Liang, Gaoqi; Weller, Steven R.; Luo, Fengji; Zhao, Junhua & Dong, Zhao Yang. “Generalized FDIA-based cyber topology attack with application to the Australian electricity market trading mechanism” IEEE Transactions on Smart Grid, Vol. 9, Issue 4, p. 3820-3829 from: http://dx.doi.org/10.1109/TSG.2017.2677911

© 2018 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.

Accessed from: http://hdl.handle.net/1959.13/1409531
Generalized FDIA-Based Cyber Topology Attack with Application to the Australian Electricity Market Trading Mechanism

Gaoqi Liang, Student Member, IEEE, Steven R. Weller, Member, IEEE, Fengji Luo, Member, IEEE, Junhua Zhao, Member, IEEE, and Zhao Yang Dong, Fellow, IEEE

Abstract—This paper proposes a generalized false data injection attack (FDIA)-based cyber topology attack capable of disturbing conventional transactions in the electricity market. The proposed attack aims to mislead customers pay higher electricity bills in the wholesale market by making small, undetected price deviations during each attack interval over an extended period. In this paper, the Australian electricity market trading mechanism is considered, in which an extended attack over a single day is proposed, spanning totally 288 5-minute dispatch (attack) intervals. The proposed attack poses no security threat to the power system, affecting only the economic costs borne by customers. A defining feature of the proposed model is the joint consideration of both topology error processing and bad data detection constraints in order to ensure validity of the proposed attack. The rolling horizon optimization (RHO) technique is used to make appropriate adjustment to the attacker’s strategy considering the practical operating condition. A new metaheuristic optimization algorithm previously proposed by the authors, Natural Aggregation Algorithm (NAA), is used to find the corresponding attack strategies in this paper. Case studies on the IEEE-118 benchmark system are conducted to validate the proposed attack methodology.

Index Terms—Cyber-attacks, false data injection attack, cyber topology attack, Australian electricity market trading mechanism, rolling horizon optimization

This work is partially supported by a China Southern Power Grid research grant (WYK300000027), a Visiting Scholarship of State Key Laboratory of Power Transmission Equipment & System Security and New Technology (Chongqing University, China) (2007DAI0512716401), and a Shenzhen Municipal Science and Technology Innovation Committee International R&D project (GHZ2016030116572718).

G. Liang is with the Center for Intelligent Electricity Networks (CIEN), University of Newcastle, Callaghan, NSW, 2308, Australia (e-mail: gaoqi.liang@uon.edu.au).

S.R. Weller is with the School of Electrical Engineering and Computer Science, University of Newcastle, Callaghan, NSW, 2308, Australia (e-mail: steven.weller@newcastle.edu.au).

F. Luo is with the State Key Laboratory of Power Transmission Equipment & System Security and New Technology, Chongqing University, China, and also with the School of Civil Engineering, The University of Sydney, Sydney, NSW, 2006, Australia (e-mail: tracyluofengji@gmail.com).

J. Zhao is with Chinese University of Hong Kong (Shenzhen), Shenzhen, Guangdong, China (e-mail: junhua.zhao@outlook.com).

Z.Y. Dong is with the Electric Power Research Institute, CSG, Guangzhou, China, and also with the School of Electrical and Information Engineering, University of Sydney, Sydney, NSW, 2006, Australia (e-mail: joe.dong@sydney.edu.au).

NOMENCLATURE

Sets

\( N \) Set of all nodes.

\( G \) Set of all generators.

\( G_n \) Set of generators connected to node \( n \).

\( K_{i}^{n}, K_{n}^{i} \) Set of transmission lines to or from node \( n \).

\( \Phi^k \) Set of all binary variables on transmission lines of the \( k \)-th interval.

Indices

\( n \) Nodes.

\( g \) Generators.

Variables

\( \varphi_{ij}^k \) Binary variable for the \( k \)-th interval indicating whether the status of the transmission line from node \( i \) to node \( j \) is manipulated. (\( \varphi_{ij}^k = 0 \), OPEN; \( \varphi_{ij}^k = 1 \), CLOSED).

\( v_i^k, q_i^k \) Voltage magnitude and angle at node \( i \) in the \( k \)-th interval.

\( p_i^k, q_i^k \) Real and reactive generator output in the \( k \)-th interval.

\( \bar{p}_{ij}^{k-1} \) Measured generator output in \((k-1)\)-th interval.

\( p_j^k, q_j^k \) Real and reactive power flow from node \( i \) to node \( j \) in the \( k \)-th interval.

\( V_n^k \) Voltage at node \( n \) in the \( k \)-th interval.

\( \bar{p}_{ij}^k, \bar{q}_{ij}^k \) Real and reactive power flow that flows on the actual topology network in the \( k \)-th interval.

\( a_{k-1} \) Malicious injection data in the \( k \)-th interval.

Parameters

\( \Delta P_{ij}^\text{min}, \Delta P_{ij}^\text{max} \) Minimum and maximum generator ramping limits.

\( P_{ij}^\text{min}, P_{ij}^\text{max} \) Minimum and maximum real and reactive power flow limits.

\( Q_{ij}^\text{min}, Q_{ij}^\text{max} \) Minimum and maximum voltage limits.

\( V_{ij}^\text{min}, V_{ij}^\text{max} \) Forecasted real and reactive load on node \( n \) in the \( k \)-th interval.

