Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

TC 11 Briefing Papers

CPMTD: Cyber-physical moving target defense for hardening the security of power system against false data injected attack

Yifan Hu[a], *Peidong Zhu*[c,1,*], *Peng Xun*[a], *Bo Liu*[b,*], *Wenjie Kang*[d,e,f], *Yinqiao Xiong*[a,c], *Weiheng Shi*[g]

[a] College of Computer, National University of Defense Technology, Changsha 410073, China
[b] National Key Laboratory of Parallel and Distributed Processing, College of Computer, National University of Defense Technology, Changsha 410073, China
[c] Department of Electronic Information and Electrical Engineering, Changsha University, Changsha 410022, China
[d] Hunan Provincial Key Laboratory of Network Investigational Technology, Hunan Police Academy, Changsha 410138, China
[e] College of Systems Engineering, National University of Defense Technology, Changsha 410073, China
[f] Key Laboratory of Police Internet of Things Application Ministry of Public Security, Beijing 100089, China
[g] College of Meteorology and Oceanography, National University of Defense Technology, Nanjing 211101, China

ARTICLE INFO

Article history:
Received 5 May 2021
Revised 13 August 2021
Accepted 2 September 2021
Available online 9 September 2021

Keywords:
Cyber-physical system
Moving target defense
Attack prevetion and detection
Bi-level framework
False data injection attack

ABSTRACT

Cyber-physical system (CPS) like smart grids deeply integrated with communication networks are often subjected to sophisticated cyber-attacks, such as false data injection attack (FDIA) with a strong capability of strategic reconnaissance required to learn the environment, where the static characteristics of the system enable an easier profiling of the critical infrastructure resources by the adversary. In this paper, we propose a cyber-physical moving target defense (CPMTD) technique that focuses on both attack prevention and detection to mitigate such static vulnerabilities and provide a combination of defense strategies for power system. For attack prevention, we design the Cyber-MTD strategy to mislead and disrupt attack preparation by randomizing the data acquisition with controlled change across multiple system dimensions based on the network programmability of protocol oblivious forwarding (POF). For attack detection, we design the Physical-MTD strategy to improve the detection probability of FDIA by periodically changing the measurement matrix of state estimation based on the D-FACTS devices' capability of perturbing the transmission line susceptance. Simulations on IEEE 14 bus and 57 bus systems demonstrate the effectiveness of CPMTD against FDIA with small overhead. The probability of cyber-attacks in two cases can be reduced by more than 90%; FDIA introduces little operation cost as most of them are detected. Network throughput barely changes and network latency increases by less than 9%.

* Corresponding authors.
E-mail addresses: huyifan17@nudt.edu.cn (Y. Hu), pdz@ccsu.edu.cn (P. Zhu), xunpeng12@nudt.edu.cn (P. Xun), kyle.liu@nudt.edu.cn (B. Liu), kangwenjie@nudt.edu.cn (W. Kang), yq.xiong@ccsu.edu.cn (Y. Xiong), tfoterye@gmail.com (W. Shi).
[1] Senior Member, IEEE

https://doi.org/10.1016/j.cose.2021.102465
0167-4048/

1. Introduction

Ubiquitous electric Internet of Things (UEIoT) plays a critically important role in human society as a smart service system by the interconnection of everything and human-computer interaction based on mobile Internet technology, artificial intelligence technology, and advanced communication technology (Wang et al., 2019). With the organic integration and deep collaboration of 3C (Computation, Communication and Control) technologies, power system has gradually developed into a cyber-physical system (CPS) that provides real-time perception, dynamic control and information service (Zacchia Lun et al., 2019). In such multi-dimensional complex system that covers computing, networking and physical environment, there is a sharp increase in vulnerabilities to cyber-attacks and many of them are difficult to detect. Based on in-depth research of recent cyber-attacks, such as StuxNet attack (Langner 2011), Blackenergy attack and Industroyer attack (Case 2016), the development of cyber-attacks can be divided into five stages, as shown in Fig. 1, where the first four stages are regarded as attack preparation. In the "penetration" stage, the attacker establishes the access connection to communication networks. In the "collection" stage, the attacker explores system properties like version numbers, vulnerabilities and configurations. In the "modeling" stage, the attacker develops a blueprint of system architecture with the acquired knowledge. In the "scheming" stage, information is turned into weapons, i.e., attack scheme is formulated based on system vulnerabilities. In the "execution" stage, the attacker performs malicious activities on the target system and improves his system model for future attacks.

Owing to the openness of communication networks and the intelligence of distributed meters, false data injection attack (FDIA) achieves the possibility of establishing footholds on power grid devices when the authentication weaknesses and the restart communications option vulnerability in Modbus/TCP protocols are exploited by the adversary (Liu et al., 2017). For example, fundamental applications in power system may be misled by injecting false data into the reading of smart meters. As a kind of sophisticated cyber-attack against the integrity of telemetry measurements, FDIA has drawn extensive attention to scholars in the fields of network security and industrial control (Chaojun et al., 2015a; Lin et al., 2018; Valenzuela et al., 2013). Great efforts have been made in preventing and detecting FDIA including (i) extracting the power flow data from the network traffic to evaluate the physical impact of power system, (ii) protecting certain sensor measurements and identifying certain state variables, and (iii) detecting anomalies in the input data related to transmission lines. In practice, these methods have a good effect on some specific cyber-attacks. However, they will not be feasible when the adversary optimizes his strategy and does not obey the same execution principle. In addition, the danger of cyber-attacks is always perceived only during their executions and the reaction time is too short for system operators to take preventative measures, such as mitigating or delaying these cyber-attacks (Lin et al., 2018). A carefully planned cyber-attack only has a few hours' execution after a long-time investigation and study of system knowledge, which may last more than half a year (Case 2016). These persistent reconnaissance operations are the strongest capability of the adversary indeed.

Fig. 1 – Five stages of cyber-attacks.

Unlike previous studies against cyber-attacks in the execution stage, we focus on attack preparation. Obstructing the attacker's access to the power grid data in network communications is our primary objective. Converting the study point from "attack execution" to "attack preparation", there are two advantages: expansion containment and risk absorption. Expansion containment means that we can prevent a broad scope of cyber-attacks besides some specific ones. Before different cyber-attacks are performed in different execution channels, system model based on the current operation state cannot be established without data acquisition. Risk absorption means that we can suppress cyber-attacks at their inception. Exposing misleading data to the adversary on purpose or disrupting the process of data acquisition invalidate cyber-attacks. During attack preparation, we obscure the system architecture for the adversary by randomizing different ways of data acquisition: (i) introducing various private protocols (PP) to diversify the network protocol, (ii) mixing deception packets into the network traffic to disguise the normal packets, (iii) encapsulating the data packets into different PPs to randomize the network groups, and (vi) forwarding these PPs over a routing path pool to enable the dynamic paths. Finally, maybe a cyber-attack will take an extremely long time to develop with little physical damage on power system.

Although this multidimensional network-based randomization strategy can enhance the security of power system, it is by no means a complete defense because the possibility cannot be ruled out that the adversary who eventually finds unpatched vulnerabilities to exploit after an enough long-term reconnaissance. For example, FDIA can stealthily compromise the results of state estimation owing to the vulnerability of the cyber-physical marriage (Liu et al., 2011). Since "stealthy" is a specific characteristic of FDIA that can easily bypass bad data detection (BDD) based on the measurement residual in state estimation, our work focuses not only on disrupting the attacker's data acquisition but also on making stealthy FDIA detectable. The knowledgeable attacker is capable of designing such stealthy FDIA that can cover its tracks in power system without being detected in state estimation. If the attack vector falls in the column space of the measurement matrix, an attack could cheat and pass BDD (Liu et al., 2011). This means that sufficient knowledge of the measurement matrix is required for the attacker to construct such stealthy FDIA. To secure power system against FDIA, passive defense approaches were proposed to prevent the attacker from critical measurements in Kosut et al. (2011) and Chaojun et al. (2015b). They aimed to protect a specific set of smart meters by introducing enhanced security, such as traffic control or data encryption. However, it is too costly and time-consuming to deploy these security measures in edge devices where the limited

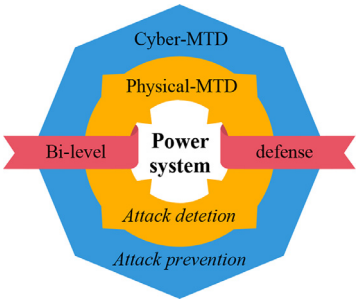

Fig. 2 – Bi-level defense based on CPMTD.

computing and storage space may not support such complicated strategies.

Since legacy BDD was not feasible against the attacker with full system knowledge, moving target defense (MTD) was proposed to invalidate the FDIA's stealth with misleading information by changing the set of measurements and topology properties in Rahman et al. (2014). Considering existing MTDs ignored the possibility that a powerful attacker was able to perceive the activation of them, a hidden MTD technique was proposed in Tian et al. (2017a) and Tian et al. (2019), where necessary parameter perturbations were calculated under a basic feasibility condition for this hidden MTD. Although these studies achieve significant performance in mitigating FDIA by obstructing the attacker's access to critical information of the measurement matrix, the cost of physical perturbations has been ignored. Distinct from MTDs that relied on changing physical parameters, network-based MTD for power system was first proposed to mislead the attacker's ability to acquire data from the communication network in Lin et al. (2019) and Lin et al. (2020), where Raincoat was designed to disrupt the network reconnaissance by randomizing the data acquisition in multiple rounds and DefRec was designed to complicate network communications by introducing virtual interactions and decoy data. In these ways, the difficulty in knowledge exploring of the critical infrastructure resources for the adversary significantly increases without introducing any physical perturbation in power system. However, these network-based MTDs can only reduce the intrusion probability of FDIA but cannot defend against stealthy FDIA.

In this paper, we propose a cyber-physical MTD (CPMTD) technique to not only mitigate FDIA but also improve the detection probability of stealthy FDIA. CPMTD specifies and implements a combination of defense strategies involving attack prevention and detection to provide the enhanced security for power system. The bi-level defense framework of CPMTD is shown in Fig. 2. As the first-level defense, we design a cyber-based MTD (Cyber-MTD) strategy that focuses on cyberspace protection for power system. Cyber-MTD aims to mislead and disrupt the attacker's reconnaissance to critical infrastructure resources by multiple rounds of randomizing the data acquisition. Compared to the network-based MTD in Lin et al. (2019), we expand the attack space into multiple dimensions to further increase the unpredictability of network communications. As the second-level defense, we design a physics-based MTD (Physical-MTD) strategy that focuses on physical space protection for power system. Physical-MTD aims to obstruct the attacker's access to critical power grid data by periodically changing the measurement matrix that is usually assumed to be fixed, thereby indirectly improving the detection probability of FDIA. Since the change of transmission line susceptances may increase power system operation cost, Physical-MTD also explores the optimality in susceptance perturbations for FDIA detection. Finally, Cyber-MTD and Physical-MTD constitute a bi-level defense mechanism that can both prevent FDIA during attack preparation and improve FDIA detection in the execution stage. Specifically,

- We propose the concept of CPMTD that combines the Cyber-MTD and Physical-MTD strategies to enhance the security of both the cyber and physical spaces for power system by (i) disrupting the attacker's reconnaissance of critical infrastructure resources, and (ii) obstructing the attacker's access to measurement matrix information. These two strategies are combined into a bi-level defense framework where Cyber-MTD is progressed by Physical-MTD, which means even if attacks bypass Cyber-MTD, they can still be detected by Physical-MTD.
- We focus on disrupting the development of cyber-attacks during attack preparation before the physical system is damaged. To randomize the attacker's data acquisition, we design the Cyber-MTD strategy to increase the apparent complexity and uncertainty in network communications with controlled change across multiple system dimensions. Because of end-to-end oblivious communications based on the packet dropping policy, Cyber-MTD ensures transparent network transmission without introducing additional burdens on the communication entities.
- We focus on adjusting the measurement matrix of state estimation to make stealthy FDIA detectable without significantly increasing power system operation cost. To make the measurement matrix unpredictable, we design the Physical-MTD strategy to arrange periodic variations of the measurement matrix by leveraging susceptance perturbation of transmission lines. Based on the cost-benefit analysis, we formulate an optimization in maximizing the detection probability of FDIA while minimizing the impact on power system.

The remainder of this paper is organized as follows. Section 2 provides an overview of the related work. Section 3 introduces the necessary background and the research motivation. Cyber-MTD and Physical-MTD strategies are designed in Section 4 and 5, respectively. Evaluation results of CPMTD are presented in Section 6. Concluding remarks are drawn in Section 7 with future work.

2. Related work

We review two kinds of MTDs used in different spaces of power system and discuss some of the limitations of these techniques.

2.1. Network-based MTD

To both confuse the attacker's reconnaissance and conceal the service's TCP identity (i.e., IP address and TCP port), Atighetchi et al. (2003) proposed a network-centric defense mechanism based on port/address hopping supported by network address translation (NAT) with the capability of reverse mapping from false IP-port to true IP-port. Based on software defined networking (SDN), Jafarian et al. (2012) presented a OpenFlow random host mutation (OF-RHM) technique to manipulate IP addresses in unpredictable and rapid mutation in the MTD architecture where each host was frequently assigned a random virtual IP by the OpenFlow controller. These two MTD techniques can both achieve IP randomization and the latter has the SDN's advantage of flexible infrastructure for efficient network attribute transformation with minimal operation overhead. However, These work only introduce one or two moving targets that may only prevent a few kinds of cyber-attacks or some specific ones.

To mitigate Internet service DDoS attacks, Wang, Jia, Fleck, Powell, Li, Stavrou (2014) proposed the MOTAG mechanism to relay the traffic between authenticated clients and servers by employing a group of dynamic proxy nodes to hide their IP addresses. Considering the attack vectors in critical infrastructure control systems, Chavez et al. (2015) developed three network randomization techniques to prevent the adversary from targeting known static attributes of network devices and systems by automatically reconfiguring network settings. Both of the work construct three moving targets based on SDN by randomizing TCP/UDP ports, IP addresses, and network paths with the goal of the limited adversaries may be DDoS, targeting a specific service or host. To expand the defense space, Groat et al. (2012) proposed a moving target IPv6 defense (MT6D) technique to secure smart grid communications at the network layer by exploiting the immense subnet address space of IPv6. However, MT6D may create extra latency and overhead in smart grid communications because of the encapsulation in MT6D tunnels.

