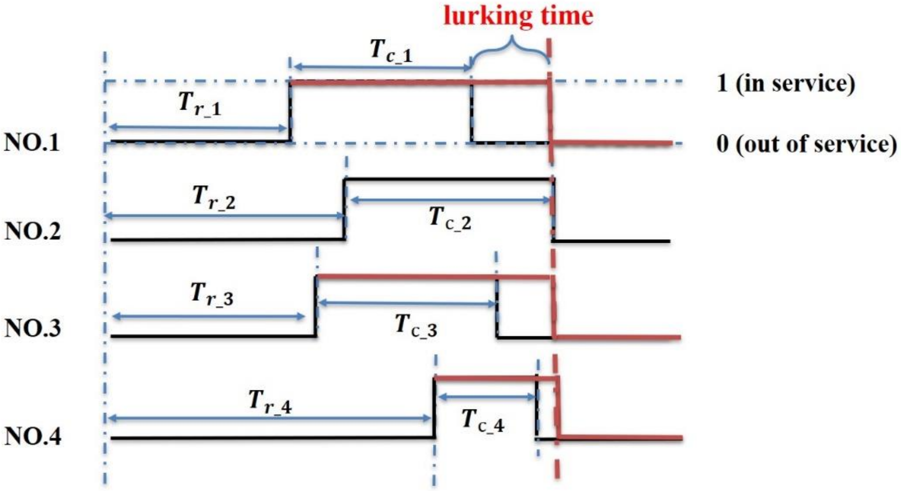


Figure 4-1 Example of lurking strategy 1

In Figure 4-1, there are 4 generator buses in the group, and T_{c_i} is the time to compromise of each generator bus, which is exponentially related to MTTC, and T_{r_i} is the time to repair of each generator bus that is exponentially related to MTTR. When the bus status is 1, the bus is in service, otherwise, the bus is out of service. The time that is prolonged is the lurking time of each generator bus. It assumed that when the longest T_{c_i}, for example, T_{c_2} of bus NO.2 in this example, is reached, which means that the last compromise time is finished, all other buses in this group will take actions and the bus status will change into "0" immediately at the same time. This kind of attacks might occur when there is no protection in the newly-built electric power system, so cyber attacks can hide from the users as long as possible.

4.2.2 Reliability analysis considering lurking threat

Sequential Monte Carlo Simulation is used to evaluate the reliability indexes of the SCADA system of the electric power system. LOLP and EENS are chosen to reflect the system reliability in this study. LOLP values of the system considering cyber attacks under lurking strategy 1 is shown in Figure 4-2.

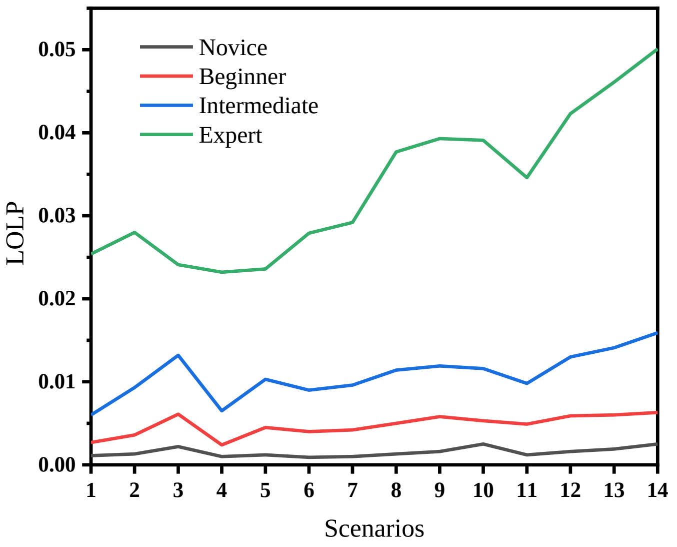


Figure 4-2 LOLP values of scenarios considering cyber attacks under lurking strategy 1

Compared with the scenarios under cyber attacks without lurking behavior, LOLP values decrease than previous values. The highest LOLP value now is 0.050, which is about 3 times lower than before. This is because with the classification of generator buses, the freedom of cyber attacks will be limited within one group, and the compromise time of some cyber attacks will be shorten owing to the limitation created by other cyber attacks. But the expert level still shows the highest LOLP due to the low MTTC. EENS values are also calculated as shown in Figure 4-3.

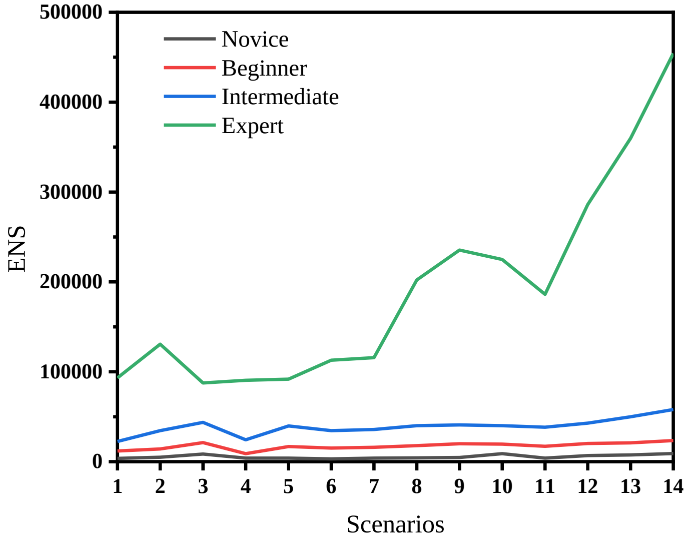


Figure 4-3 EENS values of scenarios considering cyber attacks under lurking strategy 1

It can be seen that, after taking lurk into consideration, EENS values don't change as much as LOLP values, and some of them even a little higher than EENS values of scenarios facing with cyber attacks which are without lurk. Different from the LOLP values, EENS values can show the predictability of the electrical system. So after considering lurk, the electric power system becomes more unpredictable and much more dangerous.

As EENS values are better to reflect the influence of cyber attacks with lurking strategies and are more appropriate to analysis the system reliability than LOLP values, it will be more focused as the reliability index in the following studies.

4.3 Reliability Analysis of the SCADA System Considering Lurking Time and Its Limitation

4.3.1 Lurking strategy

In lurking strategy 1, as every cyber attack can hide their presence to the user, the drastic measures for cyber attacks is to wait till the last compromise time is reached among all generator buses and all the cyber attacks take actions together, creating the hugest impact on the electric power system. However, for the electric power system under various overall protection, no attacker is willing to do as above, because there are probabilities that cyber attacks in the system can be detected or found during their lurking time. Hence, the limitation of the lurking time is set to simulate the smart cyber attacks. Only generator buses are discussed.

It is assumed that every attack against on the generator bus is able to lurk, and a maximum lurking time is set as 5days, 15days, 30days, and 90days, which are corresponding to that attackers will take actions at least one time per weekdays, per half month, per month, and per three months. When the limitation of lurking time is reach, all the generator buses will be under effectively attacks and out of service immediately at the same time. Figure 4-4 illustrates an example of lurking strategy 2.

