Topology Attacks on Power System Operation and Consequences Analysis

by

Jiazi Zhang

A Thesis Presented in Partial Fulfillment
of the Requirements for the Degree
Master of Science

Approved June 2015 by the
Graduate Supervisory Committee:

Lalitha Sankar, Chair
Kory Hedman
Oliver Kosut

ARIZONA STATE UNIVERSITY

August 2015

ABSTRACT

The large distributed electric power system is a hierarchical network involving the transportation of power from the sources of power generation via an intermediate densely connected transmission network to a large distribution network of end-users at the lowest level of the hierarchy. At each level of the hierarchy (generation/ transmission/ distribution), the system is managed and monitored with a combination of (a) supervisory control and data acquisition (SCADA); and (b) energy management systems (EMSs) that process the collected data and make control and actuation decisions using the collected data. However, at all levels of the hierarchy, both SCADA and EMSs are vulnerable to cyber attacks. Furthermore, given the criticality of the electric power infrastructure, cyber attacks can have severe economic and social consequences.

This thesis focuses on cyber attacks on SCADA and EMS at the transmission level of the electric power system. The goal is to study the consequences of three classes of cyber attacks that can change topology data. These classes include: (i) *unobservable* state-preserving cyber attacks that only change the topology data; (ii) *unobservable* state-and-topology cyber-physical attacks that change both states and topology data to enable a coordinated physical and cyber attack; and (iii) topology-targeted man-in-the-middle (MitM) communication attacks that alter topology data shared during inter-EMS communication. Specifically, attack class (i) and (ii) focus on the unobservable attacks on single regional EMS while class (iii) focuses on the MitM attacks on communication links between regional EMSs. For each class of attacks, the theoretical attack model and the implementation of attacks are provided, and the worst-case attack and its consequences are exhaustively studied. In particularly, for class (ii), a two-stage optimization problem is introduced to study worst-case attacks that can cause a physical line overflow that is unobservable in the cyber layer. The

long-term implication and the system anomalies are demonstrated via simulation.

For attack classes (i) and (ii), both mathematical and experimental analyses suggest that these unobservable attacks can be limited or even detected with resiliency mechanisms including load monitoring, anomalous re-dispatches checking, and historical data comparison. For attack class (iii), countermeasures including anomalous tie-line interchange verification, anomalous re-dispatch alarms, and external contingency lists sharing are needed to thwart such attacks.

DEDICATION

This dissertation is dedicated to my father Guoqing Zhang, my mother Xihua Zhao, and my aunts Xiumei Zhang and Xiuyi Zhang, for their endless love and support through all these years.

ACKNOWLEDGEMENTS

I would like to express my deepest appreciation and thanks to my advisor, Dr. Sankar, for her guidance, encouragement and invaluable support throughout my research work and my life as a graduate student.

I am also grateful to the members of my committee, Dr. Kory Hedman, and Dr. Oliver Kosut for their valuable suggestions and comments.

In addition, I would like to express my gratitude to the Power Systems Engineering Research Center (PSERC) and National Science Foundation (NSF) for the financial support provided.

Last but not least, I would like to thank all my friends in the areas of electric power and energy systems, industrial engineering, and economics for their compelling intellectual discussion as well as their friendship and support.

TABLE OF CONTENTS

CHAPTER Page

CHAPTER Page

LIST OF TABLES

LIST OF FIGURES

Figure Page

LIST OF SYMBOLS

A_{GN}	Generator-to-bus matrix
A_{KN}	Overall branch-to-bus incidence matrix
A_{Kf}	"From" branch-to-bus incidence matrix
A_{Kt}	"To" branch-to-bus incidence matrix
a	Measurement attack vector
b	Line status attack vector
b_{nm}	The susceptance of line k from bus n to bus m
b_{sn}	The shunt branch susceptance of bus n
$C_g(\cdot)$	The cost function for generator g
c	Attack vector
D	Static branch admittance matrix
$\mathcal{E}$	Set of lines
e	Noise vector
G_n	The set of generators at bus n
$\mathcal{G}$	System topology
g_{nm}	The conductance of line k from bus n to bus m
g_{sn}	The shunt branch conductance of bus n
H	Jacobian matrix
H_1	Dependency matrix between power injection and voltage angle
H_2	Dependency matrix between power flow and voltage angle
$\bar{H}_1$	Faulty dependency matrix between power injection and voltage angle
$\bar{H}_2$	Faulty dependency matrix between power flow and voltage angle
$h(x, \mathcal{G})$	A vector of nonlinear functions that describes the relationship between the system states and measurements for a topology $\mathcal{G}$
$I_{\mathcal{T}}$	The set of measurements the attacker needs to modify to launch an attack
$k(;, n)$	A set lines with bus n as its sending bus

$k(n,;)$	A set of lines with bus n as its receiving bus
$\mathcal{L}$	Set of load buses
N_0	The maximum number of center buses that can be attacked
N_1	The maximum l_1-norm constraint limit
N_T	The maximum number of switching attack lines
$\mathcal{N}$	Set of buses
n_{br}	Number of branch
n_b	Number of bus
n_g	Number of generator
n_{load}	Number of load
n_z	Number of measurement
P	Active power injection vector
P_D	Active power load vector
P_G	Active power generation vector
$P_G^{\max}$	Maximum generation limit
$P_G^{\min}$	Minimum generation limit
P_K	Active power flow vector
$P_K^{\max}$	Thermal limit vector
$p_{\text{detection}}$	The detection probabilities of attacks
Q	Reactive power injection vector
Q_D	Reactive power load vector
Q_G	Reactive power generation vector
Q_K	Reactive power flow vector
R	Measurement error covariance matrix
r	Residual vector
S^{max}	Line capacity limit vector
S_T	"To" complex power flow vector

S_{bus}	Complex power injection vector
S_f	"From" complex power flow vector
$\mathcal{S}$	Attack sub-graph
s	Line status vector
u	Non-negative slack variable vector
V	Voltage magnitude state vector
$\boldsymbol{V}$	Complex voltage vector
x	State vector
$\hat{x}$	Estimated state vector
Y_{br}	Branch admittance matrix
Y_{bus}	Bus admittance matrix
z	Measurement vector
$\bar{z}$	False measurement vector
$\alpha^{\mp}$	Dual variable vectors of minimum and maximum active power generation output constraints, respectively
λ	Dual variable vector of power balance constraints
$\mu^{\mp}$	Dual variable vectors of minimum and maximum power flow limit constraints, respectively
σ_i^2	covariance of noise of measurement i
σ_{r_i}	The standard deviation of the ith residual error r_i
τ	Maximum load shift percentage
θ	Voltage angle state vector
ζ	The weight of the norm of attack vector c
$\mathrm{diag}\,(\cdot)$	An operator that takes an $n \times 1$ vector and creates the corresponding $n \times n$ diagonal matrix with the vector elements along the diagonal
BFS	Breadth-first search
CA	Contingency analysis
EMS	Energy management system
FDI	False data injection

LMP	Locational marginal price
MitM	Man-in-the-middle
OPF	Optimal power flow
PF	Power flow
PTDF	Power transfer distribution factor
RTS	Reliable test system
SCADA	Supervisory control and data acquisition
SE	State estimation
WLS	Weight least-squares

Chapter 1

INTRODUCTION

1.1 Overview

The large distributed electric power system is a hierarchical network involving the transportation of power from the sources of power generation via an intermediate densely connected transmission network to a large distribution network of end-users at the lowest level of the hierarchy. To ensure reliable operation of the entire power system, the system operator at each level should be aware of the real-time operation states. Therefore, secure and intelligent cyber data processing systems that monitor and control each level of the physical power system are crucial for reliable real-time operations. Such a cyber layer includes (a) supervisory control and data acquisition (SCADA) system, and (b) energy management systems (EMSs) for data processing. Figure 1.1 illustrates an example of the hierarchical electric power system. The figure demonstrates how at various levels from generation through transmission, substation, distribution, and even end-users, the network appropriate at each level is monitored using the collected SCADA data via an EMS to enable control and actuation of the undelaying physical system.

However, at all levels of the hierarchy, both SCADA and EMSs are vulnerable to cyber attacks. In fact, such cyber attacks can undermine the observability of physical systems, and hence, lead to mis-operation, violation, and inappropriate and untimely contingency response. In addition of cyber attacks, delays and errors on communication links between regional EMSs also reduce the global awareness of the system. Both cyber attacks and communication errors can potentially lead to severe

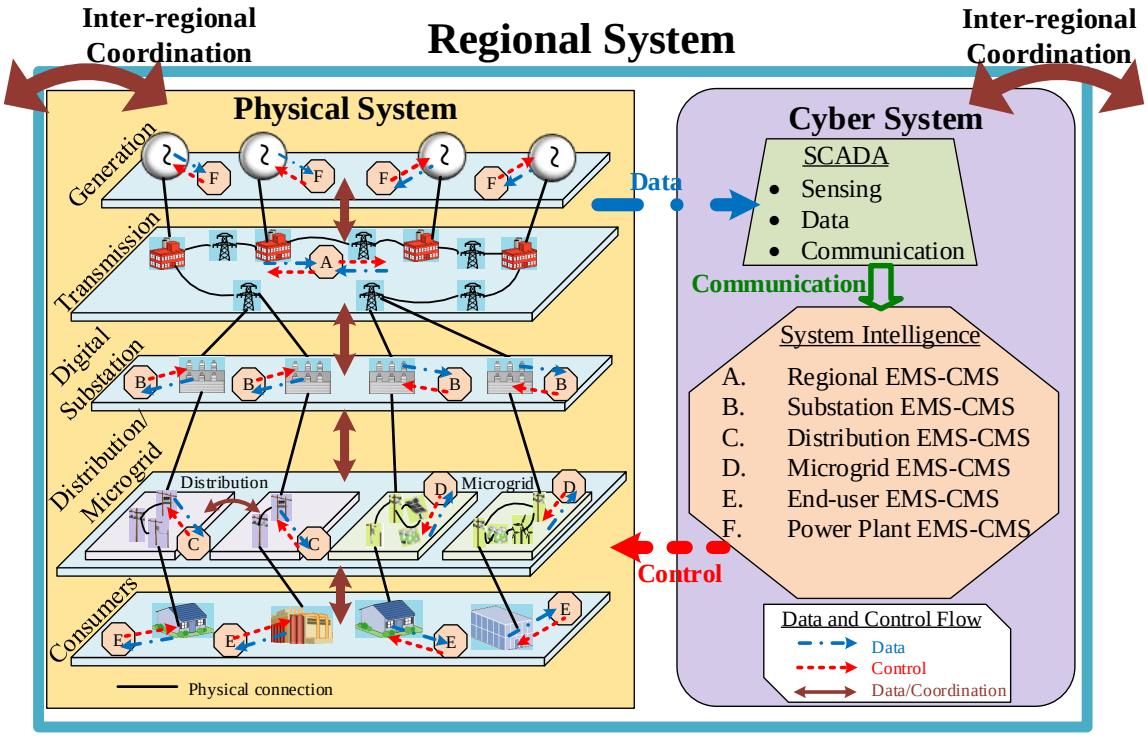


Figure 1.1: Hierarchical Cyber-physical Power System.

economic and social consequences.

The transmission level of electric power system is both the generation and large scale distribution of bulk power happens and correspondingly, is the most monitored and controlled by the cyber layer. To this end, this thesis focuses on the cyber attacks on the transmission system. The goal is to study the consequences of three classes of cyber attacks that can change topology data. These classes include: (i) *unobservable* state-preserving cyber attacks that only change the topology data; (ii) *unobservable* state-and-topology cyber-physical attacks that can change both states and topology data to coordinate physical attacks; and (iii) topology-targeted man-in-the-middle (MitM) communication attacks that target on limiting topology sharing on inter-area communication. Specifically, attack class (i) and (ii) focus on the unobservable cyber attacks in which the data changed by attacker appears like normal states and can bypass the bad data detector on single region EMS. The attack class (iii) focuses on

the MitM attacks on multi-regional EMSs data communication. For each class of attacks, the theoretical attack model is presented, the implementation of attacks is provided, and the worst-case attack and its consequences on the physical system are exhaustively studied. In particularly, for class (ii), the goal is to study attacks that can cause a physical line overflow that is unobservable in the cyber system via a two-stage optimization formulation. The long-term implication of each attack class and the system anomalies resulting from such attacks are demonstrated via simulation.

1.2 Thesis Motivation

In recent years, several incidents have shown that cyber attacks can have severe consequences on power system. In addition, communication delays which can lead to devastating social and economic losses can also be mimicked by cyber attacks. The corresponding incidents are listed as follows.

- In the Northeast blackout of 2003, a line out in one area (Ohio) was not conveyed for a sufficient period of time to the Midwest Operator, leading to failure of convergence of the state estimator, and thereby, unobservability of the system. It eventually resulted in a widespread blackout throughout parts of the Northeastern and Midwestern United States and the Canadian province of Ontario, causing 4 to 10 billion dollars loss and affecting 55 million people [1]. A similar event resulting from an attack can have devastating economic consequences.

- In 2007, Idaho National Laboratory ran the Aurora Generator Test and demonstrated a cyber attack in which a diesel generator's circuit breaker was rapidly opened and closed by the attack. Such attacks can lead to the generator getting out of phase from the rest of the power system and eventually exploding [2].

- In 2009, Stuxnet virus ravaged roughly 20% of Iran's nuclear centrifuges by

causing them to spin out of control [3].

- In 2010, Stuxnet malware attacked SCADA systems that use Siemens WinCC SCADA software, which in turn infected 14 power plants in Germany [4].

- In 2012, the Industrial Control Systems Cyber Emergency Response Team revealed that the number of reported cyber attacks is growing and the companies with access to the country's power grid become the cyber attack targets [5]. The U.S. Department of Energy reported that from 2011 to 2014, 362 reports were received from electric utilities of physical or cyber attacks that interrupted power services [6]. In 2013, CNN reported that hacker hits on US power and nuclear targets spiked in 2012 [5]. A Department of Homeland Security branch recorded 161 cyber attacks on the energy sector in 2013, compared to just 31 in 2011 [6], which comprises 60% of all cyber attacks on cyber-physical systems.

From the list above, it is clear that the cyber layer and communication network of power system are vulnerable to both cyber attacks and communication delays and errors. Thus, secure and trustworthy cyber systems are crucial for the security and reliability of power system operation.

Among all the monitoring and sharing data, topology information plays an essential role in power system operation. In transmission level EMSs, various data processing modules including SE, contingency analysis (CA), and optimal power flow (OPF) are highly dependent on topology information. Cyber attacks that alter the system topology information can result in wrong solutions within these modules with potential consequences including systematic problems and failures. Furthermore, as the physical components of the electric power system become vulnerable to attacks, an intelligent attacker can simultaneously attack cyber data with the goal of masking the physical attack, and hence, worsen the consequences resulting from physical

attacks. Therefore, it is crucial to fully understand the consequences of realistic and credible topology-based cyber-attacks as a first step to thwart such attacks.

1.3 Literature Review

There has been much recent interest in understanding the cyber-security challenges facing the electric power system. Since it is not possible to review all these challenges, we will focus on the class of unobservable attacks. The *unobservable attacks* are a class of cyber attacks in which the attacker focuses on a particular module and within the module, the data change made by attacker appears like normal states instead of random noise that can be detected by existing mechanism such as bad data detection. Although such attacks have been studied, the attack consequences are still not clear. Our work focus on not only developing unobservable attacks, but also studying the attack consequences. We briefly review the existing literatures on unobservable attacks.

In [7], the authors are the first to introduce a class of false data injection (FDI) attacks on DC SE. The authors show that an attacker with sufficient system knowledge can inject malicious measurements without being detected by existing bad data detection techniques that are subsequent to SE. In [8], Sandberg *et al.* introduce two security indices which quantify the least efforts to launch unobservable FDI attacks on DC SE. In [9], Teixeira *et al.* analyze how to completely protect SE by placing encrypted devices on a set of measurements in power system. In [10], the authors further propose the minimum cost protection scheme to thwart unobservable FDI attacks. In [11], Kosut *et al.* discuss the trade-off between attacker's efforts to maximize the attack strength and minimize the detection rate.

In contrast to the above mentioned references, in [12], Hug and Giampapa focus on FDI attacks on AC SE and introduce a class of unobservable attacks that are limited

to a sub-graph of the networks. They demonstrate that though AC SE is vulnerable to unobservable FDI attacks, it requires the knowledge of both system topology and states to launch such attacks. In [13], Liang *et al.* introduce unobservable FDI attacks for a nonlinear measurement model of AC SE and demonstrate that such FDI attacks can lead to a physical generation re-dispatch when none was actually needed which in turn can cause a line to overload in the physical system.

The impact of FDI attacks on electric power markets is studied in [14]. The authors demonstrate that the FDI attacks can be utilized to manipulate the locational marginal prices (LMPs) of ex-post real-time market, and thus, allow the attacker to profit. In general, attacking the electric power system to create profit in the market seems complicated since making a profit on market can be done in many other ways. That is why we need to focus on whether the cyber attacks can have physical consequences on the power system.

Yet another class of FDI attacks is one that alters topology data in an unobservable manner. As stated in Section 1.2, topology model is crucial for power system since incorrect topology data in SE, OPF, and CA can lead to systematic problems and failures. In [15], Kim and Tong formally introduce an undetectable topology attack as a specific class of FDI attacks on power systems and evaluate the attack's impact on the electric market. The authors design the attack to alter the system topology estimate by injecting malicious measurements and false line status data while remaining undetected. In [16], Rahman *et al.* study the impact of the undetectable topology attack introduced in [15] on DC OPF when DC SE is used; the attack is optimized to increase total operation cost of the system. In [17], Ashok and Govindarasu analyze a different class of topology attacks. In these attacks, the attacker compromises the critical measurements of the system. This leads to incorrect contingency analysis results, as a result of which, some subsets of the contingencies can be potentially

neglected by the control center.

In addition of snap-shot attacks, there are growing concerns on the optimal attacks based on system response to the attacks. In [18] and [19], the authors propose a max-min attacker-defender model to study the most damaging FDI attacks with both immediate attacking goal and delayed attacking goal. They formulate a class of load redistribution attacks as a two-stage optimization problem. They model the attack as well as the system response in the next time interval, which in turn lead to the optimal attack which can maximize operation costs based on the system response. More recently, in [20], the authors introduce a two-stage optimization for the worst unobservable attacks on AC SE. The objective of the attack is to maximize power flow on a specific line, and hence, lead to violation in physical system. While [20] is more closely related, our work focuses on joint physical and unobservable topology attacks, and therefore, the optimization problem introduced here is different from [20].

1.4 Thesis Objective and Contribution

In this thesis, we focus on cyber attacks that target to change the topology information of the system. Although references [15] - [17] have already studied several classes of topology attacks, the analysis of attacks is either limited to market consequences or the attack model is based on DC SE. The actual physical consequences of topology attacks are still unclear. Therefore, we seek to understand both the physical consequences and anomalies resulting from various topology attacks, that in turn can be used to develop attack detection resiliency mechanisms. To this end, three classes of attacks are studied in this thesis.

The first class of attacks is *unobservable state-preserving topology attacks* in which an attacker can change topology data of the system without changing the states. We

focus on line-maintaining attacks that can maintain a physically outaged line as active in cyber layer. An algorithm based on breadth-first search (BFS) is proposed to find the minimum set of topology and measurements required to launch such attacks. We demonstrate that such algorithm can enable an attacker to obtain the localized topology and corresponding measurement data to mount an attack that bypasses bad data detector and successfully changes topology information of the system in the cyber layer. However, the experimental analyses suggest that such attacks can be limited or even detected due to few feasible targets and large load shifts.

The second class of unobservable state-and-topology cyber-physical attacks that change both states and topology data to enable a coordinated physical and cyber attack. Our motivation for including both state and topology information is to focus on worst-case attacks and to limit detectability via load shifts. We propose a two-step worst attack strategy to optimize the long-term attack consequences. We define an optimal attack is one which maximizes power flow on a line subsequent to attacks followed by SE and DC OPF processing by the system. We demonstrate that attacks designed with the proposed strategy can successfully mask the physical line outage from AC SE with limited load shifts and lead to severe physical overflow on the target line. Resilience detection mechanism as valid historical data comparison for generation dispatch is proposed to protect the power system.

The third class of attacks is *topology-targeted man-in-the-middle communication attacks* which changes the topology alteration information sharing between areas. Our results demonstrate that such an attack in a distributed power network leads to a range of possibilities including actual physical line overloads that are not observable from the cyber measurements; false overload alert in cyber layer; and progressively severe lack of convergence of OPF in both areas. Countermeasures including anomalous tie-line interchange verification, anomalous re-dispatch alarms, and external contin-

gency lists sharing are provided to thwart such attacks.