To introduce additional uncertainty, Hamada et al. (2018) proposed a Honeypot-like MTD mechanism to establish virtual IoT modules acting as a honeypot by exploiting mobile devices surrounding the network. They constructed the moving targets by these mobile devices that were chosen as real or fake gateways and sensors to confuse the adversary. To increase system complexity, Ghourab et al. (2019) proposed a novel spatiotemporal MTD mechanism to obfuscate signal transmission-patterns and the transmitted data across the entire spectrum by spatiotemporal multidimensional manipulations. Considering MTD spatial and temporal decision-makings together, Tan et al. (2021) proposed an MTD decision-making method based on a FlipIt differential game (FDG-MTD). These work achieve spatio-temporal diversity as the moving targets to secure wireless communications against eavesdropping attacks. However, all the above techniques only introduce no more than three moving targets in the dimensions of time and space against some specific cyber-attacks. Therefore, we design a multidimensional network-based MTD strategy as Cyber-MTD with more moving targets added for a larger defense space to secure network communications for power system.

2.2. Perturbation-based MTD

To the best of our knowledge, Morrow et al. (2012) pioneered a perturbation-based approach for BDD in power system by changing the impedance on a set of chosen transmission lines by leveraging D-FACTS devices. They were the first to apply known perturbations to the physical system for attack detection. Considering that previous MTDs were not always effective in detecting attacks, Lakshminarayana and Yau (2018) presented a heuristic design criteria to proactively perturb transmission line reactances that were selected for effective attack detection. They provided analysis for the cost-benefit tradeoff of the perturbation-based MTD for the first time. To thwart FDIA constructed by former system information, Zhang et al. (2020) presented a comprehensive analysis of the perturbation-based MTD including completeness, deployment, and increasing operation cost. Hidden MTD (HMTD) was first proposed in Tian et al. (2017b) and improved in Tian et al. (2018), where the stealthiness and completeness of MTD were discussed to construct the HMTD. To ensure MTD's hiddenness and maximal detection effectiveness, Liu and Wu (2021) explored the optimal planning and operation of D-FACTS devices by first deriving a novel hiddenness operation condition. These work give primary guidances on effective MTD to system operators as an insurance against possible FDIA. Above research results provide necessary theory foundation for the perturbation-based MTD in power system. However, they have not considered cyber-attacks and countermeasures in special cases.

Given that FDIA was constructed based on limited information of transmission line susceptances, Deng and Liang (2019) provided a new countermeasure to reduce the number of meter measurements/state variables for FDIA detection by preventing the adversary from a certain set of transmission line susceptances. To detect coordinated cyber-physical attack (CCPA) that involved a physical attack followed by a coordinated cyber-attack, Lakshminarayana et al. (2019) identified the MTD design criteria where D-FACTS devices were deployed based on a graph-theoretic approach. This work was improved in Lakshminarayana et al. (2021) to identify the optimal set of links for D-FACTS device deployment. Alerted by recent cybersecurity incidents, Tian et al. (2020) focused on Stuxnet-like (SL) attacks in CPS control loops and proposed the MTD-based SL attack detection framework against different SL attacks. Although these MTDs are capable of thwarting some specific cyber-attacks, they have not considered the operation cost caused by proactively changing system configurations. Therefore, we present a formal design criteria in Physical-MTD to achieve the optimal susceptance perturbation with minimal operation cost for FDIA detection in power system.

Compared to the above references, the novelty of our work is twofold. First, with the exception of our preliminary work in Hu et al. (2021), none of them has created a multidimensional attack space for power system by randomizing attacker's data acquisition into multiple rounds in network communications. The solution requires more moving targets included in the MTD-based method. Second, existing work have designed MTDs that provide only one line of cyber or physical de-

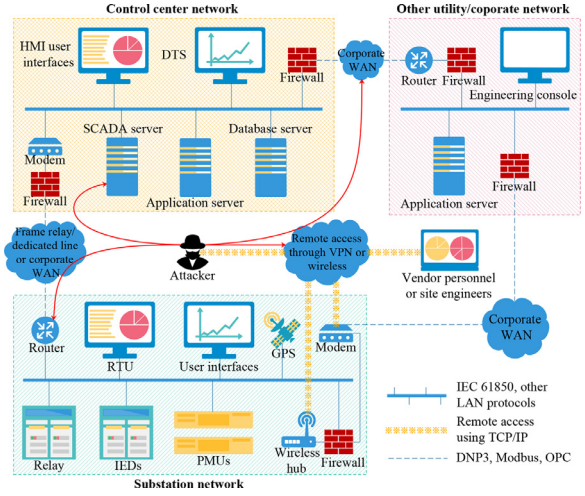

Fig. 3 – SCADA network architecture.

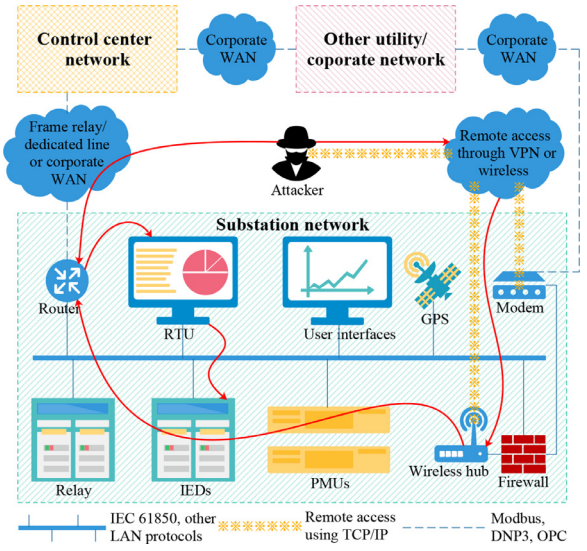

Fig. 4 – Security problems in the SCADA network.

fense for power system against potential cyber-attacks. In fact, many cyber-attacks require a combination of cyber and physical defenses to prevent. We formalize this idea in the context of MTD using a bi-level defense mechanism based on CPMTD.

3. Background and motivation

Modern power system gets very huge with increasing uncertain and unknown cyber risks that may have a serious impact on the involved critical infrastructures. In traditional policy, static system resources and network configurations are always protected against these cyber risks, which are calculated by

Cyber risk = Threats * Vulnerabilities * Consequences

However, this model cannot achieve absolute accuracy because of the extremely time-consuming and costly vulnerability checks in such a vast and complex system. Even if all these vulnerabilities are checked out, the false positive should also be considered. Since intrusions are inevitable, it is wise to thwart cyber-attacks by confusing the attacker with a proactive defense technique.

3.1. *SCADA network*

Supervisory control and data acquisition (SCADA) system plays an important role in ensuring the safe and stable operation of power system by monitoring, controlling, and protecting the involved critical infrastructure resources (Stouffer et al., 2011). Fig. 3 shows the hierarchical network architecture of a SCADA system. Different a lot from the regular communication network, SCADA protocols are more precise for the network traffic where only application specific information is permitted by the master station (MS) in the control center (CC). The communication links are established between the CC and substation network by wireless, wireline, and other hybrid technologies like synchronous optical networking/synchronous digital hierarchy (SONET/SDH) that is usually applied in smart grids. Intelligent electronic devices (IED) in the substation, such as remote terminal units (RTU) and programmable logic controllers (PLC), are located at the edge of communication networks based on TCP/IP with an aggregation of measurement data from end devices, such as relays and phasor measurement units (PMU), to achieve fast local processing.

It has been recently shown that smart attackers are experienced in creating malicious activities based on static network configurations and potential system vulnerabilities in the conventional communication network (Fairley 2016; Langner 2011). For example, they installed backdoors in the embedded IEDs that employed possibly vulnerable firmware for the rootkit, such as Stuxnet worm (Langner 2011), which wreaked havoc to Iranian uranium enrichment facilities by sabotaging the internal centrifuges based on the exposed vulnerabilities in Siemens PLCs. Although legacy security measures like firewall, IPS, and antivirus are already deployed in these IEDs, they are still subjected to underlying strategic threats that can invalidate security enforcement by exploiting static system resources. This indicates that these static characteristics of power system can be potentially dangerous factors that provide the adversary a long-term sitting target. In addition, lack of intelligence disables the detection mechanism in some of the security devices for more complicated cyber-attacks like FDIA..

3.2. *Attack identification in SCADA communications*

Security problems with a specific attack scenario are shown in Fig. 4, where the CC and substation networks are bridged through the wide area network (WAN) whose network traffic is exposed to outside world. By eavesdropping on the DNP3 traffic in communication links that are established between the SCADA Server in the CC and RTU in the substation, the IP addresses of both the communication entities can be traced. Thus, the adversary achieves the possibility of attacking the system by targeting one of them, such as tripping the boot of a relay under the control of the RTU by replaying the legitimate trip command that is issued by the MS in the CC.

Considering such security problems, system operators usually add a firewall or IDS rule in gateway routers and other security devices in the substation for traffic control, by which trip command packets will be discarded if the source IP addresses are detected to be unauthenticated. However, this conventional security best practice is not feasible against sophisticated attackers with the capability of disguising the source IP addresses by legitimate ones. In this case, firewall and IDS are unable to discard the disguised packets with proper authentications via just a detection rule. Although the co-distributed IDSs in both the CC and substation can mitigate such attacks with event correlations, it is too costly and time-consuming to check for every event and this work may result in a unacceptable delay for normal legitimate communications.

3.3. Attack identification in state estimation

Power systems are currently at risk of FDIA, an advanced sustained cyber-attack that maliciously manipulates the results of state estimation by leveraging vulnerabilities of BDD and results in system disruptions. In the DC state estimation, the FDIA model can be described as

$$z_a = z + a = H \cdot \theta + a + e \tag{1}$$

where $z_a \in \mathbb{R}^m$ denotes the compromised measurement vector, $a \in \mathbb{R}^m$ denotes the attack vector, i.e., the injected false data in the measurements, and $z \in \mathbb{R}^m$ denotes the actual measurements without being attacked.

To bypass detection by the BDD mechanism based on the residual, FDIA must satisfy

$$a = H \cdot \Delta\theta \tag{2}$$

In other words, the attack vector must be within the column space of the measurement matrix, i.e., $a \in C(H)$. If (2) is satisfied by the attack vector, the measurement residual in the presence of attacks is consistent with that in the absence of attacks:

$$\begin{aligned} &\left\| z_a - H \cdot \hat{\theta}_{bad} \right\| \\ &= \left\| z + a - H \cdot (\hat{\theta} + \Delta\theta) \right\| \\ &= \left\| z - H \cdot \hat{\theta} + (a - H \cdot \Delta\theta) \right\| \\ &= \| z - H \cdot \theta \| \le \gamma \end{aligned} \tag{3}$$

where γ denotes a preset threshold for the detection confidence. Therefore, in order not to trigger the BDD alarm, the adversary needs to obtain essential measurement information from power system.

Although it is difficult for an adversary to observe H directly, he can estimate H by observing the information related to it. For example, Esmalifalak et al. (2011) and Yu and Chin (2015) estimated the measurement matrix of state estimation by ICA or PCA with power grid measurements. Kim, Tong, Thomas (2015) estimated a set of basis for the column space of the measurement matrix from the observed power grid measurements by the subspace estimation method. Even so, the adversary needs to observe numerous measurements to estimate the measurement matrix. However, when the measurement matrix of power system changes from the current H_0 to a new H, the estimated result obtained by the adversary is still a set of basis for the column space corresponding to H_0. Thus, the FDIA model under the change of the measurement matrix can be described as

$$z_a = H \cdot \theta + H_0 \cdot \Delta\theta + e \tag{4}$$

where H_0 denotes the measurement matrix known to the attacker before changing, H denotes the current measurement matrix known only to the system, and system operators know that the undetectable attack should be located in the column space of the measurement matrix, i.e., $a \in C(H_0)$. In Section 5, we will discuss in depth how to change the measurement matrix to improve the capability of detecting FDIA.

3.4. Need for moving target defense

The idea of MTD has been around for two decades and many achievements have made, especially in the field of cybersecurity (Jajodia et al., 2011). In practice, traditional network system will not change network configurations like IP addresses, port numbers, DNS names, gateway addresses, network protocols, routing policies, and firewall policies over a relatively long period of time for the sake of low-cost operation. The same is true for power system, where physical parameters like network topology (i.e., connectivity among buses), susceptances on transmission lines, and distribution of measurement units are always fixed. This means that power system operates in a highly static environment from an adversary's point of view and he has plenty of time to study system knowledge and explore system vulnerabilities for the development of an impactful cyber-attack.

Different from passive defense techniques focusing on protecting static targets from the attacker, MTD is the concept of confusing the attacker with controlled system change, which can increase (i) the unpredictability of operation states and complexity of system properties, (ii) the cost of data collection and time of attack development, and (iii) the detection probability of sophisticated cyber-attacks (Zhuang et al., 2014). The objective of MTD is to randomize or perturb one or more rounds of data acquisition and expose misleading information to the adversary without affecting the physical system. Considering the CPS nature of power system, only cyber-based or physics-based MTD cannot provide a comprehensive protection because the introduction of system uncertainty only means less attack angles rather than no attack angle, i.e., cyber-attacks are still possible in a compromised environment. In this paper, we propose a combination of cyber-based and physics-based MTDs as CPMTD where both attack prevention and detection are considered, as shown in Fig. 5. Reconnaissance disrupting is what Cyber-MTD focuses on, by which the adversary is hard to guess or know the exact system knowledge. As the first-level defense, Cyber-MTD aims to prevent FDIA during attack preparation. Susceptance perturbing is what Physical-MTD focuses on, by which the adversary is hard to observe the measurement matrix of state estimation. As the second-level defense, Physical-MTD aims to make stealthy FDIA detectable in the execution stage. Based on the bi-level defense mechanism, CPMTD provides a combination of protections for power system.