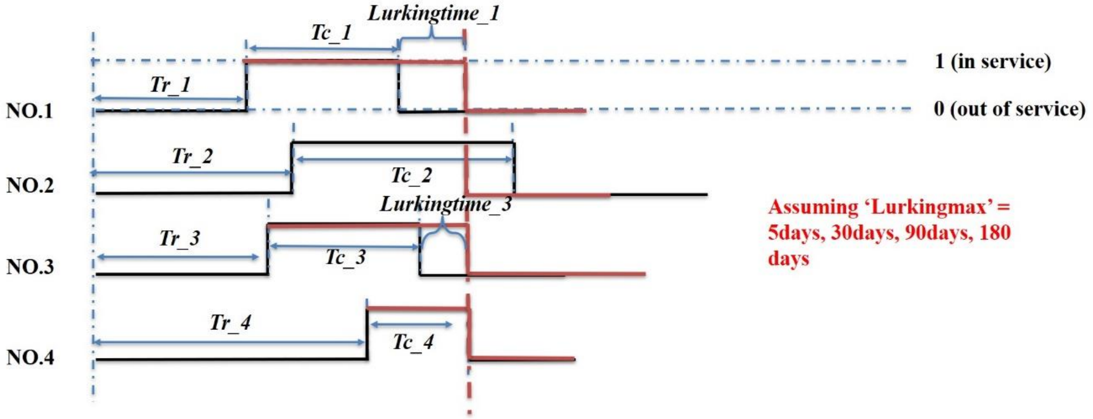


Figure 4-4 Example of lurking strategy 2

In Figure 4-4, assuming the maximum of the lurking time of each bus is 5 days, 15days, 30 days, and 90 days respectively, when the limitation of lurking is reach on one bus, all T_{c_i} in this group will be renewed to equal as the T_{c_i} of the attack on bus which reach the lurking limitation. Lurking strategy 2 is much more practical and closer to the cases in reality, because the original intention of attackers is to create the damage on the electric power system successfully.

4.3.2 Reliability Analysis Facing with Attacks within Different Limitation of Lurking Time

Sequential Monte Carlo Simulation is used to evaluate the reliability factors of the SCADA system of the electric power system. The limitation of the lurking time of buses are set as 5days, 30days, 90days, and 180 days. EENS values of scenarios under cyber attacks considering the limitation of lurking time (5days, 30days, 90days, 180days) are stated as follows.

It can be seen that EENS values are almost higher than that in the Figure 4-3 and that of scenarios under cyber attacks without lurking action. The highest EENS value in Figure 4-5 (a)-(d) are 521988, 489132, 421678, and 399976 respectively. And the expert level still creates the highest EENS values, and with the increase of limitation time, gaps between the novice level, beginner level, intermediate level and expert level are more and more narrow. It indicates that, because of the limitation of lurking time, even though the compromise time of each attack is shortened, the frequency of attacks is raised owing to the fast renewing speed of the compromise time and repair time, so cyber attacks will cause worse damage on generator buses, finally embodied in the increase of EENS values.

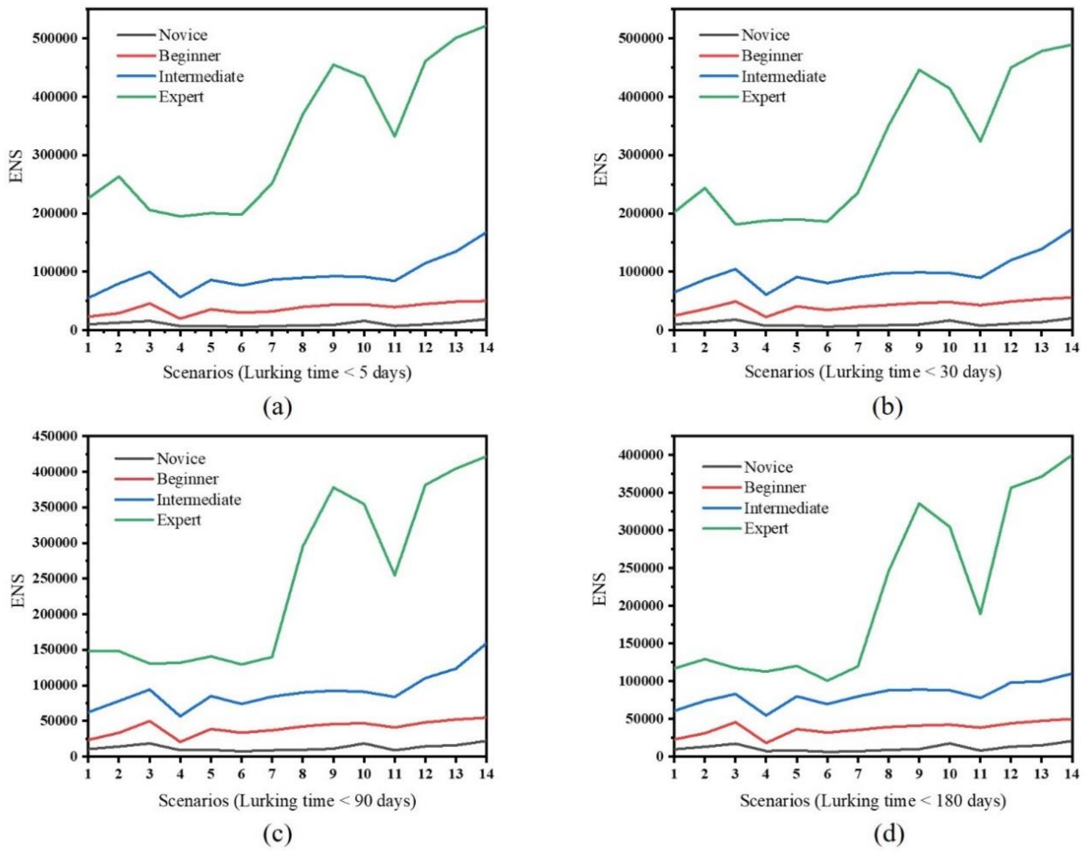


Figure 4-5 EENS values of scenarios considering cyber attacks under lurking strategy 2：(a) the limitation of lurking time = 5 days, (b) the limitation of lurking time = 30 days, (c) the limitation of lurking time = 90 days, (d) the limitation of lurking time = 180 days

4.4 Reliability Analysis of the SCADA System Considering the Optimization of Lurking Strategies

4.4.1 The optimization of the lurking strategy

From Figure 4-5, it is obvious that even though most of the EENS values of 4 different attack skill levels are higher than before, there are some values decreasing, and the turning points are different among 4 different attack skill levels. This means that the change of the EENS values are not only related to the different lurking time limitation, but also to the attack skill levels. Under each skill level, to creating the worst impact on the reliability of the electric power system, the lurking strategy needs to be optimized by finding the right limitation of lurking time.

Hill Climbing (HC) algorithm is used to find the optimized limitation of lurking time. Hill Climbing algorithm is a locally preferred method. The heuristic method is an improvement on depth-first search. It uses feedback information to help generate the solution decision, which is a kind of artificial intelligence algorithm. Starting with the current node and comparing it with the values of surrounding neighbor nodes, if the current node is the largest, then the current node is returned as the maximum value (the highest point of the mountain); otherwise, the highest neighbor node is used to replace the current node, thereby achieving the purpose of climbing to the height of the mountain, which will keep cycling until the highest point is reached [51]. The optimization of the limitation of lurking time can be found via HC algorithm, and the corresponding reliability index can be evaluated via MCS.

4.4.2 Case study

Taking scenarios 1 as an example, scenario 1 is about the situation that the cyber threat attacks the control center LAN in SCADA system of the electric power system, and MTTCs of scenario

1 are 1039 days, 401 days, 163.5 days, and 44 days respectively when the skill levels are novice, beginner, intermediate and expert. The limitation of lurking time is set as 5 days, 30 days, 90 days and 180 days. EENS values are calculated and compared among different limitation as shown in Figure 4-6.

Figure 4-6 is the EENS value curve which shows that different curvilinear trends occur among different skill levels. For expert and intermediate, EENS values increase firstly and decrease later. This is because the MTTC of these two levels are 44 days and 163.5 days respectively. After closing to or even exceeding the limitation which is close to the MTTC of each skill level, the limitation of lurking time will have less function on the cyber attacks, resulting in smaller EENS values. However, for novice and beginner, EENS values don’t change as much as previous higher levels. This is because the MTTC of these two levels are 1039 days and 401 days, while the maximum limitation lurking time is only 180 days. There is light effect on each attack on every bus by setting the limitation of lurking time.