1.5 Thesis Organization

The principal content of this report is partitioned into 6 chapters.

Chapter 1 presents an overview of research background, a literature review, study objective and contribution.

Chapter 2 presents the mathematical formulation for the various computational units of power system operation, including SCADA, topology processor, state estimation, and optimal power flow.

In chapter 3, the attack model, implementation, and long-term consequences of the unobservable state-preserving topology attacks are provided.

In chapter 4, unobservable state-and-topology cyber-physical attacks are studied. A two-step worst attack strategy based on two-stage optimization problem is proposed to study the worst-case attacks. The performance of the attack strategy and the long-term consequences of such attacks are illustrated via simulation.

In chapter 5, a class of topology-targeted man-in-the-middle (MitM) communication attacks which changes the topology alteration data sharing between areas is introduced. The long-term consequences and countermeasures of such attacks are proposed.

In chapter 6, conclusions and future works are provided.

Chapter 2

SYSTEM MATHEMATIC MODEL

In this section, we introduce the mathematical formulation for the various computational units of power system operation, including topology processor, state estimation, and optimal power flow units. Throughout, we assume there are n_b buses, n_{br} branches, n_g generators, n_{load} load buses, and n_z measurements in the system. The temporal nature processing of real-time power operation is illustrated in Figure 2.1. In this figure, z and s denote the measurement vector and line status vector, respectively; $\mathcal{G}$ represents the system topology, $x = [\theta, V]^T$ is the system state vector where θ and V are voltage angle and voltage magnitude, respectively; P_D and Q_D represent the active and reactive loads, respectively; P_G and Q_G represent the active and reactive power generation. We denote each estimated value with the same alphabet with a hat, and the optimal value with a star.

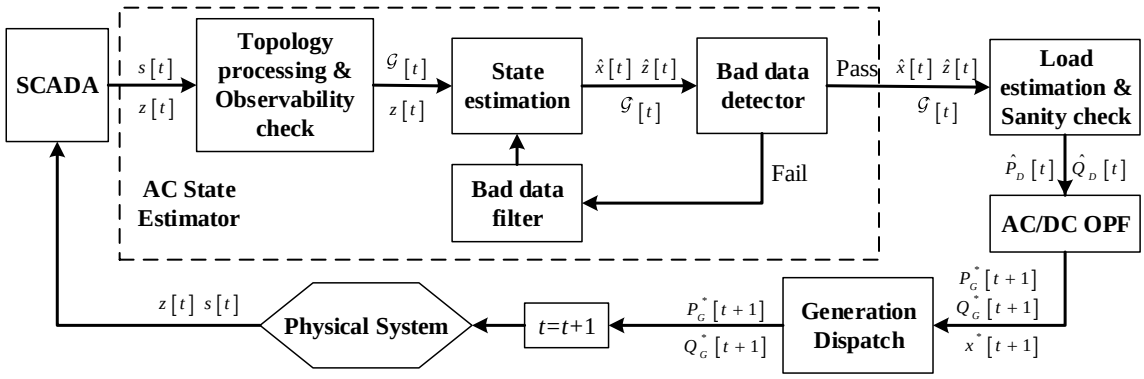


Figure 2.1: Temporal Nature of Real-time Power System Operation.

In this operation loop, SCADA collects line status vector and noisy measurements of the physical system and passes these data to AC state estimator. The AC state

estimator then uses these data to estimate topology (topology processing module) and states (state estimation module). In sequel to SE, bad data detector filtered the bad data from states. After that, the estimated topology and states are then utilized to estimate loads, which also need sanity check from operator. Once the estimate loads pass the sanity check, these data as well as the estimated topology are then used to compute the OPF. Eventually, the optimal generation dispatch that obtained from OPF are implemented, and the system comes to a new operation loop.

2.1 System Network and Topology Processor

The electric power system can be represented by a graph $\mathcal{G} = \{\mathcal{N}, \mathcal{E}\}$ where $\mathcal{N}$ and $\mathcal{E}$ are the sets of buses and lines, respectively. For a specific system, we assume the static topology is $\mathcal{G}_0 = \{\mathcal{N}_0, \mathcal{E}_0\}$ where $\mathcal{N}_0$ and $\mathcal{E}_0$ are the sets of all existing buses and branches, respectively. Then, the connectivity of $\mathcal{N}_0$ with $\mathcal{E}_0$ can be represented with $n_{br} \times n_b$ "from" and "to" branch-to-bus incidence matrices A_{Kf} and A_{Kt}, respectively. If a branch k exists to connect bus i to bus j, the $(k,\ i)^{th}$ element of A_{Kf} and $(k,\ j)^{th}$ element of A_{Kt} are 1 and all other entries of A_{Kf} and A_{Kt} are set to zeros. The overall $n_{br} \times n_b$ branch-to-bus incidence matrix A_{KN} is calculated using A_{Kf} and A_{Kt} as follows

$$A_{KN} = A_{Kf} - A_{Kt}. \tag{2.1}$$

At the control center, SCADA collects line status data as a $n_{br} \times 1$ vector s with entries $s_k \in \{0, 1\}$ for $k \in \{1, ..., n_{br}\}$ that indicate the on and off status of circuit-breakers on each line. The data is then passed to a topology processor which maps the real-time power system topology along with network connectivity data. The complete topology information is captured by two matrices Y_{br}, the branch admittance matrix,

and Y_{bus}, the bus admittance matrix, defined as

$$Y_{br} = D[\text{diag}(s)A_{KN}], \tag{2.2}$$

$$\text{and} \qquad Y_{bus} = [\text{diag}(s)A_{KN}]^T D[\text{diag}(s)A_{KN}] \tag{2.3}$$

where D denotes the $n_{br} \times n_{br}$ branch admittance matrix for $\mathcal{G}_0$, diag $(\cdot)$ denotes an operator that takes an $n \times 1$ vector and creates the corresponding $n \times n$ diagonal matrix with the vector elements along the diagonal.

The topology data plays a crucial role in power system operation. It determines the real-time AC power flow model. Assume $\boldsymbol{V}$ denotes the $n_b \times 1$ complex voltage vector, such that $\boldsymbol{V} = V\angle\theta$, where voltage angle and voltage magnitude, θ and V are both $n_b \times 1$ vectors. The AC power flow model for the system can be written as

$$\begin{bmatrix} S_f \\ S_t \\ S_{bus} \end{bmatrix} = \begin{bmatrix} A_{Kf}\boldsymbol{V} \cdot Y_{br}^* \boldsymbol{V}^* \\ -A_{Kt}\boldsymbol{V} \cdot Y_{br}^* \boldsymbol{V}^* \\ \text{diag}\,(\boldsymbol{V}) \cdot Y_{bus}^* \boldsymbol{V}^* \end{bmatrix} \tag{2.4}$$

where S_f and S_t are $n_{br} \times 1$ "from" and "to" complex power flow vectors, respectively, S_{bus} is $n_b \times 1$ complex power injection vector, $*$ represents conjugate of vector in this subsection.

This model is used in the subsequent SE and OPF modules. In AC SE, the "from" and "to" power flow measurements of all branches and the power injection measurements of buses with injection (generation and/or loads) are used to estimate the states. In AC OPF, "from", "to" power flows and power injection are used to form constraints of power balance of buses and thermal limit of branches. Therefore, a correct topology information ensures the validity of SE and OPF results. If the line status information is altered by attackers, the topology processor will export incorrect topology information and hence, lead to wrong estimated states and OPF solutions.

2.2 State Estimation

Consider an $n_z \times 1$ vector z of nonlinear measurements given as

$$z = h(x, \mathcal{G}) + e \tag{2.5}$$

where $x = [\theta,\ V]^T$ is the system state vector, and e is an $n_z \times 1$ noise vector which is independent of x and is modeled as Gaussian distributed with 0 mean and σ_i^2 covariance such that the measurement error covariance matrix is given by $R = diag(\{\sigma_i^2\}_{i=1}^M)$. The function $h(x, \mathcal{G})$ is a vector of nonlinear functions that describes the relationship between the system states and measurements for a topology $\mathcal{G}$. Both the line status data s and the measurements z are collected by the SCADA system. The commonly obtained measurements in the grid are the active and reactive power flows and bus injections.

We use weighted least-squares (WLS) AC SE to calculate the θ and V [21]. The objective of the estimation process is to minimize the sum of the squares of the weighted deviations of the estimated measurements from z. The states are solved as a least square problem with the following objective function

$$\min J(x) = (h(x) - z)^T R^{-1} (h(x) - z), \tag{2.6}$$

the solution to which satisfies

$$g(\hat{x}) = \frac{\partial J(\hat{x})}{\partial x} = H^T(\hat{x}) \cdot R^{-1} \cdot (h(\hat{x}) - z) = 0 \tag{2.7}$$

where the system Jacobian matrix $H = \frac{\partial h(x)}{\partial x} \mid_{x=\hat{x}}$, and $\hat{x}$ is the $2n_b \times 1$ estimated state vectors. The WLS solution for this nonlinear optimization problem can be solved iteratively.

In fact, measurements collected by SCADA may contain errors that can undermine the accuracy of estimated states. Therefore, bad data detector should be equipped

with SE to detect faulty measurements, and hence, protect SE from large errors. The measurement residual vector is used to detect bad data, as

$$r = z - h(x, \mathcal{G}) \tag{2.8}$$

where r is the $n_z \times 1$ residual vector.

In this paper, the χ^2-detector is utilized to detect bad data. The threshold is determined by the χ^2-test. To bypass the bad data detection, the residuals should satisfy the following relationship

$$r^T R^{-1} r \leqslant \chi^2_{(m-n),p} \tag{2.9}$$

where $\chi^2_{(m-n),p}$ is the value from χ^2 distribution tables corresponding to a detection confidence with probability p (*e.g.* 95%) and $m - n$ degrees of freedom.

If the threshold in (2.9) is violated, largest normalized residual method is further used for bad data identification as in (2.10).

$$\underset{i}{\text{Max}} \frac{|r_i|}{\sigma_{r_i}} \leqslant \tau_r \tag{2.10}$$

where σ_{r_i} is the standard deviation of the ith residual error r_i. If the largest norm residue test is not passed, the measurement with maximum residue is identified as bad measurement. The bad measurement is then removed from the measurement vector and SE is repeated until no bad data is detected.

The SE solution that pass the bad data detection is used to compute the power flow of the system, which hence yields the estimated loads of the system. The estimated loads then pass to OPF module for optimal power dispatch solution as describe in the following subsection. If the state vector is maliciously altered by attacker, it can result in wrong dispatch solution which can lead the system to uneconomic and insecure operation states.

2.3 Optimal Power Flow

The optimal power flow (OPF) problem aims to solve for the optimal power dispatch solution. The AC OPF problem can be written as

$$min \sum_{g \in G} C_g(P_g) \tag{2.11}$$

$$s.t. \sum_{g \epsilon G_n} P_g + \sum_{\forall k(n,;)} P_k - \sum_{\forall k(;,n)} P_k = P_{dn}, \quad \forall n \in B, \tag{2.12}$$

$$\sum_{g \epsilon G_n} Q_g + \sum_{\forall k(n,;)} Q_k - \sum_{\forall k(;,n)} Q_k = Q_{dn}, \quad \forall n \in B, \tag{2.13}$$

$$P_k = V_n^2(g_{sn} + g_{nm}) - V_n V_m(g_{nm} cos(\theta_n - \theta_m) \tag{2.14}$$

$$+ b_{nm} sin(\theta_n - \theta_m)), \ k \in Br$$

$$Q_k = -V_n^2(b_{sn} + b_{nm}) - V_n V_m(g_{nm} sin(\theta_n - \theta_m) \tag{2.15}$$

$$- b_{nm} cos(\theta_n - \theta_m)), \ k \in Br$$

$$P_k^2 + Q_k^2 \leq (S_k^{max})^2 \quad \forall k \in Br \tag{2.16}$$

$$P_g^{min} \leq P_g \leq P_g^{max} \quad \forall g \in G_i \tag{2.17}$$

$$Q_g^{min} \leq Q_g \leq Q_g^{max} \quad \forall g \in G_i \tag{2.18}$$

$$V_n^{min} \leq V_n \leq V_n^{max} \quad \forall n \in B \tag{2.19}$$

where $C_g(\cdot)$ is the cost function for generator g; b_{nm} and g_{nm} are the susceptance and conductance, respectively, of line k from bus n to bus m, b_{sn} and g_{sn} are the shunt branch susceptance and conductance, respectively, of bus n; $k(n,;)$ is one of a set of lines with bus n as its receiving bus and $k(;,n)$ is one of a set lines with bus n as its sending bus; G_n is the set of generators at bus n; P_g is the active power output of generator g with maximum and minimum limit $P_g^{\max}$ and $P_g^{\min}$, respectively; Q_g is the reactive power output of generator g with maximum and minimum limit $Q_g^{\max}$ and

$Q_g^{\min}$, respectively; P_k and Q_k are the active and reactive power flows, respectively, on line k with line capacity limit S_k^{max}; P_{dn} and Q_{dn} are the active and reactive power demands, respectively, at bus n; and V_n is the voltage magnitude for bus n with maximum and minimum limits $V_n^{\max}$and $V_n^{\min}$, respectively.

The objective in (5.1) is to minimize the total active power generation cost of the whole power system. Constraints (5.2) and (5.3) represents the active and reactive power balance constraints for each bus in the system. The constraints in (5.4) and (5.5) are the active and reactive transmission line power flow constraints for the whole system while (5.6) is the thermal limit for each transmission line. Constraints (5.7) and (5.8) are the active and reactive power output limits for each generator while (5.9) defines the voltage magnitude limits for each bus in the whole system.

Chapter 3

UNOBSERVABLE STATE-PRESERVING TOPOLOGY ATTACKS

In this chapter, we focus on a non-linear system model (*i.e.,* AC SE) and on a class of unobservable topology attacks in which an attacker can change topology information of the system without changing the states. We henceforth refer to such attacks as *unobservable state-preserving topology attacks*. These attacks can be of two types: *line-maintaining* and *line-removing*. In a line-maintaining attack, the attacker changes measurements and line status information to make it appear that line which is not in the system is now shown as active at the control center via changes to SCADA data; the opposite is achieved by a line-removing attack. Kim and Tong in [15] introduce unobservable state-preserving topology attacks; however the analysis in [15] is restricted to line-removing attacks. To launch such attacks, the authors propose an attack heuristic in which the attacker can set the power flow measurements for a specific line to zero and change the power injection measurements at the end buses of that line.

In this chapter, we focus on a class of unobservable state-preserving line-maintaining attacks. We seek to understand the minimum amount of information an attacker needs to launch such attacks. We assume the attacker is aware of a physical outage in the system and changes the resulting SCADA data (prior to SE) to make it appear that the line is in service. We denote such a line as the *switching attack line* hereinafter. Specifically, false line flow measurements need to be created for the switching attack line; however, this cannot be achieved by just adjusting the measurements at the end buses and requires estimating states at those buses as well, since the flow on the outage line has to be computed. For a reliable state estimate, the attacker

needs to identify a physical connection (we denote as path hereinafter) between the end buses of the switching attack line, over which it can estimate states with local measurements, and thereby, create an unobservable attack. However, there are multiple such paths in the system. To create an attack with the smallest set of information, the attacker needs to find the shortest path. Since the power system can be represented as an undirected and unweighted graph, algorithms such as Dijkstra's and Bellman-Ford, which are used to find the shortest path in directed and weighted graph, are not suitable in this problem. Therefore, we propose an algorithm based on breadth-first search (BFS), which is generally used for traversing or searching graph data structures [22]. We need such an algorithm to search for the shortest path that connected the end buses of the switching attack line in power system.

3.1 Attack Model

In an unobservable state-preserving topology attack, the attacker aims to maliciously change the system topology from $\mathcal{G}$ to a different "target" topology $\bar{\mathcal{G}} = \{\mathcal{N}, \bar{\mathcal{E}}\}$ without changing the states. In this paper, we only consider topology attacks that perturb line connection $\mathcal{E}$ to $\bar{\mathcal{E}}$; the attacks aiming to split or merge buses are out of scope, *i.e.*, $\mathcal{N}$ remains unchanged. We define the line with status data changed by attacker as *switching attack line* and the end buses of the switching attack line as *switching attack buses*.

Topology attacks can be of two types: *line-maintaining* and *line-removing*. For a line-maintaining attack, the attacker maliciously alters the line status data of the switching attack line and injects false data to make it appear that line which is not in the original graph $\mathcal{E}$ is now shown as active in $\bar{\mathcal{E}}$; the opposite is achieved by a line-removing attack. To launch a state-preserving topology attack, the attacker injects $n_{br} \times 1$ line status attack vector b and $n_z \times 1$ measurement attack vector a.

The line status attack vector b has entries $b_k \in \{-1, 0, 1\}$ for $k \in \{1, ..., n_{br}\}$ such that $b_k = 1, -1,$ and 0, correspond to line-maintaining, line-removing and no attack cases, respectively. This attack modifies (s, z) for topology $\mathcal{G}$ to $(\bar{s}, \bar{z})$ for topology $\bar{\mathcal{G}}$ such that

$$\bar{s} = s + b, \text{ and } \bar{z} = z + a. \tag{3.1}$$

In the absence of noise, the attack vector satisfies

$$a = h(x, \bar{\mathcal{G}}) - h(x, \mathcal{G}). \tag{3.2}$$

For a cyber-based topology attack considered here, when the states are preserved, *i.e.*, unchanged, and the system topology except for the switching attack line remains the same, the attacker needs to change the power flow of the switching attack line. To achieve this, the attacker only needs to change the power flow measurements on the switching attack line and power injection measurements on the switching attack buses to make such attack unobservable.

3.1.1 Line-removing vs. Line-maintaining Attacks

For line-removing attack, as stated in [15], when the attacker sets the switching attack line status to zero, the "from" and "to" power flow measurements should also be changed to zero. The modified power injection measurements for bus i are

$$\begin{aligned} P_i^a &= P_i - P_{ij} \\ Q_i^a &= Q_i - Q_{ij} \end{aligned} \tag{3.3}$$

where P_{ij} and Q_{ij} are the physical active and reactive "from" power flows of line ij, respectively. The modified power injection measurements on bus j obey (3.3), as well. An example of such attack is shown in Figure 4.1(a). In this case, to create a precise

attack, the line flow P_{ij} and Q_{ij} have to be estimated using all the relevant SCADA measurements. A heuristic way to creating such attacks is to use just the local power flow measurements at both ends of the switching attack line. This is proposed in [15] and the authors have demonstrated its performance via simulation.

In contrast, we argue that for a line-maintaining attack, such a heuristic will not work. This is because for a line-maintaining attack, the actual "from" and "to" power flows on the switching attack line are already zero since the switching attack line is out. When the attacker sets the switching attack line status to 1, the "from" and "to" power flow measurements should be non-zero since the line appears active at control center. The modified "from" power flow measurements P_{ij}^a and Q_{ij}^a should satisfy

$$\begin{aligned} P_{ij}^a &= V_i^2(g_{si} + g_{ij}) - V_i V_j(g_{ij}cos(\theta_i - \theta_j) + b_{ij}sin(\theta_i - \theta_j)) \\ Q_{ij}^a &= -V_i^2(b_{si} + b_{ij}) - V_i V_j(g_{ij}sin(\theta_i - \theta_j) - b_{ij}cos(\theta_i - \theta_j)) \end{aligned} \tag{3.4}$$

where b_{ij} and g_{ij} are the susceptance and conductance of the switching attack line, respectively, b_{si} and g_{si} are the shunt branch susceptance and conductance of bus i, respectively. The modified "to" power flow measurements P_{ji}^a and Q_{ji}^a also obey (3.4). From (3.4), we can see that to calculate the false power flow measurements on the target line, the attacker needs to estimate the states. For the power injection measurements for bus i, since the power injection for bus i should equal to the sum of all line power flows from bus i, the measurements should be modified as

$$\begin{aligned} P_i^a &= P_i + P_{ij}^a \\ Q_i^a &= Q_i + Q_{ij}^a \end{aligned} \tag{3.5}$$

where P_i and Q_i are the physical active and reactive power injection measurements, respectively; P_i^a and Q_i^a are the injection measurements modified by attacker. The power injection measurements on bus j also satisfy the relationship in (3.5). An example of such an attack is shown in Figure 4.1(b).

