Review of the false data injection attack against the cyber-physical power system

Qi Wang¹, Wei Tai¹, Yi Tang⁴, Ming Ni²

¹Jiangsu Provincial Key Laboratory of Smart Grid Technology & Equipment, Southeast University, Sipailou 2#, Nanjing, People’s Republic of China
²NARI Group Corporation, State Grid Electric Power Research Institute, No. 19 Chengxin Avenue, Nanjing, People’s Republic of China
E-mail: tangyi@seu.edu.cn

Abstract: With the development of synchronous measuring technology and communication technology, the units of measurement, calculation, execution and communication are deeply integrated into energy manage system, which can achieve panoramic state awareness through the fast and accurate state estimation algorithm. Meanwhile, the cyber-attack has become an important issue posing severe threats to the secure operation of power systems. A well-designed false data injection attack (FDIA) against state estimation can effectively bypass the traditional bad data detection methods and interfere with the decision of the control centre, thus causing the power system incidents. This study comprehensively discusses the characteristics of FDIA including not only the goals, construction methods and consequences of FDIA from the perspective of attackers but also the protection and detection countermeasures from the perspective of defenders. Moreover, a game-theory-based FDIA against the substation information network is simulated to reveal the interactions between attackers and defenders.

1 Introduction

With the development of the cyber-physical power system (CPPS), and the application of advanced information technology such as perception, calculation, communication and control, the power system has gradually realised informatisation, networking and intelligentisation [1, 2]. While promoting the real-time analysis, scientific decision and efficient allocation of power systems, the open communication networks and interface terminals also bring potential security risks [3, 4]. Compared to the relatively robust power primary system, the researches on the security protection of the power information system are on the initial stage, with plenty of security vulnerabilities undiscovered [5]. Owing to the significant interest relevance and high transmissibility of power system, once attacked, it will engender a serious impact on power safety, industrial production and people’s livelihood, which has captured significant attention [6]. As a novel attack mode for basic industrial facilities, the cyber-attack has become a threat to the safe and stable operation of power systems, whose attack and defence mechanism requires being further studied [7].

According to attack targets, the cyber-attack against power systems can be classified into destroying the availability, integrity and confidentiality of information. The availability destruction is embodied in unavailable information resulting from communication interruption, whose typical methods are denial-of-service (DOS) attack, black hole attack and attacks modifying network topology. The integrity destruction is embodied in incorrect information resulting from false data injection, whose typical methods are false data injection attack (FDIA), man-in-the-middle attack and replay attack. The confidentiality destruction is embodied in data leakage and illegal usage, whose typical methods are brute force password cracking, utilisation of malware and internal employee attack [8]. As a typical mode to destroy the information integrity, FDIA can disrupt the analysis results of state estimation, thus misleading the decision of the control centre. FDIA was first proposed by Liu in 2009, and the principle of FDIA is to perform coordinated attacks against sensors, falsify certain measurements and manipulate specific data of state estimation [9]. As a result, the control centre misjudges the power grid into emergency and implements mal-operation, thus damaging the economic benefits, monitoring capability and safe operation of power system.

In recent years, a series of power network security accidents such as BlackEnergy virus attack against Ukraine power grid, have triggered severe security loss [10]. These cyber-attacks are aimed at the destruction of the communication, calculation and control loop in the CPPS. The cyber-attack against Ukraine power grid is taken as the example. An email containing malicious macro files was sent to the system operators. Afterwards, the operation system was infected by BlackEnergy Trojan horse, which not only provided a backdoor server to open connecting ports for attackers but also embedded KillDisk components in the supervisory control and data acquisition (SCADA) system to cause the system failure. The combination of both strategies can build a long-term latent attack.

In fact, attackers tend to deploy Trojan horses in multiple distributed areas ahead of time in a latent way. When the power system operates in the most vulnerable condition, the horses will burst together to realise the coordinated attack, thus causing serious damage to the security and stability of the power grid. In addition, it can be speculated that the attackers are highly aware of the target network information and knowledge. It is necessary to strengthen the researches on the origins of various cyber-attacks and their synergies.

This paper summarises the comprehensive researches of FDIA in the power system, which will be elaborated in the following aspects. First, from the perspective of attackers, the goals, construction methods and consequences of the FDIA are analysed, so that the invasion process against the information, communication and physical networks of CPPS and corresponding influence on detailed CPPS services are summarised. Then, from the perspective of defenders, several critical sections during the defence procedures are discussed, in which the detection and protection processes are analysed in detail. Finally, to reveal the dynamic behaviour between attackers and defenders, the substation network is chosen as the object of the FDIA, and a game theory is adapted to analyse the practical process of FDIA and the optimised strategies of both players.
transmission side [e.g. SCADA, energy management system (EMS), electricity market operation system and tele meter reading] and in the user side (e.g. demand response management). Owing to the tightly protective design of the control devices, they are often difficult for invasion. Therefore, the FDIA is usually implemented in the first two ways. To destroy the data in the measurement units such as RTUs and phasor measurement units (PMUs), the inherent vulnerabilities in encryption and authentication mechanisms are utilised to modify the original data. In [11], the susceptibility of PMUs to the time synchronisation attack by spoofing its global positioning system (GPS) has been revealed. Since the GPS signal does not have any encryption or authorisation mechanism, attackers could generate the counterfeit GPS signals which receivers are unable to distinguish from the original data. In [12], the coloured Petri net is used to describe the information flows and vulnerabilities among smart metres. On the basis of this, a threat model to describe specific attacks toward smart meters is established.