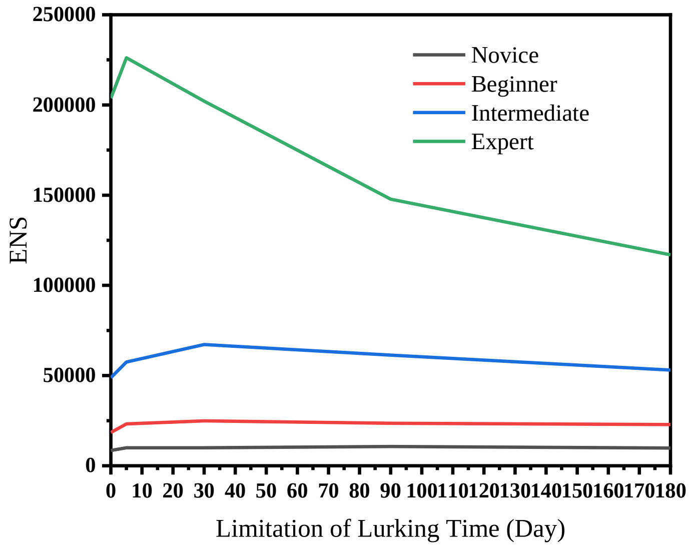


Figure 4-6 Comparison of EENS values among different limited lurking time

As the impact caused by attackers at novice and beginner levels is much lower than that caused by attackers at intermediate and expert levels, the latter two levels are more focused in this part. Figure 4-7 is the fitted curve which shows the EENS values of the system under expert and intermediate attacks with more different limitation of the lurking time.

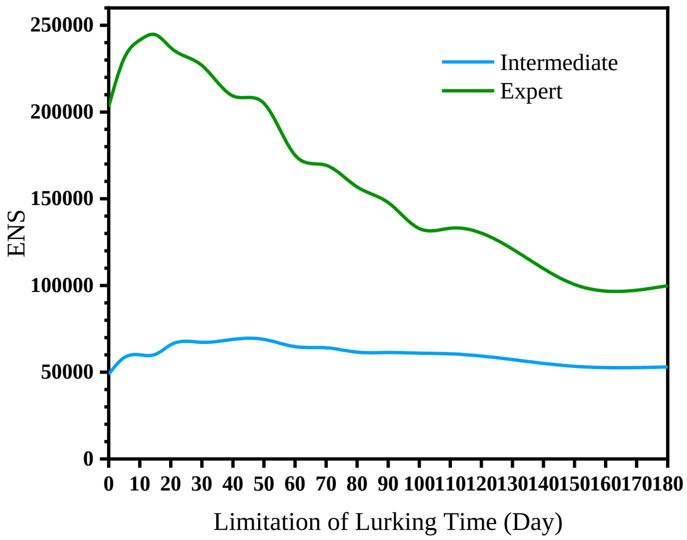


Figure 4-7 The fitted curve of EENS values

Hill Climbing (HC) algorithm is used to find the best limitation of lurking time which can result in the worst damage on the system reliability. Table 4-2 shows the optimization results of the right limitation of lurking time, and the corresponding EENS values are compared between the simulation result and fitted result in Figure 4-7.

Attack Skill Levels	The Right Limited Lurking	EENS Values	
Expert	16 days	Simulation Result	244776
		Fitted Result	245601
Intermediate	50 days	Simulation Result	68968
		Fitted Result	69374

Table 4-2 Optimization result of the right limitation of lurking time

EENS values in Table 4-2 have slight difference between the simulation result and fitted result, which indicates that the right limitation of the lurking time is found correctly. Under this limitation of the lurking time, EENS values are the highest, so cyber attacks create the worst damage on the corresponding generator buses, resulting in the harm on the reliability of the electric power system. Other scenarios can optimize their right limitation of the lurking time in the same way.

4.5 Reliability Analysis of the SCADA System Considering the Probability of Detection under Optimized Limitation of Lurking Time

4.5.1 Lurking Strategy

In reality, attackers are always facing with the detection from system protection software or hardware, which means, even though the limitation of lurking time is set, there's still probability for attackers to be found during the lurking process. Different probabilities of detection are set as 0.0005, 0.001, 0.005, 0.01 to imitate the process that cyber attacks could be found during their luring process. It is assumed that, once the attack is found, it will influence the status of corresponding bus immediately, and the T_{c_i} of this bus will be renewed. Considering the right limitation of lurking time, lurking strategies change, which will influence the result of system reliability.

4.5.2 Case Study

Taking scenarios 1 as an example, scenario 1 is about the situation that the cyber threat attacks the control center LAN in SCADA system of the electric power system. Based on results in 4.4, 16 days and 50 days are the right limitation of lurking time of expert-level cyber attacks and intermediate-level cyber attacks, which are used to be discussed here. Different probabilities of detection are set as 0.0005, 0.001, 0.005, 0.01. System reliability facing with cyber attacks of expert and intermediate levels are analyzed by MCS considering the detection of cyber attacks under the optimized limitation of luring time. EENS values of cases are shown as Figure 4-8 (a) and (b).

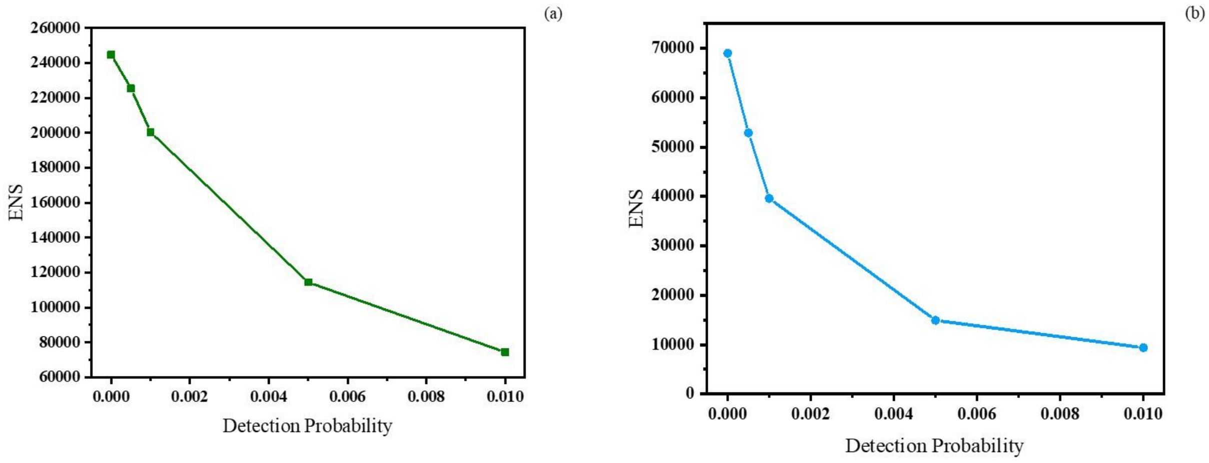


Figure 4-8 EENS values of cases: (a) considering the detection of expert-level cyber attacks, (b) considering the detection of intermediate-level cyber attacks

In Figure 4-8, it is obvious that both EENS values of two cases are decreased with the increase of the probability of detection. This is because once the cyber attack is found, the attack action will be taken immediately, the corresponding lurking time is shortened, so the system status is more predictable. For expert-level cyber attacks, the EENS value decreases from 244776 to 74450, almost 70%, and for intermediate-level cyber attacks, the EENS values decrease from 68968 to 9374, almost 87%. It can be inferred that when the probability of detection of cyber attacks is high enough, the EENS value will be as low as possible, the reliability of system will be the best. This result can be used to guide to draw up the protection strategy of the reliability of the SCADA/EMS system of the electric power system.

