

A Dynamic Cyber-attack Approach for Real-time Hardware-in-the-loop Simulation of Power Grid

Zijiao ZHOU*, Haowei YANG*, Huibo LI*, Jihao ZHANG *, Siqi LI*, Xiang GAO*, Peng GONG*

* National Key Laboratory of Mechatronic Engineering and Control, School of Mechatronic Engineering, Beijing Institute of Technology, Beijing, China

zhouzijiao995@163.com, yhw@bit.edu.cn, 2569826229@qq.com, 3120180275@bit.edu.cn, lsqbit@163.com, bitxianggao@163.com, penggong@bit.edu.cn

Abstract—Cyber-attacks on the power grid happen frequently nowadays which results in a high incidence of power fault, like power blackouts. The current cyber-physical co-simulation technology for power grid vulnerability researches still adopt script simulation rather than dynamic simulation, making the dynamic analysis unavailable. In this paper, a real-time hardware-in-the-loop simulation platform integrated by QualNet and Real-time Digital Simulator (RTDS) is investigated. On this platform, a dynamic cyber-attack approach, i.e., DoS attack and data tampering attack, is proposed, where users can dynamically configure the cyber-attack situations of power grid via a designed panel during the simulation process, to estimate and analyse the impact of cyber-attacks on the power grid system. Experiment results verify the operability and effectiveness of the proposed approach.

Keywords— Smart Grid; QualNet; RTDS; Real-time simulation; Cyber-attack; Dynamic simulation

I. INTRODUCTION

With the integration of communication-information system and traditional power grid, a new intelligent power system which is called smart grid has emerged, developing in the direction of Cyber-Physical Systems (CPS). The smart grid makes the power system more efficient and energy-saving. However, it also exposes many security problems making the power grid vulnerable [1]-[3]. For example, in 2014, a hacker team called Dragonfly attacked more than 1000 energy companies in a way of emails, websites, and third-party programs [4]. Additionally, on December 25, 2015, during the Bulb Civil War in Ukraine, Ivano-Frankivsk, a power station was attacked by a kind of network virus named BlackEnergy, which could delete data, destroy hard disks, and control infected computers, forcing 80,000 people into darkness [5]. As a result, it's urgent to pay more attention to the security and stability of smart grid to prevent further damages from cyber-attacks.

Cyber-physical co-simulation technology, which is divided into 3 kinds: non-real-time co-simulation, embedded simulation and real-time co-simulation, has been widely applied to cyber-attack simulation area of smart grid. An HLA-based solution for complex and distributed hybrid simulation, as a representative of non-real-time co-simulation, was presented in [6]. RTI was used as the interface between

simulation software for periodic data exchange to ensure time synchronization and routing communication. In addition, Lightweight Co-simulation of Power and Information and communication technology (ICT) systems for performance Evaluation of smart grid (LICPIE), was developed based on the concepts of software bus and middleware in [7]. However, RTI and the middleware of LICPIE make the process much complicated, and the simulation process cannot match the dynamic characteristics and actual interaction. To avoid synchronization issues of different simulators, embedded simulation was discussed where communication modules were embedded in the power system simulation software [8]. But it is difficult to simulate accurate communication process in power system simulation software, only rough simulation can be carried out. Therefore, real-time co-simulation of high precision came into being. In order to make the simulation software run in real time, physical equipment was added into the simulation loop. In [9], a real-time cyber-physical co-simulation testbed with hardware-in-the-loop capability was proposed, where RTDS, Synchrophasor devices, DeterLab, and a wide area monitoring application with closed-loop control were utilized. What's more, a Cyber Attack Simulation Framework for Smart Grids, GridAttackSim, was described in [10], which was based on the combination of GridLAB-D, ns-3, and FNCS, allowing us to simulate smart grid infrastructure features with various cybersecurity attacks and then visualize their consequences automatically. However, the current researches are still using script simulation rather than dynamic simulation. Thus, the influence of cyber-attack on power grid is unavailable to be analysed in a dynamic manner.