To invade the communication networks, DOS attacks and man-in-the-middle attacks may be deployed between measurement units and the control centre so that the measurements or control information through the communication channels could be tampered. In [13], an interference matrix of communication data is put forward to deflect the transmitted data from the original value. In [14], a cyber threat called grey-hole attack is addressed, where the PMU data packets are dropped during the transmission in the network, resulting in loss of observability, and subsequently incorrect control decisions.

After successfully injecting false data into the information layer, attackers can subsequently manipulate the controlling services in the power physical layer, which requires the adequate knowledge of power system operation and protection.

2.1 Hierarchical analysis of attack goals

2.1.1 FDIA aiming at the information layer: The invasion toward power communication network is the first step of the FDIA. The possible option includes the measuring units, communication networks and control devices. Owing to the tightly protective design of the control devices, they are often difficult for invasion. Therefore, the FDIA is usually implemented in the first two ways.

To destroy the data in the measurement units such as RTUs and phasor measurement units (PMUs), the inherent vulnerabilities in encryption and authentication mechanisms are utilised to modify the original data. In [11], the susceptibility of PMUs to the time synchronisation attack by spoofing its global positioning system (GPS) has been revealed. Since the GPS signal does not have any encryption or authorisation mechanism, attackers could generate the counterfeit GPS signals which receivers are unable to distinguish from the original data. In [12], the coloured Petri net is used to describe the information flows and vulnerabilities among smart metres. On the basis of this, a threat model to describe specific attacks toward smart meters is established.

To invade the communication networks, DOS attacks and man-in-the-middle attacks may be deployed between measurement units and the control centre so that the measurements or control information through the communication channels could be tampered. In [13], an interference matrix of communication data is put forward to deflect the transmitted data from the original value. In [14], a cyber threat called grey-hole attack is addressed, where the PMU data packets are dropped during the transmission in the network, resulting in loss of observability, and subsequently incorrect control decisions.

After successfully injecting false data into the information layer, attackers can subsequently manipulate the controlling services in the power physical layer, which requires the adequate knowledge of power system operation and protection.

2.1.2 FDIA aiming at the physical layer: After the invasion of the information layer, attackers can obtain the capability of measurement modification. Through modifying the real-time price, load and power flow information, which are enabled to bypass the bad data detection module, attackers could interfere with the subsequent control services [15].

Generally speaking, the state estimation can be formalised by

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

(1)

where \( z \) represents measurements including bus voltage, generator output and branch active and reactive power flows. \( x \) represents the state vector including the amplitude and phase angle of the node voltage. Here, \( h(x) \) is the mapping matrix between the
measurement variables and the state variables, which covers the topology of the system. Generally, the number of measured variables is larger than that of state variables, and the redundancy is used to improve the estimation accuracy.

In reality, the measurements EMS received are not totally correct. Owing to the equipment failure, sensor offset, error connection and communication interference, the state estimation would deviate from the true value. In this paper, we focus on the AC-state estimation model and corresponding largest normalised residual (LNR) method to detect and eliminate the possible errors. The judging formula is as follows:

$$LNR = \| z - h(x) \| \leq \zeta$$

where $z - h(x)$ represents the estimation error of measurements, and LNR follows the chi-square distribution. When LNR is larger than the threshold $\zeta$, it suggests that the measurement vector contains bad data. The largest error value is eliminated, and the detection method is repeated until the condition of (2) is satisfied or the number of measurements is not enough to perform the state estimation.

2.2 Construction methods of FDIA

The change of one certain measurement will cause changes of adjacent measurements according to the power flow. When falsifying one element (e.g. measurements of the node or line), to bypass the bad data detection, attackers should consider the power flow law to find a minimum space where the measurements change accordingly. Therefore, the minimum space requiring a coordinated attack is defined as the minimum related space of this element, which satisfies the power flow law and optimal resource utilisation law when performing an FDIA.