4.6 Summary

In this chapter, the lurking behavior is taken into consideration and the corresponding reliability indexes are calculated by using sequential Monte Carlo Simulation. EENS values are more focused to reflect the system reliability. By setting the parameter, lurking time, different lurking strategies are models. It shows that after considering the lurking behavior of cyber attacks, the system reliability will be facing with bigger challenge, and the EENS values increase a lot. To analyze the deepest impact on the system reliability, Hill Climbing (HC) algorithm is used to find the best limitation of lurking time, and EENS values are estimated and compared with the fitted results. Simulation results are very close to fitted results, so the optimization is successful to find the right limitation of the lurking time, and under found limitation, the system reliability will face the huge damage. Additionally, different probabilities of detection of cyber attacks are considered and discussed based on the optimizing results of limited lurking time. EENS values decrease with the increase of the probability of detection, and it can be inferred that when the probability of detection of cyber attacks is high enough, the EENS value will be as low as possible, and the reliability of system will be the best.

Chapter 5 Reliability Analysis of SCADA System Facing with Insider Attacks

5.1 Introduction

In the previous discussion, attacks focused are mainly from the external system and intrude the SCADA system via internet connecting facilities. However, the most harmful threat is the insider attacks which apply rights for despiteful purposes [52]. It is reported by the US Computer Security Institute (CSI) that the influence of insider attacks has exceeded the impact cause by viruses and worm since 2007 [53]. Though insider attacks have drawn attentions among the cyber security fields, there’s no standard definition reached a consensus by the researchers. In [54], the insider attack is defined and classified into two kinds of offenders, traitors and masqueraders:

- Traitors: Traitors are will-organized to grant access to systems and information database and take actions which are not in compliance with policies to impact confidentially, integrity, or availability of some information quality [55]. For example, in 2004, the Vodafone Greece, one of the Greek cell phone providers, faced with the issue that unwelcome software was hided into the operating systems and finally lead to a bad insider problem resulting in the equal of a rootkit on an internal Ericsson phone switch [56].

- Masqueraders: Masqueraders are attackers that successfully steal a user’s permission and act as another user for bad purposes. One of the best metaphors is credit card fraudsters.

Though much mature researches about insider attacks are studied in computer security, financial security, and information security in recent years, unfortunately, insider attacks in electric power system reliability and its countermeasures are far less focused. There seems to be little researches focused to study the insider attacks in the electric power system, so in this chapter, reliability of the SCADA system in the electric power system is analyzed considering insider attacks.

In 5.2, newly Semi-Markov models based on insider attacks in relevant components in the SCADA system are built, and corresponding MTTCs are evaluated. In 5.3, system reliability considering insider attacks is analyzed via LOLP curve estimated by MCS and compared with the original result in Chapter 3. Besides, lurking behavior and insider attacks are considered together, and EENS values are evaluated by MCS. Results are compared with them in Chapter 4.

5.2 SMP Models and MTTCs Evaluation of Insider Attacks in the SCADA System

SMP models are used to show the process of insider attacks on the SCADA system of the electric power system, and Figure 5-1 is the general model of the intrusion process. In Figure 5-1, G represents the good state which is safe in the system, and n states the process that the attack behavior. With the process is pushed forward, higher privileges will be stolen by the attacker, finally reaching the state F which is the failure state. States G and n are intrusion states with the transition ratio T_i, and the state F is the absorbing state. The transition probability of state changing from state i to state j is set as p_{ij}. In this study, the transition probability of state changing caused by insider attacks is set as 0.5. Obviously, insider attacks will change the transition probability in the same component.

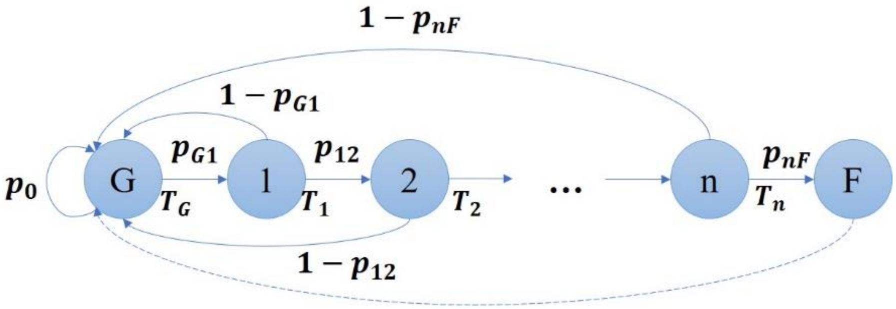


Figure 5-1 General SMP model of the intrusion process

The MTTC of SMP models is the mean time that transient states develop into absorbing states. It can be calculated from the transition matrix Q which consists of the transition probabilities p_{ij} as equation (5.1). With the change of transition probabilities, MTTCs value will change.

$$MTTC \ = \ \sum_{j \in S_i} V_j \, T_j \tag{5.1}$$

where V_j is the average times that state j has been performed till the final failure states are reached, and T_j is the mean sojourn time in state j which can be referred in [41]. V_j can be calculated as equation (5.2).

$$V_j \ = \ q_j \ + \ \sum_i V_i \, q_{ij} \, , \quad i, j \ \in \ S_i \tag{5.2}$$

where q_j is the probability that state j is the starting of the discrete-time Markov chain (DTMC) [39], and as assumption that initial state in this study is state G, so q_G is 1 and others are 0. $q_{ij}$is the element in transition matrix Q.

Insider attacks may realize via many approaches on the various components in the SCADA system of the electric power system. Details are as mentioned as follows.

5.2.1 Insider attacks in the control center LAN

Figure 5-2 illustrates the SMP model of insider attacks in the control center LAN. Similar to external cyber attacks, insider attacks can exist in the historian serve without calling the attention of the IDS as well, resulting in the loss of root privileges of the application serve at last. p_{G2} is the transition probability of insider attacks.

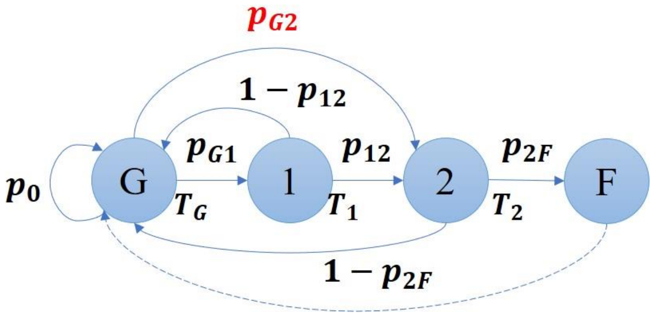


Figure 5-2 SMP model of insider attacks in the control center LAN

The transition matrix Q of this case is Q_1:

$$Q_1 = \begin{array}{c} \\ G \\ 1 \\ 2 \end{array} \begin{array}{c} \begin{array}{ccc} G & 1 & 2 \end{array} \\ \begin{bmatrix} (1-p_{G1}-p_{G2}) & p_{G1} & p_{G2} \\ 1-p_{12} & 0 & p_{12} \\ 1-p_{2F} & 0 & 0 \end{bmatrix} \end{array} \qquad (5.3)$$

Thus, MTTC of insider attacks in the control center LAN can be calculated as Figure 5-3. It can be seen that MTTC values of all four skill levels are 728, 269, 94, and 20, which are much lower than the previous results. This is because insider attacks are easier to attack successfully faster than external cyber attacks.