\( V_{n}^\text{min}, V_{n}^\text{max} \) Real and imaginary parts of admittance matrix on element \( ij \) in the \( k \)-th interval.

\( g_{ij}, b_{ij} \) The maximum number of lines permitted to be open in the proposed attack formulation.
POWER SYSTEMS are critical societal infrastructures. Since the information and communication systems in modern power systems play an important role in stable and reliable operations, cyber security of modern power systems is of significant and growing interest [1], [2]. As a consequence of the tight integration of physical and information systems in modern power systems, an intelligent coordinated cyber-attack on a power system is potentially more efficient, stealthy and destructive than a localized physical attack. On 23 December 2015, multiple Ukrainian power substations experienced coordinated cyber-attacks. The electricity supplies of around 225,000 customers in the Ivano-Frankivsk region were cut off for several hours [4]–[6]. This event highlights the research on cyber security of modern power systems.

Research on cyber-attacks has to date principally focused on false data injection attacks (FDIAs), topology attacks, load redistribution attacks, data framing attacks, timing attacks, denial of service (DoS) attacks, replay attacks, and etc. Different cyber-attacks may emphasize and utilize different vulnerabilities of the power system with different attack objectives and strategies. In this paper, we propose a coordinated cyber-attack consisting of a joint FDIA and topology attack, hereafter referred to as a generalized FDIA-based cyber-attack. The proposed attack has a long-term latency plan, in units of 24 hours, with a view to stealthily making customers pay more for electricity purchased from the wholesale market.

The cyber-attack behavior posited in this paper could conceivably derive from one or more agents, including professional hacking groups, government-based espionage organizations, individuals with detailed power systems knowledge, and even from within the organization/s managing the power system. By hacking into a power system, destructive outcomes (e.g. disturbances and blackouts) can be achieved or economic benefits gained by adversaries. In this paper, the cyber-attack behavioral agent is assumed to have the motivation to disturb the electricity market trading transactions and thereby impose substantial economic losses on customers without being noticed by other parties. In the real-time wholesale market, records are maintained on the total amount of electricity in each transaction, either by retailers or other large customers who buy electricity from the market pool. The financial settlement follows the basic economic principle that \[ \text{Revenue (\$)} = \text{Price (\$/MWh)} \times \text{Amount (MWh)}. \]

Here the price refers to the settlement price, which depends strongly on the locational marginal price (LMP). Since the LMP is subject to regular fluctuation according to real-time economic dispatch, there is an opportunity for the attackers to stealthily introduce small deviations in the LMP in a way that disturbs market transactions.

Research relating to topology attacks has been extensive. Ashok et al. in [7] discussed the effect of intentional topology errors created on the state estimation function and showed that topology error could cause mistaken contingency analysis. Choi and Xie in [8] analyzed the impact of power transmission network topology errors on real-time LMPs. Deka et al. in [9] showed that a single breaker status change is sufficient to be undetectable. Kim and Tong in [10], [11] studied the impacts and countermeasures of FDIA against topology information on electricity markets and showed that secure phasor measurement units are capable to detecting topology attacks. In [12], [13] sequential topology attacks are proposed, aimed at causing cascading outages. In particular, the Q-learning based vulnerability analysis in [12] identified critical components in the potential sequential attack scheme. References [14]–[17] study the situation wherein a power line is first physically disconnected, followed by topology-preserving and FDIA to mask the physical attack.

FDIA is a newly proposed cyber-attack that may lead to incorrect state estimation results without being noticed by the control centre [18]. Liang et al. in [19] made a comprehensive review of state-of-the-art in FDIA against modern power system. Yu et al. [20] proposed a stealthy and blind attack without assuming knowledge of the Jacobian matrix or the distribution of state variables. Sun et al. in [21] showed that an attacker can exploit the local power system configuration to launch attacks that could bypass the existing techniques for false data detection. Hug et al. [22] studied the vulnerability assessment of FDIA based on the AC state estimation model. Yuan et al. [23], [24] showed that by attacking the security-constrained economic dispatch (SCED), the attacker is capable of affecting the system secure operation. Xie et al. [25] and Jia et al. [26] showed that by injecting false data into meters, the real-time LMPs can be manipulated, respectively.

Distinct from the existing literature, this paper proposes an attack strategy applied over an extended period, applied to the actual market trading mechanism employed in a real system (in this case, the Australian national electricity grid). This paper makes the following four key contributions:

1. The assumed cyber-attack behavioral agent has the motivation to disturb the electricity market trading transactions by stealthily introducing small deviations into calculated LMPs by launching a valid coordinated cyber-attack in the wholesale market without affecting the security;

2. Previous research on FDIA has focused on “one-shot” attacks, without considering the continuous cycle of sensor information gathering, state estimation, and economic dispatch. The attack proposed in this paper integrates the aforementioned elements, thereby exploiting the opportunities afforded by a “continuous attack” formulation;

3. In this paper, the proposed attack combines a generalized FDIA and cyber topology attack, and the rolling horizon optimization (RHO) technique [28] that rolling every 5 minutes is applied in a way to avoid detection by both topology error processing and bad data detection; and
(4) A latest metaheuristic algorithm, Natural Aggregation Algorithm (NAA) [29], is used to solve the proposed model.