In addition to the above conditions, a successful FDIA is required to meet the following constraints due to the power system operation characteristics:

(i) The boundary node of the attacking element's minimum related space should not be zero injection nodes. Since the sum line power of the number of measurements is not enough to perform the state estimation would deviate from the true value. In this paper, we focus on the AC-state estimation model and corresponding largest normalised residual (LNR) method to detect and eliminate the possible errors. The judging formula is as follows:

$$LNR = \| z - h(x) \| \leq \zeta$$

where $z - h(x)$ represents the estimation error of measurements, and LNR follows the chi-square distribution. When LNR is larger than the threshold $\zeta$, it suggests that the measurement vector contains bad data. The largest error value is eliminated, and the detection method is repeated until the condition of (2) is satisfied or the number of measurements is not enough to perform the state estimation.

2.2 Construction methods of FDIA

The change of one certain measurement will cause changes of adjacent measurements according to the power flow. When falsifying one element (e.g. measurements of the node or line), to bypass the bad data detection, attackers should consider the power flow law to find a minimum space where the measurements change accordingly. Therefore, the minimum space requiring a coordinated attack is defined as the minimum related space of this element, which satisfies the power flow law and optimal resource utilisation law when performing an FDIA.

In addition to the above conditions, a successful FDIA is required to meet the following constraints due to the power system operation characteristics:

(i) The boundary node of the attacking element's minimum related space should not be zero injection nodes. Since the sum line power of the number of measurements is not enough to perform the state estimation would deviate from the true value. In this paper, we focus on the AC-state estimation model and corresponding largest normalised residual (LNR) method to detect and eliminate the possible errors. The judging formula is as follows:

$$LNR = \| z - h(x) \| \leq \zeta$$

where $z - h(x)$ represents the estimation error of measurements, and LNR follows the chi-square distribution. When LNR is larger than the threshold $\zeta$, it suggests that the measurement vector contains bad data. The largest error value is eliminated, and the detection method is repeated until the condition of (2) is satisfied or the number of measurements is not enough to perform the state estimation.

2.2 Construction methods of FDIA

The change of one certain measurement will cause changes of adjacent measurements according to the power flow. When falsifying one element (e.g. measurements of the node or line), to bypass the bad data detection, attackers should consider the power flow law to find a minimum space where the measurements change accordingly. Therefore, the minimum space requiring a coordinated attack is defined as the minimum related space of this element, which satisfies the power flow law and optimal resource utilisation law when performing an FDIA.

In addition to the above conditions, a successful FDIA is required to meet the following constraints due to the power system operation characteristics:

(i) The boundary node of the attacking element's minimum related space should not be zero injection nodes. Since the sum line power of the number of measurements is not enough to perform the state estimation would deviate from the true value. In this paper, we focus on the AC-state estimation model and corresponding largest normalised residual (LNR) method to detect and eliminate the possible errors. The judging formula is as follows:

$$LNR = \| z - h(x) \| \leq \zeta$$

where $z - h(x)$ represents the estimation error of measurements, and LNR follows the chi-square distribution. When LNR is larger than the threshold $\zeta$, it suggests that the measurement vector contains bad data. The largest error value is eliminated, and the detection method is repeated until the condition of (2) is satisfied or the number of measurements is not enough to perform the state estimation.

2.2 Construction methods of FDIA

The change of one certain measurement will cause changes of adjacent measurements according to the power flow. When falsifying one element (e.g. measurements of the node or line), to bypass the bad data detection, attackers should consider the power flow law to find a minimum space where the measurements change accordingly. Therefore, the minimum space requiring a coordinated attack is defined as the minimum related space of this element, which satisfies the power flow law and optimal resource utilisation law when performing an FDIA.

In addition to the above conditions, a successful FDIA is required to meet the following constraints due to the power system operation characteristics:

(i) The boundary node of the attacking element's minimum related space should not be zero injection nodes. Since the sum line power of the number of measurements is not enough to perform the state estimation would deviate from the true value. In this paper, we focus on the AC-state estimation model and corresponding largest normalised residual (LNR) method to detect and eliminate the possible errors. The judging formula is as follows:

$$LNR = \| z - h(x) \| \leq \zeta$$

where $z - h(x)$ represents the estimation error of measurements, and LNR follows the chi-square distribution. When LNR is larger than the threshold $\zeta$, it suggests that the measurement vector contains bad data. The largest error value is eliminated, and the detection method is repeated until the condition of (2) is satisfied or the number of measurements is not enough to perform the state estimation.

2.2 Construction methods of FDIA

The change of one certain measurement will cause changes of adjacent measurements according to the power flow. When falsifying one element (e.g. measurements of the node or line), to bypass the bad data detection, attackers should consider the power flow law to find a minimum space where the measurements change accordingly. Therefore, the minimum space requiring a coordinated attack is defined as the minimum related space of this element, which satisfies the power flow law and optimal resource utilisation law when performing an FDIA.