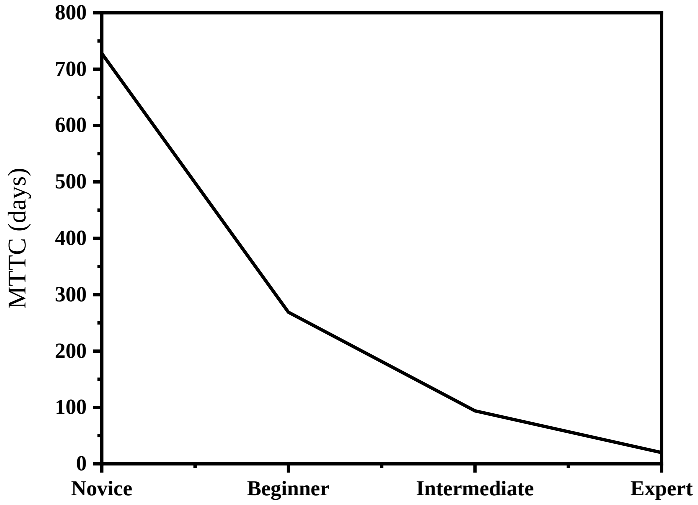


Figure 5-3 The MTTCs of insider attacks in the control center LAN

5.2.2 Insider attacks in the corporation LAN

The SMP model of insider attacks in the corporation LAN is as shown in Figure 5-4. If insider attacks have already existed into the FTP server, there is no need to use its vulnerability again and insider attacks can immediately affect the database serve. p_{2F} is the transition probability of insider attacks.

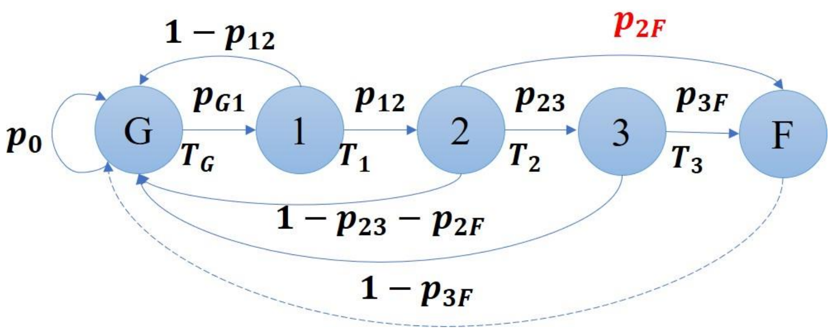


Figure 5-4 SMP model of insider attacks in the corporation LAN

The transition matrix Q of this case is Q_2. MTTC values under different skill levels are shown in Figure 5-5. Only 441, 103, 52, and 9.8 days are needed to realize the successful attack.

$$Q_2 = \begin{array}{c} \\ G \\ 1 \\ 2 \\ 3 \end{array} \begin{array}{c} \begin{array}{cccc} G & 1 & 2 & 3 \end{array} \\ \begin{bmatrix} 1-p_{G1} & p_{G1} & 0 & 0 \\ 1-p_{12} & 0 & p_{12} & 0 \\ 1-p_{23}-\ p_{2F} & 0 & 0 & p_{23} \\ 1-p_{3F} & 0 & 0 & 0 \end{bmatrix} \end{array} \tag{5.4}$$

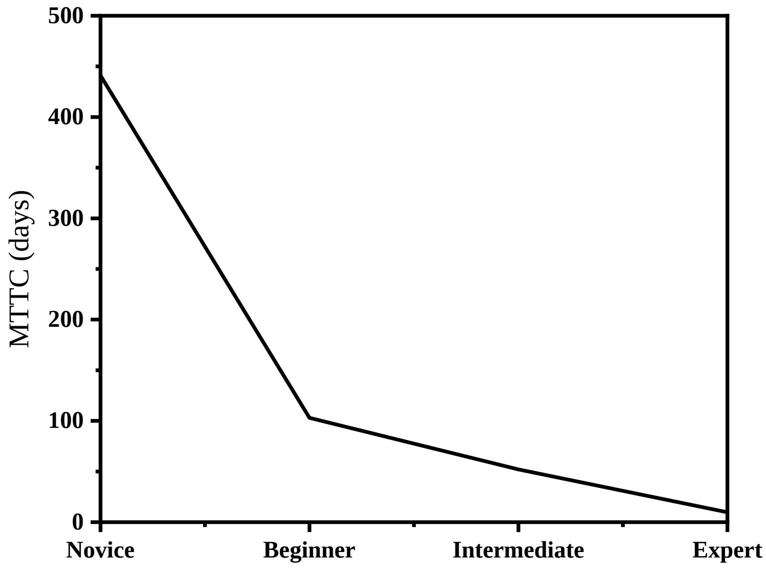


Figure 5-5 The MTTCs of insider attacks in the corporation LAN

5.2.3 Insider attacks in the substation LANs

Figure 5-6 (a)–(c) states SMP models that insider attacks happen in the substation LAN 1, LAN 2, and LAN 3. In the substation LAN 1, HMI is the target of insider attacks. Once insider attacks are successfully in the HMI, whole system is exposed to all attacks, which is extremely harmful to the system reliability. p_{GF} is the transition probability of insider attacks. In the substation LAN 2, as VLAN is equipped, shared server may be injected insider attacks. $p *_{G2}$ is the transition probability of insider attacks. And for the substation LAN 3, as local SCADA is the only component that is able to be externally controlled, insider attacks can only exist in HMI, and root privilege is easy to be obtained by attackers. p_{1F} is the transition probability of insider attacks.

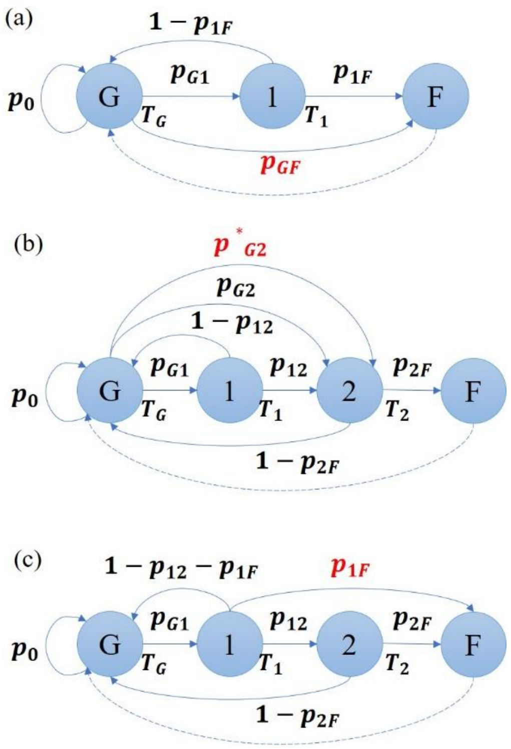


Figure 5-6 SMP model of insider attacks in the substation LANs

The transition matrix Q of these cases are Q_3, Q_4, Q_5. MTTC curves under different skill levels are shown in Figure 5-7.

$$Q_3 = \begin{array}{c} \\ G \\ 1 \end{array} \begin{array}{cc} G & 1 \\ \left[\begin{array}{c} (1 - p_{G1} - p_{GF}) \\ 1 - p_{1F} \end{array}\right. & \left.\begin{array}{c} p_{G1} \\ 0 \end{array}\right] \end{array} \quad (5.5)$$

$$Q_4 = \begin{array}{c|ccc} & G & 1 & 2 \\ \hline G & (1 - p_{G1} - p_{G2} - p^{*}_{G2}) & p_{G1} & p_{G2} * p^{*}_{G2} \\ 1 & 1 - p_{12} & 0 & p_{12} \\ 2 & 1 - p_{2F} & 0 & 0 \end{array} \quad (5.6)$$

$$Q_5 = \begin{array}{c|ccc} & G & 1 & 2 \\ \hline G & 1 - p_{G1} & p_{G1} & 0 \\ 1 & 1 - p_{12} - p_{1F} & 0 & p_{12} \\ 2 & 1 - p_{2F} & 0 & 0 \end{array} \quad (5.7)$$