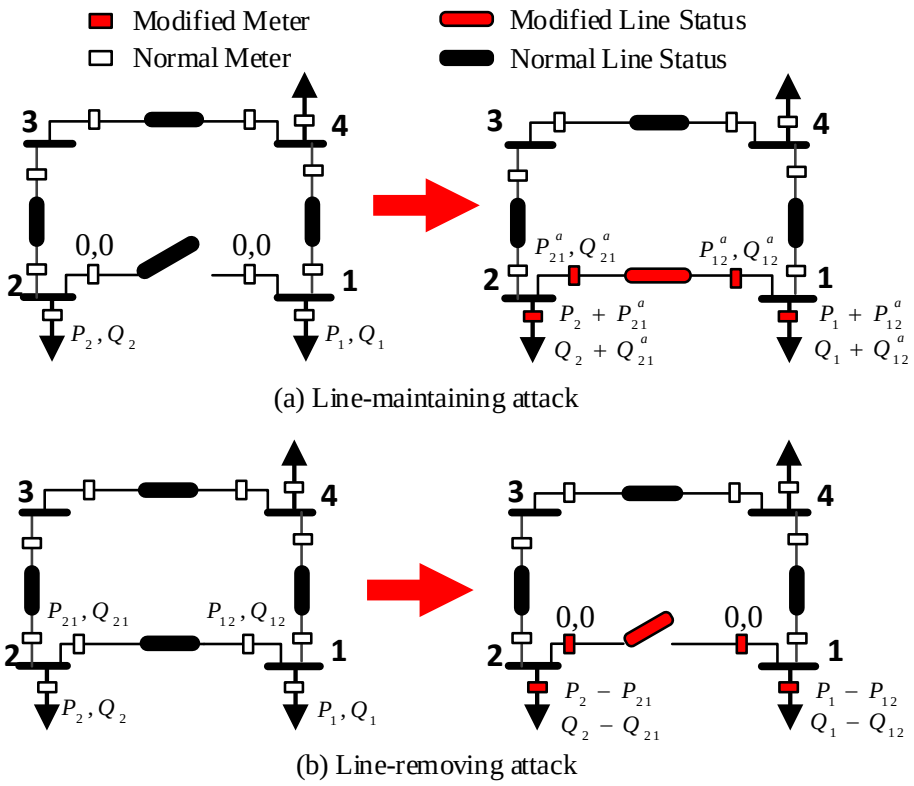


Figure 3.1: Examples of Unobservable State-preserving Topology Attacks.

3.2 Unobservable State-preserving Line-maintaining Attacks with Local Information

We assume the attacker has the following capabilities:

1. Attacker has knowledge of the topology $\mathcal{G}$ of the entire network.

2. Attacker has the capability to observe measurements only for a sub-network $\mathcal{S}$ of $\mathcal{G}$ and perform SE for $\mathcal{S}$. The choice of $\mathcal{S}$ is described in detail in the sequel.

3. Attacker has the capability to change both the line status data of the switching attack line and the measurements on both switching attack line and target buses.

For the system, we assume that the power system is observable prior to the attack.

For nonlinear measurement model and AC SE, the attacker cannot construct a only with the knowledge of system configuration. In fact, recent work in [12, 13] show that attack vector constructed with DC measurement model can be detected when the system uses AC SE. To this end, we model a sophisticated attacker who attacks the line status data and measurements of the switching attack line and the power injection measurements on the end buses of switching attack line (switching attack buses) by first estimating the system states $\hat{x}_{\mathcal{S}}$ for $\mathcal{S}$ using AC SE. Let $I_{\mathcal{T}}$ represent the set of measurements the attacker needs to modify to launch an attack. The resulting modified measurement vector $\bar{z}$ input to SE has entries

$$\bar{z}_i = \begin{cases} z_i \,, & i \notin I_{\mathcal{T}} \\ h_i(\hat{x}_{\mathcal{S}}, \bar{\mathcal{G}}) \,, & i \in I_{\mathcal{T}} \end{cases} \tag{3.6}$$

For line-maintaining attacks, equations (3.4)−(3.5) imply that the voltage magnitudes and voltage angle difference of the switching attack buses are required to form the unobservable attack vector. Thus, the attacker has to obtain a good estimate of the voltage magnitudes and voltage angle difference of the switching attack buses. Since the target line is physically disconnected, the attacker needs to find a sub-network of the physical system to estimate states on the switching attack buses. Such a sub-network should contain at least one physical path that connects the two switching attack buses. By using power flow measurements on the lines of the path, attacker can estimate the voltage magnitudes and voltage angle differences of the buses on the path, and thus, obtain a good estimate of the states of the switching attack buses. For clarification, consider the example shown in Figure 3.2. In this case, the switching attack line is the line connecting bus 1 and 2. The goal of attacker is to obtain a good estimate of states on switching attack buses 1 and 2. Assume bus 1 is

the reference bus. Attacker can use power flow measurements on the line connecting bus 1 and 4 to calculate V_4 and $\triangle\ \theta_{14} = \theta_1 - \theta_4$. Then, the V_3 and $\triangle\ \theta_{43} = \theta_4 - \theta_3$ can be estimated with power flow measurements on the line connecting bus 4 and 3 and the estimated $V_4\angle\theta_4$. It is the same for estimation of V_2 and $\triangle\ \theta_{32} = \theta_3 - \theta_2$. Then, attacker can obtain a good estimation of voltage magnitudes V_1 and V_2, and voltage angle difference$\triangle\ \theta_{12} = \triangle\ \theta_{14} + \triangle\ \theta_{43} + \triangle\ \theta_{32}$, and hence, calculate the modified measurements.

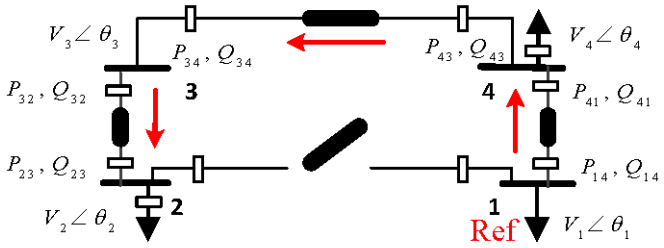


Figure 3.2: Illustration of A Shortest Path for Unobservable State-preserving Attack

For a specific switching attack line, there are multiple paths between the two switching attack buses in the system. To reduce the cost of attacks, attacker needs to analyze the system topology $\mathcal{G}$ and find the shortest path between the two switching attack buses. Thus, the attack can be launched by estimating a minimal set of measurements.

We use a BFS algorithm to identify the shortest path that connects the switching attack buses. The *minimal observation sub-network* $\mathcal{S}$ denotes the connectivity of the buses and lines on the shortest path. The physical power grid $\mathcal{G}$ is represented as an unweighted and undirected graph in which an edge is a line and a node is a bus. We assign one of the switching attack buses as the *starting bus* and the remaining switching attack bus is the *destination bus*. The procedure to determine $\mathcal{S}$ is as

follows:

Algorithm 1 BFS for Shortest Path Connecting Switching Attack Buses

Input: $\mathcal{G}$, *starting bus*, *destination bus*

Output: shortest path connecting the *starting bus* and the *destination*

1. Set the *starting bus* as the *in progress bus* and the rest buses as *unvisited buses*. Set the level of the current set of *in progress buses* as $k = 0$.

2. Search all *unvisited buses* that are connected (by a branch) to the set of *in progress buses*. Mark such *unvisited buses* as the *in progress buses* and the previous set of *in progress buses* as *visited buses*. Set the level of the current set of *in progress buses* as $k = k + 1$. If the *destination bus* is in the set of *in progress buses*, that means the *shortest path tree* has been identified, go to step 3. Otherwise, repeat step 2.

3. Backtrack from the *desination bus* to the *starting bus* level-by-level, and identify the shortest path. If there is more than one shortest path, repeat step 3 until all shortest paths are identified.

Once $\mathcal{S}$ is found, attacker can assign one of the switching attack buses as a slack bus, collect and use the power flow measurements $z_{\mathcal{S}}$ inside $\mathcal{S}$ to perform local SE as follows

$$\min J_{\mathcal{S}}(x_{\mathcal{S}}) = (h(x_{\mathcal{S}}, \mathcal{S}) - z_{\mathcal{S}})^T R_{\mathcal{S}}^{-1} (h(x_{\mathcal{S}}, \mathcal{S}) - z_{\mathcal{S}}), \tag{3.7}$$

the solution to which satisfies

$$g(\hat{x}_{\mathcal{S}}) = \frac{\partial J(\hat{x}_{\mathcal{S}})}{\partial x_{\mathcal{S}}} = H^T(\hat{x}_{\mathcal{S}}) \cdot R_{\mathcal{S}}^{-1} \cdot (h(x_{\mathcal{S}}, \mathcal{S}) - z_{\mathcal{S}}) = 0 \tag{3.8}$$

where the system Jacobian matrix $H = \frac{\partial h(x_{\mathcal{S}}, \mathcal{S})}{\partial x_{\mathcal{S}}} \mid_{x_{\mathcal{S}} = \hat{x}_{\mathcal{S}}}$. The WLS solution for this nonlinear optimization problem can be solved iteratively. Then attacker can calculate

the modified measurements with (4.3).

Since the power system is a complex geographically distributed network, attacker may be limited to a subset of the network static topology. Under such conditions, this method can also be applied to find the minimal observation sub-network.

3.3 Switching Attack Line Selection

In practice, to launch an unobservable state-preserving line-maintaining attack, attackers are limited to finite sets of switching attack lines due to the following reasons:

1. The power injection measurements can only be altered by redistributing loads in cyber layer. Attacker cannot change generator output data due to direct communication between control center and power plant.

2. The power injection for no load buses cannot be altered, since load occurring in no load buses can be immediately detected by operator.

3. Any attacks that can lead to negative loads in cyber layer can be detected.

4. The significant alteration of the system such as system dividing to several islands (line-removing attack) or islands combining to a whole system (line-maintaining attack) can lead to operator's intervention.

Therefore, to launch a successful line-maintaining attack, attacker should analyze the system topology and operation states prudently to choose a switching attack line. The following three classes of lines should be avoided as switching attack lines:

1. Single critical line or critical pairs of lines.

2. Lines that once being attacked can lead to negative loads in cyber layer.

3. Lines that connected to no load buses.

When eliminates the three classes of lines listed above, the choice of feasible switching attack lines for attacker can be significantly reduced. Another limitation of these attacks is that to cause a physical line overload in the system, the load shifts required at the switching attack buses have to be greater than 10%. Such a change can lead detection of anomaly. Considering the two defects, we can conclude that vulnerability of the system to unobservable state-preserving topology attacks is limited.

3.4 Numerical Results

In this section, we use the IEEE 24-bus RTS shown in Figure 3.3 as the test system. We assume that the measurements in the test system are: (a) active and reactive power flows on both ends of all lines; and (b) active and reactive power injection on buses with loads and/or generation; *i.e.*, overall, the number of total measurements in the test system is 192. We run our simulations with MATLAB R2014a and MATPOWER 4.1.

3.4.1 Feasible Switching Attack Line Selection

In this subsection, we analyze the test system to identify all feasible switching attack lines for unobservable state-preserving line-maintaining attacks. We first exclude critical lines and the lines that connected to a no load buses in the system. For the rest lines, we perform a whole network SE and use the estimated states to calculate the attack vector. We check the modified loads in cyber layer for each line and exclude the lines that can lead to negative loads. Table 3.1 demonstrates all the lines we exclude from the set of feasible target lines and the reason for exclusion. Overall, for line-maintaining attacks, there are 8 feasible switching attack lines in the test system, for which the line indices are #2, #5, #8, #9, #12, #13, #34, #35.

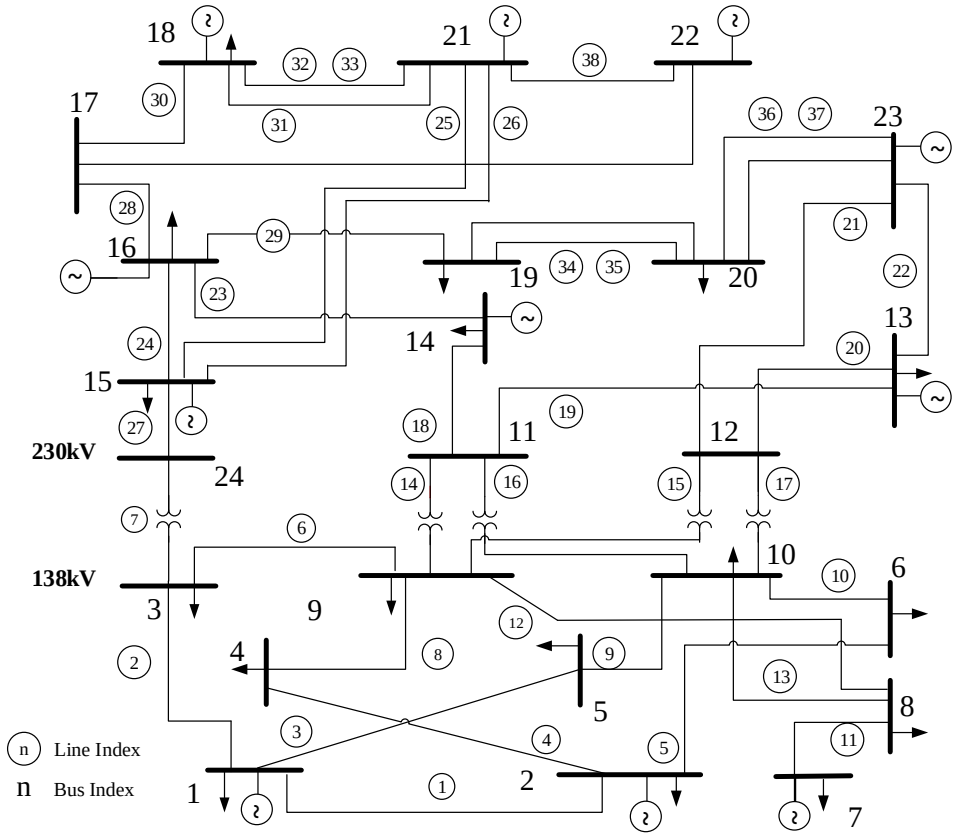


Figure 3.3: IEEE 24-bus Reliable Test System

3.4.2 Minimal Observation Sub-network

In this subsection, we exhaustively illustrate the minimal observation sub-network of each feasible switching attack line according to the algorithm introduced in Section **??**. The details of each minimal observation sub-network for each switching attack line are demonstrated in Table 3.2. The minimal number of lines and buses (denote as $n_{\mathcal{S}l}$ and $n_{\mathcal{S}b}$, respectively) inside the minimal observation sub-network for each switching attack line is illustrated in Figure 3.4. That is the minimal information the attacker needs to observe before launching a successful attack. Since the system is under full monitoring redundancy, there are 4 measurements which are active and reactive power flow measurements on both "from" and "to" ends placing on a line. Therefore, the

Table 3.1: Classification of Infeasible Switching Attack Lines for Undetectable State-preserving Line-maintaining Attack

Infeasible Reason	Infeasible Switching Attack Line
Critical Line	#11
Connect to No Load Bus	#7, #14−#22, #25−#28, #30−#33, #36−#38
Lead to Negative Load	#1, #3, #4, #6, #10, #23, #24

minimum number measurements the attacker needs to access is the minimum number of observation measurements along the path, as well as the measurements placed on the switching attack line and the switching attack buses, *i.e.,* $4n_{\mathcal{SL}} + 8$.

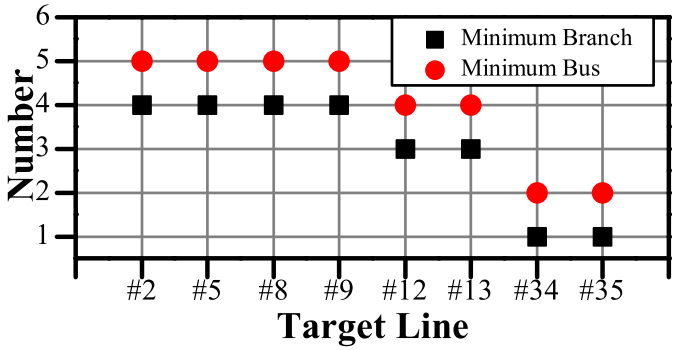


Figure 3.4: Number of Branches and Buses of the Minimal Observation Sub-network of Each Switching Attack Line

From these results, we can see that the minimal observation sub-network for each switching attack line is relatively small compared with the whole network topology even for a small system such as IEEE 24-bus RTS. The largest minimal observation sub-network in the test system consists of 4 branches and 5 buses, in which the total observation measurements number is 16. The number of measurements of this sub-network that attacker need to access inside is 24, which is 12.5% of the test system. Therefore, it is possible for attacker to launch such attacks with only a small subset of information of the system.

Table 3.2: Minimal Observation Sub-network for All Feasible Switching Attack Lines

Target Line #	Branches of Minimal Observation Sub-network	Connectivity of Buses
2	#1, #4, #8, #6	1⇒2⇒4⇒9⇒3
5	#1, #3, #9, #10	2⇒1⇒5⇒10⇒6
8	#4, #1, #5, #6	4⇒2⇒1⇒3⇒9
9	#3, #1, #5, #10	5⇒1⇒2⇒6⇒10
12	#13, #16, #14	8⇒10⇒11⇒9
13	#12, #14, #16	8⇒9⇒11⇒10
34	#35	19⇒20
35	#34	19⇒20

3.4.3 Undetectability of Attacks

In this subsection, we test the unobservable state-preserving line-maintaining attacks with both global information and local information on the test system. In our simulation, we use MATPOWER to generate measurements and perform state estimation. The default setting of the IEEE 24-bus system in MATPOWER is utilized for simulation. We assume the system is operating under optimal power flow and the loads of the system are constant. The errors for all measurements are assumed to be $e_i \sim N(0, 0.01)$ and the χ^2 detector threshold is chosen for a 95% confidence in detection.

We test 1000 trials for each switching attack line with two attack regimes, *global information regime* and *local information regime*. The global information regime is that attacker can observe all measurements in the system and perform AC SE with whole network topology and measurements. While the local information regime is that attacker can only observe the measurements inside the minimal sub-network

$\mathcal{S}$ and perform AC SE with topology and measurements of $\mathcal{S}$. In each trial, the measurements are generated by adding random Gaussian noise to the actual power flows and injections of the test system. The attacker first uses both global and local information regime to obtain the estimated states. Then the attack vectors are calculated with both regimes, and added to the corresponding measurements to get two sets of corrupted measurements. We use these corrupted measurements to perform AC SE of the whole network to obtain residuals and use χ^2-test with the residuals. If the residual is greater than the threshold, we assume this trial as detected trial. We calculate the detection probability as $p_{\text{detection}} = \frac{\#\text{detection trials}}{\#\text{trials}}$. The detection probabilities of attacks with both global information and local information for each switching attack line are demonstrated in Figure 3.5. The blue dash and dot line represents the 5% false alarm constraint of the χ^2 detector.

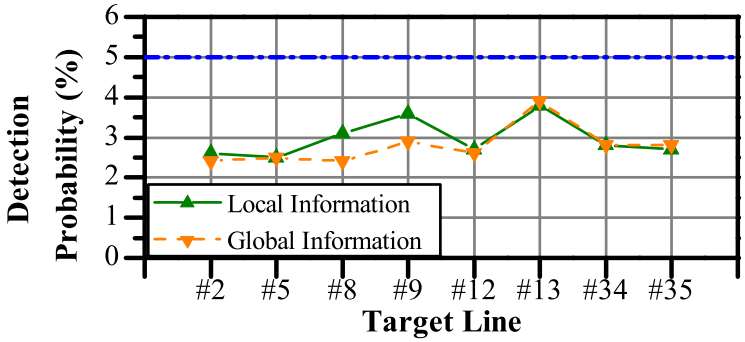


Figure 3.5: Detection Probability (1000 Trials) of Unobservable State-preserving Line-maintaining Attacks on Both Global Information and Local Information (False Alarm Const. = 5%).

From Figure 3.5, we can see that for most switching attack lines, the detection probabilities of attacks generated with global information are lower than those with local information. However, both of them are lower than the false alarm constraint, which means the proposed attacks will not be detected.

3.4.4 Load Shifts and Long-term Consequences

In this subsection, we illustrate the physical consequences of unobservable state-preserving line-maintaining attacks. The number of switching attack lines is limited to 1. We assume the system is operating under optimal power flow and the loads of the system are constant during the simulation time period. To model realistic power systems, we assume that there are a few lines congested prior to the attack and the attacker chooses one such line as target to maximize power flow.

For each switching attack line, we exhaustively test the long-term consequences under all feasible 1 congested line pattern. This is achieved in simulation by reducing the line rating to 90% of the base case power flow to create congestion. These attack consequences are quantified by comparing the cyber power flow and physical power flow over the entire attack time duration. The cyber power flow is the power flow obtained from the OPF result in the control center. The physical power flow, on the other hand, is the real power flow values of the system after dispatching with the most recent OPF dispatch solution with the correct topology information. The overall statistics results are demonstrated in Table 3.3. It should be noticed that, even for the potential feasible switching attack lines, under some specific congestion pattern, the unobservable state-preserving topology attack can be generated at the first few events. Then after several re-dispatching processes, the updated attack vector under current operation state can lead to negative loads in cyber layer, which will be detected by the operator. Thus, such cases can not be assumed as feasible attack cases.