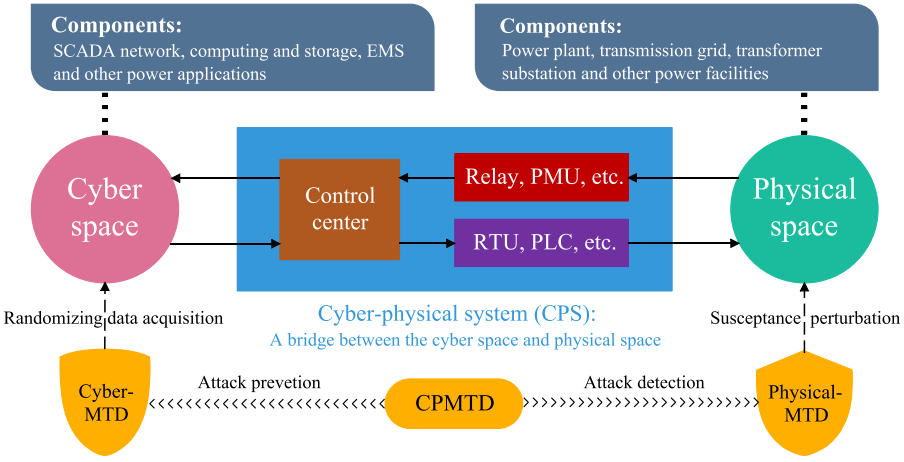

Fig. 5 – A combination of defense strategies based on CPMTD.

4. Cyber-MTD: Disrupting the attacker's reconnaissance in network communications

To increase the uncertainty of system knowledge, we take controlled change in network communications across multiple system dimensions including network protocol (NP), data packet (DP), network group (NG), and routing path (RP). Based on Cyber-MTD, a compromised system can be transformed into a protected system:

$$\langle \boldsymbol{NP}^c, \boldsymbol{DP}^c, \boldsymbol{NG}^c, \boldsymbol{RP}^c \rangle \xrightarrow{\mathbb{C}_{\mathrm{MTD}}(\cdot)} \langle \boldsymbol{NP}^p, \boldsymbol{DP}^p, \boldsymbol{NG}^p, \boldsymbol{RP}^p \rangle \tag{5}$$

where $\mathbb{C}_{\mathrm{MTD}}(\cdot)$ denotes the Cyber-MTD strategy deployed in network communications, as shown in Fig. 6. The idea behind Cyber-MTD is to construct a diversity of these four system properties to expand the attack space, thereby obtaining further unpredictability of attack surface transformation.

4.1. *Diversifying network protocols*

Protocol type and structure can be easily resolved by the attacker in traditional networks because protocols are identified by some fixed structured fields within them. Considering the security liability of the fixed protocol, Cyber-MTD achieves flexible PPs based on protocol oblivious forwarding (POF) for network communications. POF uses a collection of triples $\{type, offset, length\}$ to describe the protocol field, where *type* denotes the data type (e.g., packet data and metadata), *offset* denotes the packet offset from the protocol header, and *length* denotes the packet length (Li et al., 2017). Fig. 7 shows an example of a POF packet that contains a three-layer protocol header processed by three flow tables, where the move-packet-offset and goto-table actions make *offset* point to the next layer of the protocol header.

As a significant improvement over OpenFlow, POF obtains two advantages in packet processing: (i) any field is allowed for the action to modify the packet data, whereas only the match fields are allowed in OpenFlow because of the data pipeline consistency; (ii) the fields are resolved just according to their triples $\{type, offset, length\}$, whereas the match fields are defined by OpenFlow based on the existing experience and can only be extracted by the specialized resolver.

Redundancy is a classic MTD idea to construct a diversity of the system property (Xu et al., 2014). Drawing on this idea, we create diverse PPs by inserting invalid fields into a standard protocol. In the case of TCP/IP, we randomly insert invalid binary strings into the original standard protocol containing MAC, Type, IP, and other structured fields to construct different PPs, as shown in Fig. 8. To enable effective network communications over PPs, all the triples of PPs are shared by the communication entities offline in advance through a secure channel.

Thus, the communication entities can select several PPs to compose a PP pool for random encapsulations of normal data and invalid data. In the POF controller, the PPID of the PP that encapsulates invalid data is marked with the deception flag and the TLL of the PP, i.e., the maximum transmission distance, is marked with the deception distance.

4.2. *Randomizing data encapsulations*

To deter the attacker from rebuilding the communication session, Cyber-MTD decomposes the session message into data fields and encapsulates them in different PPs. The same is done for the deception message consisting of some invalid data to mislead the attacker's data acquisition. Compared with network communications based on a single standard protocol, the risk of information leakage is significantly reduced when the network traffic is transmitted by diverse PPs. In addition, the attacker will take much time in differentiating between normal packets and deception packets.

The data encapsulation process is shown in Fig. 9, where the session message is decomposed equally into j data fields: $\mathrm{SM}=\{\mathrm{ND}_1, \mathrm{ND}_2, \mathrm{ND}_3, \cdots, \mathrm{ND}_j\}$, and the deception message is decomposed equally into k data fields: $\mathrm{DM}=\{\mathrm{ID}_1, \mathrm{ID}_2, \mathrm{ID}_3, \cdots, \mathrm{ID}_k\}$. We select j PPs to encapsulate the normal data: $\mathrm{NP}=\{\mathrm{PP}_{a1}, \mathrm{PP}_{a2}, \mathrm{PP}_{a3}, \cdots, \mathrm{PP}_j\}$, and select k PPs to encapsulate the invalid data: $\mathrm{IP}=\{\mathrm{PP}_{b1}, \mathrm{PP}_{b2}, \mathrm{PP}_{b3}, \cdots, \mathrm{PP}_k\}$.

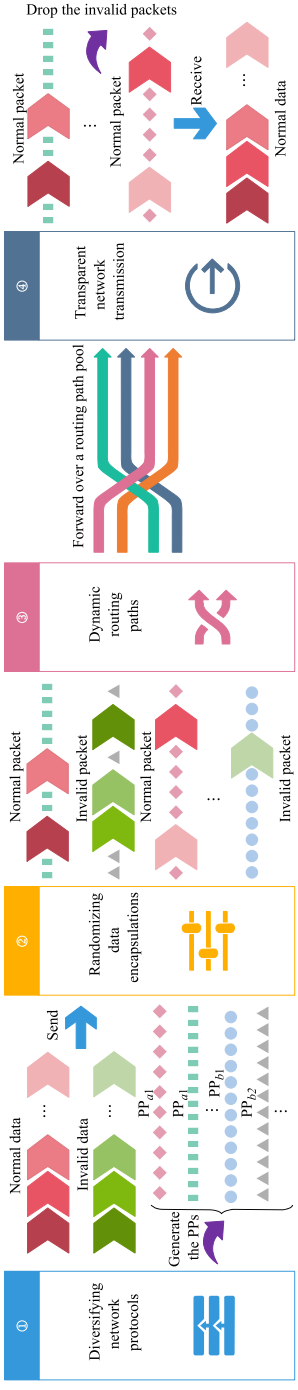

Fig. 6 – Network communication architecture based on Cyber-MTD.

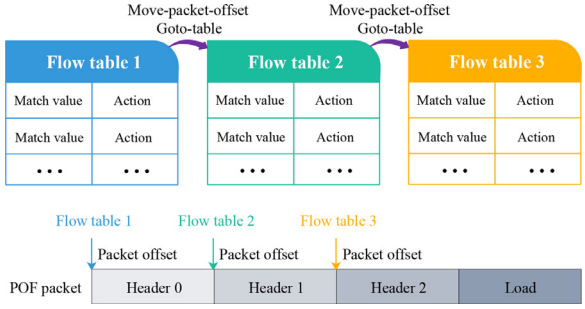

Fig. 7 – POF flow tables and packet processing principle.

4.3. *Dynamic routing paths*

In traditional networks, the optimal routing path is calculated based on the shortest path algorithm and will not be changed in a short-term once the communication link is established (Cherkassky et al., 1996). However, the fixed routing path as a sitting duck for the adversary is likely to expose vulnerabilities of the communication link. Instead of the static routing policy, Cyber-MTD selects some suboptimal routing paths in addition to the optimal one to compose a routing path pool for the dynamic routing policy, as shown in Fig. 10.

Suppose that there are q feasible routing paths between the communication entities: $P = \{p_1, p_2, p_3, \cdots, p_q\}$. $S_{i,r}$ (in_port, out_port) represents the switch on the routing path, where in_port and out_port denote the entry and exit ports between the switch and its neighbors, respectively. Each routing path represents a set of the switches that pass through it: $p_i = \left\{S_{i,1}, S_{i,2}, S_{i,3}, \cdots, S_{i,t_i}\right\}$. After $j + k$ PPs are selected to compose a PP pool: PP=$\{PP_1, PP_2, PP_3, \cdots, PP_{j+k}\}$, the POF controller randomly assigns these PPs to q routing paths for network transmission and each switch achieves fast forwarding of data packets based on PPID identification.

4.4. *Transparent network transmission*

To confuse the attacker in rebuilding the session message, a small amount of invalid data is encapsulated in the PPs as deception packets. Before these deception packets reach any reliable receiving end, POF switches will discard them after a random transmission distance by setting the TLL of the PPs. In this way, Cyber-MTD is not only unburdensome for the receiving ends but also can mislead the attacker on the intermediate nodes. Fig. 10 shows an example of the packet dropping policy, where PP_{a1}, PP_{a2}, PP_{a3}, PP_{b1}, PP_{b2}, and PP_{b3} are sent from Host A to Host B and PP_{b1}, PP_{b2}, and PP_{b3} are discarded by three random nodes where the drop action is issued, respectively. Finally, Host B only receives PP_{a1}, PP_{a2}, and PP_{a3} and is oblivious to these deception packets. On the other hand, the dynamic routing policy is implemented by the POF controller that updates the primary flow table of each switch based on a random algorithm and this update process is also transparent to the end-to-end communication entities.

Suppose that there are x deception packets of size S each transmitted over u routing paths: $P = \{p_1, p_2, p_3, \cdots, p_u\}$ with v nodes of each. To achieve a tradeoff between security ben-

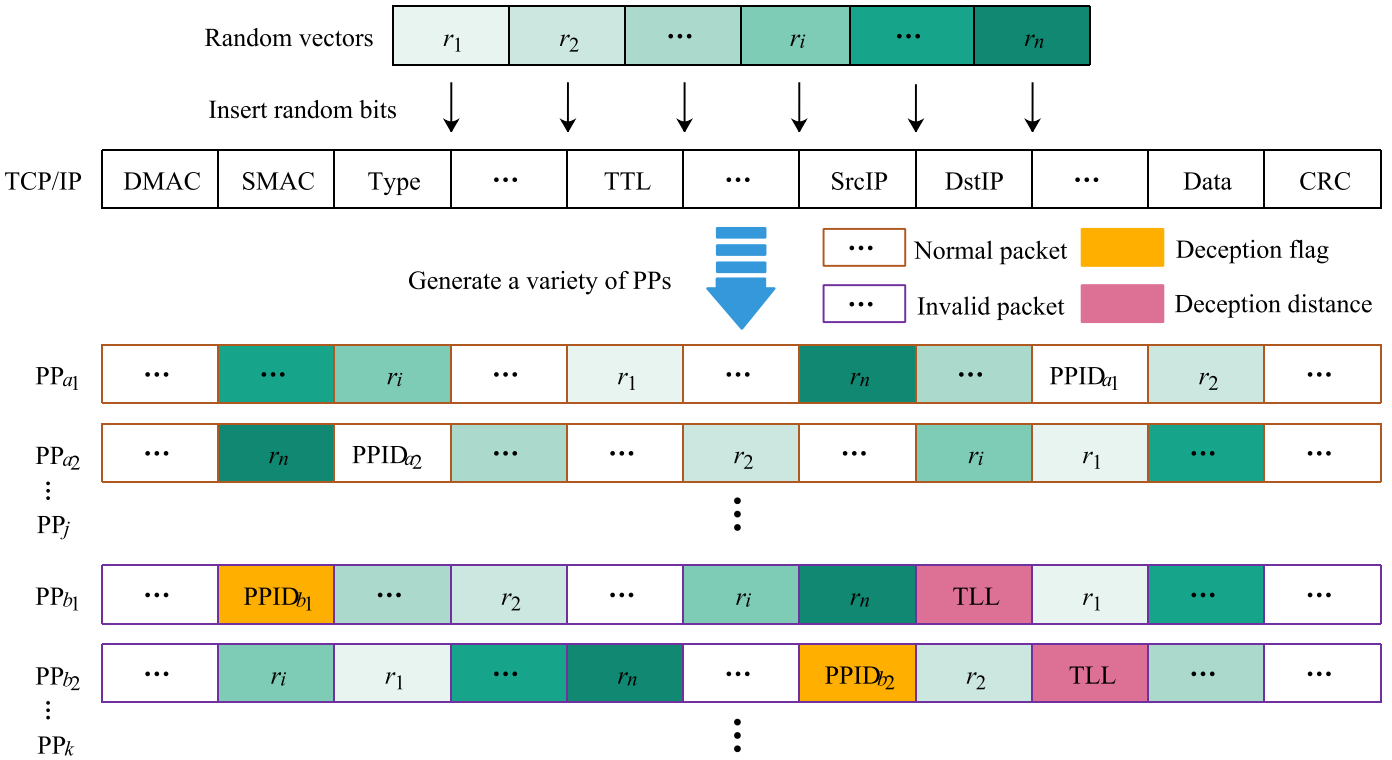

Fig. 8 – Private protocol (PP) construction based on TCP/IP.