This paper is organized as follows: Section II gives some basic theoretical backgrounds on FDIs and topology attacks; Section III provides a brief introduction to the Australian electricity market trading mechanism; Section IV introduces the proposed attack, models the optimization problem and proposes the solution method; Section V presents an experimental study using the IEEE-118 benchmark system; finally, conclusions are drawn in Section VI.

II. BACKGROUND

A. Assumptions and Preliminaries

This study is based on following assumptions:
1) The attacker has full knowledge of topology information, system parameters, bad data detection strategy, etc.; and
2) The attacker is capable of falsifying any digital and analog measurements from circuit breakers and meters.

These two assumptions are consistent with those in [7]-[27].

B. State Estimation and Its Cyber Security

State estimation is one of the vital components in the SCADA system of the energy management system (EMS), calculating the operational state of each bus from various meter measurements. The result of state estimation is used in higher layer applications, such as security assessment, security-constraint economic dispatch (SCED), contingency selection, etc.

The AC-based state estimation model is formulated as:

\[ z = h(x) + e \]

where the vector \( z = (z_1, z_2, ..., z_m)^T \) denotes the real-time measurement data which includes power injection measurements at buses and power flow measurements on transmission lines; the vector \( x = (x_1, x_2, ..., x_n)^T \) denotes the state system which includes the voltages and phase angles at buses; the vector \( e = (e_1, e_2, ..., e_n)^T \) denotes the measurement noise, here assumed to be Gaussian distributed [18]; \( m > n \); \( h(x) \) denotes the functional dependency between measurements and state variables. The precise form of \( h(x) \) is determined by the topology structure derived from the breaker/switch devices.

Model (1) is commonly solved by the weighted least squares method. In this method, the vector of estimated state variables \( \hat{x} \) is obtained by solving the following optimization problem:

\[ \min J(x) = \frac{1}{2} (z - h(x))^T W (z - h(x)) \]  

where \( W \) is a diagonal matrix represented as \( W = \text{diag}(\sigma_i^2, 0) \), where \( \sigma_i^2 \) is the variance of the measurement errors associated with the \( i \)-th meter (\( 1 \leq i \leq m \)).

The estimated state variable is calculated by solving (2) using an iterative algorithm. The validity (or otherwise) of \( \hat{x} \) is determined by the bad data detection which uses largest normalized residual (LNR) test and \( J(\hat{x}) \) performance index [18].

\[ J(\hat{x}) < C \]  

where \( J(\hat{x}) \) assumed to follow a chi-square distribution, with threshold \( C \) set to some pre-determined significance level.

Only when model (3) is satisfied can the estimated state variable \( \hat{x} \) be used in other applications. Otherwise, the state estimation needs to identify and remove the corresponding bad data until model (3) is satisfied.

Since the original resources processed by the state estimation come from both analog and digital measurements provided by meters and breaker/switch devices, any disruptive behaviour against meters and breakers/switch devices may cause a security issue for the power system. The FDIA and cyber topology attacks described below are specific attacks that influence the state estimation results by manipulating measurements of meters and breaker/switch devices.

C. False Data Injection Attacks

The FDIA, first proposed by Liu et al. [18], is a cyber-attack in which state estimation results are corrupted by injecting false data into meter measurements in a carefully coordinated fashion. A successful FDIA ensures that the state estimation residual falls below the hypothesis test threshold, despite the presence of malicious injection data.

Briefly, the attack stealthily manipulates the input of state estimation as \( z_{bad} = z + a \), in which \( a \) is the vector of malicious injection data. Therefore, model (1) is then formulated as:

\[ z_{bad} = h(x) + e \]

Based on the iterative algorithm, the estimated state variable \( \hat{x} \) would have a deviation, expressed as \( \hat{x}_{bad} = \hat{x} + c \). Provided the false estimated state variable \( \hat{x}_{bad} \) passes the bad data detection, it is a successful attack, satisfying

\[ J(\hat{x}_{bad}) < C \]

The attacker should solve model (4) and satisfy test (5) to launch this attack. The key to this problem is finding a valid vector of \( a \), and many methods can achieve this.

In the situation that an attack satisfies test (5), if the attacker can simultaneously satisfy \( J(\hat{x}_{bad}) = J(\hat{x}) \), such an attack is called an FDIA; otherwise, it is called a generalized FDIA. The former one is typically based on the DC model, whilst the latter one is often based on the AC model. In this paper, we consider the AC model for the state estimation, an assumption with greater relevance to practical grid operation.

D. Cyber Topology Attacks

The network topology processor is one of the important components in the SCADA system of the EMS, producing the topology state by obtaining the connectivity status within the network from various switching devices [31], [32]. Usually, the switching devices refer to circuit breakers, which are used to connect (or disconnect) a power system component to (resp., from) the rest of the network [33]. The result of network topology processing therefore form the foundation of all EMS functions. In particular, the aforementioned form of \( h(x) \) in model (1) is determined by network topology processing.
The topology graph can be represented as,

\[ G = (V, E) \]

where \( V \) and \( E \) represent the set of buses and connected transmission lines, respectively [34]. The topology graph therefore encodes binary (0,1)-valued information, where ‘1’ indicates that the circuit breaker is CLOSED, and ‘0’ indicates that the circuit breaker is OPEN.