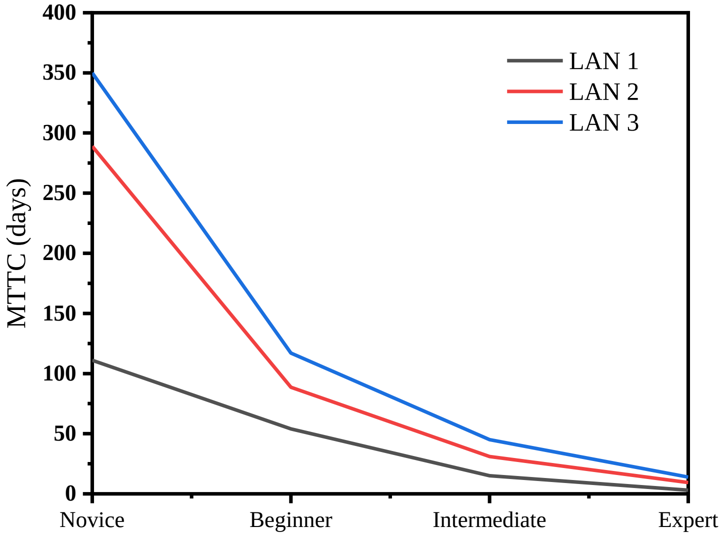


Figure 5-7 The MTTCs of insider attacks in the substation LANs

5.2.4 Insider attacks in the communication links

24 links in the SCADA system are studied. Because each of links can become the hidden point of insider attacks, according to equation (3.13) and equation (3.14), the MTTCs of insider attacks in the communication links are shown in Figure 5-8.

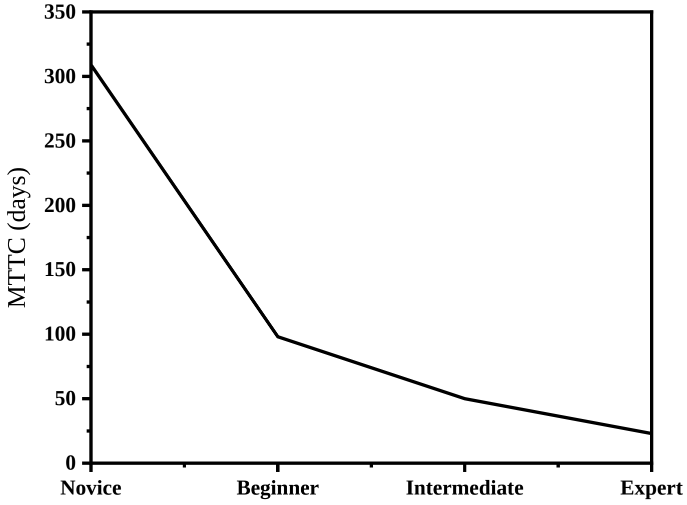


Figure 5-8 The MTTCs of insider attacks in the communication links

5.3 Reliability Analysis

5.3.1 LOLP values without considering lurking behavior

Based on IEEE Reliability Test System 96 (RTS 96), the same 14 targets in Table 3-1 are assumed to be facing with insider attacks and discussed here to get better comparison. MCS is used to simulate the reliability analysis. The MTTR in this study is still set as 4 hours. Considering 4 different attack skill levels, Figure 5-9 shows the LOLP values of scenarios.

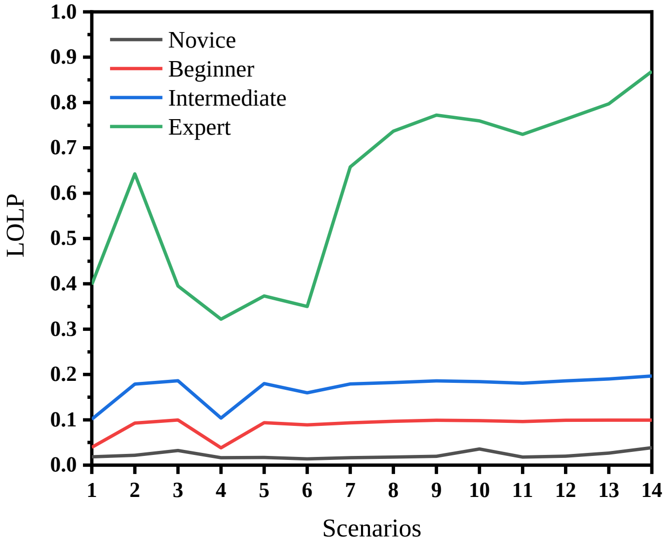


Figure 5-9 LOLP curves of 14 scenarios under insider attacks

In Figure 5-9, the value of LOLP are much higher than that in the results of external cyber attacks. This is because due to the insider attacks, shorter attacking paths are needed which result in the lower MTTCs. Under insider attacks, system reliability is worse and the whole system is in more dangerous situation.

5.3.2 EENS values considering both insider attacks and lurking behavior

Only 33 generator buses are discussed here and divided into 9 groups as shown in Table 4-1. Under the lurking strategy 1 in Figure 4-1, when the maximum lurking time of insider attacks of each bus in the group is reached, all other generator buses in this group will under effectively attacks and out of service immediately at the same time. Sequential Monte Carlo Simulation is used to calculate the EENS of 14 scenarios which is facing with insider threats and lurking behavior together. Results are shown in Figure 5-10.

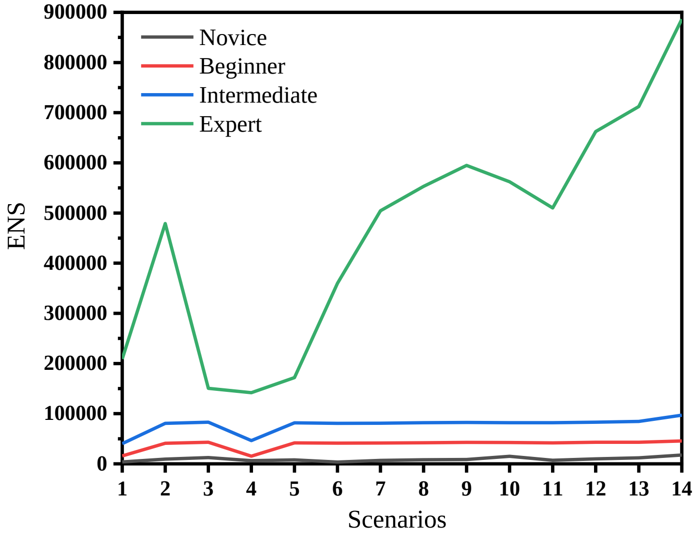


Figure 5-10 EENS curves of 14 scenarios under insider attacks considering lurking time

Compared with Figure 4-3, EENS values of scenarios considering insider attacks and lurking behavior dramatically increase, especially when the skill level of insider attacker is higher. It states that facing with insider attacks and lurking behavior at the same time, the SCADA system of the electric power system become more unpredictable and uncontrolled. These results prove again that in the reliability analysis of the electric power system, insider attacks create much more severe consequences than external cyber attacks, which require more attention and studies.

5.4 Summary

In this chapter, insider attacks in the SCADA system of the electric power system is focused and analyze. Different SMP models are built given with different attacking targets. MTTCs are calculated based on corresponding SMP models. MTTC values dramatically decrease after considering insider attacks compared with external cyber attacks, which is because shorter attacking paths are needed to complete a successful attack. Via Monte Carlo Simulation, LOLP values of 14 scenarios considering all buses in the RTS 96 under real-time insider attacks and EENS values of 14 scenarios only considering that 33 generator buses are facing with insider attacks and lurking behavior estimated. Both LOLP values and EENS values massively increase in all 4 attacking skill levels, which states that insider attacks are much more harmful to the system reliability and make the whole system more unpredictable, more unpredictable, and in more loss. It can easily imagine that if the electric power system is under both a large amount of external cyber attacks and insider attacks, it will be extremely unreliable, resulting in huge economic losses and energy losses. These results provide evidence and references for subsequent researches and the follow-up establishment of countermeasures.