To solve the problem above, this paper investigates a real-time hardware-in-the-loop simulation architecture based on QualNet and RTDS, where QualNet is responsible for communication simulation and RTDS is responsible for power simulation. At the same time, a dynamic cyber-attack approach is designed on the basis of the joint simulation platform to conduct dynamic simulation for DoS attack and data tampering attack. Compared with the existing co-simulation platforms, the proposed cyber-attack approach can achieve the function of real-time dynamic configuration, and make users be able to view the impact on power grid automatically and dynamically.

The remainder of the paper is organized as follows. In Section II, the proposed dynamic cyber-attack approach based on the co-simulation platform is described in detail. Besides, intensive experiments are performed to simulate DoS attack and data tampering attack in Section III. Finally, conclusions are drawn in Section IV.

II. PROPOSED APPROACH OF DYNAMIC CYBER-ATTACK

A. Overall architecture

The real-time hardware-in-the-loop simulation architecture considered in this paper is shown in Fig.1. The joint simulation architecture is composed of QualNet simulator, Protocol Conversion Module (PCM), physical equipment module, RTDS, Dynamic Cyber Attack Module (DCAM) and Real-Time User Interface (RTUI). Each part cooperates with each other co-ordinately, and plays their respective roles.

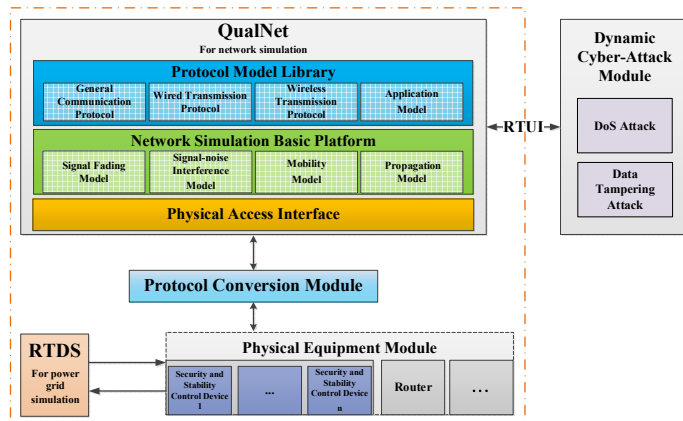


Figure 1. Real-time hardware-in-the-loop simulation architecture

QualNet: As the simulator of communication network for power grid system, it includes a protocol model library, a network simulation basic platform and some physical access interfaces. The library not only provides protocol models for the layers of TCP/IP according RFC, but also supports dedicated network models, such as optical transmission network model based on Synchronous Digital Hierarchy (SDH), micro-grid model, and scheduling model.

PCM: A kind of device which can transform non-standard packets into standard packets. Since the access interfaces of QualNet only accept the injection of standard IP packets, non-standard packets from Phasor Measurement Unit (PMU) or other Security and Stability Control Device (SSCD) must be converted through PCM.

RTDS: As the simulator of physical power grid system, which contains almost all common analysis functions of power system, such as power flow, short circuit calculation, electromechanical transient, electromagnetic transient calculation, harmonic analysis, interference stability analysis, etc., RTDS is the main verification platform of experimental effect.

DCAM: Users can dynamically configure the parameters of cyber-attacks through the panel, and load them into the simulation scenario in real time. These parameters will be

capsuled into the uniform format packets and sent to QualNet through RTUI.

RTUI: As a UDP socket, RTUI can realize the data interaction between DCAM and QualNet. It is responsible for parsing configuration packets into corresponding recognizable packets by QualNet and precaching them into event queues of QualNet depending on the execution time. Moreover, RTUI is a real-time interface which can dynamically transmit the attack information from the DCAM panel.

B. Function flow chart of DoS Attack

The function flow chart of DoS attack is shown in Fig.2, and corresponding key functions are described as follows.