In addition to the above conditions, a successful FDIA is required to meet the following constraints due to the power system operation characteristics:

(i) The boundary node of the attacking element's minimum related space should not be zero injection nodes. Since the sum line power of the number of measurements is not enough to perform the state estimation would deviate from the true value. In this paper, we focus on the AC-state estimation model and corresponding largest normalised residual (LNR) method to detect and eliminate the possible errors. The judging formula is as follows:

$$LNR = \| z - h(x) \| \leq \zeta$$

where $z - h(x)$ represents the estimation error of measurements, and LNR follows the chi-square distribution. When LNR is larger than the threshold $\zeta$, it suggests that the measurement vector contains bad data. The largest error value is eliminated, and the detection method is repeated until the condition of (2) is satisfied or the number of measurements is not enough to perform the state estimation.

2.2 Construction methods of FDIA

The change of one certain measurement will cause changes of adjacent measurements according to the power flow. When falsifying one element (e.g. measurements of the node or line), to bypass the bad data detection, attackers should consider the power flow law to find a minimum space where the measurements change accordingly. Therefore, the minimum space requiring a coordinated attack is defined as the minimum related space of this element, which satisfies the power flow law and optimal resource utilisation law when performing an FDIA. In addition to the above conditions, a successful FDIA is required to meet the following constraints due to the power system operation characteristics:

(i) The boundary node of the attacking element's minimum related space should not be zero injection nodes. Since the sum line power of the number of measurements is not enough to perform the state estimation would deviate from the true value. In this paper, we focus on the AC-state estimation model and corresponding largest normalised residual (LNR) method to detect and eliminate the possible errors. The judging formula is as follows:

$$LNR = \| z - h(x) \| \leq \zeta$$

where $z - h(x)$ represents the estimation error of measurements, and LNR follows the chi-square distribution. When LNR is larger than the threshold $\zeta$, it suggests that the measurement vector contains bad data. The largest error value is eliminated, and the detection method is repeated until the condition of (2) is satisfied or the number of measurements is not enough to perform the state estimation.
3.1.2 Trajectory prediction-based detection methods: The detection method based on state estimation is mainly used in the static analysis to detect the attack behaviour at a certain time point. In the continuous dynamic operation of the power system, there is a strong spatial and temporal relationship among multiple states. Therefore, we can perform the trajectory analysis based on historical data, so as to match the current measurements of the power grid with the prediction results. The contradiction between two sets of variables can be utilised to find out possible attacked areas. Main detection methods using trajectory prediction include the statistical consistence detection, sequential detection for generalised likelihood ratio and sensor track prediction [25–27].

3.1.3 Artificial intelligence-based detection methods: In addition to the traditional mathematical modelling methods, some artificial intelligence-related detection methods have been put forward in recent years, which are mainly based on neural network, deep learning and fuzzy clustering [28, 29].

The uniqueness of the neural network method is simple in structure but uneasy in the parameter adjustment. Numerous tests should be utilised to train the network model. The choice of model depth and the threshold will affect the model precision and correct rate of results. The deep learning method originates from the neural network, which can solve the over fitting problems well but the training method is more complex.

From the perspective of fuzzy clustering, V data analysis technique is used. Moreover, the data mining method and fuzzy integration method are combined to judge the false data. However, this method requires the artificial measurement and determination of the membership degrees, which contains a strong subjectivity.

The remarkable characteristics of artificial intelligence methods are the strong computing power and clear framework. However, due to the complexity of power system operations, the interpretability of these methods is usually poor.

3.2 Protection-based defence methods

In the security planning of power grid, the important and fragile areas in the power grid are analysed to deploy the limited protection resources. The direct protection methods include physical isolation, channel encryption and firewalls, while the indirect protection method is to enhance the measurement redundancy by deploying redundant sensors.

3.2.1 Programming-based protection methods: From the constraint conditions, the programming method can be divided into linear programming for DC power flow and non-linear programming for AC flow. The mixed integer linear programming (MILP) model is the most common method to judge the critical regions in the power system. In [30], a bi-level MILP model is proposed to determine the least number of measurements to be protected. To reduce the computational complexity, a decomposition approach is adopted to obtain the suboptimal solution. In [31], to solve a novel problem of price modification attacks in the smart grid, a bi-level MILP protection scheme against price modification attacks is proposed; afterwards, an efficient heuristic algorithm is adapted to protect most critical nodes. Overall, the programming methods are fit for the off-line optimisation of protection resources.