Cyber topology attacks against power systems usually manipulate the topology estimate and evade detection by topology error processing. Topology error processing is also a component in EMS, checking for consistency between digital and analog data. Traditionally, topology errors are categorized into two classes: transmission line inclusion/exclusion error; and bus split/merging error [8]. In this paper, we only focus on the transmission line inclusion/exclusion error.

By fully utilizing the correlation between digital and analog measurements, the attacker can make a successful topology attack without being noticed. The typical strategy for the attacker is: when a transmission line is perturbed from CLOSED status to OPEN status, the corresponding meter measurements on the line, desired by the attacker, should set to be 0; when a transmission line status is perturbed from OPEN status to CLOSED status, the corresponding meter measurements on the line should set to be a nonzero value.

It should be noted that it is only the physically deployed transmission line and its circuit breaker that matters. For example, if node \( i \) and node \( j \) are not physically connected, it is unreasonable for the attacker to manipulate its status to CLOSED. In this paper we therefore assume that all physically deployed transmission lines are included in the network used as the base case, i.e., we only focus on cases where transmission line status is manipulated from CLOSED to OPEN.

III. AUSTRALIAN ELECTRICITY MARKET TRADING MECHANISM

The two largest electricity networks in Australia are the National Electricity Market (NEM) and the South-West Interconnected System (SWIS) [35]. The market operator for the NEM is the Australian Energy Market Operator (AEMO), responsible for generator dispatch, forecasting demand, reliability management and financial settlements [36].

The framework of the Australian electricity market is shown in Fig. 1. In the spot market, generators offer to supply the market with specific amounts of electricity at particular prices. Offers are submitted every five minutes. From the submitted generator bids, AEMO balances the supply and demand every five minutes by performing SCED, and in so doing determining the generator dispatch plan and spot price. The generator dispatch plan shows which generators are required to produce electricity, at what time. The spot price is the feedback to the bids reflecting the settlement price that paid to generators. The generator settlement price for a 30-minute interval is the average of six spot prices during a half-hour period.

Electricity selling can be transacted through wholesale market. Bilateral contracts are also permitted between electricity generators and large customers, with the balance setting the wholesale market price. All electricity sold at the wholesale level is merchandised through the pool [36]. Retailers and large customers buy electricity at settlement prices from the market pool. In this paper, we consider LMP as the dispatch price for the wholesale market, which is the by-product of the every five minutes SCED, and reflects the settlement price used for settlement purposes. The wholesale market settlement price for a 30-minute interval is the average of six dispatch prices during the half-hour period.

In the retail market, retailers make selling plans, and customers choose their suppliers and pay for the electricity bills.

In this paper we focus on the wholesale market, which is composed of 48 trading intervals and 288 dispatch intervals per day, as shown in Fig. 2. In the Australian electricity market, each trading day starts at 4:00 am, and each trading interval consists of six dispatch intervals. Each trading interval, representing the settlement slot, is a half-hour period; and each dispatch interval, representing the real-time economic dispatch slot, is a 5-minute period.

Based on the Australian electricity market trading mechanism, the settlement price in the wholesale market is different from the real-time dispatch price. The settlement price for all 30-minute trading intervals each day is the average of the six dispatch prices during the preceding half-hour [35]. For example, in the \( J \)-th trading interval, the settlement price \( \bar{L}_J \) is formulated as:

\[ \bar{L}_J = \frac{1}{6} \sum_{k=1}^{6} l_{k}^J \]  

where \( l_{k}^J \) represents the \( k \)-th dispatch price, \( k = 1, 2, ..., 6 \).

All market customers are required to install equipment, mainly smart-meters, to record their electricity consumption [35]. Information from smart-meters is recorded every half-hour.
and forwarded to AEMO for use in calculating and preparing accounts for financial settlement. Therefore, the settlement account for the buyers buying electricity from market pool during a day is formulated as:

\[ f = \sum_{j=1}^{48} (\bar{L}_j \times D_j) \]  

(8)

where \( D_j \) represents the total consumption of electricity during the \( J \)-th trading interval, and \( f \) represents the transaction for a one-day period.

IV. GENERALIZED FDIA-BASED CYBER TOPOLOGY ATTACK

A. Overview of the Proposed Attack

Real-time monitoring is typically done through remote terminal units (RTUs) within the SCADA system. Both digital and analog measurements are polled once every 2 to 10 seconds from RTUs in every substation [37], [38]. These measurements then travel through a wide-area communication system to the control center and stored in a real-time database waiting to be processed [39]. Network topology processing, topology error processing, state estimation, and bad data detection modules calculate and identify state variables and topology state based on these network measurements.

State estimation run-time intervals in the control center are typically in the range 90 seconds to 5 minutes, with intervals varying between independent system operators (ISOs) [7]. In this paper, we consider the 5-minute interval adopted by the Australia ISO as the state estimation run-time. Since there are 288 intervals of both state estimation and SCED during a single day, an attacker may choose any interval as his/her attack target. Given a specific targeted interval, an attacker is required to manipulate digital and analog measurements for 5 minutes until these altered data are used by the state estimation module and economic dispatch.