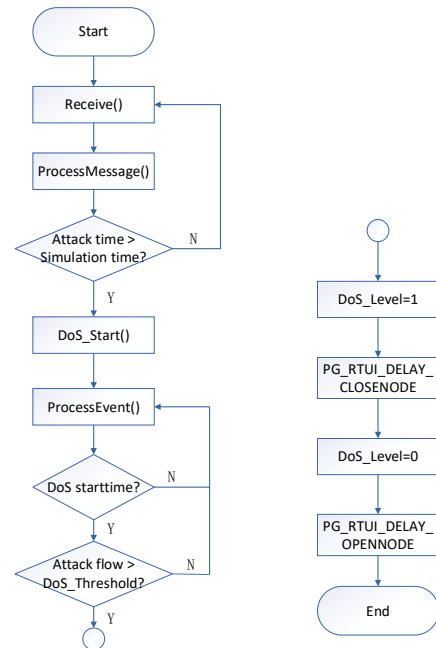


Figure 2. Function flow chart of DoS Attack

Receive(): Function keeps on listening a UDP socket RTUI to receive configuration packets sent by DCAM panel.

ProcessMessage(): Function first parses the configuration packets to look up the attack type. If the attack type is DoS attack, function will read the information of the received packets and calls the corresponding functions to deal with the messages. Fig.3 illustrates the data structure of DoS attack packet, where “length” is the length of one attack packet, “src” is the attack node sending numerous packets, “dest” is the node to be attacked, “PacketNum” is the total number of packets sent by DoS attack node.

4 bytes	4 bytes	8 bytes	8 bytes	8 bytes	20 bytes	20 bytes	20 bytes
type	length	src	dest	packet Num	startTimS tr[]	intervalSt r[]	endTimSt r[]

Figure 3. Data structure for DoS attack

ProcessEvent(): Function will first judge the attack start time. If the attack start time is greater than the simulation time, the server node will send meaningless packets of a certain size to the client node at the data flow configured by the user. And

when the attack flow is higher than “DoS_Threshold”, function will set “DoS_Level” equal to 1, and close the client node. When the end time comes, function will set “DoS_Level” equal to 0, and open the client node.

C. Function flow chart of Data Tampering Attack

The function flow chart of data tampering attack is shown in Fig.4, and corresponding key functions are described as follows.

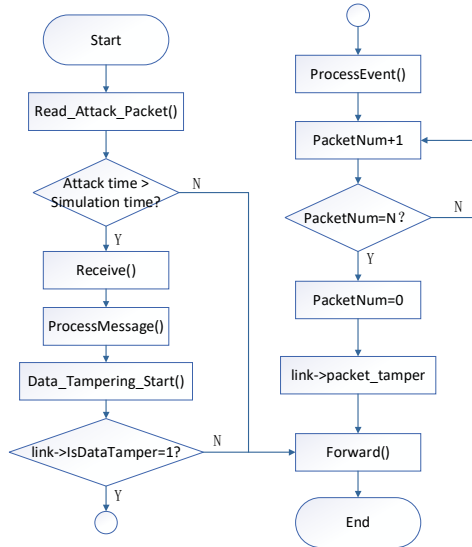


Figure 4. Function flow chart of Data Tampering Attack

Read_Attack_Packet(): The details of heartbeat packet and control measurement packet have been stored in the scenario file in advance before simulation. When the simulation starts, function will read the information of the two kinds of packets.

Receive(): Function keeps on listening a UDP socket RTUI to receive configuration packets sent by DCAM panel.

ProcessMessage(): Function first parses the configuration packets to look up the attack type. If the attack type is data tampering attack, function will read the information of the received packets and set the flag bit “IsDataTamer” true. Fig.5 shows the data structure for data tampering attack packet, where “nodeId” is the node to be attacked, “PacketNum” is the total number of packets to be tampered, “starttime” is the start time of data tampering, and “content” is the specific content of data tampering.

4 bytes	4 bytes	4 bytes	8 bytes	8 bytes	32 bytes
type	length	nodeId	packetNum	starttime	content

Figure 5. Data structure for data tampering attack

ProcessEvent(): Function first judges whether the flag bit “IsDataTamer” is true to decide the start time of data tampering attack. When attack starts, function will tamper the packets to be received according to the request of DCAM panel configuration by forwarding packet_tamper as the replacement packets.

Forward(): Function achieves packets forwarding to the destination according to the routing table.