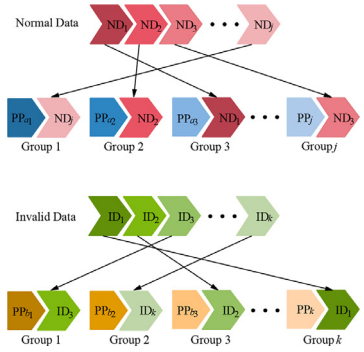

Fig. 9 – Data encapsulations by random matching.

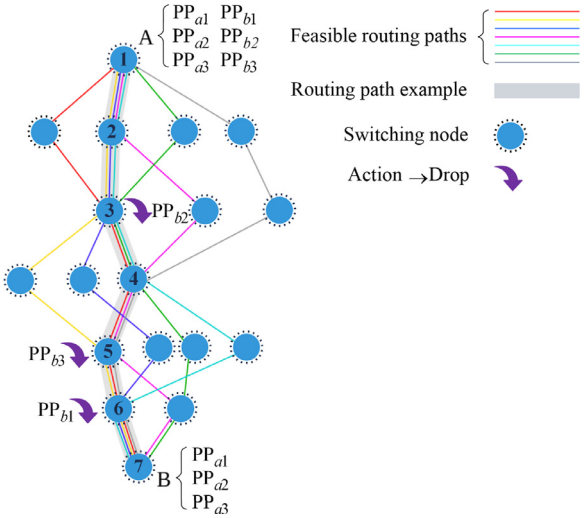

Fig. 10 – Dynamic routing policy and random dropping policy.

efits and bandwidth consumption, the following two metrics are introduced:

Deception coverage. If all nodes on all paths are represented by a $u \times v$ matrix, any deception packet passing through the nodes within the $u \times v$ matrix means that these nodes are deception covered. Since x deception packets are generated by random encapsulations of k PPs: IP=$\{PP_{b1}, PP_{b2}, PP_{b3}, \cdots, PP_k\}$, the average number of deception packets for each PP are $\frac{x}{k}$. Given that these PPs are forwarded by one of the u routing paths each time and these deception packets are discarded by one of the v nodes on each routing path with probability ρ, the average deception distance is $E = \rho v$. Thus, the deception coverage can be calculated by

$$DC = \frac{\frac{x}{k}Ek}{uv} = \frac{x\rho v}{uv} = \frac{x\rho}{u} \tag{6}$$

When the deception coverage is satisfied, the number of deception packets x is inversely proportional to probability ρ. For example, $x > 20$ can cover all nodes when $\rho = 0.5$, $u = 10$.

Transmission loss. The actual bandwidth consumption of network transmission based on the packet dropping policy can be calculated by

$$TL = \frac{(\frac{x}{k}S)Ek}{Bv} = \frac{(xS)\rho v}{Bv} = \frac{(xS)\rho}{B} \tag{7}$$

where B denotes the total bandwidth. However, the impact of deception packets on bandwidth consumption can be reduced by controlling the number of them and adjusting the probability in the random dropping policy.

5. Physical-MTD: Invalidating the attacker's knowledge in state estimation

To improve the detection probability of FDIA, we analyze the detection conditions for general and specific FDIAs in the presence of susceptance perturbation and design an attack detector with an enhanced capability of detecting FDIA. Considering the impact of susceptance perturbation on operation cost, we characterize the dependency between the transmission line loss and susceptance perturbation by the linear sensitivity matrix and formulate an optimization for susceptance perturbation based on a cost-benefit analysis.

5.1. *Susceptance perturbation using D-FACTS*

Distributed flexible AC transmission system (D-FACTS) devices including distributed static series compensators (DSSC) and distributed series compensators (DSI) are directly connected to transmission lines, which achieves the possibility of susceptance perturbation (Divan and Johal 2005). To optimize the power flow on transmission lines, D-FACTS devices are widely distributed in power grids, as shown in Fig. 11, where the perturbation in transmission line susceptances must satisfies the following constraints:

i. The upper and lower limits of the perturbation depend on the capability of D-FACTS devices:

$$\underline{\tau} \cdot x \le \Delta x \le \overline{\tau} \cdot x \tag{8}$$

where $x \in \mathbb{R}^p$ denotes the susceptance vector of all transmission lines in a power grid, $\Delta x \in \mathbb{R}^p$ denotes the perturbation of the susceptance vector, p denotes the number of transmission lines, and $\underline{\tau} \cdot x$, $\overline{\tau} \cdot x$ denote the minimum and maximum perturbations of the susceptance vector, respectively. For example, the range of DSSC is $\pm 10\% \sim 20\%$ of the actual transmission line susceptance.

ii. The perturbation in transmission line susceptances must not be too small to improve the detection probability of FDIA:

$$\Delta x_{ij} = 0 \text{ or } \left|\Delta x_{ij}\right| \ge \omega \cdot \left|x_{ij}\right|, i, j \in A \tag{9}$$

where x_{ij} denotes the susceptance of the transmission line connecting buses i and j, and ω denotes the preset maximum perturbation in transmission line susceptances.

To estimate the system state, it is necessary to measure the power flow and current magnitude of transmission lines,

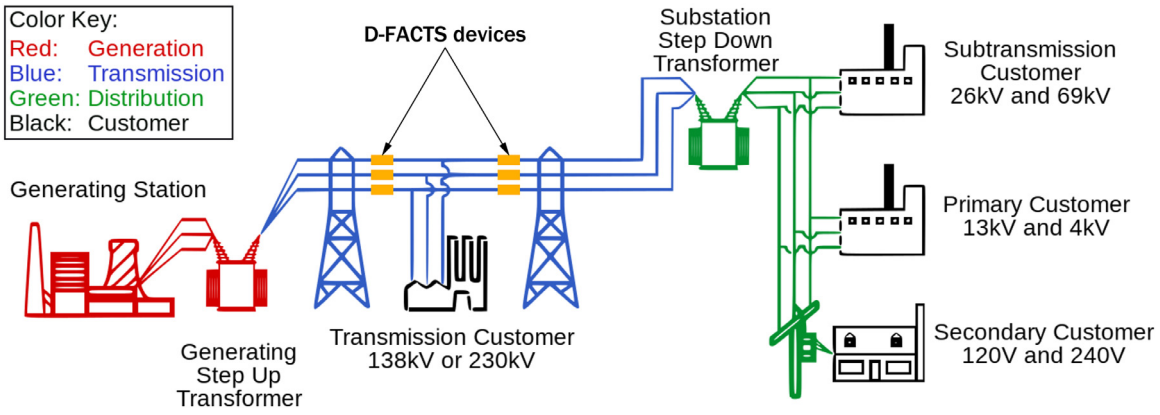

Fig. 11 – D-FACTS devices on transmission lines.

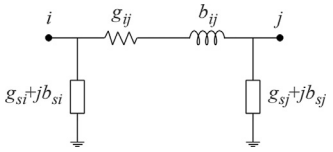

Fig. 12 – Two-port π-model of a branch.

the power injection and voltage amplitude on buses, and other power grid parameters (Abur and Exposito, 2004). Based on the two-port π-model, as shown in Fig.12, the active and reactive power flows of the transmission line connecting buses i and j and the system state can be related as

$$\begin{aligned} P_{ij} &= V^2 \cdot (g_{si} + g_{ij}) - V_i \cdot V_j \cdot (g_{ij} \cdot \cos\theta_{ij} + b_{ij} \cdot \sin\theta_{ij}) \\ Q_{ij} &= -V^2 \cdot (b_{si} + b_{ij}) - V_i \cdot V_j \cdot (g_{ij} \cdot \sin\theta_{ij} - b_{ij} \cdot \cos\theta_{ij}) \end{aligned} \tag{10}$$

The current of the transmission line connecting buses i and j can be calculated by

$$I_{ij} = \frac{\sqrt{P_{ij}^2 + Q_{ij}^2}}{V_i} \tag{11}$$

Based on (10), (11) can be extended to

$$I_{ij} = \sqrt{\left(g_{ij}^2 + b_{ij}^2\right) \cdot \left(V_i^2 + V_j^2 - 2 \cdot V_i \cdot V_j \cdot \cos\theta_{ij}\right)} \tag{12}$$

In (10)–(12), V_i, θ_i denote the voltage amplitude and phase angle on bus i, respectively, $\theta_{ij} = \theta_i - \theta_j$, $g_{ij} + jb_{ij}$, $g_{si} + jb_{si}$ denote the admittance and shunt admittance of the transmission line connecting buses i and j, respectively. Given the admittance, the resistance can be obtained:

$$r_{ij} + j \cdot x_{ij} = \frac{1}{g_{ij} + j \cdot b_{ij}} \tag{13}$$

Thus, g_{ij}, b_{ij}, and the resistance can be related as

$$g_{ij} = \frac{r_{ij}}{r_{ij}^2 + x_{ij}^2}, \; b_{ij} = \frac{-x_{ij}}{r_{ij}^2 + x_{ij}^2} \tag{14}$$

Given the current and resistance, the active power loss of the transmission line connecting buses i and j can be expressed as

$$P_{ij}^l = |I_{ij}|^2 \cdot r_{ij} = \frac{r_{ij}}{r_{ij}^2 + x_{ij}^2} \cdot (V_i^2 + V_j^2 - 2 \cdot V_i \cdot V_j \cdot \cos\theta_{ij}) \tag{15}$$

Thus, the active power loss of a power grid can be expressed as

$$P^l = \sum_{i=1}^{n} \sum_{j=1}^{n} P_{ij}^l, \; i \neq j \tag{16}$$

Given active power loss P_{ij}^l and reactance x_{ij}, the linear sensitivity relationship between the transmission line loss and susceptance perturbation can be described as

$$\frac{dP^l}{dx_{ij}} = \frac{\partial P^l}{\partial x_{ij}} + \frac{\partial P^l}{\partial s_{(\theta,V)}} \cdot \frac{\partial s_{(\theta,V)}}{\partial x_{ij}} \tag{17}$$

where $\partial s_{(\theta,V)}$ denotes the cascade vector of all voltage amplitudes and all phase angles in a power grid, and $\frac{\partial s_{(\theta,V)}}{\partial x_{ij}}$ can be derived and calculated referring to Rogers and Overbye (2008).

5.2. *Complete and incomplete detection conditions*

Based on (4), the FDIA model without considering the measurement noise can be expressed as

$$z_a = H \cdot \theta + H_0 \cdot \Delta\theta \tag{18}$$

In this model, we define the undetectable attack as

Definition 1. (Undetectable attack for susceptance perturbation) In power system, $\forall a = H_0 \cdot \Delta\theta, \Delta\theta \in \mathbb{R}^{n-1}, \Delta\theta \neq 0$ cannot be detected by H, iff $H \cdot \theta + H_0 \cdot \Delta\theta = H \cdot \theta'$ for $\exists\theta, \theta'$.

Accordingly, the general condition for attack detection can be described as

Remark 1. (General attack detection condition) The hidden attack in the original system $a = H_0 \cdot \Delta\theta, \Delta\theta \in \mathbb{R}^{n-1}$ can be detected by H, iff $H \cdot (\theta' - \theta) \neq H_0 \cdot \Delta\theta$ for $\forall\theta, \theta'$.

For ease of calculation, Remark 1 can be equivalent to

Theorem 1. (Complete attack detection condition) The hidden attack in the original system $a = H_0 \cdot \Delta\theta, \Delta\theta \in \mathbb{R}^{n-1}$ can be detected by H, iff $r(M) = 2 \cdot (n-1)$, where $M = [H_0 \; H]$, $H_0, H \in \mathbb{R}^{m \times (n-1)}$.

Proof. (Sufficiency) Suppose that the hidden attack in the original system $a = H_0 \cdot \Delta\theta, \Delta\theta \in \mathbb{R}^{n-1}$ can be detected by H, we have that $H \cdot (\theta' - \theta) \neq H_0 \cdot \Delta\theta$ holds for $\forall\theta, \theta', \Delta\theta \neq 0$, which can be rewritten as

$$\begin{bmatrix} H_0 & H \end{bmatrix} \cdot \begin{bmatrix} \Delta\theta \\ \theta - \theta' \end{bmatrix} \neq 0 \tag{19}$$

Thus, the non-zero vector $\begin{bmatrix} \Delta\theta^T & (\theta - \theta')^T \end{bmatrix}^T$ cannot exist in $N(M)$ for $\forall\Delta\theta \neq 0$. Considering that $r(H) = n-1$, $H \cdot (\theta' - \theta) \neq 0$ holds for $\Delta\theta = 0, \theta - \theta' \neq 0$. This means that (19) holds and such non-zero vector is also not in $C(M)$. Therefore, we have that $N(M) = \{0\}$, i.e., $r(M) = 2 \cdot (n-1)$.

(Necessity) Suppose that $r(M) = 2 \cdot (n-1)$, we have that $N(M) = \{0\}$. This means that (19) holds for $\forall\Delta\theta \neq 0$. Therefore, we have that $H \cdot (\theta' - \theta) \neq H_0 \cdot \Delta\theta$ holds for $\forall\theta, \theta', \Delta\theta \in \mathbb{R}^{n-1}, \Delta\theta \neq 0$, and the attack is detectable for $\forall a = H_0 \cdot \Delta\theta, \Delta\theta \neq 0$.

Owing to the harsh requirement of Theorem 1 for the topology of power grids and deployment of power sensors, complete attack detection cannot be achieved in all power systems. However, partial FDIAs can still be detected in some systems that do not satisfy Theorem 1 but satisfy the following condition:

Theorem 2. (Incomplete attack detection condition) The specific attack in the original system $a = H_0 \cdot \Delta\theta, \Delta\theta \in \mathbb{R}^{n-1}$ for $i \in S^d, \Delta\theta_i \neq 0$ can be detected by H when $r([H_0^d\ H]) = n - 1 + |S^d|$, where S^d denotes the index set of column vectors in H_0 that are not linearly dependent on those in H, and H_0^d denotes a submatrix of column vectors indexed by S^d.