Table 3.3: Post E0 System Behavior with Sustained Unobservable State-preserving Line-maintaining Attack.

Total Feasible Case	Power Flow Overload	No Violation
255	3.92%	96.08%

In Table 3.3, 3 disparities have been observed between the cyber and physical power flow, which we classified as *Power Flow Overload* cases and *No Violation* cases. In Power Flow Overload cases, the overload problems keep occurring due to re-dispatching with incorrect topology information. In *No Violation* cases, there's no overload or a line overloaded in Event 0 but the power flow can finally reduce below 100% of the rating in the simulation time period. In *Not Converge* cases, AC OPF module with false topology information in the cyber layer finally fails to converge after several events. We assume cases with overload as *successful attacks* and cases with no violation as *unsuccessful attacks*. Then from Table 3.3, we can see that the percentage of total successful unobservable state-preserving attacks is 3.92%. It shows the vulnerability of the test system to such attacks. Since successful attack cases are in low proportion, the long term negative implication for the undetected state-preserving topology attack is limited.

The active load shift percentage for all feasible state-preserving line-maintaining attacks in IEEE 24-bus reliable test system is shown in Figure 3.6. We can observe that only 10.98% of the total feasible cases with the active power load shift within 4% for line-maintaining attacks. Cases with active power load shift greater than 50% are 60% of the total feasible cases. In practice, a large active power load shift will lead to operator intervention. Thus, for the test system, most of the feasible attack cases can lead to large load shifts, and hence, being detected. Furthermore, by observing the cases that cause less than 10% load shift, we find that none of these cases can lead to successful attack results. Thus, we can conclude that it is difficult for unobservable state-preserving topology attacks to pass the sanity check in the system while causing severe consequences.

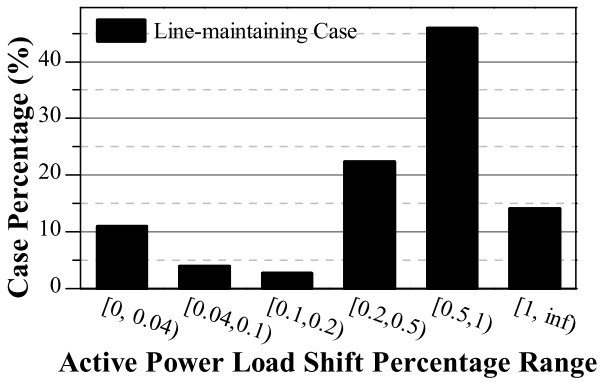


Figure 3.6: Overall Statistics Results of Active Power Load Shift Percentage for All Feasible Attack Cases within Unobservable State-preserving Topology Attack.

3.5 Concluding Remarks

In this chapter, we focus on unobservable state-preserving topology attacks, especially the line-maintaining attacks. We propose an algorithm based on BFS to find the minimum local information required to perform such attacks. We have shown that our proposed algorithm can enable an attacker to obtain the localized topology and corresponding measurement data to mount an attack that bypasses bad data detector and successfully changes topology information of the system in the cyber layer. Moreover, we identify that such attacks have three categories of limitations for (a) limit set of switching attack lines due to system characteristics; (b) large load shifts resulting from attacks; and (c) less severe long-term consequences caused by attacks. Therefore, such attacks can be detected with a valid load shifts monitoring mechanism.

To overcome such limitations, a class of more sophisticated attacks in which both topology information and system states are changed by attacker in an unobservable manner are introduced in the next chapter.

Chapter 4

UNOBSERVABLE STATE-AND-TOPOLOGY CYBER-PHYSICAL ATTACKS

In this chapter, we study a class of more powerful attacks in which an attacker can change both states and topology data to enable a coordinated physical and cyber attack and intensify its damage. While changes in LMP and operation costs demonstrate the economic effect of unobservable attacks, an important question that remains to be addressed is whether serious damage such as instability, cascading failures, and blackouts that can potentially cripple society and the economy can be caused by cyber-physical attacks on the grid. In this chapter, we introduce a long-term attack model that focus on masking physical attack, creating overloading on a line while avoiding being detected in both SE and the subsequent modules.

The attacks studied in this chapter consist of physical attacks that cause transmission line outage in physical layer and cyber attacks that change both states and topology data in cyber layer. These attacks in cyber layer are formally introduced in [15]; however the analysis in [15] is restricted to unobservable state-preserving topology attacks. As stated in Chapter 3, the state-preserving attacks are limited due to few feasible switching attack lines, large load shifts, and such attacks can hardly lead to long-term severe consequences. Therefore, our motivation for including both state and topology information in this chapter is to focus on worst-case attacks and to limit detectability via the data processing modules subsequent to SE (*e.g.,* load monitoring). Furthermore, an attack by itself is meaningless unless its consequences on the physical grid can be quantified. To this end, we seek to understand whether an unobservable topology attack coordinating with a physical attack can lead to another physical line overloading. We propose a two-step strategy to determine the worst

attack. The first step determines the physical attack target and the worst operation states resulting from cyber attack, while the second step determines the cyber attack vector that can move the system from any operation states to the worst operation states. Each step is a two-stage optimization problem in which the first stage models the attack and the second stage models the system response via re-dispatch to the attack. Thus, an optimal attack is one which maximizes power flow on a line subsequent to FDI changes by attacker followed by SE and DC OPF processing by the system. It is this temporal and modular processing aspect of the cyber layer of the electric grid that our two-step attack strategy captures. Such a two-stage optimization is studied in [18] from the viewpoint of the attacker maximizing the system dispatch operating costs. More recently, in [20], the authors introduce a two-stage optimization for unobservable attacks on AC SE. While [20] is more closely related, our work focuses on joint physical and unobservable topology attacks, and therefore, the optimization problem introduced here is different from [20].

An important contribution of our work is the observation that FDI attacks designed to be unobservable within a specific computing module (*e.g.,* SE) can be detected when the end-to-end processing units of the system are jointly modeled. For a state-preserving attack introduced in Chapter 3, to cause a physical line overload of an adjacent line, our experiments have shown that the load shift required at the attack buses have to be larger than 10%; such a change leads to operator intervention, and detection of anomaly. Therefore, for detectability reasons, the attacker changes both states and topology information in order to distribute the load shift over a sub-graph of the network. However resources constraints limit the attacker's network size. Thus, in our formulation, the goal is to maximize the power flow on a particular line subject to constraints on (a) attacker resources (number of bus and

line measurements to change); and (b) detection via bounds on load shift.

4.1 Attack Model

The unobservable state-and-topology attack modeling both a physical attack and a coordinated cyber attack. We will first discuss the physical attack and then the coordinated cyber attack that mask the physical attack.

4.1.1 Physical Attack

In power system, components such as generators, substations, buses, lines and transformers are all vulnerable to physical attacks. Among these components, attackers prefer to selecting transmission lines as targets since they are the most unprotected [23]. Attacking transmission line can reduce the reliability of power system and under some conditions, lead to violations such as overloading on other lines or load shedding. Furthermore, physical attacks that target at transmission lines are easier to become unobservable when coordinating with cyber attacks. Thus, we only consider the physical attack aims to cause transmission line outage in this chapter.

When a transmission line is taking down by physical attack, the topology of the system are altered. To hide such topology change, attacker must launch unobservable cyber topology attacks which modify the line status data and corresponding measurements. Therefore, it is important to understand the attack model and characteristics of unobservable topology attacks in cyber layer.

4.1.2 Cyber Attack: Masking Physical Attack via an Unobservable Topology Attack

In a general topology attack, the attacker modifies line status as well as related bus measurements to alter the system topology $\mathcal{G}$ to a different "target" topology

$\bar{\mathcal{G}} = \{\mathcal{N}, \bar{\mathcal{E}}\}$. As stated in Chapter 3, we only consider topology attacks that perturb branch connection $\mathcal{E}$ to $\bar{\mathcal{E}}$; the attacks aiming to split or merge buses are out of scope, *i.e.*, $\mathcal{N}$ remains unchanged. We define lines with line status data changed by attacker as *switching attack line*.

Topology attacks can be of two types: *line-maintaining* and *line-removing*. For a line-maintaining attack, the attacker changes measurements and line status data to make it appear that line which is not in the original graph $\mathcal{E}$ is now shown as active in $\bar{\mathcal{E}}$; the opposite is achieved by a line-removing attack. To launch a general topology attack, the attacker injects $n_{br} \times 1$ line status attack vector b and $n_z \times 1$ measurement attack vector a. The line status attack vector b has entries $b_k \in \{-1, 0, 1\}$ for $k \in \{1, ..., n_{br}\}$ such that $b_k = 1, -1,$ and 0, correspond to line-maintaining, line-removing and no attack cases, respectively. These changes lead to a new system state $\bar{x}$ for the system under attack. This attack modifies (s, z) for topology $\mathcal{G}$ to $(\bar{s}, \bar{z})$ for topology $\bar{\mathcal{G}}$ such that

$$\bar{s} = s + b, \quad \text{and} \quad \bar{z} = z + a. \tag{4.1}$$

In the absence of noise, the attack vector satisfies

$$a = h(\bar{x}, \bar{\mathcal{G}}) - h\left(x, \mathcal{G}\right). \tag{4.2}$$

Since the physical attack we focus on is to trip lines, to hide such attacks, the unobservable topology attacks studied hereinafter are the line-maintaining attacks.

The simplest subclass of unobservable topology attacks that can hide the physical attacks are state-preserving attacks introduced in Chapter 3. These attacks aim to change the system topology information while preserving the states. Attacker only need to modify (a) the line status data of switching attack line, (b) power flow measurements on the line, and (c) the power injection measurements on buses connecting to the switching attack line to accomplish such attacks. Therefore, the

resources required by state-preserving topology attacks are relatively less. However, since the power injection measurements can only be altered by shifting loads in cyber layer, attackers are limited to a small set of switching attack lines which connecting two load buses as stated in Subsection 3.4.4. Another crucial limitation of these attacks is that the load shifts caused by such attacks can be greater than 10% on load buses (see Section 3.4.4). Such a change can lead to detection of anomaly.

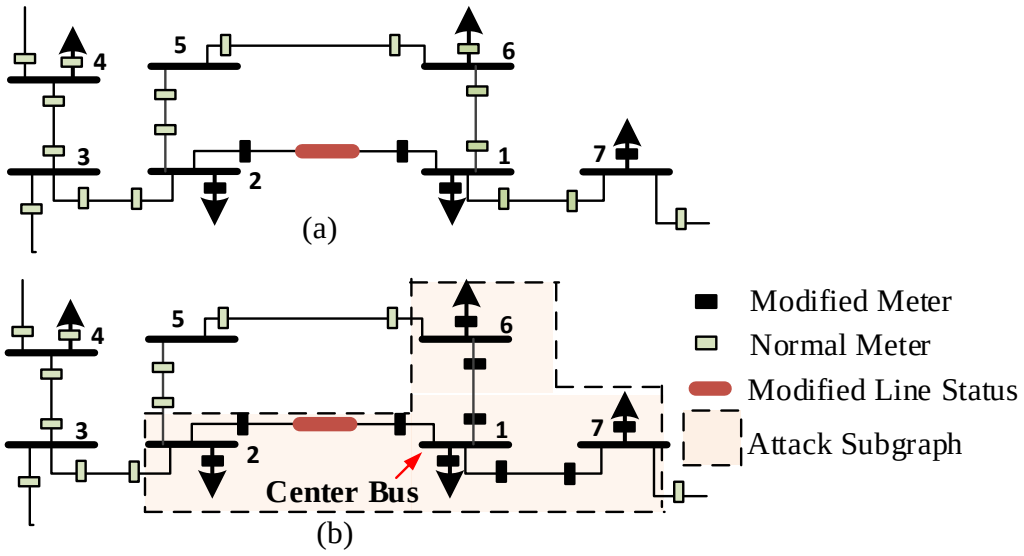


Figure 4.1: Example of Modified Meters and Line Status Data for (a) Unobservable State-preserving Topology Attack; and (b) Unobservable Joint Topology and State Attack.

To avoid these defects, we focus on general topology attacks, in which attacker change both states and topology information, hereinbelow.

We assume the attacker has the following capabilities:

1. Attacker has knowledge of the static topology $\bar{\mathcal{G}}_0$ of the entire network prior to physical attacks.

2. Attacker has the capability to launch physical attack, observe and change mea-

surements only for a sub-graph $\mathcal{S}$ of $\mathcal{G}_0$. The choice of $\mathcal{S}$ is described in detail in the sequel.

3. Attacker has the capability to perform SE and compute modified measurements for $\mathcal{S}$.

For the system, we assume that the power system is observable prior and post to the physical attack.

As stated in Section 3.2, for nonlinear measurement model, we model a sophisticated attacker who attacks measurements and line status data for a sub-graph $\mathcal{S}$ of the network by first estimating the system states $\hat{x}_{\mathcal{S}}$ for $\mathcal{S}$ using AC SE. The attacker then chooses a small set of buses in $\mathcal{S}$ to change states from the estimate $\hat{x}_{\mathcal{S}}$ to $\bar{x}_{\mathcal{S}} = \hat{x}_{\mathcal{S}} + c$ such that the measurement vector after attack $\bar{z}$ is

$$\bar{z}_i = \begin{cases} z_i \,, & i \notin \mathcal{I}_{\mathcal{S}} \\ h_i(\hat{x}_{\mathcal{S}} + c, \bar{\mathcal{G}}) \,, & i \in \mathcal{I}_{\mathcal{S}} \end{cases} . \tag{4.3}$$

Changing states and topology data both lead to changes in power flow measurements on branches and power injection measurements on load buses in $\mathcal{S}$. For non-load buses in $\mathcal{S}$, the attacker should ensure that within attacks, the sum of power flow on the buses and generation (if exists) should be zeros. Thus, the states changing of non-load buses is dependent on the states changing of the neighboring load buses. We hence define the load buses with states changing as *center buses* of $\mathcal{S}$.

Another characteristics of $\mathcal{S}$ is that all states inside $\mathcal{S}$ are observable to attacker. For the switching attack line, since they are disconnected in physical system, attacker should satisfy that there are path inside $\mathcal{S}$ to connect the switching attack buses as introduced in Section 3.2.

The methods to identify a sub-graph for unobservable FDI attacks that change states with topology unchanged in non-linear model are introduced in [12, 13] and method to identify sub-graph for unobservable state-preserving topology attacks are introduced in Section 3.2. In this chapter, we use a similar method to identify the sub-graph for a general topology attacks as follows.

1. Determine the center buses, and include all center buses in $\mathcal{S}$.

2. Extend $\mathcal{S}$ from center buses by including all buses and branches connected to center buses.

3. If there are non-load buses on the boundary of $\mathcal{S}$, extend $\mathcal{S}$ by including all adjacent buses of the non-load boundary buses and the corresponding branches.

4. Repeat Step 3 until all boundary buses of $\mathcal{S}$ are load buses.

5. Check if there is a path in $\mathcal{S}$ that can connect the two end buses of the switching attack line. If such path exits, then $\mathcal{S}$ is the attack sub-graph. If there is no such path, go to Step 6.

6. Use Algorithm 1 introduced in Section 3.2 to find the shortest path connecting the two switching attack buses. Include the shortest path (buses and branches) in $\mathcal{S}$. Then this $\mathcal{S}$ is the attack sub-graph.

Sub-graph identified with this method ensures the observability of states inside it to attacker. It also allows the states of the boundary buses to remain unchanged via changes to load injections. As stated in Chapter 3, large changes in load estimates can be detected. Thus, the attacker has to determine the state change vector c such that the load shifts at all load buses in $\mathcal{S}$ are bounded.

4.2 Worst Attack Strategy

In this section, we develop a worst attack strategy in which attacker determines a cyber-physical attack to (a) trip a line in physical system and hide the physical attack in cyber layer; and (b) maximize power flow on a specific line in physical system with sparsest attack vector. In particularly, we define the line that attacker choose to maximize power flow on as *target line*.

The strategy we proposed consists of two steps. In the first step, we determine the switching attack line that attacker prefer to trip and a cyber attack vector that can lead to the maximum power flow on the target line within limited number of center buses and bounds on load shifts. Specifically, the cyber attack vector solved in this step is corresponding to the optimal states after re-dispatch within OPF instead of the current operation states. Thus, such attack vector cannot be applied directly to launch unobservable attacks under current operation states. To solve this problem, we use the second step to determine the attack vector that can be injected to the current operation states and lead to the worst operation states solved in Step 1 that can cause maximum power flow on the target line after re-dispatch. We henceforth define the attack vector solved in the second step as *initial attack vector*. The details of the two steps are introduced in the following subsections.

4.2.1 Step 1: Maximize Power Flow on a Line

In the first step, we propose a two-stage optimization problem. Such a problem determines the attack vector c and the line status change vector b such that at least one line in $\mathcal{S}$ has maximal power flow subject to bounds on load shift and number of center buses with states changed. The two-stage optimization is given as

$$\max \; P_{Kl} - \zeta \left\| c_{\mathcal{L}} \right\|_0 \tag{4.4}$$

$$\text{s.t.} \quad -\tau P_D \leqslant \bar{H}_1 \left(\theta^* + c\right) - A_{KN} P_K^* \leqslant \tau P_D \tag{4.5}$$

$$\left\|c_{\mathcal{L}}\right\|_0 \leqslant N_0 \tag{4.6}$$

$$\sum_{k=1}^{n_{br}} (1 - s_k) = N_T, \quad s_k \in \{0, 1\} \tag{4.7}$$

$$\left(A_{Kf} + A_{Kt}\right) s \geqslant 1 \tag{4.8}$$

$$\left\{\theta^*, P_G^*, P_K^*\right\} = arg \left\{ \underset{\theta, P_G, P_K}{min} \sum_{g=1}^{n_g} C_g \left(P_{Gg}\right) \right\} \tag{4.9}$$

$$\text{s.t. } A_{GN} P_G - A_{KN} P_K = P_D \left(\lambda\right) \tag{4.10}$$

$$-P_K^{\max} \leqslant \bar{H}_2 \left(\theta + c\right) \leqslant P_K^{\max} \quad \left(\mu^-, \mu^+\right) \tag{4.11}$$

$$P_G^{\min} \leqslant P_G \leqslant P_G^{\max} \quad \left(\alpha^-, \alpha^+\right) \tag{4.12}$$

$$P_K = \text{diag}\left(s\right) \cdot \bar{H}_2 \theta^* \tag{4.13}$$

where c is $n_b \times 1$ attack vector; A_{GN} is $n_b \times n_g$ generator to bus connectivity matrix; $C_g\left(\cdot\right)$ is the cost function for generator g; P_G is $n_g \times 1$ active power generation vector with maximum and minimum limit $P_G^{\max}$ and $P_G^{\min}$, respectively; P_K is $n_{br} \times 1$ physical power flow vector with thermal limit $P_K^{\max}$; λ is $n_b \times 1$ dual variable vector of power balance constraints; $\mu^{\mp}$ are $n_{br} \times 1$ dual variable vectors of minimum and maximum power flow limit constraints, respectively; $\alpha^{\mp}$ are $n_b \times 1$ dual variable vectors of minimum and maximum active power generation output constraints, respectively; $\bar{H}_1$ is $n_b \times n_b$ dependency matrix between power injection and voltage angle related to $\bar{\mathcal{G}}$; $\bar{H}_2$ is $n_{br} \times n_b$ dependency matrix between power flow and voltage angle related to $\bar{\mathcal{G}}$; P_D is $n_b \times 1$ active power load vector in physical system, which has maximum load shift percentage τ; ζ is the weight of the norm of attack vector c; N_0 is the maximum number of center buses that can be attacked; N_T is the maximum number of switching attack lines; $\mathcal{L}$ is the set of load buses.

The goal of the attack in (4.4) is a multi-objective problem which includes maxi-

mizing the power flow on a specific line l to create an overload, while minimizing the l_0-norm of the attack vector. The power flow on l is maximized along the direction of the power flow prior to attack. The first stage optimization is to determine the cyber attack vector subject to limits on (a) load shift as in (4.4), and (b) an l_0-norm constraint on the cyber attack vector corresponding to load buses as in (4.6); and physical attack targets subject to a bound on the total number of switching attack lines as in (4.7). Constraint (4.8) guarantees the observability of the physical power system post to the selected physical attack. The second stage optimization represents DCOPF, whose aim is to minimize operation cost in (4.9), subject to power balance, thermal limit and generation limit constraints in (4.10)−(4.12), respectively, and the physical power flow on each line is computed in (4.13). Thus, only the voltage angle states are formulated in this problem, and all voltage magnitudes are set to 1.

This two-stage optimization problem is nonlinear and non-convex. For tractability, we modify several constraints.