Fig. 3. SCED Sequence

Neighboring dispatch intervals have interconnections with each other, as shown in Fig. 3. Suppose in the \( J \)-th trading interval, the \( k \)-th dispatch interval is the current dispatch interval, and the \((k-1)\)-th interval is the previous one. Before launching the \( k \)-th SCED, the system should estimate the network connections and the corresponding operating conditions at the end of the \((k-1)\)-th interval. Therefore, the topology attack strategy implemented on the current interval should take full consideration of the operating condition of the previous one; otherwise the attack might be an invalid one.

In this paper, the proposed generalized FDIA-based cyber topology attack has a long-term latency plan, in units of 24 hours, with the purpose of making customers pay more for electricity purchased from the wholesale market. Since it is a long-term latency plan, the proposed attack should be intelligent enough to evade detection and avoid creating security issues for the power system. Huge economic losses are caused via accumulation over an extended sequence of small attacks, each introducing a slight price deviation, rather than a single large attack in which an obvious price deviation risks detection.

In this paper, we take 24 hours (including 288 prospective 5-minute attack times) to illustrate the cumulative influence of slight price deviation across the proposed attack. Based on the Australian electricity market settlement mechanism, the formulation and solving approach are introduced as follows.

B. Formulation of the Proposed Attack

The proposed generalized FDIA-based cyber topology attack has the objective of maximizing the transaction during 24 hour period, shown as,

\[ \max f = \sum_{j=1}^{48} \left( \frac{1}{6} \sum_{k=1}^{6} l_{ij}^j \times D_j \right) \]  

(9)

When launching the attack, the solving of SCED process and some practical constraints must also be taken into account as follows.

1) SCED Process

In our formulation, each transmission line is assigned a binary variable, \( \phi_{ij}^k \), represents whether or not the line from node \( i \) to node \( j \) is manipulated so as to be included in the network during the \( k \)-th interval. Thus \( \phi_{ij}^k = 1 \) denotes that the breaker status on the line is not manipulated; whereas \( \phi_{ij}^k = 0 \) denotes that the breaker status on the line is manipulated from CLOSED to OPEN. Denote by \( \Phi^i = [\phi_{ij}^k, \phi_{ji}^k, \ldots, \phi_{ij}^2] \) the vector of CLOSED or OPEN statuses of all lines, in which \( T \) is the number of physically deployed transmission lines and where for compactness of notation, \( \phi_{ij}^t, t \in [1,2,...,T] \) denotes the status of the \( t \)-th transmission line, assumed to connect nodes \( i \) and \( j \).

As shown in Eq. (9), the settlement price is calculated from six consecutive dispatch prices. For each dispatch price, the term \( l_{ij}^j \) is the by-product of the corresponding SCED process, as follows:

\[ \min \sum_G c(P_g^k) \]  

s.t. \[ P_g^k = \hat{P}_g^{k-1} + \Delta P_g \]  

(10)

(11)

\[ \Delta P_{g_{\min}}^k < \Delta P_g < \Delta P_{g_{\max}}^k \]  

\[ P_{g_{\min}}^k < P_{g_{\max}}^k \]  

(12)

(13)

\[ O_{ij_{\min}}^k < O_{ij}^k < O_{ij_{\max}}^k \]  

\[ V_{in_{\min}}^k < V_{in}^k < V_{in_{\max}}^k, n \in N \]  

(14)

(15)

\[ \sum_{(i,j) \in k \cup k_{\max}} P_{ij}^k - \sum_{(i,j) \in k \cup k_{\max}} P_{ij}^k + \sum_{g \in G} P_g^k = P_{\text{net}}^k, n \in N \]  

(16)
\[
\sum_{i \in \mathbb{K}^k} Q_{ij}^k - \sum_{i \in \mathbb{K}^k} Q_{ij}^k + \sum_{g \in \mathbb{G}} Q_g^k = Q_{d,a}^k, \quad n \in N \tag{17}
\]
\[
P_{ij}^k = \varphi_y^k \times [-v_i^k v_j^k (g_{ij}^k \cos \theta_{ij}^k + b_{ij}^k \sin \theta_{ij}^k) + g_{ij}^k v_i^k v_j^k] \tag{18}
\]
\[
Q_{ij}^k = \varphi_y^k \times [v_i^k v_j^k (b_{ij}^k \cos \theta_{ij}^k - g_{ij}^k \sin \theta_{ij}^k) + b_{ij}^k v_i^k v_j^k] \tag{19}
\]
\[
\sum_{(i,j) \in \mathbb{K}} (1 - \varphi_y^k) \leq S \tag{20}
\]

where (10) aims to minimize the total generation cost, \(c(\cdot)\) is the generator cost function; Eq. (11) ensures that the generator output in the \(k\)-th interval is an increment of the measured generator output in the \((k-1)\)-th interval; Eq. (12) is the generator ramping limit; Eq. (13), (14) and (15) represent the power flow and voltage limits; Power balance at each node is enforced by Eq. (16) and (17); Power flow on each transmission line is represented by Eq. (18) and (19) with the binary variable \(\varphi_y^k\); \(\theta_{ij}^k = \theta_{ij}^{k-1} - \theta_{ij}^k\); Eq. (20) limits the total number of manipulated transmission lines to at most \(S\).

2) Power Flow Feasibility Constraints

It should be noticed that the cyber topology attack only focuses on the information manipulation and does not physically falsify the status of breakers. Consequently, the aforementioned generator dispatch plan based on the false topology information will be applied on the actual topology network. The actual power flow might probably be out of limits. Since the purpose of the proposed attack is to focus on economic benefits by remaining concealed for extended periods of time, it is important that security issues are not created by this attack.