Proof. Since $r([H_0^d\ H]) = n - 1 + |S^d|$, column vectors in $[H_0^d\ H]$ are linearly independent of each other. Thus, we have that $\sum_{i\in S^d} \Delta\theta_i \cdot h_{0,i} \neq \sum_{j\in N_{-r}} \theta_j \cdot h_j$ holds for $\forall i \in S^d, \Delta\theta_i \neq 0, \theta \in \mathbb{R}^{n-1}$, where $h_{0,i}, h_j$ denote the ith column vector in H_0 and the jth column vector in H, respectively, and N_{-r} denotes the index set of column vectors in H of the power grid except the reference bus. Since $h_{0,i}, i \notin S^d$ is linearly dependent on column vectors in H, we have that θ' exists for $\forall\Delta\theta_i$ such that $\sum_{i\notin S^d} \Delta\theta_i \cdot h_{0,i} = \sum_{j\in N_{-r}} \theta_j \cdot h_j$. Thus, we have that $a - \sum_{i\notin S^d} \Delta\theta_i \cdot h_{0,i} \neq \sum_{j\in N_{-r}} \theta_j \cdot h_j$ holds for $\forall a = H_0 \cdot \Delta\theta$, where $\Delta\theta_i \neq 0, i \in S$, i.e., we have that $a = H_0 \cdot \Delta\theta$ exists for $i \in S^d, \Delta\theta_i \neq 0$ such that $a \neq \sum_{j\in N_{-r}} (\theta_j + \theta_j') \cdot h_j$. This means that such specific attack vector is not in $C(H)$, i.e., the attack is detectable.

Based on Theorem 2, the detection probability of the specific FDIA and the rank of matrix M can be related as

Remark 2. The detection probability of the specific FDIA increases with the increase of the number of the attacked states and the rank of matrix M that satisfies $r(M) = n - 1 + |S^d|$ since $r([H_0\ H]) = r([H_0^d\ H])$.

Therefore, the optimization of MTD's effectiveness depends on the maximization of the rank of matrix M.

5.3. *MTD's effectiveness and operation cost*

To maximize the detection probability of FDIA and minimize the physical impact on power system caused by susceptance perturbation, we formalize the tradeoff between MTD's effectiveness and operation cost as

$$\begin{aligned} &\min_{\Delta x} \{ -\alpha \cdot r(M) + M^{ls} \cdot \Delta x \} \\ &\text{s.t. } (8), (9) \end{aligned} \tag{20}$$

where α denotes the accommodation coefficient that must be positive and sufficiently large for the priority of maximizing the detection probability of FDIA, and M^{ls} denotes the linear sensitivity matrix calculated by (17).

To maximize the rank of matrix M, we update the transmission line susceptance in a power grid one by one based on

Theorem 3. If the transmission line susceptance changes from x_{ij} to x'_{ij} causing the increase of the rank of matrix M that satisfies $r(M(x_{ij})) < \min\{m, 2\cdot(n-1)\}$, i.e., $r(M(x'_{ij})) > r(M(x_{ij}))$, we have that $r(M(x''_{ij})) > r(M(x_{ij}))$ holds for $\forall x''_{ij} \neq x'_{ij} \neq x_{ij}$, where $M(x_{ij}), M(x'_{ij})$, and $M(x''_{ij})$ denote a matrix M when the susceptance on the transmission line connecting buses i and j is x_{ij}, x'_{ij}, and x''_{ij}, respectively.

Proof. First, we take $M^s(x_{ij})$ indexed by row index set v_r and column index set v_c as the submatrix of $M(x_{ij})$ indexed by row index set V_r and column index set V_c, where $|v_r| = r(M(x_{ij})) + 1, v_r \in V_r$, $|v_c| = r(M(x_{ij})) + 1, v_c \in V_c$, i.e., $M^s(x_{ij}) = M(x_{ij})_{[v_r, v_c]}$, $r(M^s(x_{ij})) \leq r(M(x_{ij}))$. Then, we consider two cases regarding the determinant of $M^s(x_{ij})$: 1) all nonzero elements in $M^s(x_{ij})$ are irrelevant to x_{ij}; 2) some nonzero elements in $M^s(x_{ij})$ denoted as $h_{ij}, \cdots, h_{kl}$ are relevant to x_{ij}.

Case 1: We have that $\det(M^s x'_{ij})) = (M^s(x_{ij})) = 0$ holds for $\forall x'_{ij} \neq x_{ij}$, i.e., $r(M^s(x_{ij})) \leq r(M(x_{ij}))$.

Case 2: The determinant of $M^s(x_{ij})$ can be expanded by referring to Geelen (1999):

$$\begin{aligned} \det(M^s(x_{ij})) = 1/x_{xj} \cdot (\beta \cdot \det(M^s(x_{ij})_{[v_r\setminus\{i\}, v_c\setminus\{j\}]}) + \\ \cdots + \lambda \cdot \det(M^s(x_{ij})_{[v_r\setminus\{k\}, v_c\setminus\{l\}]}) + \det(M^s(\infty)) + b = 0 \end{aligned} \tag{21}$$

where $M^s(\infty)$ denotes a matrix $M^s(x_{ij})$ when the susceptance is $x_{ij} \to \infty$ on the transmission line connecting buses i and j, and b is a constant. This is a linear function of $1/x_{ij}$ with multiplier $k = \beta \cdot \det(M^s(x_{ij})_{[v_r\setminus\{i\}, v_c\setminus\{j\}]}$. If $k \neq 0$, $\exists! x$ makes $\det(x_{ij}) = 0$ hold, i.e., we have that $\det(M(x'_{ij})) \neq 0$, $r(M(x'_{ij})) = r(M(x_{ij})) + 1$ hold for $\forall x'_{ij} \neq x_{ij}$; otherwise, we have that $\det(M^s(x_{ij})) = 0$ holds for $\forall x'_{ij} \neq x_{ij}$, i.e., $r(M^s(x'_{ij})) \leq r(M(x_{ij}))$.

Since $r(M(x'_{ij})) = \max\{M(x'_{ij})_{[v_r, v_c]} | v'_r \in V_r, v'_c \in V_c, |v'_r| \geq r(M(x_{ij})) + 1, |v'_c| \geq r(M(x_{ij})) + 1\}$, $\exists M^s(x_{ij})$ makes $r(M^s(x'_{ij})) > r(M(x_{ij})) \geq r(M^s(x_{ij}))$ hold if $\exists x'_{ij} \neq x_{ij}$ makes $r(M(x'_{ij})) > r(M(x_{ij}))$ hold. Therefore, we have that $r(M(x''_{ij})) \geq r(M^s(x''_{ij})) > r(M(x_{ij}))$ holds for $\forall x''_{ij} \neq x_{ij}$.

The update steps of transmission line susceptances are as follows: 1) check whether the rank of matrix M increases after changing transmission line susceptance x_{ij}; 2) if the rank of matrix M increases, update transmission line susceptance x_{ij} by $x_{ij} + \Delta x_{ij}$; 3) check whether all transmission line susceptances in the power grid are traversed before changing another transmission line susceptance; 4) if the rank of matrix M does not increase after traversing all transmission line susceptances in the power grid or $r(M) = \min\{m, 2\cdot(n-1)\}$, finish the update; otherwise, start a new round of the update.

To calculate the increasing operation cost, the transmission line loss resulted from the change of the transmission line susceptance in each update can be modeled as

$$\begin{aligned} \min_{\Delta x^{(k)}} \quad & M^{ls}(x^{(k)}) \cdot \Delta x^{(k)} \\ \text{s.t.} \quad & \underline{\tau} \cdot x_{ij}^{(0)} \leq \Delta x_{ij}^{(k)} \leq \overline{\tau} \cdot x_{ij}^{(k)} \\ & |\Delta x_{ij}^{(k)}| \geq \gamma \cdot |x_{ij}^{(0)}| \\ & \Delta x_{-ij}^{(k)} = 0 \end{aligned} \tag{22}$$

where $x^{(k)}$ denotes the susceptance vector of all transmission line susceptances in a power grid in the kth update, $M^{ls}(x^k)$ denotes the linear sensitivity matrix under the state of $x^{(k)}$ in the kth update, and $x^{(k)}_{-ij}$ denotes transmission line susceptances in $x^{(k)}$ except $x^{(k)}_{ij}$.

To minimize the operation cost, we calculate $\Delta x^{(k)}_{ij}$ by solving (22) as the optimal susceptance perturbation and update linear sensitivity matrix $M^{ls}(x^{(k-1)})$ by $M^{ls}(x^{(k)})$ at step 2) in the update. However, the final operation cost related to the traversal sequence of transmission line susceptances does not represent the global optimal solution and the final rank of matrix M also does not represent the maximal rank for the optimal susceptance perturbation because we just minimize the impact of susceptance perturbation on the operation cost in each round of updates.

5.4. *Construction of attack detector*

Referring to Pasqualetti et al. (2013), we design an attack detector with an input $\Lambda = \{H_0, H, z_a\}$ and an output $\Psi(\Lambda) = \{\psi_1(\Lambda), \psi_2(\Lambda)\}, \psi_1(\Lambda) \in \{\text{True}, \text{False}\}, \psi_2(\Lambda) \in \mathbb{R}^m$. If an attack vector a can be detected by the detector, we have that $\psi_1(\Lambda) = \text{True}$ & $\psi_2(\Lambda) = a$; otherwise, we have that $\psi_1(\Lambda) = \text{False}$ & $\psi_2(\Lambda) = \text{None}$.

In a noiseless system, an attack vector $a = H_0 \cdot \Delta\theta$ can be detected if $a \notin C(H)$ according to our discussion in Section 5.2. For a normal measurement vector $z = H \cdot \theta$, we have that $z \in C(H)$. Similarly, a compromised measurement vector $z_a = H \cdot \theta + H_0 \cdot \Delta\theta$ can be detected if $z_a \notin C(H)$. Thus, $\psi_1(\Lambda)$ can be calculated by

$$\psi_1(\Lambda) = \begin{cases} \text{True} & r([H\ z_a]) > r(H) \\ \text{False} & \text{otherwise} \end{cases} \tag{23}$$

In an actual system, the impact of the measurement noise on the accuracy of detection results should be considered. To detect FDIA in a noisy system, we introduce the measurement residual to calculate $\psi_1(\Lambda)$ by

$$\left\| z_a - H \cdot (H^T \cdot H)^{-1} \cdot H^T \cdot z_a \right\|^2 > \gamma^2 \tag{24}$$

where γ denotes the detection confidence. Similar to (23), the attack detector will alarm if $\psi_1(\Lambda)$ satisfies (24).

Whether in the noiseless or noisy systems, if the changes in system states, outside index set S^d, are set as zeros, $\psi_2(\Lambda)$ can be calculated by

$$\psi_2(\Lambda) = H \cdot \begin{bmatrix} \Delta\hat{\theta}_i \\ 0 \end{bmatrix} \tag{25}$$

where $\Delta\hat{\theta}_i$ denotes the estimated change of the phase angle that represents the system state caused by attack vector a, $i \in S^d$. Based on Theorem 2, $\Delta\hat{\theta}_i$ can be calculated by

$$\begin{bmatrix} \Delta\hat{\theta}_i \\ \hat{\theta} \end{bmatrix} = \left(\left[H_0^d\ H \right]^T \cdot \left[H_0^d\ H \right] \right)^{-1} \cdot \left[H_0^d\ H \right]^T \cdot z_a \tag{26}$$

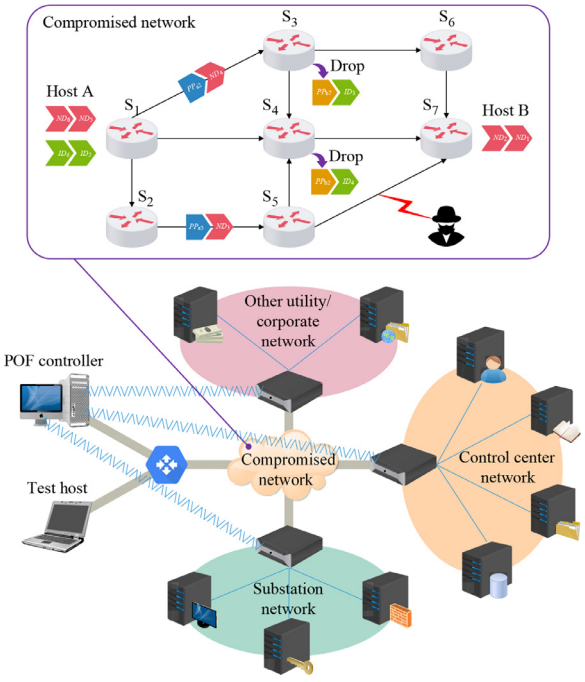

Fig. 13 – Cyber-physical testbed.

6. Evaluation

We develop a cyber-physical testbed that simulates both the cyber and physical infrastructures of power system to evaluate CPMTD, as shown in Fig. 13.

As communication networks of the kinds used by SCADA, we used the GENI testbed, a nationwide network experiment platform, to construct three different function networks to deliver commands and measurements and each of them had several specific servers that were connected to an edge switch by DNP3 protocol, a protocol widely used in US power grids. We constructed a backbone network by deploying real SDN-enabled hardware switches and virtual machines in different physical locations to support communications between the POF controller, the test host, and edge switches. We assumed that there was a compromised network targeted by the attacker in the backbone network.

On the other hand, we used MATPOWER to simulate the part of physical infrastructures Zimmerman et al. (2011). We assumed that the control center issued a command to the substation or the other utility across communication networks, and built the network traffic by estimating the impact of the command on measurements.