Constraint (4.13) is a nonlinear constraint which includes the product of binary variable s and continuous variable θ. It can be replaced by a linear form as follows

$$\begin{cases} P_K - \bar{H}_2\theta^* \leqslant M_1\,(1-s) & (\beta^+) \\ -P_K + \bar{H}_2\theta^* \leqslant M_1\,(1-s) & (\beta^-) \\ P_K \leqslant M_1 \cdot s & (\gamma^+) \\ -P_K \leqslant M_1 \cdot s & (\gamma^-) \end{cases} \tag{4.14}$$

where $\beta^{\pm}$ and $\gamma^{\pm}$ are $n_{br} \times 1$ dual variable vectors for the corresponding constraints and M_1 is a large number.

Constraint (4.6) is l_0-norm constraint of the attack vector corresponding to load buses, which is nonlinear and generally non-convex. It can be relaxed to a corre-

sponding conditional l_1-norm constraint as:

$$\|c_{\mathcal{L}}\|_1 = \sum_{n\in\mathcal{L}} |c_n| \leqslant N_1 \tag{4.15}$$

where N_1 is the non-negative.

However, constraint (4.15) is still nonlinear. We hence linearize it as follows:

$$\begin{cases} c_n \leqslant u_n \\ -c_n \leqslant u_n \\ \sum\limits_{n\in\mathcal{L}} u_n \leqslant N_1 \end{cases} \tag{4.16}$$

where u is $n_{load} \times 1$ non-negative slack variable vector.

Once the attack vector determined by s and c is given in the first stage optimization problem, the second stage DCOPF problem (4.9)$-$(4.12) and (4.14) is then convex. The second stage optimization problem can then be replaced by its Karush-Kuhn-Tucker (KKT) optimality conditions. The two-stage optimization problem can hence be converted to a single-stage problem.

The KKT condition of the second stage problem can be written as

$$\begin{aligned}
&\nabla\left(\sum_{g=1}^{n_g} C_g\left(P_{Gg}^*\right)\right) + \lambda^T \cdot \nabla\left(A_{GN}P_G^* - A_{KN}P_K^* - P_D\right) \\
&+ \left[\mu^-;\mu^+\right]^T \cdot \nabla\left(\begin{bmatrix} -\bar{H}_2\left(\theta^* + c\right) \\ \bar{H}_2\left(\theta^* + c\right) \end{bmatrix} - \begin{bmatrix} P_K^{\max} \\ P_K^{\max} \end{bmatrix}\right) \\
&+ \left[\alpha^-;\alpha^+\right]^T \cdot \nabla\left(\begin{bmatrix} -P_G^* \\ P_G^* \end{bmatrix} - \begin{bmatrix} -P_G^{\min} \\ P_G^{\max} \end{bmatrix}\right) \\
&+ \left[\beta^-;\beta^+\right]^T \cdot \nabla\left(\begin{bmatrix} -P_K^* \\ P_K^* \end{bmatrix} + \begin{bmatrix} \bar{H}_2\theta^* \\ -\bar{H}_2\theta^* \end{bmatrix} - M_1 \cdot \begin{bmatrix} 1-s \\ 1-s \end{bmatrix}\right) \\
&+ \left[\gamma^-;\gamma^+\right]^T \cdot \nabla\left(\begin{bmatrix} -P_K^* \\ P_K^* \end{bmatrix} - M_1 \cdot \begin{bmatrix} s \\ s \end{bmatrix}\right) = 0
\end{aligned} \tag{4.17}$$

$$\operatorname{diag}\left(\left[\mu^{-};\mu^{+}\right]\right)\cdot\left(\left[\begin{array}{c}-\bar{H}_2\left(\theta^{*}+c\right)\\ \bar{H}_2\left(\theta^{*}+c\right)\end{array}\right]-\left[\begin{array}{c}P_K^{\max}\\ P_K^{\max}\end{array}\right]\right)=0 \tag{4.18}$$

$$\operatorname{diag}\left(\left[\alpha^{-};\alpha^{+}\right]\right)\cdot\left(\left[\begin{array}{c}-P_G^{*}\\ P_G^{*}\end{array}\right]-\left[\begin{array}{c}-P_G^{\min}\\ P_G^{\max}\end{array}\right]\right)=0 \tag{4.19}$$

$$\operatorname{diag}\left(\left[\beta^{-};\beta^{+}\right]\right)\cdot\left(\left[\begin{array}{c}-P_K^{*}\\ P_K^{*}\end{array}\right]+\left[\begin{array}{c}\bar{H}_2\theta^{*}\\ -\bar{H}_2\theta^{*}\end{array}\right]-M_1\cdot\left[\begin{array}{c}1-s\\ 1-s\end{array}\right]\right)=0 \tag{4.20}$$

$$\operatorname{diag}\left(\left[\gamma^{-};\gamma^{+}\right]\right)\cdot\left(\left[\begin{array}{c}-P_K^{*}\\ P_K^{*}\end{array}\right]-M_1\cdot\left[\begin{array}{c}s\\ s\end{array}\right]\right)=0 \tag{4.21}$$

$$(4.10)-(4.12),(4.14)$$

$$\left[\mu^{-};\mu^{+};\alpha^{-};\alpha^{+};\beta^{-};\beta^{-};\gamma^{-};\gamma^{+}\right]\geqslant 0 \tag{4.22}$$

where constraint (4.17) is the partial gradient optimal condition, (4.18)−(4.21) are the complementary slackness constraints, (4.10)−(4.12) and (4.14) are the primal feasibility constraints, and (4.22) represents the dual feasibility constraints.

Particularly, the complementary slackness constraints (4.18)−(4.21) are nonlinear since they include product of continuous variables. We then linearize them by introducing new binary variables $\delta_{\mu^{\pm}}$, $\delta_{\alpha^{\pm}}$, $\delta_{\beta^{\pm}}$, and $\delta_{\gamma^{\pm}}$ which can be written as (4.23)−(4.27).

The equivalent single-stage mix-integer linearize expression of the original two-stage problem (4.4)−(4.27) can be modeled as following:

$$\begin{aligned}\max\ & P_{Kl}-\zeta\sum_{n\in\mathcal{L}}u_n\\ s.t.\quad & (4.4),(4.7)-(4.8),(4.14),(4.16)\\ & (4.10)-(4.12)\\ & (4.17),(4.22)\end{aligned}$$

$$\begin{cases} \mu^- - M \cdot \delta_{\mu^-} \leqslant 0 \\ \bar{H}_2 (\theta^* + c) + P_K^{\max} \leqslant M (1 - \delta_{\mu^-}) \\ \mu^+ - M \cdot \delta_{\mu^+} \leqslant 0 \\ -\bar{H}_2 (\theta^* + c) + P_K^{\max} \leqslant M (1 - \delta_{\mu^+}) \end{cases} \tag{4.23}$$

$$\begin{cases} \alpha^- - M \cdot \delta_{\alpha^-} \leqslant 0 \\ P_G^* - P_G^{\min} \leqslant M (1 - \delta_{\alpha^-}) \\ \alpha^+ - M \cdot \delta_{\alpha^+} \leqslant 0 \\ -P_G^* + P_G^{\max} \leqslant M (1 - \delta_{\alpha^+}) \end{cases} \tag{4.24}$$

$$\begin{cases} \beta^- - M \cdot \delta_{\beta^-} \leqslant 0 \\ P_K^* - \bar{H}_2 \theta^* + M_1 (1 - s) \leqslant M (1 - \delta_{\beta^-}) \\ \beta^+ - M \cdot \delta_{\beta^+} \leqslant 0 \\ -P_K^* + \bar{H}_2 \theta^* + M_1 (1 - s) \leqslant M (1 - \delta_{\beta^+}) \end{cases} \tag{4.25}$$

$$\begin{cases} \gamma^- - M \cdot \delta_{\gamma^-} \leqslant 0 \\ P_K^* + M_1 \cdot s \leqslant M (1 - \delta_{\gamma^-}) \\ \gamma^+ - M \cdot \delta_{\gamma^+} \leqslant 0 \\ -P_K^* + M_1 \cdot s \leqslant M (1 - \delta_{\gamma^+}) \end{cases} \tag{4.26}$$

$$\delta_{\mu^-}, \delta_{\mu^+}, \delta_{\alpha^-}, \delta_{\alpha^+}, \delta_{\beta^-}, \delta_{\beta^+}, \delta_{\gamma^-}, \delta_{\gamma^+} \in \{0, 1\} \tag{4.27}$$

where M is a large positive number. Particularly, M_1 and M are different values and $M_1 \ll M$.

4.2.2 Step 2: Determine Initial Attack Vector

For general topology attacks, the physical loads and cyber loads (denote as $\bar{P}_D$) satisfy the relationship in (4.28) and (4.29), respectively.

$$P_D = A_{GN} P_G - H_1 \theta, \tag{4.28}$$

$$\bar{P}_D = A_{GN} P_G - \bar{H}_1 (\theta + c). \tag{4.29}$$

Therefore, the load shift caused by general unobservable topology attacks can be calculated as

$$\triangle P_D = \bar{P}_D - P_D = H_1 \theta - \bar{H}_1 (\theta + c). \tag{4.30}$$

From equation (4.30), it is obvious that the load shift values are determined by both cyber attack vector and physical states values. Thus, the attack vector c determined in Step 1 is only unobservable when system voltage angel is θ^*. For system under different operation states, such attack vector cannot guarantee the load shifts resulting from attacks are within the load shift bounds. Therefore, an initial attack vector which can move the system from the operation states immediately after the physical attack to the worst states solved in the previous step should be determined. We use the following two-stage optimization problem to choose an initial attack vector within the minimum attack subgraph.

$$\min \sum_{n \in \mathcal{L}} u_n \tag{4.31}$$

$$\text{s.t.} \quad -\tau P_D \leqslant \bar{H}_1 \left(\theta_0 + c^0\right) - H_1 \theta_0 \leqslant \tau P_D \tag{4.32}$$

$$\begin{cases} c_n^0 \leqslant u_n \\ -c_n^0 \leqslant u_n \end{cases} \tag{4.33}$$

$$\{\theta^*, P_G^*\} = arg \left\{ \min_{\theta, P_G} \sum_{g=1}^{n_g} C_g (P_{Gg}) \right\} \tag{4.34}$$

$$\text{s.t. } A_{GN} P_G - \bar{H}_1 \theta = P_D + H_1 \theta_0 - \bar{H}_1 \left(\theta_0 + c^0\right) \ (\lambda) \tag{4.35}$$

$$-P_K^{\max} \leqslant \bar{H}_2 \theta \leqslant P_K^{\max} \quad (\mu^-, \mu^+) \tag{4.36}$$

$$P_G = P_{G1}^* \quad (\alpha) \tag{4.37}$$

where c^0 is $n_b \times 1$ initial attack vector; θ_0 is $n_b \times 1$ voltage angle vector immediately after physical attack; P^*_{G1} is $n_g \times 1$ optimal generation vector solved in step 1; α is $n_g \times 1$ dual variable vector of constraints (4.37). The objective (4.31) combining with constraints (4.33) is to minimize the l_1-norm of the attack vector. Constraint (4.31) represents load shift limitation. Constraints (4.34)$-$(4.37) represent the second stage DCOPF problem, which guarantee that the attack vector selected in the first stage can lead to the optimal dispatch P^*_{G1}. This problem can be converted to a single stage optimization problem by replacing the second stage problem to its KKT condition as well. The modification of second stage problem to its KKT condition is similar as stated in the first step.

4.3 Implementation

The worst attack strategy introduced in Section 4.2 determines the attack vector under DC measurement model. As stated in 4.1.2, such attack can be detected by AC SE. Thus, to implement an unobservable joint physical and cyber attack, attacker should construct an AC attack with the attack vector solved in the worst attack strategy.

The procedure of attack implementation is as follows:

1. Solve the two-step worst attack strategy problem as introduced in Section 4.2.

2. Determine the attack sub-graph $\mathcal{S}$. As stated in 4.1.2, $\mathcal{S}$ is determined by the switching attack line and center buses. Attackers can identify the center buses with cyber attack vector c, and then use center buses and the switching attack line to determine $\mathcal{S}$ within the sub-graph searching method stated in Subsection 4.1.2.

3. Observe the measurements inside $\mathcal{S}$.

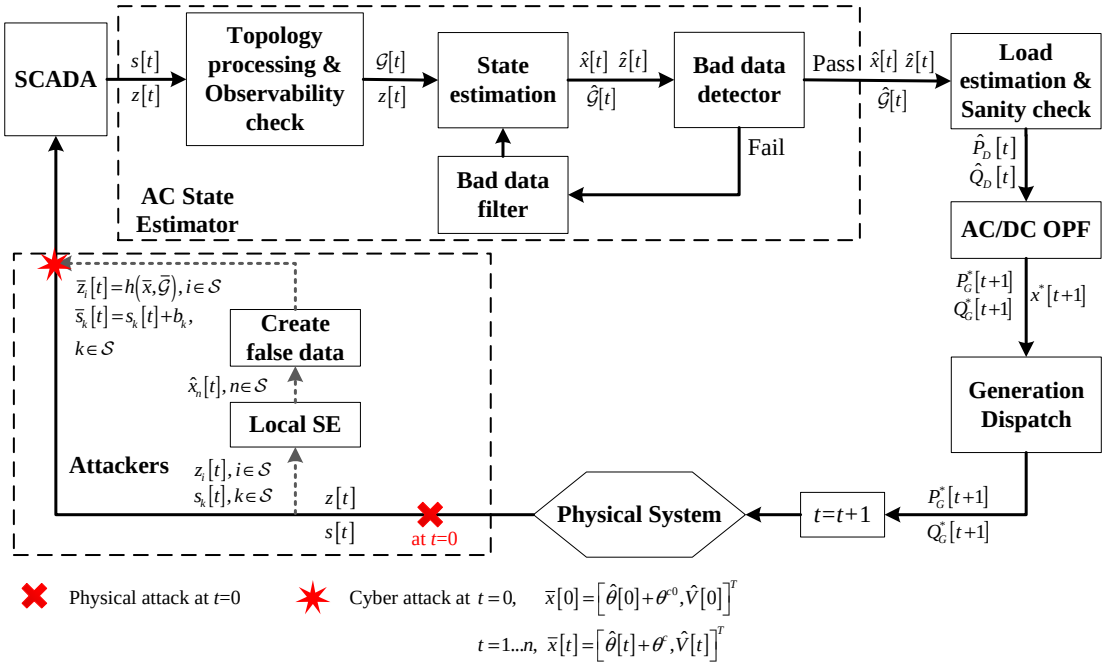


Figure 4.2: Temporal Nature of Real-time Power System Operation within Attack.

4. Launch the physical attack on the switching attack line and denote the corresponding operation loop as Event 0.

5. Launch the initial unobservable topology attack immediately after Event 0 as: 1) perform local SE inside $\mathcal{S}$; 2) calculate the modified measurements with the estimated states inside $\mathcal{S}$ and c^0 as (4.3); and 3) replace the measurements with the modified ones. Such an attack can mislead the system operation from the current states to the worst states.

6. Sustain the attack by injecting modified measurements computed with the estimated states and c in Event t, $t = 1...T$. T represents the operation loop when the target line is tripped by protection or the system configuration is changed.

The temporal nature of system operation within attack is shown in Figure 4.2.

4.4 Numerical Results

In this section, we test the behavior of attacks designed with the two-step worst attack strategy (in Section 4.2) and long-term consequences of such attacks in non-linear model. The test system is the IEEE 24-bus reliable test system (RTS). We assume the system is operating under optimal power flow and the loads of the system are constant during the simulation time period. To model realistic power systems, we assume that there are congestions prior to the attack and the attacker chooses one congested line as target to maximize power flow. We use MATPOWER to run AC power flow and AC OPF. The optimization problem is solved with CPLEX.

4.4.1 Solution for Worst Unobservable Topology Attack Designed with Two-step Attack Strategy

The solution of the worst unobservable topology attack determined by the two-step worst attack strategy is tested in this subsection. In order to understand the worst-case effect of attacks, we assume there was a line congested prior to the physical attack. This is achieved in simulation by reducing the line rating to 90% of the original power to create congestion. The attacker favors on the congested line and aims to maximize the power flow with limited l_1-norm of attack vector. We exhaustively test the 38 lines as power flow maximization targets in the system. We choose ζ to be 1% of the original power flow on the target line. Table 4.3 demonstrates the overall solutions with load shift bounds $\tau = 10\%$, $N_T = 1$, and the l_1-norm constraint $N_1 = 0.06$.

Table 4.3: Summary of Attack Cases for 38 Target Lines with $\tau = 10\%$, $N_T = 1$, and $N_1 = 0.06$.

Congested Line #	Outaged Line #	l_1- norm	Center Bus #	DC PF (%)	AC PF (%)
1	6	0.0267	2	75.23	99.60
2	6	0.0267	2	94.11	120.78
3	1	0.033	4	127.31	121.41
4	6	0.038	4	118.24	114.81
5	6	0.06	6	118.42	114.00
6	2	0.0093	2	132.52	123.57
7	24	0.0467	5	111.84	114.12
8	1	0.0328	3	129.66	127.88
9	2	0	0	19.71	99.96
10	1	0.0275	4	58.98	100.01
11	2	0	0	57.42	100.00
12	2	0.06	4	133.18	121.19
13	9	0.06	4	143.87	127.31
14	6	0.06	6	119.73	117.06
15	33	0.0573	10	109.00	108.62
16	38	0.0535	8	109.17	109.78
17	12	0.0308	3	101.25	102.06
18	35	0.06	8	114.14	114.33
19	38	0.06	8	114.59	109.50
20	6	0.031	3	107.22	106.28

continued on next page

continued from previous page					
Congested Line #	Outaged Line #	l_1- norm	Center Bus #	DC PF (%)	AC PF (%)
21	37	0.06	9	108.81	108.84
22	36	0.0046	3	109.70	109.92
23	38	0.0063	2	104.88	104.49
24	31	0.0085	2	168.38	166.54
25	26	0.0563	3	164.74	164.21
26	25	0.0563	3	164.74	164.21
27	24	0.0531	6	112.47	114.58
28	26	0.06	3	138.98	138.27
29	37	0.0157	3	130.25	128.06
30	31	0.0221	4	172.20	170.87
31	38	0.0029	2	211.12	213.57
32	31	0.0065	2	204.64	202.47
33	31	0.0065	2	204.64	202.47
34	35	0.0146	2	184.34	182.85
35	34	0.0146	2	184.34	182.85
36	37	0.06	6	197.82	196.61
37	36	0.06	6	197.82	196.61
38	31	0.0025	1	191.31	192.33

*PF: Power flow

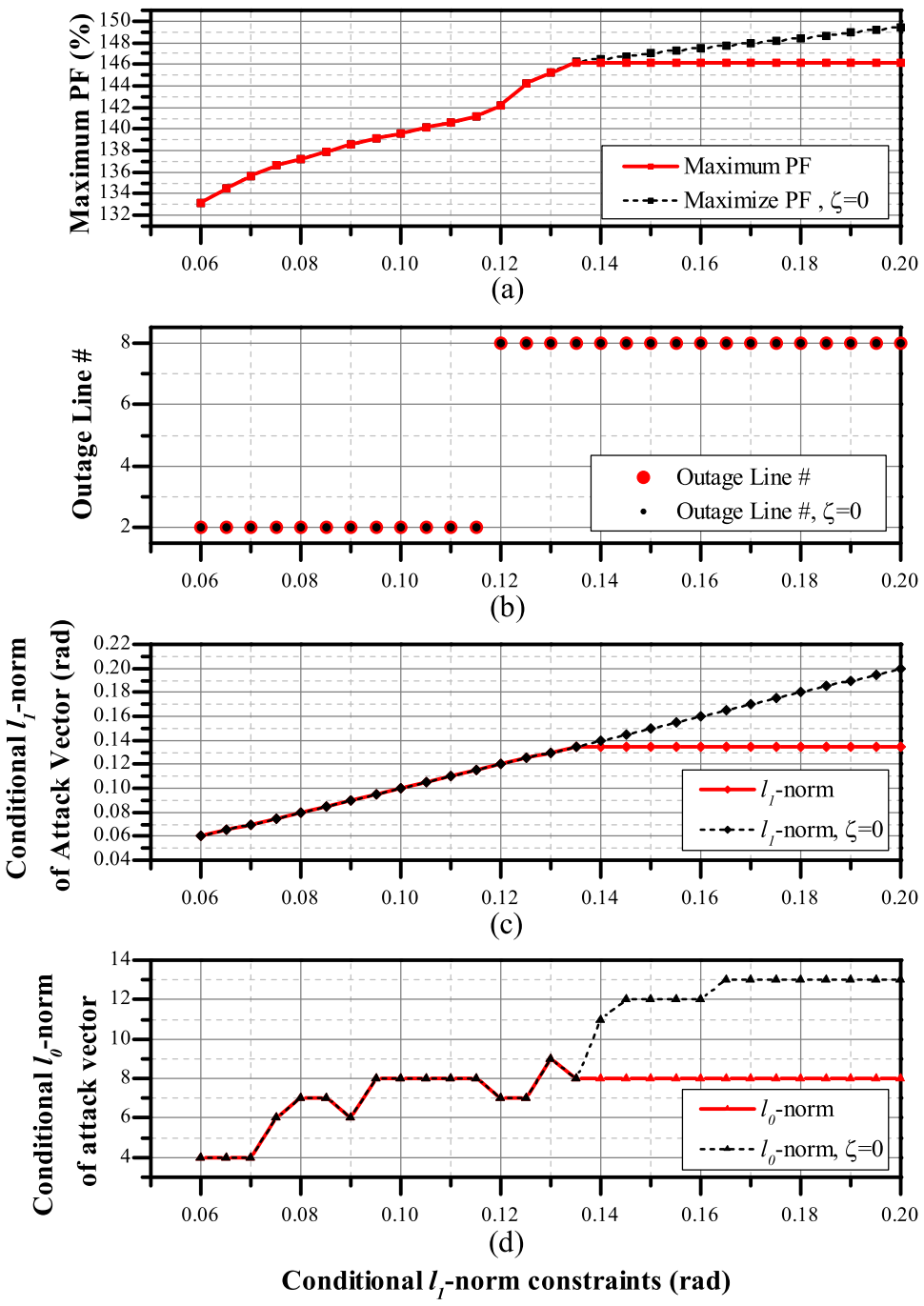
From Table4.3 we can observe that the attack vector determined by the two-stage optimization problem can lead to overflow in 31 target lines in linear model, which are 81.58% successful attacks. For all successful attack cases, when applying the attack

vector in non-linear model, the physical power flow (we denote it as AC PF in Table 4.3) in each line is comparable to the power flow solved in linear model (we denote it as DC PF in the table). For the 7 cases without DC overflow, the physical power flow on each line is larger than the computed DC power flow. This is caused by the losses and reactive power flow on the non-linear model. In particular, 2 cases with target lines #9 and #11, respectively, have no center buses, which are equivalent to the state-preserving attacks introduced in Chapter 3. For these cases, the maximum power flow on the target lines under the limited bounds for load shifts and l_1-norm of attack vector, the maximum power flows that can be obtained are equivalent to those resulting from state-preserving attacks. The constraint $N_1 = 0.06$ is a small l_1-norm constraint that corresponds to a sparse attack vector. Therefore, we can conclude that under limited attack resources, the worst unobservable state-and-topology cyber physical attacks determined by the proposed attack strategy can lead to overflow in most target lines. Thus, the test system is vulnerable to such attacks.