III. EXPERIMENTS AND RESULTS

A. Scenario configuration

This test experiment adopts SDH self-healing network model where a test scenario including 18 power stations is established. Half of the stations contain SSCDs, i.e., PMUs, while the other half do not. The parameters of simulation servers are listed in Table 1, and the protocols utilized in communication layers are showed in Table 2.

TABLE 1. PARAMETERS OF SIMULATION SERVERS

	QualNet	RTDS	DCAM Panel
Operation System	Ubuntu 12.04	Win10 professional	Win10 professional
CPU	Intel core i7 4700MQ	Intel core i7 Q720	Intel core i7 Q720
RAM	3.5GiB	4.0GiB	4.0GiB

TABLE 2. PROTOCOLS OF COMMUNICATION LAYERS

Physical Layer Protocol	802.11b
MAC Layer Protocol	Abstract Link MAC
Network Layer Protocol	IPv4
Routing Protocol	Specify Static Protocol

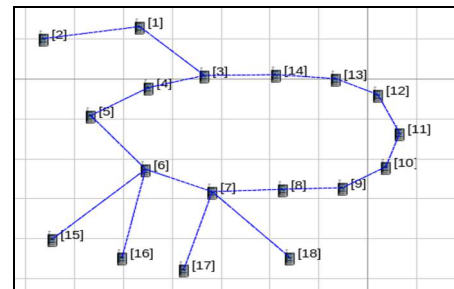


Figure 6. Network topology established in QualNet

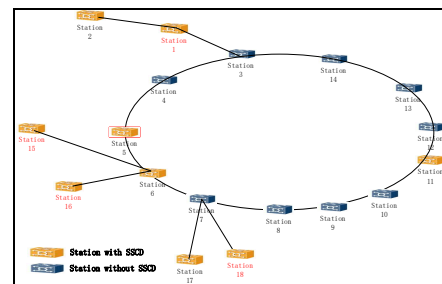


Figure 7. Communication secure topology of 18-node system

Fig.6 and Fig.7 show the topology of the 18-node system. As a matter of fact, the nodes in QualNet and the power stations are in one-to-one relationship. We suppose that the central station (corresponding to Node 1) sends control messages to Substation 1 (corresponding to Node 15), Substation 2 (corresponding to Node 16) and Substation 3 (corresponding to Node 18). The following experiments focus

on the actions of the substations receiving the control measurement packets.

B. DoS attack performance test

To ensure the accuracy and sensitivity of the simulation, the packets of the simulated DoS attack in this test are not real packets sent by the physical devices, but virtual packets generated in QualNet by attack instructions. Fig.8(a) shows the data flow in condition of the previously planned scenario in QualNet without DoS attack, and the packets transmission paths are 1-3-4-5-6-15, 1-3-4-5-6-16 and 1-3-4-5-6-7-18. Fig.8(b) presents the actions of substations without DoS attack, where the time delay of Substation 1, Substation 2 and Substation 3 are 90ms, 90ms and 95ms.

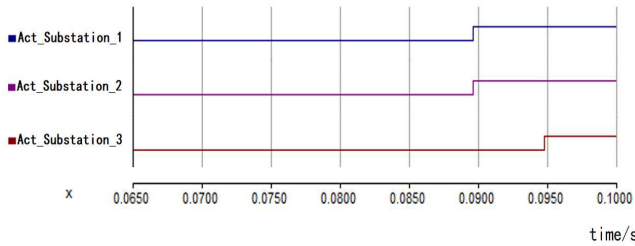
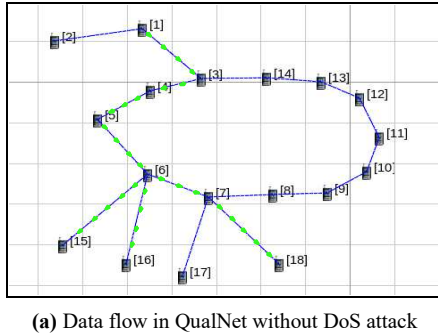


Figure 8. Data flow in QualNet and substations' actions without DoS attack

Figure 9. DoS attack configuration

Server node can be selected outside or inside the scenario as needed. The product of the reciprocal of the packet length and the packet interval determines the size of the data flow for DoS attack. Besides, a threshold parameter "DoS_Threshold" is set in the algorithm. When the data flow is larger than the threshold value, the DoS attack starts. In this test, DoS attack experiment is carried out on Node 5, and we choose one

outside Node 19 as the attack node.