3.2.2 Game-based protection methods: The traditional protection methods for the FDIA are usually based on the process analysis of attack or defence mechanism. According to the consequences and difficulties of an FDIA, the weak or important regions can be found out. From the perspective of attack analysis, the existing research focuses on the vulnerability and accessibility of information devices. Accordingly, the attack target, intrusion process and construction method of false data are optimised [32, 33]. From the perspective of defence analysis, the existing research focuses on optimising the performance of bad data identification algorithm, data encryption algorithm and invasion detection mechanism, so as to enhance the multi-level defence ability against FDIA [34]. On this basis, solutions of attack-defence strategy mostly remain in the state level, the weakest or the most important region is taken as the attack-defense object. In fact, because of the limited resources, both sides need to optimise their choices based on the rival's other's possible choices actions, which is a typical forming a double-player dynamic game process [35]. Therefore, the process analysis of FDIA should be integrated with the game theory where both the attacker and defender are seen as rational decision makers.

From the perspective of the joint game, the goal of an FDIA is usually economic loss or stability reducing. Regarding economic loss, the power market price is used as an attack object in [36], a Stackelberg game process is operated using a distributed learning algorithm to reflect the interactions between one defender and several attackers. The attack and defence means are simplified by choosing a certain number of measurements to be changeable or unchangeable, without considering the principle of intrusion process. Regarding stability reduction, in [37, 38], a multistage stochastic game and a Markov model are, respectively, used to simulate the FDIA against the line and the load shedding consequences. The state transition matrix is used to characterise the anticipatory actions of both players, and optimal load shedding is used to quantify the attack consequences. In former two types of researches, a simplification lies in that the attack and defence processes are represented by the failure rate and repair rate of power lines. In [39], the economic and stability indexes are combined. The manipulation of the transformers and power line breakers is chosen as the attack method, while the generator re-dispatching is adopted to reduce the power loss. The load shedding and generator tripping are taken to qualify the economic benefits of FDIA. The attack graph-based game process is used to analyse the optimal paths for both players, where the defender is only allowed to deploy an ex-post remedy instead of premeditated defence.

Overall, a set of sound defence strategies include the coordination among warning, protection, detection, response, recovery and counterattacks. Moreover, in the environment of CPSs, in terms of the information layer, the intrusion detection system and data encryption algorithm are utilised to identify the correctness of the data protocol and logic. In terms of the physical layer, the rationality of the data content should be identified based on the power professional knowledge, and then some remedial measures need to be performed to eliminate the attack effects.

4 Case: FDIA against substation information network

In this section, the FDIA against the substation information network is taken as the case to illustrate the basic attack process and defence strategies; afterwards, the optimal resource deployment is simulated through a double-player zero-sum game. The analysis of the FDIA process requires to be combined not only with the target and strategies of attackers but also with the detection and protection strategies of defenders. The most basic knowledge is the action steps of the FDIA, which are shown in Fig. 4. Cyber-attacks fail the corresponding information services through information equipment failures, then result in the disturbance of the power system.

4.1 Attack graph of the substation

The D2-1-type substation is taken as the object of FDIA, whose information network is shown in Fig. 5. According to the information transmission path, the information layers can be divided into three layers (i.e. process layer, bay layer and station layer). According to the types of bays, they can be divided into the line bay, transformer bay and bus bay. According to the type of intelligent electronic device (IED), the devices can be divided into the breaker IED, merging unit (MU) IED and P&C IED.

Fig. 4 Flowchart of an FDIA
In the D2-1 intelligent substation, sampling signals of MU are spread by the sampled analogue values (SAV) message, while sampling signals of the P&C IED are spread by generic object oriented substation event (GOOSE) message. ‘Publisher/reader’ mode is utilised to transmit information in multicast mode. According to the data flows, we could summarise the information devices and their link relationship as an attack graph as shown in Fig. 6. Among them, points A1–A7 belong to the process layer L1; points B1–B5 belong to the bay level L2; and points C1–C4 belong to the station layer L3. We assume that if attackers invade these three layers through one certain path, they can manipulate the host to result in a power system failure.

The third layer contains the controlling service, according to the common applications of the substation, four typical services are summarised in nodes C1–C4 (i.e. information measurement, protection function, monitoring and control). The node D1 in the top layer represents the power system fault.

### 4.2 Parameter setting and model solving process

To perform the risk assessment of the power information network, factors affecting the system security should be considered. The external factors result from the cyber-attacks, while the internal factors result from the risks of devices. The comprehensive security risk of each node is determined by the vulnerability and sensitivity of it. The sensitivity is related with the in-degree and out-degree of the node, representing the frequency of being utilised by all kinds of attacks, and the vulnerability of the device is directly proportional to the safety level of the device itself.

\[ G = (N, E, S) \]

\[ S_i = \frac{d_{in}(i)}{T_{in}(i)} + \frac{d_{out}(i)}{T_{out}(i)}, \quad i \in N \]

where \( d_{in}(i) \) and \( d_{out}(i) \) represent the in-degree and out-degree of node \( i \), while \( T_{in}(i) \) and \( T_{out}(i) \) represent the number of links in the lower layer and upper layer. Therefore, the result is the relative sensitivity considering the connectedness in each layer.