In Figures. 4.3 and 4.4, we illustrate the l_1-norm constraint on the maximum power flow, the physical outage line, and the l_0-norm and the l_1-norm of the attack vector for target line #12 and #13, respectively. In each sub-figure, we illustrate the two solutions: one with (red) ζ and one without ζ (black) in the objective function. In Figure 4.3(b), the switching attack line chosen for the target line #12 overlaps for cases with or without the objective that minimize l_1-norm of the attack vector. As the l_1-norm constraint increase, the switching attack line also change from line #2 to line #8. This illustrates that as the constraint for the sparse of attack vector relax, the outage line that can lead to higher overflow can be chosen. The large load shifts caused by the physical attack can be redistributed to more buses. From Figures. 4.3(a), (c), and (d), we can see that the two solutions overlap as the l_1-norm constraint increase from 0.06 to 0.135. However, as the l_1-norm constraint continues

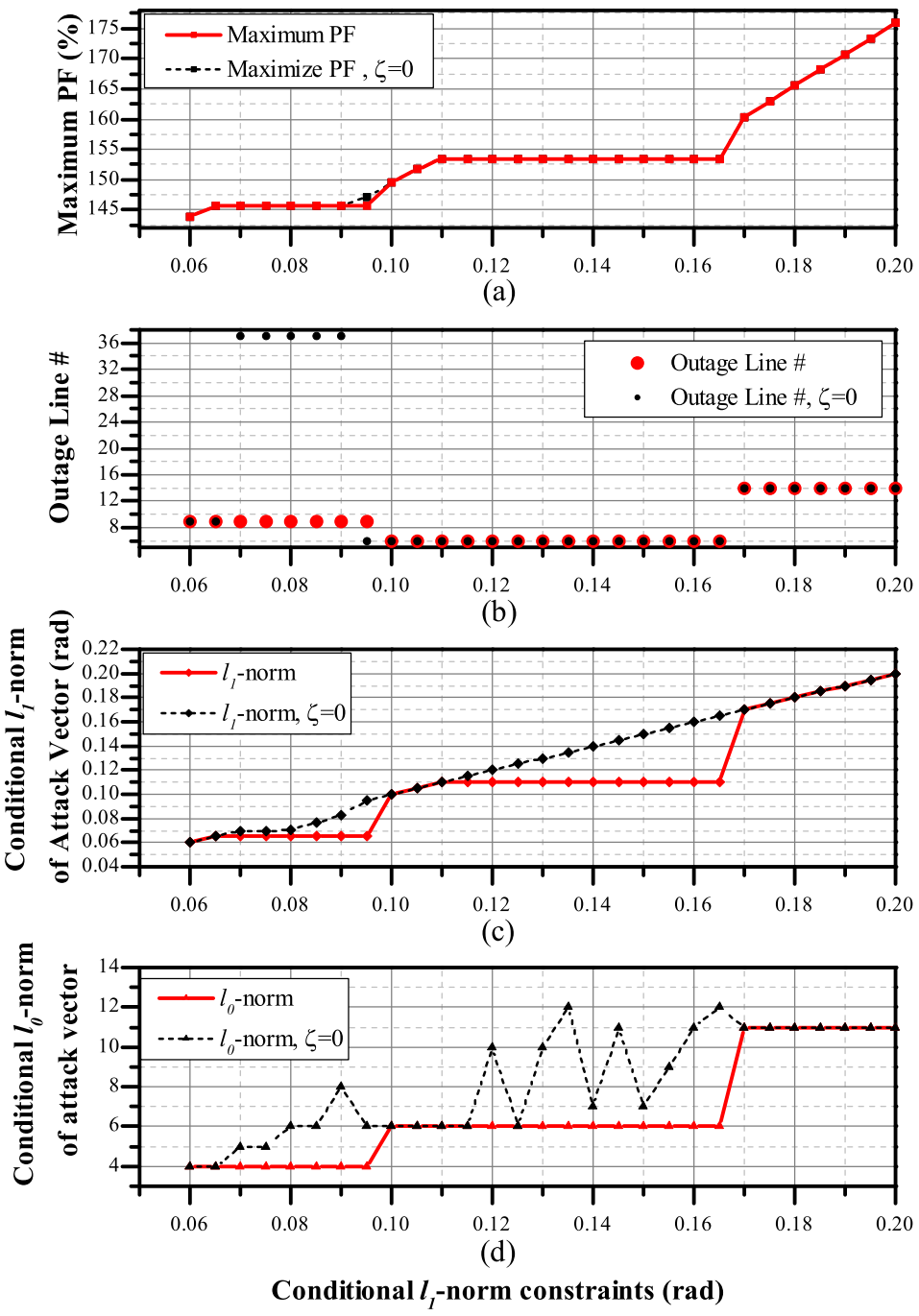
to increase, the maximum power flow for solution with ζ stop increasing while that for solution without ζ keep increasing. The variations for l_1-norm and l_0-norm of attack vector are the same, which shown in (c) and (d). This shows the trade-off between the conflict objective that maximize the target line power flow while minimize the l_1-norm of attack vector. In Figure 4.4, the second term objective also affects the chosen of switching attack line (see sub-figure (b)). The choices of switching attack line are different of the two classes of solution as the l_1-norm constraint ranges from 0.07 to 0.095. However, the maximum power flow on the target line doesn't change in this range. Sub-figure (c) and (d) show that the l_1-norm and l_0-norm of attack vector for solutions with ζ are smaller than those without ζ in this range. Such behavior shows that choice of switching attack line changes to obtain the solution that can lead to the same maximum power flow on the target line with a more sparse attack vector.

Another problem remains to be addressed is that whether the two steps of the worst attack strategy requires the same attack sub-graph. To this end, we exhaustively compare the attack sub-graphs chosen from the two steps and the corresponding load shifts for all the 38 attack scenarios under l_1-norm constraint that range from 0.06 to 0.3. We find that for all the test cases, the attack sub-graphs determined by the two steps and the load shifts resulting from the two steps are the same. As stated in Section 4.2, a specific load pattern corresponds to only one optimal dispatch plan, such results show that the initial attack vector can perfectly lead the system operation states to the worst operation states determined in Step 1.



(a) Maximum PF (b) The outage line number (c) l_1-norm of attack vector (d) l_0-norm of attack vector v.s. the conditional l_1-norm constraints.

Figure 4.3: Target Line #12 (Connecting Bus #8 - Bus #9) with $\tau = 10\%$.



(a) Maximum PF (b) The outage line number (c) l_1-norm of attack vector (d) l_0-norm of attack vector v.s. the conditional l_1-norm constraints.

Figure 4.4: Target Line #13 (Connecting Bus #8 - Bus #10) with $\tau = 10\%$.

4.4.2 *Case Study of the Long-term Impact of the Attack*

In this subsection, we select one typical case to demonstrate the long-term implication of the unobservable state-and-topology cyber-physical attack determined by the worst attack strategy. In this case, the target line is #12. The load shift bound is 10%, $N_T = 1$, and the l_1-norm constraint is 0.06. Under this condition, the switching attack line selected with the worst attack strategy is #2. The minimum sub-graph determined by the worst attack strategy is shown in Figure 4.5. In this figure, the attack sub-graph is demonstrated with red and blue where the red part is determined by the center buses #4, #7, #8, and #10, and the blue part is to complete the observable path for the switching attack line 2. The target line is represented with the thick red line while the switching attack line is with the blue dash-dot line.

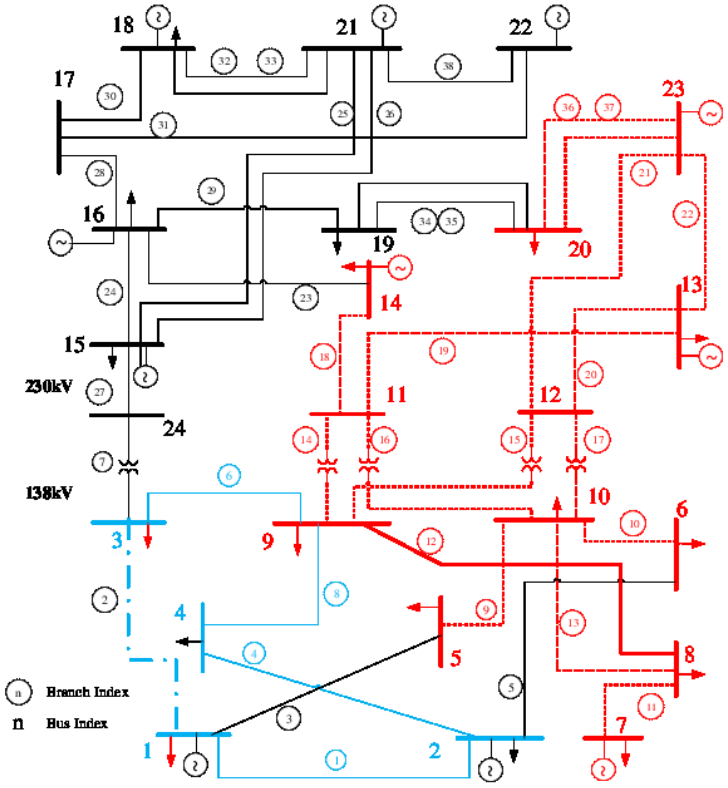


Figure 4.5: Sub-graph of Attack Case When Line #12 Congested and Line #2 Has A Physical Outage within Unobservable Topology Attack.

Figure 4.6 illustrates the cyber and physical power flow variation from Event 1 to Event 20. The active power variation for generators at bus #7 and #13 are shown in Figure 4.7 (the other generation remain unchanged). The load shift percentage caused by the attack is shown in Figure 4.8. At Event 0, a physical attack is launched on line #2. Attacker immediately perform local SE inside $\mathcal{S}$ and launch the initial unobservable topology attack calculated with c^0. In the following events, the attacker sustains the attack by modifying the power flow and power injection measurements within the attack vector calculated with c. Therefore, in the cyber layer, the power flow on line #12 is less than 100% while in physical layer, there is an overload existing. From Figure 4.6 and Figure 4.8, we can observe that once the active power generation dispatch at Event 1 is moved to the solution of Step 1, the physical overflow is maintained by injecting the same attack vector determined by Step 1. The heat accumulation may eventually cause this line to overheat and then trip offline.

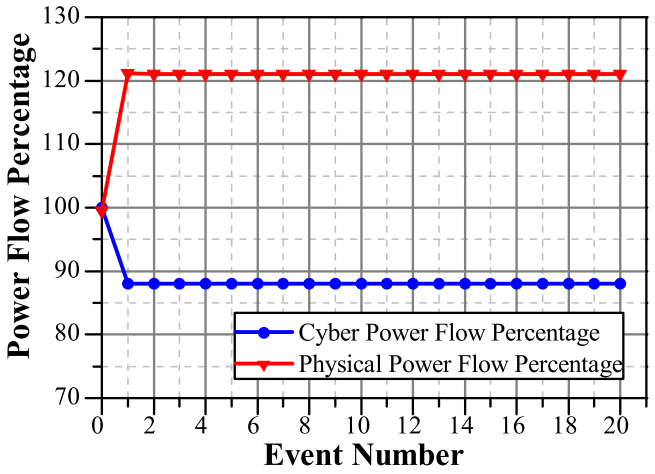


Figure 4.6: Power Flow on Line #12 When Line #2 Has A Physical Outage within Unobservable Topology Attack.

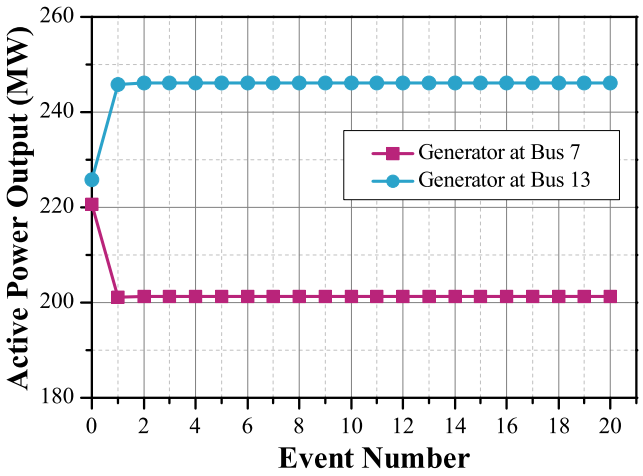


Figure 4.7: Active Power Output Variation When Line #2 Has Physical Outage and #12 Was Congested Prior to Unobservable Topology Attack.

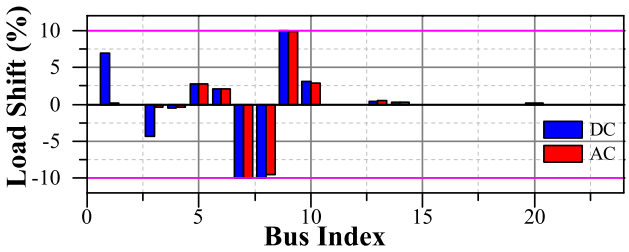


Figure 4.8: Load Shift Percentage for Each Bus of the Test System for the Case When Line #2 Has An Outage and Line #12 Was Prior Congested Within Unobservable Topology Attack.

In Figure 4.8, we can compare the load shift calculated by the optimization problem in linear model and the actual load shift in non-linear model. It is obvious that the load shifts determined by the optimization problem are all within the load shift threshold 10%. And when apply the attack vector in non-linear model, the load shifts caused by attack are also within 10%. For most buses with load shift, the non-linear (AC) load shift percentage is comparable to linear (DC) load shift percentage.

4.5 Concluding Remarks

In this chapter, we introduce a class of unobservable topology attacks in which both topology data and states for a sub-graph of the network are changed by an attacker. We proposed a two-step attack strategy to maximize the power flow on a specific line embedded with minimizing the set of measurements compromised by attackers. We have shown that the attack designed with the proposed two-step worst attack strategy can cause overload in the test system within the bound of the load shift in both linear and non-linear system models. The proportion of the successful attacks in non-linear system model is 81.58%, which shows the vulnerability of system to such attacks. In addition, we demonstrate the long-term consequences of such attacks and show that if such attacks are sustained, the overload problems can be maintained without being detected by the control center. Such overload problems can lead to the overheat of the target line, and hence, result in the outage of the target line. Thus, such attacks should draw the attention of control centers.

A potential countermeasure is to employ a more accurate historical data comparison for generation dispatch. The generation dispatch corresponding to the load patterns mimicking by attackers can also be different from the normal load shift patterns of such dispatch plan recorded in historical data. Once the anomalies are determined, operator can immediately send workers to measure the line flow in field to detect the overflow problem.

Chapter 5

TOPOLOGY-TARGETED MAN-IN-THE-MIDDLE COMMUNICATION ATTACKS

In this chapter, we focus on a class of topology-targeted man-in-the-middle (MitM) communication attacks aimed at limiting information sharing between adjacent areas, particularly when one or both areas experience topology changes (e.g., line outages). While wide-area monitoring and information sharing has been proposed by the Federal Energy Regulatory Commission based on observations that lack of seamless data sharing is an important factor in cascading failures, real-time data sharing in the grid is still done in an ad hoc manner between connected areas. For example, in the Northeast blackout of 2003 [1], [24], a line out in one area (Ohio) was not conveyed for a sufficient period of time to neighboring regions leading to convergence failure of the state estimator and other cascading problems. Furthermore, the mode, amount, and granularity of data shared is not standardized; for example, two connected areas may only share limited topology information such as low granularity network equivalent models which in turn are insufficient to capture the complexity of the electric grid and ensure wide-area reliability (e.g., the Yuma-Southern California outage of 2011 [25]). In fact, changes in the grid topology are often communicated via human operators and not in an automated manner which adds to communication delays and errors. In the light of such limitations, a smart adversary can limit information sharing in a number of ways. We seek to understand the effects of such limited data sharing scenarios (both adversarial and otherwise) on the electric power system real-time operations.

We introduce a class of distributed communication attacks wherein an attack on

the Energy Management System (EMS) of one area prevents the sharing of topology changing information with the other area (in automated systems where topology may be shared real-time or frequently, this can be achieved via man-in-the-middle attacks). We assume that the attacker is either involved in bringing down a line remotely (breakers can be remotely tripped in some cases) or is aware of a line out (again possible via presence of software trojans in the EMS). The attacker, therefore, is assumed to have some knowledge of the network topology.

In this chapter, we focus on a distributed two-area (managed by two operators and EMSs) setting to demonstrate the consequences of limited information sharing. Specifically, we focus on attacks that create or exploit outages in one area and limit information sharing via a communication attack thereby affecting the power flow solutions and dispatch in a connected area that has incorrect topology information. Specifically, we modeled the tie-lines connected the two areas under two conditions: (a) in normal operation, the tie-line interchange is fixed according to the day-ahead contract between areas, we simulate with only 10% variation on tie-line power flow interchange; and (b) under contingencies, the tie-line power flow can vary any values under the tie-line capacity, we then simulate with no tie-line interchange variation limitation. Our results demonstrate that such an attack in a distributed power network leads to a range of possibilities; these include actual physical line overloads that are not observable from the cyber measurements but can eventually cause line overheating and cascading outages; false overload alert in cyber layer while the physical system operates in normal condition; progressively severe lack of convergence of OPF in both areas; relatively benign oscillations in the power flow solutions between the two areas that eventually fix themselves; and line overloads in both physical can cyber layers. Our time progression based attack model allows us to capture the major computational components of EMSs including AC state estimation, optimal power

flow (OPF) including generation dispatch, and power flow calculation unit which adjusting dispatch mismatch between areas. Based on our observations, we also present countermeasures for such attacks.

5.1 System Model

We consider a two-area network model in which each area uses its measurements to evaluate the state of the system, compute the optimal power flow, and determine generation dispatch. It is worth noting that there are many control and actuation functions that operate at multiple timescales in the EMS and not all of them are captured by our model. Our choice of functions is driven by a specific time-scale that focuses on topology processing and state estimation, power flow computation, and generation dispatch. It is assumed that the computations are performed at a local control center as shown in Figure 5.1, and henceforth, when we refer to the two areas sharing information, it implies that information is exchanged between the control centers. We make the following assumptions about the information shared between the two areas.