Chapter 6 Conclusion

Modern electric power system is a complex system with cyber-to-physical system, and SCADA/EMS system is the main component of the C2P system. With the close connection to the internet, various cyber attacks appear to cause huge damage on the reliability of the electric power system. Issue of cyber security of power grid are calling for attention. However, few studies are focused on the reliability analysis of the SCADA/EMS system of the electric power system considering cyber security, so in this thesis, cyber attacks are considered and the system reliability is studied in various scenarios. The thesis can be divided into four parts as follows:

In the first two chapters, background and main mathematical methods are expressed. The structure of the SCADA/EMS system and their attack approaches are stated. The power SCADA/EMS system is vulnerable to different network security threats at different stages and at different levels of data and control command transmission due to different network transmission methods. Mathematical methods of the system reliability analysis against with cyber attacks are given. Bayesian Networks are explained to show its function on the establishment of cyber attack path models. Semi-Markov Process and Mean Time-to-Compromise are stated to explain the approach for probability evaluation.

Then, in chapter 3, a mean time-to-compromise (MTTC) model is expounded and used to assess the time interval of successful intrusion into network components in the control network. Additionally, to analyze different scenarios, Bayesian Networks (BNs) are described to create the attack graph models of corresponding cyber attacks on the system. 14 scenarios are studied based on IEEE RTS 96. LOLP values are calculated as the reliability index by Monte Carlo Simulation. It is found that with the increase of vulnerabilities in the system, the value of MTTC decrease, and LOLP values increase, which indicates that the reliability of the electric power system is worse.

Besides, in chapter 4, lurking behavior of cyber attacks is taken into consideration to realize more practical simulation. EENS values are calculated to reflect the influence on the system reliability by sequential Monte Carlo Simulation. Different lurking time is assumed to stand for different lurking strategies. After considering the limitation of lurking time of cyber attacks, EENS values increase a lot, which means the power system is much less reliable. To analyze the deepest impact on the system reliability, Hill Climbing (HC) algorithm is used to find the best limitation of lurking time, and EENS values are estimated and compared with the fitted results. Small difference is between two EENS values, so the right limitation of lurking time is found successful, and in this situation, the power system reliability is the worst, requiring for better protection. After considering the probability of detection of cyber attacks, it is found that EENS values decrease dramatically with the increase of the probability of detection.

At last, in Chapter 5, insider attacks are considered and analyzed. SMP models are built considering different insider attacking paths of each scenario, and MTTCs are evaluated based on SMP models. MTTCs dramatically decrease compared with them of external cyber attacks. LOLP values of 14 scenarios considering insider attacks are evaluated by MCS, and they are much higher than the previous results. EENS values of 14 scenarios considering insider attacks and lurking behavior together are calculated by MCS as well, and EENS values greatly increase than the results in the Chapter 4. It indicates that insider attacks create worse impact than external cyber attacks due to the shorter attacking paths, which can result in the more unpredictable and uncontrolled situation of the electric power system with more economic losses and energy losses.

Future work can be focused on the following aspects:

- There are more particular cyber attack scenarios in the SCADA/EMS system of the electric power system needed to be considered and studied, for example, the cyber attacks on intrusion detection system (IDS) and robust intrusion tolerant system (ITS).
- More completed and realistic probability evaluation model should be built to model the various cyber attacks in reality. Patterns and characteristic of cyber attacks needed to be clearly modeled and stated by better mathematical methods.
- In reality, scenarios are more complicated because of a variety of influence factors. More kinks of insider attacks within the system should be taken into consideration. A completed

attack model needs to be established by considering all factors.

- Calculating the system reliability for more systems with different topologies; and considering the connection to the utility and calculating reliability indices in connected modes.

References

1. Sridhar, S., Hahn, A., & Govindarasu, M. 2012. Cyber–physical system security for the electric power grid. *Proceedings of the IEEE*, *100*(1), 210-224.Andersson, Göran, et al. "Causes of the 2003 major grid blackouts in North America and Europe, and recommended means to improve system dynamic performance." *IEEE transactions on Power Systems* 20.4 (2005): 1922-1928.

2. Andersson, G., Donalek, P., Farmer, R., Hatziargyriou, N., Kamwa, I., Kundur, P., ... & Schulz, R. 2005. Causes of the 2003 major grid blackouts in North America and Europe, and recommended means to improve system dynamic performance. *IEEE transactions on Power Systems*, *20*(4), 1922-1928.

3. Stamp, J., McIntyre, A., & Ricardson, B. 2009, March. Reliability impacts from cyber attack on electric power systems. In *2009 IEEE/PES Power Systems Conference and Exposition*(pp. 1-8). IEEE.

4. Sheyner, O., Haines, J., Jha, S., Lippmann, R., & Wing, J. M. 2002. Automated generation and analysis of attack graphs. In *Proceedings 2002 IEEE Symposium on Security and Privacy*(pp. 273-284). IEEE

5. Teixeira, A., Sandberg, H., & Johansson, K. H. 2010, June. Networked control systems under cyber attacks with applications to power networks. In *Proceedings of the 2010 American Control Conference* (pp. 3690-3696). IEEE.

6. Amin, S., Litrico, X., Sastry, S., & Bayen, A. M. 2013. Cyber security of water SCADA systems—Part I: Analysis and experimentation of stealthy deception attacks. *IEEE Transactions on Control Systems Technology*, *21*(5), 1963-1970.

7. Wu, F. F., Moslehi, K., & Bose, A. 2005. Power system control centers: Past, present, and future. *Proceedings of the IEEE*, *93*(11), 1890-1908.

8. Zhang, Y., Wang, L., Xiang, Y., & Ten, C. W. 2015. Power system reliability evaluation with SCADA cybersecurity considerations. *IEEE Transactions on Smart Grid*, *6*(4), 1707-1721.

9. Ericsson, G. N. 2010. Cyber security and power system communication—essential parts of a smart grid infrastructure. *IEEE Transactions on Power Delivery*, *25*(3), 1501-1507.

10. Thomas, M. S., & McDonald, J. D. 2015. *Power system SCADA and smart grids*. CRC press.

11. Li, W. 2013. *Reliability assessment of electric power systems using Monte Carlo methods*. Springer Science & Business Media.

12. Stamp, J., Laviolette, R., Phillips, L., & Richardson, B. 2009. Impacts analysis for cyber attack on electric power systems (National SCADA Test Bed FY08). *SAND2009-1673*.

13. Bruce, A. G. 1997, May. Reliability analysis of electric utility SCADA systems. In *Proceedings of the 20th International Conference on Power Industry Computer Applications* (pp. 200-205). IEEE.

14. Byres, E., & Lowe, J. 2004, October. The myths and facts behind cyber security risks for industrial control systems. In *Proceedings of the VDE Kongress* (Vol. 116, pp. 213-218).

15. Yang, Y., McLaughlin, K., Sezer, S., Yuan, Y. B., & Huang, W. 2014, July. Stateful intrusion detection for IEC 60870-5-104 SCADA security. In *2014 IEEE PES General Meeting| Conference & Exposition* (pp. 1-5). IEEE.

16. Yang, Y., McLaughlin, K., Littler, T., Sezer, S., & Wang, H. F. 2013. Rule-based intrusion detection system for SCADA networks.

17. Ten, C. W., Liu, C. C., & Govindarasu, M. 2008, May. Cyber-vulnerability of power grid monitoring and control systems. In *Proceedings of the 4th annual workshop on Cyber security and information intelligence research: developing strategies to meet the cyber security and information intelligence challenges ahead*(p. 43). ACM.