The comprehensive risk of each node \( R_i \) can be calculated by the following equation:

\[ R_i = W_v V_i \times W_s S_i, \quad i \in N \]

where \( V_i \) and \( S_i \) are the vulnerability and sensitivity of node \( i \), respectively. Overall, there are 35 kinds of attack strategies.

### Table 1: Comprehensive risks of the substation devices

| Node   | Device     | Vulnerability | Sensitivity | Comprehensive risk |
|--------|------------|---------------|-------------|-------------------|
| A1     | feeder MU  | 0.0773        | 0.1000      | 0.0077            |
| A2     | feeder breaker | 0.0926    | 0.2000      | 0.0185            |
| A3     | bus MU     | 0.0773        | 0.1000      | 0.0077            |
| A4     | bus breaker | 0.0926        | 0.2000      | 0.0185            |
| A5     | transformer MU | 0.0773 | 0.2000      | 0.0155            |
| A6     | transformer breaker 1 | 0.0926 | 0.1000      | 0.0093            |
| A7     | transformer breaker 2 | 0.0926 | 0.1000      | 0.0093            |
| B1     | line P&C   | 0.0852        | 0.3429      | 0.0292            |
| B2     | line P&C2  | 0.0852        | 0.4857      | 0.0414            |
| B3     | bus P&C    | 0.0852        | 0.3143      | 0.0268            |
| B4     | transformer P&C | 0.0852 | 0.4143      | 0.0353            |
| B5     | transformer P&C2 | 0.0852 | 0.3429      | 0.0292            |
| C1     | information measurement | 0.01 | 0.3214      | 0.0032            |
| C2     | protection function | 0.01 | 0.5357 | 0.0054 |
| C3     | monitoring and control | 0.01 | 3.4643 | 0.0346 |
| C4     | auto-control | 0.01 | 0.5357 | 0.0054 |

Fig. 5 Information network in the substation

Fig. 6 Attack graph of an FDIA against substation network
17.06%. While there are 10 among 35 kinds of defence options for path 4 (A3, B3, C3, D1) accounts for the highest selectivity of and defence behaviours. The risk in the system is 0.0511.

Fig. 7 Optimal attack and defence strategies (a) Attack strategies, (b) Defence strategies

$U = (u_{ij})_{N \times N}$: The reward function of the players. The element $u_{ij}$ is the gain of the players under attack behaviour $a_i$ and defence behaviour $d_j$. The calculation method of the attacker's reward function is as follows:

$$u_{ij} = \sum_{i \in a_i} R_i, \quad \text{attack succeeds}$$

$$u_{ij} = 0, \quad \text{attack fails} \quad (5)$$

The comprehensive risk of the attack path is used as the reward function. Since it is a zero-sum game, the sum of both players' return function values is 0. The attacker's reward function $U_a$ is set to be positive and the defender's reward function $U_d$ is negative and satisfies $U_a - U_d$.

For a given reward matrix $U$, there is an attack strategy $A^* = (P \times (a_1), P \times (a_2), \ldots, P \times (a_N))$, a defensive strategy $D^* = (P \times (d_1), P \times (d_2), \ldots, P \times (d_N))$ and a constant $V$ that satisfy the following conditions.

For any $j$, there is

$$\sum_{i=1}^{N_A} u_{ij} P \times (a_i) \geq V \quad (6)$$

For any $i$, there is

$$\sum_{j=1}^{N_D} u_{ij} P \times (d_j) \leq V \quad (7)$$

Consequently, the strategy combination $(A^*, D^*)$ is the Nash equilibrium point for the game, and $V$ is the expected gain, which represents the expected path risks within the combination of attack and defence behaviours.

According to the above model, the results of optimal strategy and expected gain are shown in Fig. 7. Among 28 kinds of attack paths, only ten kinds will enter the attacker's options, where the path 4 (A3, B3, C3, D1) accounts for the highest selectivity of 17.06%. While there are 10 among 35 kinds of defence options for defenders, and the nodes A2 and B5 are the most possible protection nodes for a selection probability of 21.26%. Under the optimal attack–defence strategy, the expected comprehensive path risk $V$ in the system is 0.0511.

5 Conclusion

This paper provides an overview of the researches on the FDIA. First, the security vulnerabilities in the measurement equipment and communication network are analysed, which are utilised to inject the false data; therefore, the safety and economic index are weakened. A framework of FDIA considering the attack goals, construction methods and consequences is established. Second, according to pre-attack defence and ex-post defence, the method of defence based on protection and detection is analysed respectively. A multi-layer space–time cooperative defence framework is constructed. Finally, an FDIA case against the substation information network is simulated to integrate the attack principles with the game-based defence strategies.

The traditional FDIA research is to destroy the application function of SCADA and subsequent EMS system. Actually, with a wide interaction among source, network and load, information systems in the generation side, grid side and load side are all possible to be attacked by false data, thus affecting the monitoring, control, statistical analysis, economic dispatching and security decision of power systems. Therefore, the FDIA against all kinds of information systems in the CPPS requires further researches.