5.1.1 Information Sharing Model

To illustrate the distributed effects of a communication attack, we assume that the two areas share as much information as relevant and based on current practices. The primary assumption is that each area performs its own computations with some data (depending on the computation block) obtained from the other side. Our assumptions are as follows:

- Static topology information: The static topology information is shared among all areas of the interconnected power system.
- Dynamic topology information: Each area is assumed to communicate the topol-

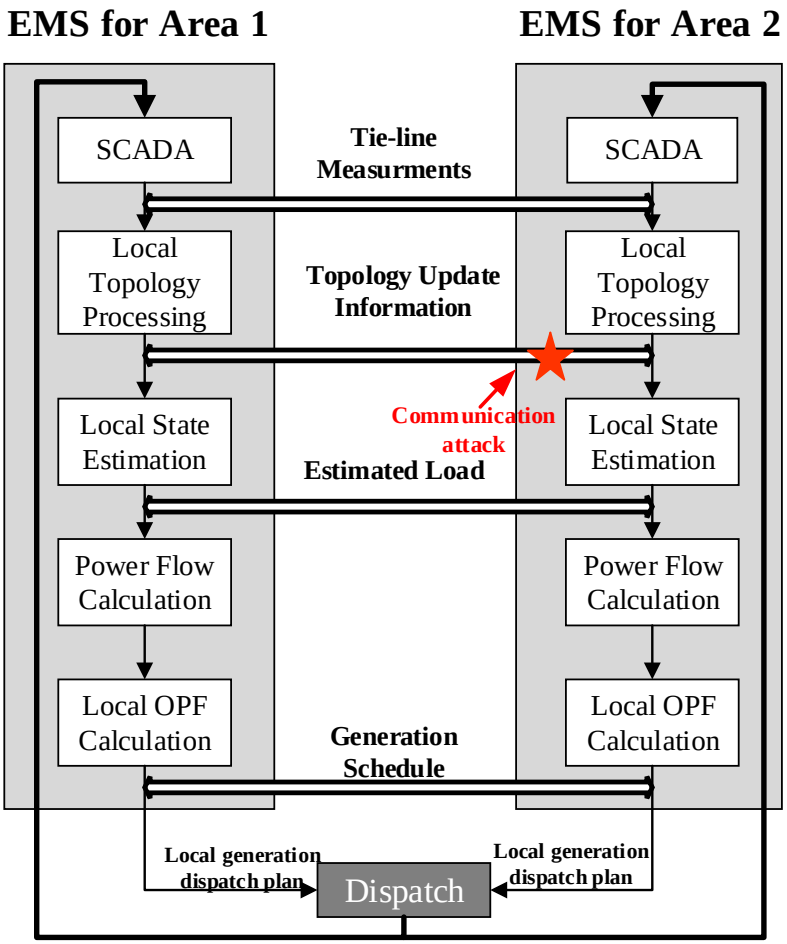


Figure 5.1: Computational Units and Data Interactions between the Two Areas of the Network.

ogy changing information among the whole system in real-time. Thus, once a topology error is found, the local operator should send this information to other areas immediately, which allows them to update the whole system topology information in time.

- Generation: The generation schedule of each unit is shared among areas in real-time.

- Measurements: The tie-line measurements are shared between adjacent areas

in real-time. In general, more measurements can be shared but we assume that each area does its own local state estimation (as is often the case in practice).

- Estimated load: The estimated load data is shared among areas in real-time.
- Network models for power flow: Each area computes its own AC OPF. In practice, each area uses a network equivalent model of its connected areas to simplify the OPF computation. However, since we seek to understand the effect of a communication cyber-attack on dispatch and power flows (line overloads often contribute to outages), we choose the best case network model, i.e., we assume each area uses the complete network model of the other side in computing its OPF. However, each area can only dispatch its own generators, and thus, computes the OPF while keeping the dispatch for the other area fixed according to the generation data sharing model.

5.1.2 Computational Models

We briefly outline the mathematical model for each of the computational units we consider here. The different computational units and their interactions across the two areas is illustrated in Figure 5.1.

State Estimation

Each area applies a weighted least-squares (WLS) AC state estimation as stated in Section 2.2 to calculate its system state (complex voltages) using the measurements from meters in its area as well as tie-line measurements.

Power Flow Calculation

Each area uses Newton's method to solve the power flow (PF) problem which involves solving for the set of voltages and flows in a network corresponding to the estimated loads and generation schedule obtained from OPF in previous time period. This unit is to adjust the overall load and generation mismatch caused by joint dispatch of two areas.

Optimal Power Flow

Assuming perfect network equivalent models (*i.e.*, complete sharing of neighboring network graphs for OPF), area i, $i = 1, 2$, runs its OPF with the dispatch for area j, fixed around values that were shared from the previous time period that area j ran its own OPF. The resulting OPF problem can be viewed as each area performing a centralized power flow problem but with the capability to only dispatch local units.

Let B and Br denote the set of buses and branches in the entire two-area network, and B_i and B_j denote the set of buses in area i, $i = 1, 2$, and area j, $j = 1, 2$, $j \neq i$, respectively. Futhermore, let G_n denotes the set of generators at bus n, $\{G_n\}_{n \in B_i}$ denotes the set of generators in area i, $i = 1, 2$. Let $c_g(\cdot)$ to denote the generation cost function for generator g. The OPF for each area can be formulated as the following optimization problem for area i, $i = 1, 2$:

$$\min \sum_{g \in \{G_n\}_{n \in B_i}} c_g(P_g) \tag{5.1}$$

$$s.t. \sum P_g + \sum_{\forall k(n,;)} P_k - \sum_{\forall k(;,n)} P_k = P_{dn}, \quad \forall n \in B, \tag{5.2}$$

$$\sum_{g \in G_n} Q_g + \sum_{\forall k(n,;)} Q_k - \sum_{\forall k(;,n)} Q_k = Q_{dn}, \quad \forall n \in B, \tag{5.3}$$

$$P_k = V_n^2(g_{sn} + g_{nm}) - V_n V_m(g_{nm} cos(\theta_n - \theta_m) \tag{5.4}$$

$$+b_{nm}sin(\theta_n - \theta_m)),\ k \in Br$$

$$Q_k = -V_n^2(b_{sn} + b_{nm}) - V_nV_m(g_{nm}sin(\theta_n - \theta_m) \tag{5.5}$$

$$-b_{nm}cos(\theta_n - \theta_m)),\ k \in Br$$

$$P_k^2 + Q_k^2 \leq (S_k^{max})^2 \quad \forall k \in Br \tag{5.6}$$

$$P_g^{min} \leq P_g \leq P_g^{max} \quad \forall g \in \{G_n\}_{n \in B_i} \tag{5.7}$$

$$Q_g^{min} \leq Q_g \leq Q_g^{max} \quad \forall g \in \{G_n\}_{n \in B_i} \tag{5.8}$$

$$V_n^{min} \leq V_n \leq V_n^{max} \quad x \in \{\theta, V\}, \forall n \in B \tag{5.9}$$

$$\hat{P}_g - \triangle\bar{P}_g \leqslant P_g \leqslant \hat{P}_g + \triangle\bar{P}_g \quad \forall g \in \{G_n\}_{n \in B_j} \tag{5.10}$$

$$\hat{Q}_g - \triangle\bar{Q}_g \leqslant Q_g \leqslant \hat{Q}_g + \triangle\bar{Q}_g \forall g \in \{G_n\}_{n \in B_j} \tag{5.11}$$

where $c_g(.)$ is the cost function for generator g, b_{nm} and g_{nm} are the susceptance and conductance, respectively, of line k from bus n to bus m, b_{sn} and g_{sn} are the shunt branch susceptance and conductance, respectively, of bus n, $k(n,;)$ is the set of lines k with bus n as its receiving bus, and $k(;,n)$ is the set of lines k with bus n as its sending bus, G_n is the set of generators at bus n, P_g is the active power output of generator g with maximum and minimum limit P_g^{max} and P_g^{min}, Q_g is the reactive power output of generator g with maximum and minimum limit Q_g^{max} and Q_g^{min}, $\hat{P}_{gj}$ and $\hat{Q}_{gj}$ are the fixed active and reactive power outputs with $\triangle\bar{P}_g$ and $\triangle\bar{Q}_g$ deviations of generator g in area j, respectively, P_k and Q_k are the active and reactive power flows, respectively, on line k with line capacity limit S_k^{max}, P_{dn} and Q_{dn} are the active and reactive power demands, respectively, at bus n, θ_n is the voltage angle for bus n, and V_n is the voltage magnitude for bus n with maximum and minimum limits V_n^{max} and V_n^{min}, respectively.

The objective in (5.1) is to minimize the total active power generation cost of the whole interconnected power system. Constraints (5.2) and (5.3) represent the

active and reactive power balance for each bus in the centralized system (two-area network). The constraints in (5.4) and (5.5) are the active and reactive transmission line power flow constraints for the whole system while (5.6) is the thermal limit for each transmission line. Constraints (5.7) and (5.8) are the local (for area i only) unit active and reactive power output limits while (5.9) defines the complex voltage stability limits for each bus in the whole system. Finally, (5.10) and (5.11) incorporate the unit active and reactive power output limits for area j, $j \neq i$, *i.e.*, the power output of generation units external to area i are fixed around the values shared by the other areas.

When no feasible solution (*i.e.*, a solution which satisfies (5.2)-(5.11)) can be found, the distributed OPF program fails to converge. In practice, to find a feasible solution, system operators often relax the constraints. In this report, the thermal limit constraint on the congested line is the first constraint to be relaxed. Multiple iterations of relaxing the line limits may be needed to obtain a feasible solution; to this end, we model the relaxed limits as follows:

$$P_k^2 + Q_k^2 \leq (S_k^{\max} + u\triangle\bar{S}_k)^2$$

where line k is the congested line, $\triangle\bar{S}_k$ is the incremental value by which the line limit is relaxed in each iteration, and $u \leqslant u_{\max}$ is the iteration number. In each iteration, the thermal limit is relaxed by increasing the rating of line k by, and the OPF program is executed to check whether it converges. This process is repeated until the OPF program converges or the relaxation time reaches its maximum value. Following this, other important lines (such as those with high reactive power flow) will be relaxed using the same procedure. If both methods fail to work, then we consider the test case as a not converge case.

5.2 Attacker Model

5.2.1 Time Progression Model of Attack

We assume that the attacker has access to the data being shared between areas and can corrupt the data. Examples abound of such data corruption attacks including the oft cited Stuxnet virus attack. The attacker is assumed to either participate in creating a line outage in one area or be aware of such an outage and then act to corrupt the topology information shared with the other area. Our attack model also captures simple human errors in information sharing between connected areas, including delays and mis-communications. In the interest of understanding worst-case attacks and data sharing limitations, the area with the outage is assumed to be aware of the outage shortly after. This assumption is based on frequently seen patterns of limited data sharing that precede (and are a cause of) large blackouts.

In order to understand the effect of such an attack, we study the time progression of the attack. We consider the following time-progression of the attack and system behavior includes the following steps:

1. Event 0: *Area i*: Outage occurs in Area i, $i = 1, 2$. Area i becomes aware of outage and updates its topology and shares with Area j. Area i then performs SE, PF, and OPF.

2. Event 0: *Attack*: Attacker replaces updated topology information shared with area j, $j \neq i, j = 1, 2$, with the previous static topology information.

3. Event 0: *Area j*: Area j uses measurements with updated topology (which has been changed by attacker) to compute SE, PF, and OPF.

4. Event 1: *System*: Area i and Area j jointly dispatch according to their own OPF results.

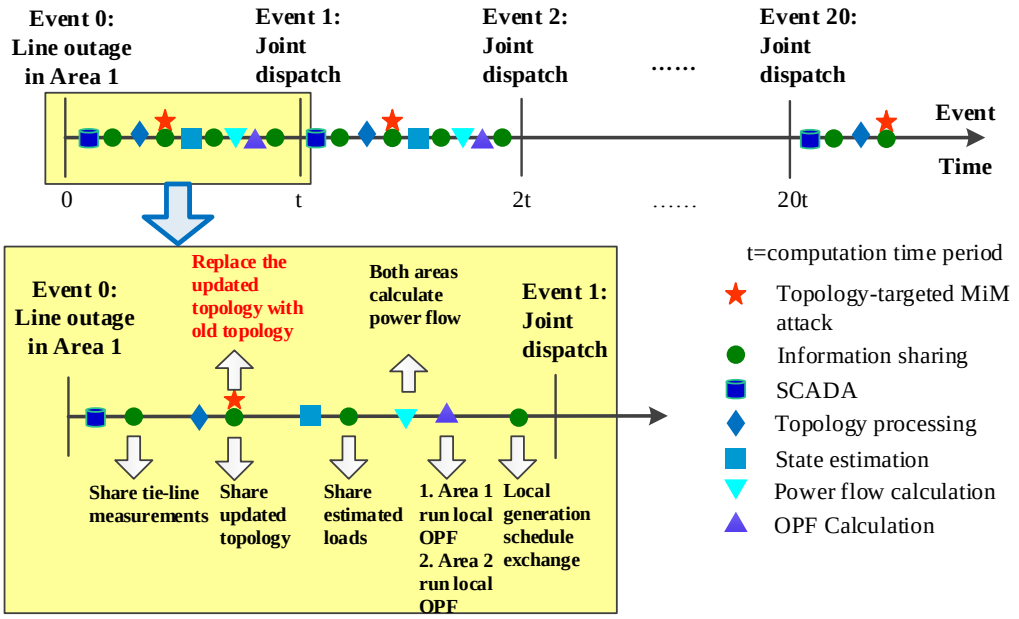


Figure 5.2: Time Sequence of Events at the Two Areas at the Time of and Following An Attack in One Area.

5. Event 1: *Area i*: Area i uses measurements with updated topology to compute SE, PF, and OPF. Shares dispatch status with Area j. Attacker sustains attack.

6. Event 1: *Area j*: Area j uses measurements with updated topology (which has been changed by attacker) to compute SE, PF, and OPF. Shares dispatch status with Area i.

7. Events repeat until alarms are set off either due to repeated lack of convergence or physical line overloads. All the while it is assumed that the attacker sustains the attack.

We illustrate this time sequence in Fig 5.2 for the case in which Area 1 experiences a line outage while Area 2 does not have the real-time topology information following the outage due to a communication attack.

5.2.2 *Tie-line Agreement Assumption*

In real-time operation, the tie-line interchange is fixed according to the day-ahead contract between areas. Therefore, under normal operation condition, the tie-line interchange should be fixed with only a small variation. However, under contingencies, the highest priority is to fix the violation. Therefore, the tie-line power flow can vary up to the tie-line capacity. In this chapter, we model the system under both normal and contingency conditions. We first assume the attack is launched under normal condition. Under this condition, there are interchange agreement values on the tie-lines that are generally smaller than the tie-line capacities. In this model, the tie-line interchange values are allowed to vary only 10% variation of the original interchange agreement values. We then model the system under contingency with tie-line interchange varying up to the tie-line capacity. The simulation results for both system models are demonstrated in Section 5.3.

5.3 Illustration of Results

In this section, we illustrate our distributed communication attack and its consequences. We consider an IEEE 24-bus reliable test system (RTS) and decompose it into two areas (henceforth referred to as Areas 1 and 2) as shown in Figure 5.3 (the dashed red line separates the two areas) such that Area 1 and Area 2 are connected by four tie lines. Each area is assumed to have its own local control center that performs local SE with local measurements and tie-line power flow measurements shared from adjacent areas, following which it shares its estimated load information with the other area. This is followed by a PF calculation unit to make up for the load and generation mismatch caused by joint dispatch and then an OPF re-dispatch keeping the generator outputs external of the other area fixed. This process alternates between

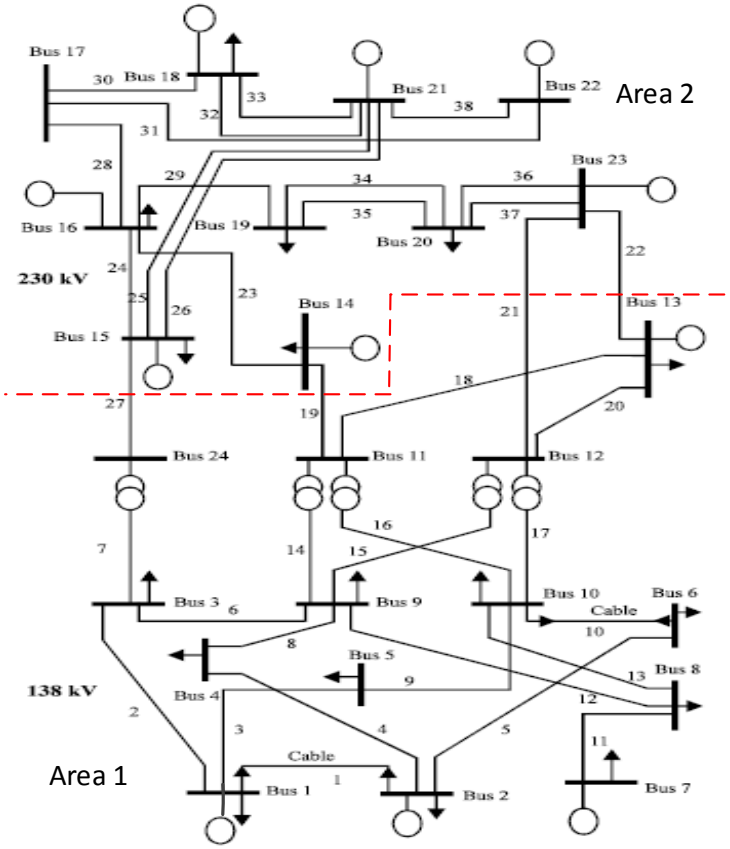


Figure 5.3: An IEEE RTS 24-bus Divided into Two Areas (Separated by Red Dashed Line).

the two areas every t time units (see Figure 5.2).

The attack is modeled as a line outage in one area (*e.g.*, line 6 in Area 1). In order to understand the worst-case effect of the attack, the area without knowledge of the outage is assumed to have a congested line prior to the attack. The attacker, aware of this outage in one area, compromises the topology changing communication signals such that the same static topology prior to the attack is shared. All possible choices of line outages in one area and congested lines in the other are considered exhaustively to demonstrate the effect of the possible attack cases. The system behavior is followed over $20t$ time units following the outage and over this time the two areas perform SE,

PF, OPF, and dispatch. The events sequence when Area 1 has an outage and Area 2 is affected by the communication attack is shown in Figure 5.2. The time immediately after topology changing is assumed as Event 0. The attacker launches a MitM attack to block the topology changing data sharing between Area 1 and Area 2 at Event 0 and sustains such an attack during the following events. Therefore, the two areas continue re-dispatching together in the simulation time period with one area (Area 1) using correct topology to obtain optimal dispatch plan while the other (Area 2) using false topology to do so.

In this chapter, we focus on worst-case attacks. We assume that the area without real-time topology information has some lines at capacity, *i.e.*, congested. This is achieved in simulation by reducing the line rating to 90% of the base case power flow to create congestion. We first model the system under tight tie-line agreement, in which only 10% variation on tie-line power flow interchange is allowed, then we model the system under contingencies, in which no tie-line interchange limit is modeled. To demonstrate our simulation, we first document our results in tables and then provide the detailed analysis and plots for both tie-line agreement cases.

Table 5.1: System Behavior with Sustained Attack for IEEE 24-bus System When Tie-line Interchange Is Fixed with 10% Variation.

Feasible Case	Physical PF Overload	Cyber PF Overload	Not Converge	No Violation Case	Cyber-Physical PF Overload
540	24.82%	14.26%	30.00%	23.33%	7.59%

*PF: Power flow

Table 5.1 shows the numbers in percentage of the five possible long term (20 or more events) outcomes of an attack after Event 0 with tie-line interchange fixed. These attack consequences are quantified by comparing the cyber power flow and

physical power flow in the area without the real-time topology (say Area 2) over the entire attack time duration. The cyber power flow is the OPF solution calculated by the control center in Area 2 with fixed external generation. The physical power flow, on the other hand, is the real power flow values of the system after dispatching with the most recent OPF dispatch solution with the true topology information. Therefore, for the area with false topology information, the cyber power flow values will be different from the physical power flow values. Five kinds of disparities are observed between the cyber and physical power flows following Event 0; we name them *physical PF Overload*, *cyber PF overload*, *Not converge*, *No violation case*, and *cyber-physical PF overload case*. We describe these disparities in detail below.