The actual power flows are calculated from the following power flow equations with full topology and the corresponding generator dispatch:

\[
\sum_{(i,j) \in \mathbb{K}} P_{ij}^k - \sum_{(i,j) \in \mathbb{K}} P_{ij}^k + \sum_{g \in \mathbb{G}} P_g^k = P_{d,a}^k, \quad n \in N \tag{21}
\]
\[
\sum_{(i,j) \in \mathbb{K}} Q_{ij}^k - \sum_{(i,j) \in \mathbb{K}} Q_{ij}^k + \sum_{g \in \mathbb{G}} Q_g^k = Q_{d,a}^k, \quad n \in N \tag{22}
\]
\[
P_{ij}^k = v_i^k v_j^k (g_{ij}^k \cos \theta_{ij}^k + b_{ij}^k \sin \theta_{ij}^k) + g_{ij}^k v_i^k v_j^k + \sum_{(k,j) \in \mathbb{K}} (1 - \varphi_y^k) \leq S \tag{23}
\]
\[
Q_{ij}^k = v_i^k v_j^k (b_{ij}^k \cos \theta_{ij}^k - g_{ij}^k \sin \theta_{ij}^k) + b_{ij}^k v_i^k v_j^k + \sum_{(k,j) \in \mathbb{K}} (1 - \varphi_y^k) \leq S \tag{24}
\]

where \(P_{ij}^k\) is the result of the aforementioned SCED model; \(\overline{P}_{ij}^k\) and \(\overline{Q}_{ij}^k\) are real and reactive power flows. Then, the actual power flows must satisfy:

\[
P_{ij}^{\text{min}} < \overline{P}_{ij}^k < P_{ij}^{\text{max}} \tag{25}
\]
\[
Q_{ij}^{\text{min}} < \overline{Q}_{ij}^k < Q_{ij}^{\text{max}} \tag{26}
\]

3) Manipulation Feasibility Constraints

In the formulation, if the breaker status of a line is manipulated to be OPEN, the corresponding meter measurements on the line should also be manipulated to be zero, because there is no power flow on an OPEN line. It should be noticed that zero the meter measurements on an OPEN line are not sufficient, since the remaining measurements could exceed the bad data detection threshold. Therefore, in order to ensure consistency between the digital and analog data, and also avoid being detected by the bad data detection, the attacker needs to calculate the corresponding malicious injection data by launching a generalized FDIA with a pre-determined \(\Phi^k\), where \(\Phi^k\) is one of the results from the SCED process.

As shown in Fig. 3, the operation of the \(k\)-th SCED process is based on the \((k-1)\)-th state estimation outputs. In order to launch a valid topology attack of the \(k\)-th SCED process, the corresponding malicious data should be injected into the meter measurement of the \((k-1)\)-th interval.

Denote \(z_{k-1} = [(zP)_j^{k-1}, (zQ)_j^{k-1}, (zP)_k^{k-1}, (zQ)_k^{k-1}]\) as the vector of analog measurements in the \((k-1)\)-th interval, where \((zP)_j^{k-1}\) and \((zQ)_j^{k-1}\) are the real and reactive power flow measurement from node \(i\) to node \(j\); \((zP)_k^{k-1}\) and \((zQ)_k^{k-1}\) are the real and reactive power injection value on node \(n\) in the \((k-1)\)-th interval. Let \(a_{k-1} = [(aP)_j^{k-1}, (aQ)_j^{k-1}, (aP)_k^{k-1}, (aQ)_k^{k-1}]\) be the denoted vector of injected analog measurements in the \((k-1)\)-th interval, where \((aP)_j^{k-1}\) and \((aQ)_j^{k-1}\) are the injected real and reactive power flow measurement from node \(i\) to node \(j\); \((aP)_k^{k-1}\) and \((aQ)_k^{k-1}\) are the injected real and reactive power injection value at node \(n\) during the \((k-1)\)-th interval. Overall, the generalized FDIA with cyber topology attack of the \(k\)-th interval is formulated as follows:

\[
\min \quad J(a_{k-1}, \varphi_{y}^k, v_{ij}^k, v_{ij}^k) \tag{27}
\]
\[
(aP)_j^{k-1} = \begin{cases} -zP_j^{k-1}, & \text{if } \varphi_{y}^k = 0 \\ r_1, & \text{otherwise} \end{cases} \tag{28}
\]
\[
(aQ)_j^{k-1} = \begin{cases} -zQ_j^{k-1}, & \text{if } \varphi_{y}^k = 0 \\ r_2, & \text{otherwise} \end{cases} \tag{29}
\]
Fig. 5. Representation of rolling optimization process

\[ s.t. \quad a_{k-1}^{\min} \leq a_{k-1} \leq a_{k-1}^{\max} \]

\[ z_{\text{tol}}^{-1} = [\phi_k^{-1} + (zP_k)^{-1} + (aP_k)^{-1}, \phi_k^{-1} + (zQ_k)^{-1} + (aQ_k)^{-1}] \]

\[ + ([zP_k^{\min} + (aP_k)^{-1}, [zQ_k^{\min} + (aQ_k)^{-1})]^T \]