18. Xin, S., Guo, Q., Sun, H., Zhang, B., Wang, J., & Chen, C. 2015. Cyber-physical modeling and cyber-contingency assessment of hierarchical control systems. *IEEE Transactions on Smart Grid*, *6*(5), 2375-2385.

19. Goh, B. 2016. Securing the Smart City. *Kennedy School Review*, *16*, 32-38.

20. Koppel, T. 2015. *Lights out: a cyberattack, a nation unprepared, surviving the aftermath*. Broadway Books.

21. Gungor, V. C., Sahin, D., Kocak, T., Ergut, S., Buccella, C., Cecati, C., & Hancke, G. P. 2011. Smart grid technologies: Communication technologies and standards. *IEEE transactions on Industrial informatics*, *7*(4), 529-539.

22. Rawat, D. B., & Bajracharya, C. 2015, April. Cyber security for smart grid systems: Status, challenges and perspectives. In *SoutheastCon 2015* (pp. 1-6). IEEE.

23. Wang, W., & Lu, Z. 2013. Cyber security in the smart grid: Survey and challenges. *Computer Networks*, *57*(5), 1344-1371.

24. El-Hawary, M. E. 2014. The smart grid—state-of-the-art and future trends. *Electric Power Components and Systems*, *42*(3-4), 239-250.

25. Case, D. U. 2016. Analysis of the cyber attack on the Ukrainian power grid. *Electricity Information Sharing and Analysis Center (E-ISAC).*

26. Deng, R., Zhuang, P., & Liang, H. 2017. CCPA: Coordinated cyber-physical attacks and countermeasures in smart grid. *IEEE Transactions on Smart Grid*, *8*(5), 2420-2430.

27. Patel, S. C., & Sanyal, P. 2008. Securing SCADA systems. *Information Management & Computer Security*, *16*(4), 398-414.

28. Coffey, V. 2014. High-energy lasers: new advances in defense applications. *Optics and Photonics News*, *25*(10), 28-35.

29. Cárdenas, A. A., Amin, S., Lin, Z. S., Huang, Y. L., Huang, C. Y., & Sastry, S. 2011, March. Attacks against process control systems: risk assessment, detection, and response. In *Proceedings of the 6th ACM symposium on information, computer and communications security* (pp. 355-366). ACM.

30. Francia III, G. A., Thornton, D., & Dawson, J. 2012, January. Security best practices and risk assessment of SCADA and industrial control systems. In *Proceedings of the international conference on security and management (SAM)* (p. 1). The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).

31. Ten, C. W., Hong, J., & Liu, C. C. 2011. Anomaly detection for cybersecurity of the substations. *IEEE Transactions on Smart Grid*, *2*(4), 865-873.

32. Bayes, T. 1991. An essay towards solving a problem in the doctrine of chances. 1763. *MD computing: computers in medical practice*, *8*(3), 157.

33. Jeffreys, H. 1946. An invariant form for the prior probability in estimation problems. *Proceedings of the Royal Society of London. Series A. Mathematical and Physical Sciences*, *186*(1007), 453-461.

34. Pearl, J. 2014. *Probabilistic reasoning in intelligent systems: networks of plausible inference*. Elsevier.

35. Nzoukou, W., Wang, L., Jajodia, S., & Singhal, A. 2013, September. A unified framework for measuring a network's mean time-to-compromise. In *2013 IEEE 32nd International Symposium on Reliable Distributed Systems* (pp. 215-224). IEEE.

36. Sommestad, T., Ekstedt, M., & Nordstrom, L. 2009. Modeling security of power communication systems using defense graphs and influence diagrams. *IEEE Transactions on Power Delivery*, *24*(4), 1801-1808.

37. Pyke, R. 1961. Markov renewal processes: definitions and preliminary properties. *The Annals of Mathematical Statistics*, 1231-1242.

38. Limnios, N., & Oprisan, G. 2012. *Semi-Markov processes and reliability*. Springer Science & Business Media.

39. Madan, B. B., Goševa-Popstojanova, K., Vaidyanathan, K., & Trivedi, K. S. 2004. A method for modeling and quantifying the security attributes of intrusion tolerant systems. *Performance Evaluation*, *56*(1-4), 167-186.

40. Leversage, D. J., & Byres, E. J. 2008. Estimating a system's mean time-to-compromise. *IEEE Security & Privacy*, *6*(1), 52-60.

41. McQueen, M. A., Boyer, W. F., Flynn, M. A., & Beitel, G. A. 2006. Time-to-compromise model for cyber risk reduction estimation. In *Quality of Protection* (pp. 49-64). Springer, Boston, MA.

42. Frigault, M., & Wang, L. 2008, July. Measuring network security using bayesian network-based attack graphs. In *2008 32nd Annual IEEE International Computer Software and Applications Conference* (pp. 698-703). IEEE.

43. Grigg, C., Wong, P., Albrecht, P., Allan, R., Bhavaraju, M., Billinton, R., ... & Li, W. 1999. The IEEE reliability

test system-1996. A report prepared by the reliability test system task force of the application of probability methods subcommittee. *IEEE Transactions on power systems*, *14*(3), 1010-1020.

44. Verba, J., & Milvich, M. 2008, May. Idaho national laboratory supervisory control and data acquisition intrusion detection system (SCADA IDS). In *2008 IEEE Conference on Technologies for Homeland Security* (pp. 469-473). IEEE.

45. Barnes, K., & Johnson, B. 2009. *National SCADA test bed substation automation evaluation report* (No. INL/EXT-09-15321). Idaho National Laboratory (INL).

46. Radvanovsky, R., & Brodsky, J. 2016. *Handbook of SCADA/control systems security*. CRC Press.

47. Zhang, Y., Wang, L., Sun, W., Green II, R. C., & Alam, M. (2011). Distributed intrusion detection system in a multi-layer network architecture of smart grids. *IEEE Transactions on Smart Grid*, *2*(4), 796-808.

48. Major, J. A. 2002. Advanced techniques for modeling terrorism risk. *The Journal of Risk Finance*, *4*(1), 15-24.

49. Smolarek, M., & Witkowski, M. 2016, June. Threat Analysis in the Network-Centric Environment. In *International conference KNOWLEDGE-BASED ORGANIZATION* (Vol. 22, No. 3, pp. 551-559). De Gruyter Open.

50. Baliga, A., Kamat, P., & Iftode, L. 2007, May. Lurking in the shadows: Identifying systemic threats to kernel data. In *2007 IEEE Symposium on Security and Privacy (SP'07)* (pp. 246-251). IEEE.

51. Tsamardinos, I., Brown, L. E., & Aliferis, C. F. 2006. The max-min hill-climbing Bayesian network structure learning algorithm. *Machine learning*, 65(1), 31-78.

52. Schultz, E. E. 2002. A framework for understanding and predicting insider attacks. Computers & Security, 21(6), 526-531.

53. Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Richardson, R. 2005. 2005 CSI/FBI computer crime and security survey. Computer Security Journal, 21(3), 1.

54. Salem, M. B., Hershkop, S., & Stolfo, S. J. 2008. A survey of insider attack detection research. In Insider Attack and Cyber Security (pp. 69-90). Springer, Boston, MA.

55. Maybury, M., Chase, P., Cheikes, B., Brackney, D., Matzner, S., Hetherington, T., ... & Longstaff, T. 2005. Analysis and detection of malicious insiders. MITRE CORP BEDFORD MA.

56. Stolfo, S. J., Bellovin, S. M., Hershkop, S., Keromytis, A. D., Sinclair, S., & Smith, S. W. (Eds.). 2008. Insider attack and cyber security: beyond the hacker (Vol. 39). Springer Science & Business Media.