6 Acknowledgments

This work was supported by the National Key Research and Development Program of China under Grant no. 2017YFB0903000 (Basic Theories and Methods of Analysis and Control of the Cyber-Physical Systems for Power Grids), the National Natural Science Foundation of China under Grant nos. 51577030 and 51707032 and the Project of State Grid Corporation of China (the Identification Method of Malicious Attack on the Power Grid and Active Defence Method on the Power Grid Side).

7 References

[1] Mo, Y., Kim, T.H.J., Brancik, K., et al.: 'Cyber-physical security of a smart grid infrastructure', Proc. IEEE, 2012, 100, (1), pp. 195–209
[2] He, H., Yan, J.: ‘Cyber-physical attacks and defences in the smart grid: a survey’, IET Cyber-Phys. Syst. Theory Appl., 2016, 1, (1), pp. 13–27
[3] Vellaiuthurai, C., Srivastava, A., Zonouz, S., et al.: ‘CP index: cyber-physical vulnerability assessment for power-grid infrastructures’, IEEE Trans. Smart Grid, 2015, 6, (2), pp. 566–575
[4] Wang, W., Lu, Z.: ‘Cyber security in the smart grid: survey and challenges’, Comput. Netw., 2015, 57, (5), pp. 1344–1371
[5] Zhang, Y., Wang, L., Xiang, Y., et al.: ‘Power system reliability evaluation with SCADA cybersecurity considerations’, IEEE Trans. Smart Grid, 2015, 6, (4), pp. 1707–1721
[6] Liu, S., Mashayekh, S., Kundur, D., et al.: ‘A framework for modeling cyberphysical switching attacks in smart grid’, IEEE Trans. Emerg. Top. Comput., 2013, 1, (2), pp. 273–285
[7] Hahn, A., Manimaran, G.: ‘Cyber attack exposure evaluation framework for the smart grid’, IEEE Trans. Smart Grid, 2011, 2, (4), pp. 835–843
[8] Tang, Y., Chen, Q., Li, M., et al.: ‘Challenge and evolution of cyber attacks in cyber physical power system’. Asia-Pacific Power Energy Engineering Conf. APPEEC, Xian, People's Republic of China, December 2016, pp. 857–862
[9] Liu, Y., Ying, P., Reiter, M.K.: ‘False data injection attacks against state estimation in electrical power grids’, ACM Trans. Inf. Syst. Secur., 2011, 14, (1), pp. 3–33
[10] Liang, G., Weller, S.R., Zhao, J., et al.: ‘The 2015 Ukraine blackout: implications for false data injection attacks’, IEEE Trans. Power Syst., 2017, 32, (4), pp. 3177–3181
[11] Fan, Y., Zhang, Z., Trinkle, M., et al.: ‘A cross-layer defense mechanism against GPS spoofing attacks on PMUs in smart grids’, IEEE Trans. Smart Grid, 2015, 6, (6), pp. 2659–2668
[12] Smart, D., Mesh, G.: ‘Advanced metering infrastructure’, South Power Syst Technol., 2011, 6, (S5), p. 29210083
[13] Bishop, A.N., Savkin, A.V.: ‘On false-data attacks in robust multi-sensor-based estimation’, IEEE Int. Conf. Control Automation ICCA, Santiago, Chile, 2011, pp. 10–17
[14] Pal, S., Sikdar, B., Chow, J.: ‘An online mechanism for detection of gray-hole attacks on PMU data’, IEEE Trans. Smart Grid, 2016, PP, (99), pp. 1–10
[15] Yang, Q., Chang, L., Yu, W., et al.: ‘On false data injection attacks against Kalman filtering in power system dynamic state estimation’, Secure Commun. Netw., 2016, 9, (9), pp. 833–849
[16] Yu, Z.H., Chin, W.L.: ‘Blind false data injection attack using PCA approximation method in smart grid’, IEEE Trans. Smart Grid, 2015, 6, (3), pp. 1219–1226
[17] Meng, T., Wang, X., Dong, Z., et al.: ‘Injected attack strategy for false data based on Lagrange multipliers method’, Autom. Electr. Power Syst., 2017, 41, (11), pp. 26–32
[18] Xie, L., Mo, Y., Sinopoli, B.: ‘Integrity data attacks in power market operations’, IEEE Trans. Smart Grid, 2011, 2, (4), pp. 659–666

This is an open access article published by the IET under the Creative Commons Attribution License (http://creativecommons.org/licenses/by/3.0/)
[19] Jia, L., Kim, J., Thomas, R.J., et al.: ‘Impact of data quality on real-time locational marginal price’, IEEE Trans. Power Syst., 2014, 29, (2), pp. 624–626