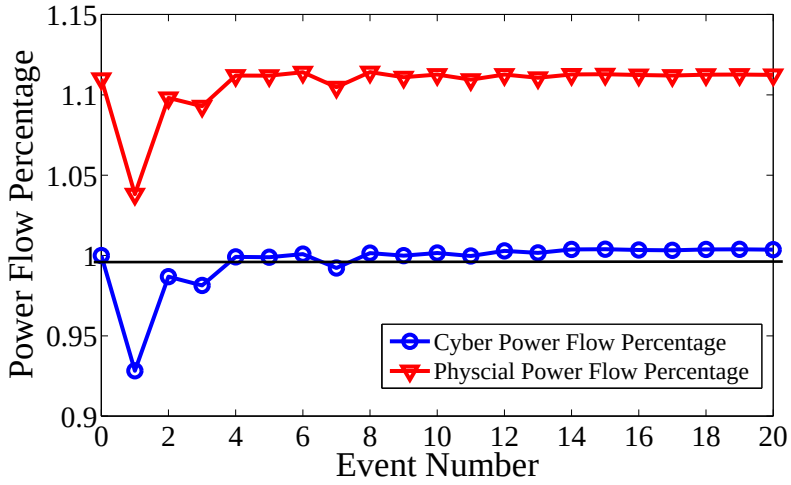


Figure 5.4: Physical PF Overload Case: Power Flow on Prior Congested Line #24 (area 2) When Line #3 (Area 1) Is Outaged.

Physical PF (power flow) Overload cases: For area with false topology in these cases, there is a mismatch between the cyber and physical power flows due to the false topology. Monitoring the cyber power flow cannot reflect the severity of the physical overload. The physical power flow on the previous congested line overloads during the simulation time period. However, such overload problem is not shown or attenuated in cyber layer. A typical physical PF overload case (Line 3 connecting

Bus 1 to Bus 5 is outaged with Line 24 connecting Bus 15 to Bus 16 congested) plot is shown in Figure 5.4. For these cases, the prior congested lines can get heated due to the dispatch of the area with false topology information. The heat accumulation may eventually cause the line to overheat and trip offline. Therefore, these cases can be viewed as *successful attack outcomes.*

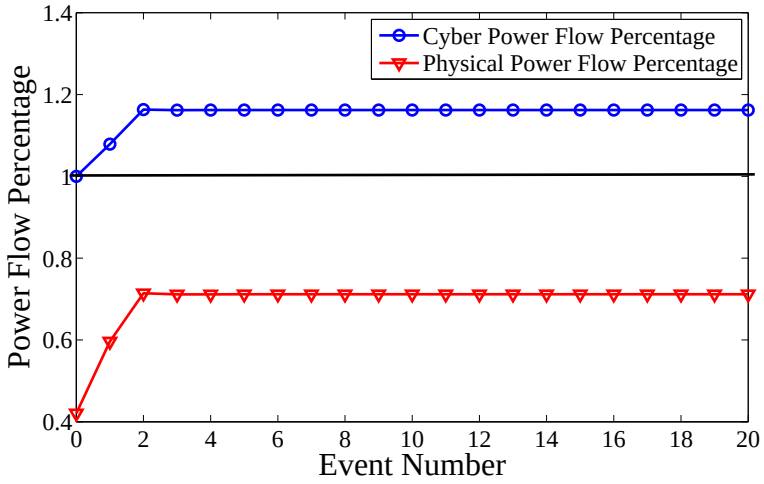


Figure 5.5: Cyber PF Overload Violation Case: Power Flow on Prior Congested Line #29 (Area 2) When Line #18 (Area 1) Is Outaged.

Cyber PF Overload cases: For area with false topology in these cases, the cyber power flow is shown as overload during the simulation time period while in the physical layer, there is no overload happened. A typical cyber PF overload case (Line 18 connecting Bus 11 to Bus 14 is outaged with Line 29 connecting Bus 16 to Bus 19 congested) plot is shown in Figure 5.5. For these cases, the incorrect cyber overload alert can lead to wrong contingency behaviors such as throttling up other nearby sources, load shedding, or even worse, tripping transmission line or generators. We hence, view such cases as *successful attack outcomes.*

Not Converge cases: In these cases, the physical power flow overload happens in the first few events but eventually the OPF program fails obtain a dispatch plan for one or both areas. This is because for a fixed power generation from one area,

there is no local dispatch plan that can satisfy all the constraints of the system even with thermal limit relaxation. In some cases, to clear the contingencies require more interchange between areas. Without the generator output changing jointly on both sides, the local center cannot find a feasible solution to solve the existing overload or stability problem. The worse operation states will continue until more serious consequences happened. Therefore, such cases can also be viewed as *successful attack outcomes*.

No violation case: For these cases, there is no overload immediately after Event 0 or a line overloaded after Event 0 can finally reduce below 100% of the rating in the simulation time period. Though the re-dispatch plan of the area with false topology still give a wrong calculation values of the system, no further problem caused by the wrong plan. We, therefore, view the attacks leading to such cases as *unsuccessful attacks*.

Cyber-physical PF Overload cases: In these cases, despite there are overloads in physical layer, there is no mismatch between the physical and cyber power flow. Therefore, the control center can be aware of the overload problems and fix such problems in time. This class of cases is then viewed as *unsuccessful attack outcomes*.

We observe a total of 373 successful attack cases, *i.e.*, 69.08% of the total attack cases. We define the subclass of successful attacks for which the power flow of 105% relative to the flow following Event 0 as *critical* (successful) attacks, and note that the total number of *critical* attacks for the RTS system is 60, which is 11.11% of the total attack cases. These results demonstrate the potential vulnerability of a topology-based communication attack.

The statisics results of the long term outcomes of an attack after Event 0 without tie-line interchange limit is demonstrated in Table 5.2. Under such tie-line interchange model, we also observe the five disparities which are *physical PF Overload*, *cyber PF*

Table 5.2: System Behavior with Sustained Attack for IEEE 24-bus System without Tie-line Interchange Limitation.

Feasible Case	Physical PF Overload	Cyber PF Overload	Not Converge	No Violation Case	Cyber-Physical PF Overload
540	35.74%	23.15%	6.11%	26.48%	8.52%

*PF: Power flow

overload, *Not converge*, *No violation case*, and *cyber-physical PF overload case* as introduced above. The proportion of successful attack cases is 65% of the total attack cases and that of the critical attack cases is 9.81% of the total attack cases. We can observe that with no tie-line interchange limitation, the number of not converge cases are largely reduced. However, such converged cases become physical PF overload cases or cyber overload cases. Hence, the proportion of the total successful attack cases are not changed too much.

Comparing the simulation results in Table 5.1 and Table 5.2, we can see that even under no tie-line interchange limitation, the MitM attacks can still lead to systematic problems and failures. Thus, the system is vulnerable to a topology-based communication attack under both tie-line interchange fixed condition and contingency condition. System operator should pay attention to such class of attacks.

5.4 Countermeasures and Concluding Remarks

In this chapter, we introduce a new class of distributed MitM attacks specifically targeting the topology sharing data between connected areas in the electric grid. We have demonstrated the time consequences of such attacks and have shown that such attacks can often lead to serious consequences if active intervention is not present. In this context, we observe that in addition to the traditional countermeasure of human

operator-based data sharing (which have been shown to be error-prone and delayed too), it is essential to have more resiliency via automated data sharing mechanisms. Our attack is successful because the two areas process data largely independently except for data sharing and do not employ sanity checks for data from the other side or a more interactive distributed processing platform. This could help both areas become aware of inconsistencies over faster time-scales including: (a) create and share a list of *external contingencies* caused to other areas by an internal component outage; (b) identify the anormalies of such attacks and enable machine learning in EMS to detect such attacks. It is worth noting that, while some of these mechanisms are being considered or even used currently in the grid, it is not done in a uniform manner and this work highlights the limitations of not doing so.

Chapter 6

CONCLUSIONS AND FUTURE WORK

6.1 Conclusions

In this thesis, three classes of cyber attacks that target on changing topology information at cyber layer are introduced. For each class of attacks, the attack model is proposed; the local information required to implement attacks is identified; the long-term consequences of attacks are demonstrated via IEEE 24-bus system. The major conclusions are drawn as follows:

- The implementation of unobservable state-preserving topology attacks, especially the line-maintaining attacks is studied in this thesis. An algorithm based on BFS is proposed to search for the minimum set of local information required to perform such attacks. The proposed algorithm can enable an attacker to obtain the localized topology and corresponding measurement data to mount an attack that bypasses bad data detector and successfully changes topology information of the system in the cyber layer. However, three categories of limitations of these attacks are identified including: (a) the choice of feasible switching attack lines is limited; (b) most of such attacks can lead to large load shifts in cyber layer, which can be detected by operators; and (c) the number of successful attacks that can lead to severe long-term violations is small. Therefore, countermeasures such as load monitoring, and checks on anomalous re-dispatches can be used to detect such attacks

- Since state-preserving topology attacks requires a large amount of load shifts that can be detected, thus, an intelligent attacker will naturally consider a new

class of attacks that involves changing both topology and states. Therefore, such attacks should be fully understood by system operators. To this end, a class of unobservable state-and-topology cyber-physical attacks is modeled and studied. A two-step worst-attack optimization problem is developed to study the long-term consequences of worst-case attacks. Attacks resulting from the optimization can maximize power flow on a specific line with limited access to only a set of topology and measurement data while masking the physical attack. Our observations include: (a) attacks designed with the worst attack strategy can cause overflow; (b) the load shifts resulting from such attacks are within setting bounds; and (c) If such attacks are sustained, the overflow on the target line can be maintained without being detected by the control center, thus, making the power system vulnerable to this attack class. System operators should pay more attention to such unobservable topology attacks. Two viable countermeasures are using valid historical data comparison to detect (i) anomalous load shifts in a subset of network, and (ii) anomalous generation dispatch.

- A class of topology-targeted man-in-the-middle communication attacks that that alter topology data shared during inter-EMS communication is studied in this thesis. We have demonstrated the time consequences of such attacks and have shown that such attacks can often lead to serious consequences if active intervention is not present. Countermeasures including anomalous tie-line interchange verification, anomalous re-dispatch alarms, and external contingency lists sharing are needed to thwart such attacks.

6.2 Future Work

To further study the implications of topology attacks on power system operation, the following work is suggested for the future.

For the unobservable state-and-topology cyber-physical attacks, the worst attack optimization problems can be formulated with subset of the network and the marginal units of the system. In fact, it is not realistic for attackers to know the whole network topology and the costs, capacity, and operation status of all generators in the system. Moreover, modeling a two-stage optimization problem for attacks in a large electric power system (*e.g.,* the PJM system which includes 15000 buses, 2800 generators and 20000 branches) requires a large set of variables and parameters; thus, it may be in the attacker's interest to design an local attack with significant local consequences as a first step. From the simulation results of Chapter 4, we can also observe that for most of the attacks, only a few set of marginal generators are influenced by attacks. Therefore, system operators should understand a class of relatively worse attack scenarios modeled in a localized network with only marginal generations. The consequences of such attacks should be fully studied as the first step to thwart such attacks.

We define the set of topology information that attacker can obtain as an *attack internal network* and the rest as the *attack external network*. The first step is to analyze the target line, figuring out the marginal units that can reduce or worsen congestion on this line. For marginal units inside the internal network, the node balance constraints and generation capacity constraints are unchanged at the second stage of the optimization problem (modeling DC OPF). The incremental output of each external marginal generator can be replaced by equivalent incremental power injections on all the boundary buses that can be computed with PTDF and the

total incremental output of the generator. Then for each boundary bus, the sum of power flows in the branches of the external network can be replaced with a pseudo-injection. The modification of the problem is illustrated in Figure 6.1. The modified second stage DC OPF for the worst attack with localized information is

$$\left\{\theta^{I*}, P_G^{I*}, \triangle P_G^{EM*}, P_K^{I*}\right\} = arg\left\{\min_{\theta, P_G, P_K} \sum_{g \in G_{in}}^{n_g} C_g\left(P_{Gg}^I\right) + \sum_{g \in G_{ex}}^{n_g} C_g\left(\triangle P_{Gg}^{EM}\right)\right\}$$

$$\text{s.t. } A_{GN}^I P_G^I - A_{KN}^I P_K^I = P_D^I \ (\lambda^I) \tag{6.1}$$

$$A_{GN}^B P_G^I - A_{KN}^B P_K^I = P_D^B + P_{Inj}^B + PTDF_B^{Mar} \cdot \triangle P_G^{EM} \quad (\lambda^B) \tag{6.2}$$

$$-P_K^{I\max} \leqslant \bar{H}^I{}_2\left(\theta^I + \theta^{Ic}\right) \leqslant P_K^{I\max} \quad (\mu^-, \mu^+) \tag{6.3}$$

$$P_G^{I\min} \leqslant P_G^I \leqslant P_G^{I\max} \quad (\alpha^-, \alpha^+) \tag{6.4}$$

$$P_K^I = \text{diag}\left(s^I\right) \cdot \bar{H}^I{}_2 \theta^I \tag{6.5}$$

where the superscript I denotes the set of internal elements (*e.g.,* bus, branch, and generator), the superscript B denotes the set of boundary buses, the superscript EM denotes the set of marginal generators in external network, $PTDF_B^{Mar}$ represent the PTDF matrix to which the from the buses where the marginal generators in the external network are connected to the boundary buses of the attack internal network, the variable P_{Inj}^B is the pseudo-injection vector for the boundary buses which equal to the sum of power flow injected into the boundary buses from the attack external network.

Another extension is to model the sequential line-switching attacks in the worst attack strategy. In this problem, attacker can determine multiple physical lines to trip in sequence with multiple-stage optimization problem. The objective of the attack can also be extended to multiple target lines in which the power flow are maximized. The system stability within such attacks should also be studied.

Finally, machine learning on system anomalies detection could further be applied

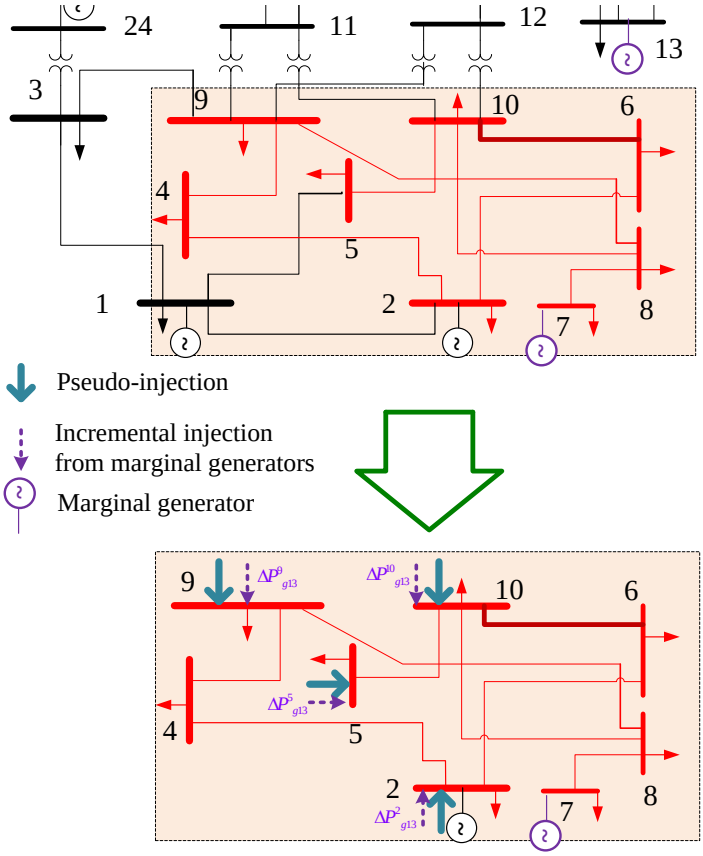


Figure 6.1: Illustration of Worst-case Attack Optimization within Local Network and Marginal Units.

to thwart the topology attacks on system operations.

REFERENCES

[1] "Federal Energy Regulatory Commission (FERC): Final report on the August 14th blackout in the United States and Canada: Causes and recommendations." http://www.ferc.gov/industries/electric/indus-act/reliability/blackout/ch1-3.pdf, April 2004. 1.2, 5

[2] M. Zeller, "Myth or reality - does the aurora vulnerability pose a risk to my generator?," in *64th Annual Conference for Protective Relay Engineers*, pp. 130–136, April 2011. 1.2

[3] "The stuxnet worm: A cyber-missile aimed at iran," tech. rep., The Economist, 24 September 2010. 1.2

[4] T. Espiner, "Siemens: Stuxnet infected 14 industrial plants." http://www.zdnet.com/article/siemens-stuxnet-infected-14-industrial-plants/, September 2010. 1.2

[5] S. Kelly, "Homeland security cites sharp rise in cyber attacks." http://security.blogs.cnn.com/2012/07/04/homeland-security-cites-sharp-rise-in-cyber-attacks/, July 2012. 1.2

[6] S. Toppa, "The national power grid is under almost continuous attack, report says." http://time.com/3757513/electricity-power-grid-attack-energy-security/, March 2015. 1.2

[7] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," in *Proceedings of the 16th ACM Conference on Computer and Communications Security*, CCS '09, (Chicago, Illinois, USA), pp. 21–32, 2009. 1.3

[8] A. T. H. Sandberg and K. H. Johansson, "On security indices for state estimators in power networks," in *1st workshop secure control system*, 2010. 1.3

[9] A. Teixeira, S. Amin, H. Sandberg, K. Johansson, and S. Sastry, "Cyber security analysis of state estimators in electric power systems," in *Decision and Control (CDC), 2010 49th IEEE Conference on*, pp. 5991–5998, Dec 2010. 1.3

[10] G. Dan and H. Sandberg, "Stealth attacks and protection schemes for state estimators in power systems," in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, pp. 214–219, Oct 2010. 1.3

[11] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "On malicious data attacks on power system state estimation," in *Universities Power Engineering Conference (UPEC), 2010 45th International*, pp. 1–6, 2010. 1.3

[12] G. Hug and J. A. Giampapa, "Vulnerability assessment of AC state estimation with respect to false data injection cyber-attacks," *IEEE Transactions on Smart Grid*, vol. 3, no. 3, pp. 1362–1370, 2012. 1.3, 3.2, 4.1.2

[13] J. Liang, O. Kosut, and L. Sankar, "Cyber-attacks on ac state estimation: Unobservability and physical consequences," in *IEEE PES General Meeting*, (Washington, DC), July 2014. 1.3, 3.2, 4.1.2

[14] L. Xie, Y. Mo, and B. Sinopoli, "Integrity data attacks in power market operations," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 659–666, 2011. 1.3

[15] J. Kim and L. Tong, "On topology attack of a smart grid," in *Innovative Smart Grid Technologies (ISGT), 2013 IEEE PES*, (Washington, DC), pp. 1–6, February 2013. 1.3, 1.4, 3, 3.1.1, 3.1.1, 4

[16] M. Rahman, E. Al-Shaer, and R. Kavasseri, "Impact analysis of topology poisoning attacks on economic operation of the smart power grid," in *Distributed Computing Systems (ICDCS), 2014 IEEE 34th International Conference on*, pp. 649–659, June 2014. 1.3

[17] A. Ashok and M. Govindarasu, "Cyber attacks on power system state estimation through topology errors," in *Power and Energy Society General Meeting, 2012 IEEE*, pp. 1–8, July 2012. 1.3, 1.4

[18] Y. Yuan, Z. Li, and K. Ren, "Modeling load redistribution attacks in power systems," *Smart Grid, IEEE Transactions on*, vol. 2, pp. 382–390, June 2011. 1.3, 4

[19] Y. Yuan, Z. Li, and K. Ren, "Quantitative analysis of load redistribution attacks in power systems," *Parallel and Distributed Systems, IEEE Transactions on*, vol. 23, pp. 1731–1738, Sept 2012. 1.3

[20] J. Liang, O. Kosut, and L. Sankar, "Consequences and vulnerability analysis of false data injection attack on power system state estimator," *to be submitted*, 2015. 1.3, 4

[21] A. Abur and A. G. Exposito, *Power System State Estimation: Theory and Implementation*. New York: CRC Press, 2004. 2.2

[22] S. Even, *Graph Algorithms (2nd ed)*. Cambridge University Press, 2011. 3

[23] W. Amador, S. Cossio, and A. Corredor, "Transmission, operation and congestion management in the colombian electricity market," in *Power Engineering Society General Meeting, 2004. IEEE*, pp. 1298–1300 Vol.2, June 2004. 4.1.1

[24] "Federal Energy Regulatory Commission (FERC): Mandatory reliability standards for interconnection reliability operating limits." http://www.ferc.gov/whats-new/comm-meet/2011/031711/E-8.pdf, March 2011. 5

[25] "Federal Energy Regulatory Commission (FERC) and the North American Reliability Corporation (NERC): Arizona-Southern California outages on September 8, 2011." http://www.nerc.com/files/AZOutage-Report-01MAY12.pdf, April 2012. 5