where \( J(a_{k-1}, \theta_k^{\pm}, v_k^{\pm}, v_j^{\pm}) \) in Eq. (27) is consistent with \( J(\bar{x}) \) in Eq. (5), and the achieved minimum is required to fall below the threshold. Eq. (30) constrains the vector of injected values \( a_{k-1} \), where the lower and upper bounds \( a_{k-1}^{\min} \) and \( a_{k-1}^{\max} \), respectively, are interpreted component-wise. Eq. (28)-(29) indicate that if the line status is manipulated to be OPEN, the injection data should be taken as the negative of the original measurement so as to ensure that no data appears on an OPEN line. If the line status is not manipulated in this way, the corresponding injection values must nonetheless ensure that Eq. (30) is satisfied, i.e. that scalar values \( r_j \) and \( r_k \) in Eq. (28)-(29) are chosen in such a way that the corresponding term in \( a_{k-1} \), lies strictly between the lower and upper limits in the vectors \( a_{k-1}^{\min} \) and \( a_{k-1}^{\max} \), respectively. By solving the above problem, the attacker obtains the malicious injection data for launching the attack during the k-th interval.

C. Solving Approach

1) Flow Chart For Each Dispatch Interval

In order to launch successful proposed attacks during a 24 hour period, each 5-minute dispatch interval should follow the aforementioned formulation. Fig. 4 shows the flow chart of the solving sequence of the k-th dispatch interval.

2) Rolling Horizon Optimization Framework

Since the real-time measurement-based SCED process repeats 288 times in a day, and neighboring dispatch intervals have interconnections with each other, a real-time rolling solution process is employed. Considering that the settlement price in the Australian electricity market trading mechanism is the average of six dispatch intervals, it contributes more to the objective, expressed in Eq. (9), if the attacker chooses six continuous dispatch intervals as the rolling time window with a 24-hour horizon.

The rolling horizon process used in this paper is depicted in Fig. 5. The time displayed in each block in Fig. 5 represents the start time of that interval. During each time window, a sub-optimization problem is solved with the objective of physically measured. In order to solve the sub-optimization problem in the current time window, the attacker needs to estimate the analog measurement of the k-th, \((k+1)\)-th, \((k+2)\)-th, \((k+3)\)-th, and \((k+4)\)-th interval. In this paper, the corresponding estimated measurement is gained by adding a deviation to the power flow calculated from Eq. (21)-Eq. (24). By solving the sub-optimization problem in the current time window, the attacker implements the attacking strategy in the k-th interval and then restarts the next time window. By solving the sub-optimization problem repeatedly on a rolling (receding) horizon, the attacker can promptly make adjustments to his/her attack strategy according to the practical operating condition.

The rolling attack proceeds until the final 30-minute period of a day, when the time window is progressively shortened (e.g. five intervals for the final 25 minutes, etc.), until finally a single window is used for the final 5-minute period.

3) Natural Aggregation Algorithm

The formulated attack problem is a combinatorial optimization over multiple time intervals. Over each dispatch interval, there are both continuous- and binary-valued decision variables. In this paper, we use a new metaheuristic algorithm recently proposed by the authors, Natural Aggregation Algorithm (NAA) [29] [30], to solve the attack problem.

NAA mimics the self-aggregation intelligence of group-living animals, essentially distributing the whole population into multiple sub-populations through a stochastic migration model. The core of NAA is the stochastic migration model which makes individuals migrate among sub-populations. After making migration decisions, each individual placed in a certain sub-population performs a located search, while each individual not included in any sub-population performs a generalized search. For a range of challenging, high-dimensional multi-modal optimization problems, NAA has been shown to exhibit very strong global search capability and fast convergence, typically outperforming the state-of-the-art differential evolution algorithm [40]. Further details on NAA can be found in [30].
V. CASE STUDY

The proposed model is tested on the IEEE-118 bus system, which contains 118 buses and 186 branches. In this case study, the maximum number of lines for which the status is permitted to be tampered from CLOSED to OPEN is two, i.e., $S = 2$. The maximum power flow on branches is set to be 350 MW. The generator ramping rate is set to be 5MW/minute. Suppose the network is fully measured, with 118 meters (one per bus) and $186 \times 2$ meters (one at each end of each branch) hence a total of 490 sensors. The threshold is set to be $C = 295.689\ (\alpha = 0.025$, the degree of freedom is $490 - 118 \times 2 = 254$). Suppose the predicted load matches the actual one. Table I gives the NAA parameter settings.

![Fig. 6. Cyber Topology Attack Plan for Dispatch Intervals](image)

(a) Cyber removed lines for dispatch intervals from the 1st to the 6th; (b) Cyber removed lines for 288 dispatch intervals.