[20] Liu, R., Vellaithurai, C., Biswas, S.S., et al.: ‘Analyzing the cyber-physical impact of cyber events on the power grid’, IEEE Trans. Smart Grid, 2015, 6, (5), pp. 2444–2453

[21] Group, W.: ‘Nistir 7628’ security’, 2010, 1, (August)

[22] Hu, Z., Wang, Y., Tian, X., et al.: ‘False data injection attacks identification for smart grids’. 2015 Third Int. Conf. Technological Advances Electrical Electronics Computer Engineering TAECE 2015, Beirut, Lebanon, 2015, pp. 139–143

[23] Bobba, R., Rogers, K., Wang, Q., et al.: ‘Detecting false data injection attacks on DC state estimation’, First Work Secur. Control Syst., 2010, 6, (5), pp. 1–9

[24] Chakhchoukh, Y., Ishii, H.: ‘Enhancing robustness to cyber-attacks in power systems through multiple least trimmed squares state estimations’, IEEE Trans. Power Syst., 2016, 31, (6), pp. 4395–4405

[25] Zhao, J., Zhang, G., Scala, M., et al.: ‘Short-term state forecasting-aided method for detection of smart grid general false data injection attacks’, IEEE Trans. Smart Grid, 2017, 8, (4), pp. 1580–1590

[26] Li, S., Yilmaz, Y., Wang, X.: ‘Quickest detection of false data injection attack in wide-area smart grids’, IEEE Trans. Smart Grid, 2015, 6, (6), pp. 2725–2735

[27] Khalid, H.M., Peng, J.C.H.: ‘Immunity toward data-injection attacks using multisensor track fusion-based model prediction’, IEEE Trans. Smart Grid, 2017, 8, (2), pp. 697–707

[28] He, Y., Mendez, G.J., Wei, J.: ‘Real-time detection of false data injection attacks in smart grid: a deep learning-based intelligent mechanism’, IEEE Trans. Smart Grid, 2017, 8, (5), pp. 2505–2516

[29] Orazi, M., Eshoala, I., Tunay, F., et al.: ‘Machine learning methods for attack detection in the smart grid’, IEEE Trans. Neural Netw. Learn. Syst., 2015, PP, (99), pp. 1–14

[30] Liu, X., Li, Z., Li, Z., et al.: ‘Optimal Protection Strategy Against False Data Injection Attacks in Power Systems’, IEEE Trans. Smart Grid, 2015, 8, (4), pp. 1–9

[31] Mishra, S., Li, X., Pan, T., et al.: ‘Price modification attack and protection scheme in smart grid’, IEEE Trans. Smart Grid, 2017, 8, (4), pp. 1864–1875

[32] Anwar, A., Mahmood, A.N., Pickering, M.: ‘Modeling and performance evaluation of stealthy false data injection attacks on smart grid in the presence of corrupted measurements’, J. Comput. Syst. Sci., 2017, 83, (1), pp. 58–72

[33] Liu, T., Sun, Y., Liu, Y., et al.: ‘Abnormal traffic-indexed state estimation: a cyber-physical fusion approach for smart grid attack detection’, Future Gener. Comput. Syst., 2015, 49, pp. 94–103

[34] Mousavian, S., Valenzuela, J., Wang, J.: ‘A probabilistic risk mitigation model for cyber-attacks to PMU networks’, IEEE Trans. Power Syst., 2015, 30, (1), pp. 156–165

[35] Chen, P.Y., Cheng, S.M., Chen, K.C.: ‘Smart attacks in smart grid communication networks’, IEEE Commun. Mag., 2012, 50, (8), pp. 24–29

[36] Sanjub, A., Saad, W.: ‘Data injection attacks on smart grids with multiple adversaries: a game-theoretic perspective’, IEEE Trans. Smart Grid, 2016, 7, (4), pp. 2038–2049

[37] Wei, L., Sarwat, A., Saad, W., et al.: ‘Stochastic games for power grid protection against coordinated cyber-physical attacks’, IEEE Trans. Smart Grid, 2016, 7, (8), pp. 4402–4413

[38] Ma, C.Y., Yang, D.K.Y., Lou, X., et al.: ‘Markov game analysis for attack-defense of power networks under possible misinformation’, IEEE Trans. Power Syst., 2013, 28, (2), pp. 1676–1686

[39] Wang, C., Hou, Y., Ten, C.W.: ‘Determination of Nash equilibrium based on plausible attack-defense dynamics’, IEEE Trans. Power Syst., 2017, 32, (5), pp. 3670–3680

[40] Yang, G., Wang, Y., Li, J., et al.: ‘An assessment method of vulnerabilities in electric CPS cyber space’. Int. Conf. Natural Computation and Fuzzy Systems and Knowledge Discovery, Changsha, China, 2016, pp. 397–402