6.1. *Network security analysis*

We discuss the cyber-attack in both the local and global cases: data packet attack and session message attack, which are described in a cyber kill chain as shown in Fig. 14, where M, N, R denote more than one attack, 1 denotes a single attack, and 0 denotes attack irrelevance. These two kinds of cyber-attacks can cause damage on network communications in different degrees. With the target of local network resources, data

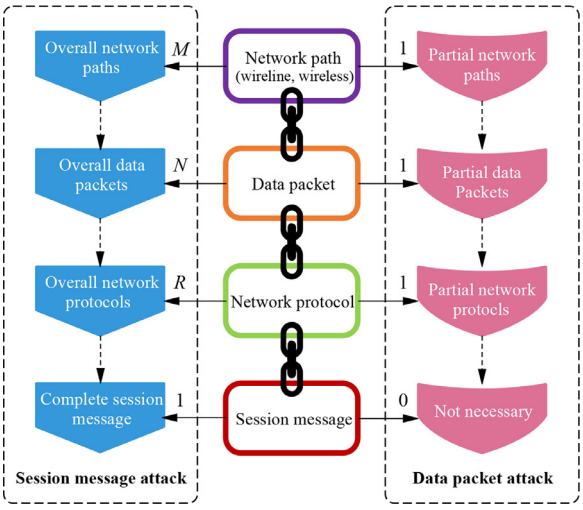

Fig. 14 – Cyber kill chain.

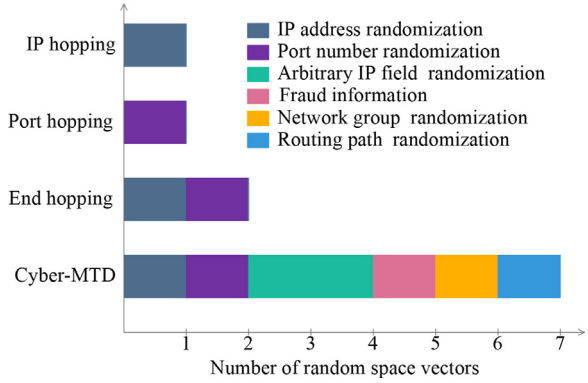

Fig. 15 – Random space of different network-based MTDs.

packet attack is launched by monitoring some of the network paths and capture a small portion of the data packets to trace the source and destination IP addresses. With the target of global network resources, session message attack is launched by monitoring all network paths and capture all data packets to rebuild the session message. The objective of network-based MTD against cyber-attacks is to disrupt one or more loops of the cyber kill chain.

First, we introduce some impact factors for the cyber-attack: the size of network protocol space is denoted as Γ, the size of routing path space is denoted as Φ, and M data packets including m normal data and ϵ invalid data are encapsulated in δ PPs, which are forwarded by $\hbar$ routing paths. To analyze these two attack cases, we define the cyber-attack probability as

$$\Pr(\mathrm{CA}) = \Pr(A_{np}(\rho), A_{rp}(\kappa), A_{pp}(\xi), A_{sm}(\varpi)) \tag{27}$$

where A_{np} denotes the incident of intercepting the network protocol, ρ denotes the number of protocol types, A_{rp} denotes the incident of invading the routing path, κ denotes the number of routing paths, A_{pp} denotes the incident of inversely resolving the PP, ξ denotes the number of PPs, A_{sm} denotes the incident of rebuilding the session message, and ϖ denotes the number of session messages.

In traditional networks, a standard protocol is used for traffic forwarding, i.e, $\Gamma = 1$. The fixed standard protocol provides a sitting target for the adversary. There are already network-based MTDs achieving dynamic network protocols by field randomization, such as IP hopping (Antonatos et al., 2007), port hopping (Lee and Thing, 2004), and end hopping (Shi et al. 2007). However, all these network-based MTDs have very limited random space for the network protocol compared with Cyber-MTD, as shown in Fig. 15. Even the two-way IP hopping with the maximum random space in IPv4 can achieve $\Gamma = 232$ in an ideal case, whereas only the class C IP address can be used for IP hopping in most cases. In contrast, Cyber-MTD with a larger random space can obtain a larger defense entropy.

6.1.1. *Data packet attack*

This is a weak security attack for which the entire session message does not need to be rebuilt. To make a successful data packet attack, the adversary only need to intercept one or more PPs with their structures inversely resolved. Even if the data load of the PP is written in ciphertext or only part of the data packets are captured, data packet attack can still be achieved by tracing the source and destination information in the heads of these PPs.

The joint probability of M data packets falling on any path that the adversary monitors can be expressed as

$$\begin{aligned}&\Pr(A_{nr}(\kappa), A_{ms}(\varpi)|\forall\varpi \in [1, M])\\ &= 1 - \left(1 - \tfrac{1}{\kappa}\right)^{\max(\varpi)} = 1 - \left(1 - \tfrac{1}{\kappa}\right)^{M}\end{aligned} \tag{28}$$

When $M \gg \hbar$, the possibility that the adversary captures a data packet is an increasing function of M. Thus, the probability of data packet attack can be defined as

$$\begin{aligned}P_{\mathrm{Loc}} &= \Pr(\mathrm{CA}|\forall\rho \in [1, \rho], \forall\kappa \in [1, \hbar], \forall\varpi[1, M])\\ &= \Pr(A_{np}(\rho), A_{rp}(\kappa), A_{pp}(\xi), A_{sm}(\varpi)|\\ &\quad \forall\rho \in [1, \rho], \forall\kappa \in [1, \hbar], \forall\varpi[1, M])\end{aligned} \tag{29}$$

The objective of our evaluation is to find the upper limit of P_{Loc}. In this attack case, it is equivalent for the adversary to capture any data packet or intercept any network protocol because he has no intention of understanding them. As we have just analyzed, the condition for a successful data packet attack is $\xi \geqslant 1$. In this paper, we take the successful condition as $\xi = 1$, i.e., the adversary can obtain the source and destination information by inversely resolving the captured data packets for the structure of only one PP.

$$\begin{aligned}P_{\mathrm{Loc}} &= \Pr(A_{np}(\rho), A_{rp}(\kappa), A_{pp}(\xi), A_{sm}(\varpi)|\\ &\quad \forall\rho \in [1, \rho], \forall\kappa \in [1, \hbar], \forall\varpi[1, M], \xi = 1)\\ &= \Pr(A_{rp}(\kappa), A_{pp}(\xi), A_{sm}(\varpi)|\\ &\quad \forall\kappa \in [1, \hbar], \forall\varpi \in [1, M])\\ &\leqslant \Pr(A_{pp}(\xi)|\xi = 1)\Pr(A_{rp}(\kappa), A_{sm}(\varpi)|\\ &\quad \forall\kappa \in [1, \hbar], \forall\varpi \in [1, M])\\ &= \Pr(A_{pp}(\xi)|\xi = 1)(1 - (1 - \tfrac{1}{\kappa})^{M})\\ &= \lim_{M\to\infty} \Pr(A_{pp}(\xi)|\xi = 1)\end{aligned} \tag{30}$$

Given the size of network protocol space Γ of the PPs that are assumed to be generated on uniform distribution,

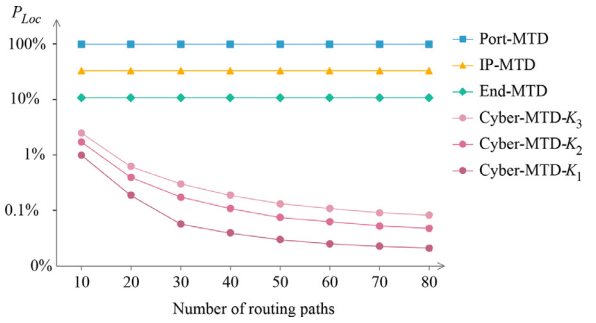

Fig. 16 – Probability of successful data packet attacks.

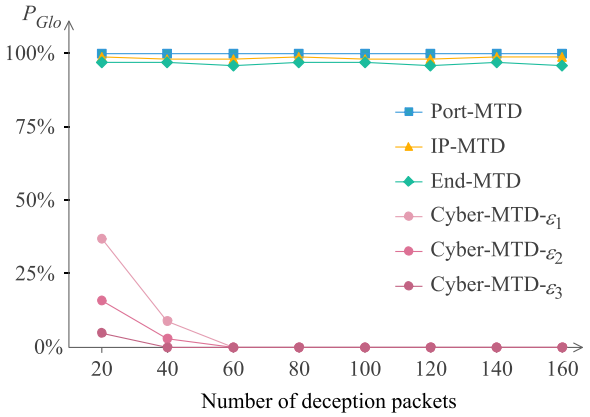

Fig. 17 – Probability of successful session message attacks.

the probability of inversely resolving a PP can be obtained by $\Pr(A_{pp}(\xi)|\xi = 1) = \frac{1}{\Gamma}$. This means that the probability of inversely resolving a PP is directly related to the network protocol space. Fig. 16 shows the security performance of various network-based MTDs against data packet attacks, where $\kappa_1 = 1, \kappa_2 = 2, \kappa_3 = 4$ and each kind of network-based MTDs undergoes 1000 attack attempts. Cyber-MTD can prevent more than 90% of the data packet attacks because when the number of routing paths increases, the probability of data packets falling on insecure paths drops dramatically, which means the cost of capturing data packets for the adversary rises substantially with the expansion of the random space. However, more than 10% of the data packet attacks cannot be prevented by the other network-based MTDs once the routing paths are compromised.

6.1.2. *Session message attack*

This is a more demanding attack than the data packet attack to rebuild the session message, because the adversary needs to capture all data packets in a communication session with the capability of inversely resolving them for the PPs. Thus, the probability of session message attack can be defined as

$$P_{Glo} = \Pr(A_{np}(\rho), A_{rp}(\kappa), A_{pp}(\xi), A_{sm}(\varpi)) = \begin{cases} \min(P_{Glo}) = \Pr(A_{rp}(\kappa))\Pr(A_{np}(\rho), A_{pp}(\xi), A_{sm}(\varpi)|A_{rp}(\kappa)), \kappa = 1 \\ \max(P_{Glo}) = \Pr(A_{rp}(\kappa))\Pr(A_{np}(\rho), A_{pp}(\xi), A_{sm}(\varpi)|A_{rp}(\kappa)), \kappa = \hbar \end{cases} \tag{31}$$

First, we analyze the best case for the adversary, i.e., $\Pr(A_{rp}(\kappa)) = 1$, $\rho = \delta$, and $\varpi = M$. In this case, we assume that the adversary can identify m normal data packets from M data packets if the PPs are inversely resolved. Thus, we just need to consider the probability of inversely resolving the PPs:

$$\begin{aligned} \max(P_{Glo}) &= \Pr(A_{rp}(\kappa))\Pr(A_{np}(\rho), A_{pp}(\xi), A_{sm}(\varpi)|A_{rp}(\kappa)) \\ &= \Pr(A_{sm}(\varpi))\Pr(A_{np}(\rho), A_{pp}(\xi)|A_{sm}(\varpi)) \\ &= \Pr(A_{np}(\rho), A_{pp}(\xi)) \\ &= \prod_{\lambda=0}^{\delta-1}\left(\frac{1}{\Gamma-\lambda}\right) \end{aligned} \tag{32}$$

Then, we analyze the worst case for the adversary, i.e., $\kappa = 1$. This means that the adversary can monitor any routing path with equal probability and capture data packets only during the communication session. Given the average switching period π for the dynamic routing path, there are $n = \frac{\Omega}{\pi}$ routing path switches within session period Ω. In this case, the probability of session message attack can be expressed as

$$\begin{aligned} \min(P_{Glo}) &= \Pr(A_{rp}(\kappa))\Pr(A_{np}(\rho), A_{pp}(\xi), A_{sm}(\varpi)|A_{rp}(\kappa)) \\ &= \Pr(A_{rp}(\kappa))\Pr(A_{sm}(\varpi)|A_{rp}(\kappa)) \cdot \\ &\quad \Pr(A_{np}(\rho), A_{pp}(\xi)|A_{rp}(\kappa), A_{sm}(\varpi)) \\ &= \frac{1}{\hbar}\left(\sum_{i=0}^{\epsilon} C_M^{m+i}\left(\frac{1}{\hbar}\right)^{m+i}\left(1-\frac{1}{\hbar}\right)^{\epsilon-i}\right) \cdot \\ &\quad \left(\frac{m}{M}\right)^m \prod_{j=0}^{\left(\min\left\{n\frac{\delta}{\hbar},\delta\right\}\right)-1}\left(\frac{1}{\Gamma-j}\right) \end{aligned} \tag{33}$$

Based on above analysis, we have that $\max(P_{Glo}) \leqslant \left(\frac{1}{\Gamma}\right)^{\delta}$, $\min(P_{Glo}) \leqslant \frac{(\hbar-1)^{\epsilon}}{\hbar^{M+1}}\left(\frac{1}{\Gamma}\right)^{\delta}$. This means that even if the adversary can monitor all routing paths, the probability of successful session message attacks is still very small in the case of such large network space of the PP. Fig. 17 shows the security performance of various network-based MTDs against session message attacks, where $\epsilon_1 = 5, \epsilon_2 = 10, \epsilon_3 = 20$ and each kind of network-based MTDs undergoes 1000 attack attempts. Cyber-MTD can prevent most of the session message attacks when more than 60 deception packets are introduced, and the increase in the number of the introduced deception packets can accelerate the reduction of the probability of successful session message attacks. However, the other network-based MTDs are barely effective in preventing such attacks.