The result of this experiment is displayed in figure 10. The data flow from Node 19 to Node 5 is much larger than that of the normal control measurement packets in Fig.10(a). And it can be seen that Substation 1, Substation 2 and Substation 3 refuse to move (Fig.10(b)) compared to the situation shown in Fig.8(b) without DoS attack. The reason is that Node 5 has lost data processing ability so far as to lose packets under DoS attack. In fact, there is a high requirement on the continuity of receiving control measurement packets for substations to determine whether and how to act. A substation needs to receive more than 20 correct control measurement packets in succession perfectly before it can act. Node 5 can no longer meet the ideal continuity requirement at this time, so the three substations refuse to move.

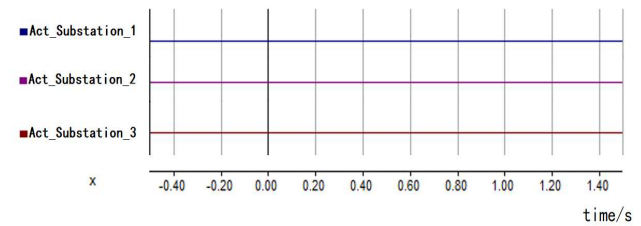
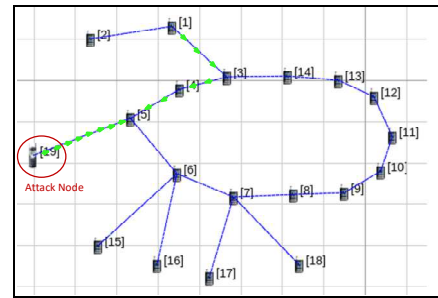


Figure 10. Data flow in QualNet and substations' actions with DoS attack

C. Data tampering attack performance test

Figure 11. Data tampering attack configuration

In this test, we assume that the downlink control measurement packets from central station to three substations are also tampered at Node 5 into heartbeat packets. There is

no demand to set the attack node in QualNet scenario. According to the DCAM panel configuration in Fig.11, the packet number is 10, the attack start time is 10s, and the tampering content is heartbeat. In other words, starting from 10th second of simulation, QualNet will replace the 10 packets to be received with heartbeat packets prestored in the scenario file. For a better view, we add one more observation node (Node 4) for comparison, and use a third-party network data packet catching software, Wireshark, to grab packets from central station to substations.

0000	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
0010	00 22 11 44 00 10 00 00	54 43 4a 5f 35 30 30 5f	..".D.... TCJ_500_
0020	38 5f 74 79 70 65 5f 38	02 00 16 07 12 01 00 00	8_type_8
0030	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
0040	00 00 00 00 00 00 00 00	00 00 00 00 12 00 ed 00	
0050	58 02 00 00 00 00 00 00	00 00 69 69 c8 ba 88 09	X.....-ii....
0060	00 22 11 44 01 20 00 00	0a 55 00 02 00 00 00 00	..".D....-U.....
0070	00 00 00 00 00 00 00 00	00 00 00 00 00 00 f5 a8	
0080	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
0090	a5 a5 00 a5 00 00 58 02	00 00 00 00 00 00 00 00	X.....
00a0	00 00 00 00 00 00 00 00	00 00 00 00 c8 ba 61 06	a.....