![Fig. 7. Dispatch Prices on Bus 18, 38, 58 and 78 of 24 Hours Period](image)

![Fig. 8. Dispatch Prices on all Buses of the 50th, 100th, 150th, and 200th Dispatch Interval](image)

![Fig. 9. Transaction Deviation of 48 Settlement Intervals](image)

### Table II

<table>
<thead>
<tr>
<th>Dispatch Interval</th>
<th>33th</th>
<th>53th</th>
<th>143th</th>
<th>213th</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAA Cyber Topology Attack Plan</td>
<td>[3,74]</td>
<td>[91,116]</td>
<td>[23,171]</td>
<td>[2,118]</td>
</tr>
<tr>
<td>Deviation ($)</td>
<td>36.09</td>
<td>114.02</td>
<td>109.91</td>
<td>170.67</td>
</tr>
<tr>
<td>$\eta$ (%)</td>
<td>56.60</td>
<td>47.92</td>
<td>71.97</td>
<td>97.01</td>
</tr>
<tr>
<td>Ave_time (Second)</td>
<td>22.31</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DE Cyber Topology Attack Plan</td>
<td>[86,152]</td>
<td>[64,120]</td>
<td>[71,140]</td>
<td>[138,171]</td>
</tr>
<tr>
<td>Deviation ($)</td>
<td>18.90</td>
<td>22.07</td>
<td>87.90</td>
<td>61.11</td>
</tr>
<tr>
<td>$\eta$ (%)</td>
<td>38.72</td>
<td>34.78</td>
<td>97.48</td>
<td>85.54</td>
</tr>
<tr>
<td>Ave_time (Second)</td>
<td>36.72</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

By implementing the cyber topology attack plan showed in Fig. 6 (b), slight deviations are introduced into the dispatch prices for each bus. The large number of buses (118) in this case study precludes an exhaustive illustration of the price deviations for each bus. We therefore select at random 4 buses (bus 18, 38, 58 and 78) as representatives. As shown in Fig. 7, each dispatch price dispatch price during an attack deviates only slightly in comparison to the non-attacked case. In this case study, the
deviation for all buses’ dispatch prices over a 24-hour period have a range of [-2.24, 6.59] $/MVA-hr.

Similarly, since there are 288 dispatch intervals a day, it is not possible to display the dispatch price comparison for all intervals. We therefore randomly choose 4 intervals (interval 50, 100, 150 and 200) as representatives, shown in Fig. 8. It can be seen that by launching the proposed attack, different dispatch interval has different dispatch price deviations on all buses.

Based on the Australian electricity market trading mechanism, there are 48 settlement prices a day. Before and after the attack, the transaction deviation for each trading interval is shown in Fig. 9. In summary, totally $98,272 economic losses are incurred in this case study by launching the proposed attack over a single 24-hour period.

B. Algorithm Comparison

The Differential Evolution (DE) algorithm [40] has been widely accepted by many researchers as it has much stronger global search capability than many other heuristic algorithms. In order to show the effectiveness of using NAA in this paper, we make comparison studies of using NAA and DE algorithm. The parameters of NAA are shown in Table I; the parameters of DE are set as follows: $F = 0.5$; $C_r = 0.1$; population size = 20; and iteration time = 20. Similarly as before, it is not possible to display 288 dispatch intervals. We therefore randomly choose 4 dispatch intervals (interval 33, 53, 143 and 213) as representatives to illustrate the NAA/DE algorithm comparison, shown in Table II.

In the cyber topology attack plans shown in Table II, pairs {· · ·} denote the labels of cyber-removed lines obtained using the NAA and DE algorithms. The deviation ($) is the sum of the economic losses at all buses over the corresponding dispatch interval under the corresponding cyber-topology attack plan. The value $\eta$ is the solution of Eq. (27) divided by the threshold $C$, i.e., $\eta = J(\alpha_k, \theta_y, v_x, \nu_x) / C$, expressed as a percentage, where $\eta < 100\%$ denotes that the corresponding cyber topology attack is under the threshold. Finally, the average time (in seconds) required to solve the program over a single dispatch interval is denoted by $Ave_{\text{time}}$.

Fig. 10 displays the malicious injection data when the current dispatch interval is the 33th, 53th, 143th and 213th, respectively, using both NAA and DE algorithms. Note that since there are in total 490 sensors, only the meter deployed at the “from side” of transmission lines are shown as representatives in Fig. 10.

The overall economic loss over a 24-hour period is $98,272 and $79,023 when using NAA and DE algorithms, respectively. It can be clearly seen that with the same population size and iteration time, NAA exhibits much stronger global search capability than DE.

VI. Conclusions

In this paper, we proposed a generalized FDIA-based cyber topology attack on the power system considering the Australian electricity market trading mechanism. By stealthily manipulating the cyber status of breakers in a carefully coordinated manner, the cyber-attack behavioral agent can cause huge economic losses to retailers or customers. Representative case studies based on the Australian market trading mechanism on the IEEE-118 bus system are conducted to validate the proposed attack mode. As a result, by causing continuous, small and undetected price deviations, the economic loss is almost $100,000 over a single 24-hour period. Future research will look to propose a framework with improved detection of coordinated cyber-attacks undertaken on both digital and analog data, so as to decrease the influence of coordinated cyber-attacks on the power system.

REFERENCES

IEEE Transactions on Smart Grid


Chair Professor and Director of the Centre for Intelligent Electricity Networks (CIEN), University of Newcastle, Australia. He also held academic and industrial positions with the Hong Kong Polytechnic University, the University of Queensland, Australia and Transend Networks, Tasmania, Australia. His research interest includes Smart Grid, power system planning, power system security, load modeling, renewable energy systems, electricity market, and computational intelligence and its application in power engineering. Prof. Dong is an editor of IEEE TRANSACTIONS ON SMART GRID and IEEE POWER ENGINEERING LETTERS.