6.2. *Power system simulation*

We simulate IEEE 14 bus and 57 bus systems that are assumed to be fully measured, i.e., both the power flow on transmission lines and power injection on buses are measured. A portion of the American Electric Power System (in the Midwestern US) in Washington Electrical Engineering (a) is used for IEEE 14 bus system and another portion of that in Washington Electrical Engineering (b) is used for IEEE 57 bus system. The baseline configurations of the two test systems including generation limits, transmission line susceptances, and power flow limits are provided by the MATPOWER package (Zimmerman et al., 2011), based on which the linear sensitivity matrix is calculated and updated. The limiting parameters

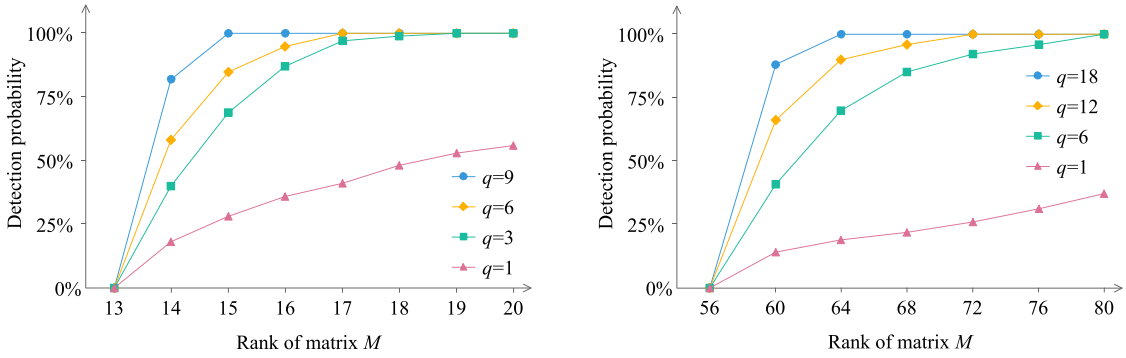

Fig. 18 – Probability of FDIA detection in noiseless systems (NLS).

of susceptance perturbation are set as $\underline{\tau} = -10\%$, $\overline{\tau} = 10\%$, and $\omega = 5\%$. We simulate 1000 times for each case where the number of attacked system states is generated in random, i.e., $\|\Delta\theta\| = q$, $q = 1, \cdots, n-1$.

6.2.1. *Attack test*

This test is conducted in the noiseless and noisy cases, respectively. First, the two test systems are simulated without considering the measurement noise and the results of FDIA detection are shown in Fig. 18. Overall, the detection probability increases significantly as the rank of matrix M or the number of attacked system states increases. Based on the attack detector constructed in Section 5.4, compromised measurement vector $z_a = H \cdot \theta + H_0 \cdot \Delta\theta$ can be detected if $z_a \notin C(H)$, where $\Delta\theta_i \neq 0, i \in S^d$. The detection results confirm our discussion in Section 5.2 that the detection probability increases with the increase of $|S^d|$ for a given $\|\Delta\theta\|$ or with the increase of $\|\Delta\theta\|$ for a given $|S^d|$ that satisfies $r(M) = n - 1 + |S^d|$. In addition, FDIA cannot be detected when $r(M) = n - 1$ and the detection probability reaches the maximum when $r(M) = 2 \cdot (n-1)$.

Then, the two test systems are simulated with zero mean Gaussian distribution noise injected, where the standard deviation is set as $\sigma_i = 0.01$p.u., where i denotes the ith meter. In this case, we compare the results of FDIA detection in both the noiseless and noisy systems when matrix M gets the maximal rank, i.e, $r(M) = 26$ in the 14 bus system and $r(M) = 80$ in the 57 bus system. The detection threshold is set as $\gamma = 0.1$, which represents the lower limit of the measurement residual that can trigger the attack detector. To measure the effect of the measurement noise, we use the true positive (TP) rate to represent the probability that the compromised measurements are correctly detected and the false positive (FP) rate to represent the probability that the normal measurements trigger the attack detector. The simulation results are shown in Fig. 19. Overall, the TP rate increases as the number of attacked system states increases without considering the measurement noise, and the TP rate in the noiseless system is slightly higher than that in the noisy system, which indicates that the measurement noise has an influence on the TP rate by a little reduction. On the other hand, the FP rate is always less than 10% and almost unaffected by the measurement noise. Inaddition, when $q \geq 4$ in the 14 bus system and $q \geq 10$ in the 57 bus system, the TP rate can reach more than 90%.

Based on the security-constrained economic dispatch (SCED) model explained in our preliminary work (Hu et al., 2021), we calculate the average system operation cost (ASOC) of the two test systems in three attack scenarios: 1. random attack: the injected false data obeys random distribution; 2. FDIA: the injected false data satisfies (2); 3. CPMTD-FDIA: CPMTD is deployed in scenario 2. We make 1000 attack attempts in each attack scenario and the simulation results are shown in Fig. 20. ASOC can be used as an indicator of the number of successful attacks, i.e., the larger the ASOC, the more attacks that can bypass detection. One can observe that the ASOC in scenario 2 is much higher than that in scenario 1, which indicates that the attacker with full knowledge of the target system (for scenario 2, FDIA) can easily leave the system in an insecure state. On the other hand, most false data (in scenario 1, random attack) has been detected by BDD, which indicates that if the attacker has little system knowledge, the probability of successful attacks is significantly smaller. Comparison of the ASOCs in scenario 2 and scenario 3 indicates that our proposed CPMTD can mislead the attacker into targeting invalid information about the measurement matrix and significantly increase the detection probability of FDIA.

6.2.2. *Performance test*

To evaluate the network performance, we compare the network throughput and delay when Cyber-MTD is performed or not. First, we transport the network traffic through two types of protocols by Scapy and record network statistics in the POF controller by Iperf. For the standard protocol (in this paper, we use UDP), the average forwarding throughputs are 930.57Mbit/s, 251.31Mbit/s when the maximum packet lengths are set as 1440B, 80B, respectively, the average network delays are 12.24ms, 25.37ms when the shortest and longest routing paths are adopted, respectively, and the average bandwidth is 49.64Mbit/s and the packet loss rate is 0.46% when a test flow is transmitted at 50Mbit/s. For the PPs, the average forwarding throughputs are 929.15Mbit/s, 253.15Mbit/s when the maximum packet lengths are set as 1440B, 80B, respectively, the average network delays are 13.32ms, 26.65ms when the shortest and longest routing paths are adopted, respectively, and the average bandwidth is 49.72Mbit/s and the packet loss rate is 0.51% when a test flow is transmitted at

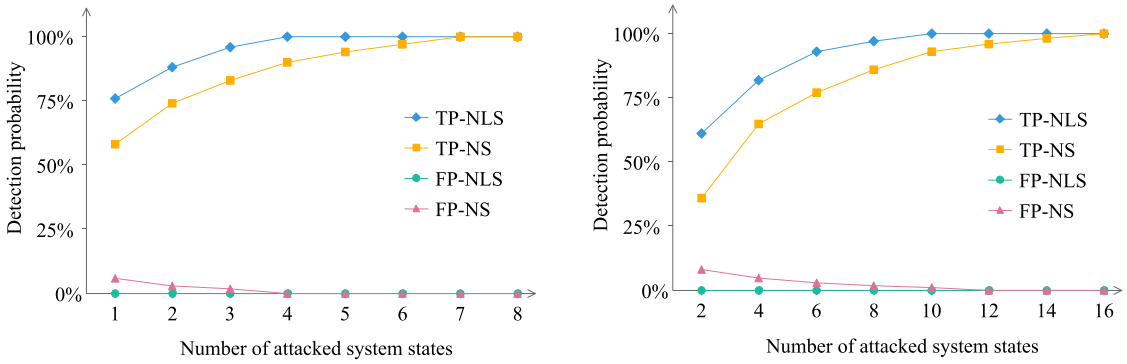

Fig. 19 – Probability of FDIA detection in noisy systems (NS).

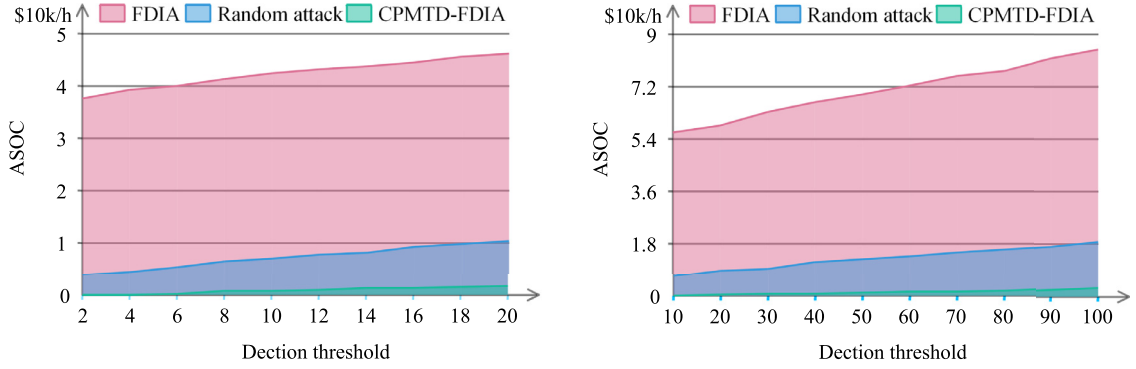

Fig. 20 – Average system operation cost (ASOC) in different attack scenarios.

50Mbit/s. The test results indicate that Cyber-MTD has little impact on the network performance while disrupting the attacker's reconnaissance in network communications.

To evaluate the system performance, we compare the active power loss of transmission lines with and without the performance of Physical-MTD, or rather with and without the performance of susceptance perturbation by D-FACTS devices. In the absence of D-FACTS devices, the active power losses of transmission lines in the 14 bus and 57 bus systems are 7.52MW, 18.24MW, respectively. When D-FACTS devices are deployed, we perform Physical-MTD by perturbing a set of transmission line susceptances in the 14 bus and 57 bus systems, respectively. In the 14 bus system, the active power loss of transmission lines is 7.75MW in the case of perturbing the transmission line susceptances of 1–2, 2–4, 3–4, 6–11, 6–12, 7–8, 9–10, 10–11, 12–13, and 13–14. In the 57 bus system, the active power loss of transmission lines is 18.46MW in the case of perturbing the transmission line susceptances of 2–3, 5–6, 7–8, 10–12, 11–13, 14–15, 18–19, 21–22, 24–25, 26–27, 27–28, 30–31, 34–35, 36–40, 44–45, 46–47, 47–48, 52–53, 54–55, and 56–57. Referring to the total load that in the 14 bus system is 330MW and in the 57 bus system is 1280MW, there is no significant increase in the active power loss of transmission lines in both the test systems before and after perturbing the set of transmission line susceptances by D-FACTS devices. The test results indicate that Physical-MTD has little impact on the system performance while changing the measurement matrix of state estimation.

7. Conclusion and future work

In this paper, we propose the concept of CPMTD that provides a combination of protections for power system. Structurally, CPMTD is a bi-level defense mechanism where Cyber-MTD serves as the first-level defense and Physical-MTD serves as the second-level defense. Functionally, CPMTD is a coordinated defense mechanism where Cyber-MTD starts with attack prevention and Physical-MTD follows with attack detection. To prevent FDIA during attack preparation, we focus on increasing the uncertainty in network communications. Based on this idea, the Cyber-MTD strategy is designed to disrupt the attacker's reconnaissance by randomizing the data acquisition into multiple rounds. To improve the detection probability of FDIA, we focus on making the measurement matrix required for attack construction unpredictable. Based on this idea, the Physical-MTD strategy is designed to obstruct the attacker's access to measurement matrix information by leveraging susceptance perturbation of transmission lines. We have demonstrated that CPMTD can prevent more than 90% of data packet attacks and most of the session message attacks when the sample size is large enough. We have verified the conditions under which FDIA can and cannot be detected and have found that the detection probability reaches the maximum when the rank of matrix M is maximized. We have evaluated the performances of CPMTD using standard IEEE systems and presented the results by graph, which show that the in-

troduced overhead of CPMTD is small enough to be negligible in power system.

In future work, we will improve our experiments to obtain more reliable results by incorporating more electrical elements into our testbed for a more realistic power system environment. In addition, we will consider cyber-attacks in the social space where large-scale CPS can be greatly influenced by the collective behavior of social users, and include social defense in our technique to provide a combination of cyber, physical, and social protections for power system.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

CRediT authorship contribution statement

Yifan Hu: Conceptualization, Methodology, Writing – original draft. **Peidong Zhu:** Writing – review & editing, Funding acquisition. **Peng Xun:** Supervision, Data curation, Writing – review & editing, Funding acquisition. **Bo Liu:** Supervision, Writing – review & editing. **Wenjie Kang:** Funding acquisition, Formal analysis, Validation. **Yinqiao Xiong:** Funding acquisition, Investigation, Project administration. **Weiheng Shi:** Software, Visualization.

Acknowledgments

The authors would like to thank support from NSFC (61572514), Hunan NSF (2020JJ5621), Changsha NSF (kq2007088), High-tech Industry Sci. and Tech. Innovation Leading Plan (2020GK2029), Fund of Hunan Education Department (19C0160, 20B064), Fund of Hunan Key Lab. of Network Investi. Tech. (2020WLZC003), Research Plan of National University of Defense Technology (ZK21-41), and Key Laboratory of Police Internet of Things Application Ministry of Public Security. People's Republic of China.

REFERENCES

Abur A, Exposito AG. Power system state estimation: Theory and implementation. CRC press; 2004.

Antonatos S, Akritidis P, Markatos E, Anagnostakis K. Defending against hitlist worms using network address space randomization. Comput. Networks 2007;51(12):3471–90. doi:10.1016/j.comnet.2007.02.006.

Atighetchi M, Pal P, Webber F, Jones C. Adaptive use of network-centric mechanisms in cyber-defense. In: Sixth IEEE International Symposium on Object-Oriented Real-Time Distributed Computing, 2003.; 2003. p. 183–92. doi:10.1109/ISORC.2003.1199253.

Case DU. Analysis of the cyber attack on the ukrainian power grid. Electricity Information Sharing and Analysis Center (E-ISAC) 2016;388.

Chaojun G, Jirutitijaroen P, Motani M. Detecting false data injection attacks in ac state estimation. IEEE Trans Smart Grid 2015;6(5):2476–83. doi:10.1109/TSG.2015.2388545.

Chaojun G, Jirutitijaroen P, Motani M. Detecting false data injection attacks in ac state estimation. IEEE Trans Smart Grid 2015;6(5):2476–83. doi:10.1109/TSG.2015.2388545.

Chavez AR, Stout WMS, Peisert S. Techniques for the dynamic randomization of network attributes. In: 2015 International Carnahan Conference on Security Technology (ICCST); 2015. p. 1–6. doi:10.1109/CCST.2015.7389661.

Cherkassky BV, Goldberg AV, Radzik T. Shortest paths algorithms: theory and experimental evaluation. Math Program 1996;73(2):129–74.

Deng R, Liang H. False data injection attacks with limited susceptance information and new countermeasures in smart grid. IEEE Trans. Ind. Inf. 2019;15(3):1619–28. doi:10.1109/TII.2018.2863256.

Divan D, Johal H. Distributed facts - a new concept for realizing grid power flow control. In: 2005 IEEE 36th Power Electronics Specialists Conference; 2005. p. 8–14. doi:10.1109/PESC.2005.1581595.

Esmalifalak M, Nguyen H, Zheng R, Zhu Han. Stealth false data injection using independent component analysis in smart grid. In: 2011 IEEE International Conference on Smart Grid Communications (SmartGridComm); 2011. p. 244–8. doi:10.1109/SmartGridComm.2011.6102326.

Fairley P. Upgrade coming to grid cybersecurity in us. IEEE Spectr.: Technol. Eng. Sci. News 2016.

Geelen JF. Maximum rank matrix completion. Linear Algebra Appl 1999;288:211–17. doi:10.1016/S0024-3795(98)10210-0.

Ghourab EM, Azab M, Mansour A. Spatiotemporal diversification by moving-target defense through benign employment of false-data injection for dynamic, secure cognitive radio network. Journal of Network and Computer Applications 2019;138:1–14. doi:10.1016/j.jnca.2019.02.020.

Groat S, Dunlop M, Urbanksi W, Marchany R, Tront J. Using an ipv6 moving target defense to protect the smart grid. In: Proceedings of the 2012 IEEE PES Innovative Smart Grid Technologies. USA: IEEE Computer Society; 2012. p. 1–7. doi:10.1109/ISGT.2012.6175633.

Hamada A, Azab M, Mokhtar A. Honeypot-like moving-target defense for secure iot operation; 2018. p. 971–7.

Hu Y, Xun P, Zhu P, Xiong Y, Zhu Y, Shi W, Hu C. Network-based multidimensional moving target defense against false data injection attack in power system. Computers & Security 2021;107:102283. doi:10.1016/j.cose.2021.102283.

Jafarian JH, Al-Shaer E, Duan Q. Openflow random host mutation: Transparent moving target defense using software defined networking. In: Proceedings of the First Workshop on Hot Topics in Software Defined Networks. New York, NY, USA: Association for Computing Machinery; 2012. p. 127–32. doi:10.1145/2342441.2342467.

Jajodia S, Ghosh AK, Swarup V, Wang C, Wang XS, 54. Springer Science & Business Media; 2011.

Kim J, Tong L, Thomas RJ. Subspace methods for data attack on state estimation: a data driven approach. IEEE Trans. Signal Process. 2015;63(5):1102–14. doi:10.1109/TSP.2014.2385670.

Kosut O, Jia L, Thomas RJ, Tong L. Malicious data attacks on the smart grid. IEEE Trans Smart Grid 2011;2(4):645–58. doi:10.1109/TSG.2011.2163807.

Lakshminarayana S, Belmega EV, Poor HV. Moving-target defense for detecting coordinated cyber-physical attacks in power grids. In: 2019 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm); 2019. p. 1–7. doi:10.1109/SmartGridComm.2019.8909767.

Lakshminarayana S, Belmega EV, Poor HV. Moving-target defense against cyber-physical attacks in power grids via game theory. IEEE Trans Smart Grid 2021. doi:10.1109/TSG.2021.3095083. 1–1

Lakshminarayana S, Yau DKY. Cost-benefit analysis of moving-target defense in power grids. In: 2018 48th Annual

IEEE/IFIP International Conference on Dependable Systems and Networks (DSN); 2018. p. 139–50. doi:10.1109/DSN.2018.00026.
Langner R. Stuxnet: dissecting a cyberwarfare weapon. IEEE Security Privacy 2011;9(3):49–51. doi:10.1109/MSP.2011.67.
Lee HCJ, Thing VLL. Port hopping for resilient networks, 5; 2004. p. 3291–5. doi:10.1109/VETECF.2004.1404672.
Li S, Hu D, Fang W, Ma S, Chen C, Huang H, Zhu Z. Protocol oblivious forwarding (pof): software-defined networking with enhanced programmability. IEEE Netw 2017;31(2):58–66. doi:10.1109/MNET.2017.1600030NM.
Lin H, Kalbarczyk ZT, Iyer RK. Raincoat: randomization of network communication in power grid cyber infrastructure to mislead attackers. IEEE Trans Smart Grid 2019;10(5):4893–906. doi:10.1109/TSG.2018.2870362.
Lin H, Slagell A, Kalbarczyk ZT, Sauer PW, Iyer RK. Runtime semantic security analysis to detect and mitigate control-related attacks in power grids. IEEE Trans Smart Grid 2018;9(1):163–78. doi:10.1109/TSG.2016.2547742.
Lin H, Zhuang J, Hu Y-C, Zhou H. Defrec: Establishing physical function virtualization to disrupt reconnaissance of power grids cyber-physical infrastructures. The Proceedings of 2020 Network and Distributed System Security Symposium (NDSS), 2020.
Liu B, Wu H. Optimal planning and operation of hidden moving target defense for maximal detection effectiveness. IEEE Trans Smart Grid 2021.
Liu C, Wu J, Long C, Wang Y. Dynamic state recovery for cyber-physical systems under switching location attacks. IEEE Trans. Control Network Syst. 2017;4(1):14–22. doi:10.1109/TCNS.2016.2580906.
Liu Y, Ning P, Reiter MK. False data injection attacks against state estimation in electric power grids. ACM Trans. Inf. Syst. Secur. 2011;14(1). doi:10.1145/1952982.1952995.
Morrow KL, Heine E, Rogers KM, Bobba RB, Overbye TJ. Topology perturbation for detecting malicious data injection. In: 2012 45th Hawaii International Conference on System Sciences; 2012. p. 2104–13. doi:10.1109/HICSS.2012.594.
Pasqualetti F, Drfler F, Bullo F. Attack detection and identification in cyber-physical systems. IEEE Trans Automat Contr 2013;58(11):2715–29. doi:10.1109/TAC.2013.2266831.
Rahman MA, Al-Shaer E, Bobba RB. Moving target defense for hardening the security of the power system state estimation. In: Proceedings of the First ACM Workshop on Moving Target Defense. New York, NY, USA: Association for Computing Machinery; 2014. p. 59–68. doi:10.1145/2663474.2663482.
Rogers KM, Overbye TJ. Some applications of distributed flexible ac transmission system (d-facts) devices in power systems. In: 2008 40th North American Power Symposium; 2008. p. 1–8. doi:10.1109/NAPS.2008.5307314.
Shi L, Jia C, Lü S, Liu Z. Port and address hopping for active cyber-defense. In: Yang CC, Zeng D, Chau M, Chang K, Yang Q, Cheng X, Wang J, Wang F-Y, Chen H, editors. In: Intelligence and Security Informatics. Berlin, Heidelberg: Springer Berlin Heidelberg; 2007. p. 295–300.
Stouffer, K. A., Falco, J. A., Scarfone, K. A., 2011. Sp 800-82. guide to industrial control systems (ics) security: Supervisory control and data acquisition (scada) systems, distributed control systems (dcs), and other control system configurations such as programmable logic controllers (plc).
Tan J, Zhang H, Zhang H, Hu H, Lei C, Qin Z. Optimal temporospatial strategy selection approach to moving target defense: a flipit differential game model. Computers & Security 2021:102342.
Tian J, Tan R, Guan X, Liu T. Hidden moving target defense in smart grids. In: Proceedings of the 2nd Workshop on Cyber-Physical Security and Resilience in Smart Grids. New York, NY, USA: Association for Computing Machinery; 2017. p. 21–6. doi:10.1145/3055386.3055388.
Tian J, Tan R, Guan X, Liu T. Hidden moving target defense in smart grids. In: Proceedings of the 2nd Workshop on Cyber-Physical Security and Resilience in Smart Grids; 2017. p. 21–6.
Tian J, Tan R, Guan X, Liu T. Enhanced hidden moving target defense in smart grids. IEEE Trans Smart Grid 2018;10(2):2208–23.
Tian J, Tan R, Guan X, Liu T. Enhanced hidden moving target defense in smart grids. IEEE Trans Smart Grid 2019;10(2):2208–23. doi:10.1109/TSG.2018.2791512.
Tian J, Tan R, Guan X, Xu Z, Liu T. Moving target defense approach to detecting stuxnet-like attacks. IEEE Trans Smart Grid 2020;11(1):291–300. doi:10.1109/TSG.2019.2921245.
Valenzuela J, Wang J, Bissinger N. Real-time intrusion detection in power system operations. IEEE Trans. Power Syst. 2013;28(2):1052–62. doi:10.1109/TPWRS.2012.2224144.
Wang G, Zhao J, Zhang X, Zhang X, Zhang X. Analysis of the relationship between electric cyber-physical systems and ubiquitous electric internet of things. In: 2019 IEEE 3rd Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC); 2019. p. 1614–18. doi:10.1109/IMCEC46724.2019.8983978.
Wang H, Jia Q, Fleck D, Powell W, Li F, Stavrou A. A moving target ddos defense mechanism. Comput Commun 2014;46:10–21. doi:10.1016/j.comcom.2014.03.009.
Washington Electrical Engineering, US., a. Power system test case archive. http://labs.ece.uw.edu/pstca/pf14/pg_tca14bus.htm.
Washington Electrical Engineering, US., b. Power system test case archive. http://labs.ece.uw.edu/pstca/pf57/pg_tca57bus.htm.
Xu J, Guo P, Zhao M, Erbacher RF, Zhu M, Liu P. Comparing different moving target defense techniques. In: Proceedings of the First ACM Workshop on Moving Target Defense. New York, NY, USA: Association for Computing Machinery; 2014. p. 97–107. doi:10.1145/2663474.2663486.
Yu Z, Chin W. Blind false data injection attack using pca approximation method in smart grid. IEEE Trans Smart Grid 2015;6(3):1219–26. doi:10.1109/TSG.2014.2382714.
Zacchia Lun Y, D'Innocenzo A, Smarra F, Malavolta I, Di Benedetto MD. State of the art of cyber-physical systems security: an automatic control perspective. Journal of Systems and Software 2019;149:174–216. doi:10.1016/j.jss.2018.12.006.
Zhang Z, Deng R, Yau DKY, Cheng P, Chen J. Analysis of moving target defense against false data injection attacks on power grid. IEEE Trans. Inf. Forensics Secur. 2020;15:2320–35. doi:10.1109/TIFS.2019.2928624.
Zhuang R, DeLoach SA, Ou X. Towards a theory of moving target defense. In: Proceedings of the First ACM Workshop on Moving Target Defense. New York, NY, USA: Association for Computing Machinery; 2014. p. 31–40. doi:10.1145/2663474.2663479.
Zimmerman RD, Murillo-Snchez CE, Thomas RJ. Matpower: steady-state operations, planning, and analysis tools for power systems research and education. IEEE Trans. Power Syst. 2011;26(1):12–19. doi:10.1109/TPWRS.2010.2051168.

Yifan Hu received the B.S. degree in communication engineering from Ocean University of China, Qingdao, China, in 2014, and the M.S. degree in signal and information processing from PLA University of Science and Technology University (PLAUST), Nanjing, China, in 2017. He is currently a Ph.D. candidate in cyberspace security from National University of Defense Technology (NUDT), Changsha, China. His interests include cyber security and smart grid. E-mail: huyifan17@nudt.edu.cn

Peidong Zhu received his Ph.D. degree in computer science from National University of Defense Technology (NUDT) in 1999. He was a professor with the College of Computer of NUDT until 2017. Currently, he works in Department of Electronic Information and Electrical Engineering of Changsha University, China. His research interests include security of large-scale Cyber-Physical network and architecture of the Internet. He is a senior member of IEEE(SM-11). E-mail: pdz@ccsu.edu.cn

Peng Xun received the B.E. degree in computer science from HeFei University of Technology, China, in 2012, and the Ph.D. degree in computer science from National University of Defense Technology (NUDT), China, in 2018. Currently, he is an assistant professor of NUDT. His research interests include cloud computing security, security of cyber-physical systems, and big data analysis of complex systems. E-mail: xunpeng12@nudt.edu.cn

Bo Liu received the B.S., M.S., and Ph.D. degrees from the National University of Defense Technology (NUDT), China, in 1994, 1997, and 2001, respectively. He is currently a Professor with the National Key Laboratory of Parallel and Distributed Processing of the College of Computer of NUDT. His current research interests focus on artificial intelligence, natural language processing, and social network analysis. E-mail: kyle.liu@nudt.edu.cn

Wenjie Kang received his Ph.D. degree in computer science from the National University of Defense Technology, China, in 2018, and the Master's degree in computer science from the National University of Defense Technology, China, in 2013. He is currently a post-doctoral research with the College of System Engineering, National University of Defense Technology and a lecturer at Hunan Police Academy, Changsha, China. His interests include big data analysis and data visualization, complex network and the cyber-physical system security. E-mail: kangwenjie@nudt.edu.cn

Yinqiao Xiong received the B.S. and M.S. degrees in computer science and technology from the School of Computer, National University of Defense and Technology (NUDT), Changsha, China, in 2007 and 2010, respectively. He is currently an Assistant Professor in Changsha University and working toward the Ph.D. in cyberspace security in the School of Computer, NUDT. His research interests include privacy preserving, information security, and IoT. E-mail: yq.xiong@ccsu.edu.cn

Weiheng Shi received the B.S. degree in applied meteorology from PLA University of Science and Technology University (PLAUST), China, in 2012, the M.S. degree in communication engineering from PLAUST in 2015. Currently, he is a visiting scholar at National University of Defense Technology (NUDT). His main research direction is meteorological and marine information processing technique. E-mail: tfoterye@gmail.com