(a) Data packet intercepted by Wireshark without data tampering attack

0000	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
0010	00 22 11 44 00 10 00 00	54 43 4a 5f 35 30 30 5f	..".D.... TCJ_500_
0020	38 5f 74 79 70 65 5f 38	02 00 16 07 12 01 00 00	8_type_8
0030	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
0040	00 00 00 00 00 00 00 00	00 00 00 00 12 00 ed 00	
0050	58 02 00 00 00 00 00 00	00 00 69 69 c8 ba 88 09	X.....-ii....
0060	00 22 11 44 01 20 00 00	0a 99 00 02 00 00 00 00	..".D....-U.....
0070	00 00 00 00 00 00 00 00	00 00 00 00 00 00 f5 a8	
0080	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
0090	a5 a5 00 a5 00 00 58 02	00 00 00 00 00 00 00 00	X.....
00a0	00 00 00 00 00 00 00 00	00 00 00 00 c8 ba 61 06	a.....

(b) Data packet intercepted by Wireshark with data tampering attack

Figure 12. Data packet intercepted by Wireshark

Fig.12 shows the data packets intercepted by Wireshark. Through contrastive analysis of Fig.12(a) and Fig.12(b), it can be seen that the flag bit in the data packet has been successfully tampered from 55 to 99, which means the downlink control measurement packets has been transformed into the heartbeat packets.

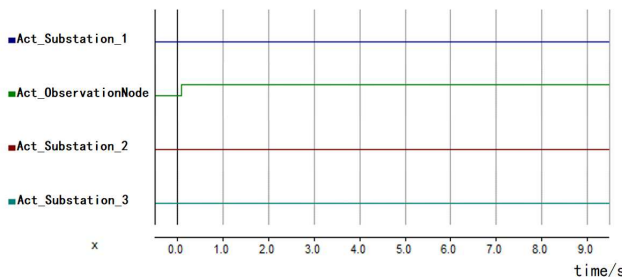


Figure 13. Actions of node 15, node 4, node 16, and node 18 with data tampering attack

In Fig.13, it can be observed that the observation node (Node 4) works normally, but Substation 1, Substation 2 and Substation 3 all refuse to move. Owing to Node 4 front to the attacked Node 5 in the transmission path, the control measurement packets from the central station can still pass through Node 4 without interference. As for the substations, they can only receive the tampered heartbeat packets instead of the control measurement packets, so they all refuse to move

and think themselves can normally communicate with the central station.

D. Interface delay test

The time delay of RTUI is composed of four parts: consumption time for calling the receiving function, consumption time for packet parsing and rebuilding, consumption time for event processing in QualNet and consumption time for packet feeding back. 100 times of experiments are performed to obtain the average time delay of RTUI. As shown in Fig.14, an average delay time of RTUI is 0.069ms, which implies the proposed approach can efficiently support the dynamic real-time configuration of cyber-attack with an acceptable time delay of the interface.

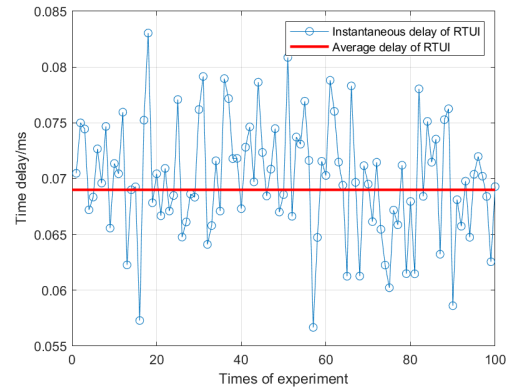


Figure 14. Time delay of RTUI

IV. CONCLUSIONS

In this paper, a dynamic cyber-attack approach containing DoS attack and data tampering attack based on a real-time hardware-in-the-loop simulation platform integrated by RTDS and QualNet is proposed to evaluate the impact of cyber-attacks on power grid system. In this approach, users can dynamically configure the cyber-attack situations of power grid in real time via DCAM panel during the simulation process. Experiment results demonstrate the operability and effectiveness of the proposed dynamic cyber-attack simulation approach.

ACKNOWLEDGMENT

This research was supported in part by National Natural Science foundation of China (No.62073039). Corresponding author: Peng Gong.

REFERENCES

- [1] Kimani K, Oduol V, Langat K. Cyber security challenges for IoT-based smart grid networks[J]. International Journal of Critical Infrastructure Protection, 2019, 25: 36-49.
- [2] Kim D H, Eisenberg D A, Chun Y H, et al. Network topology and resilience analysis of South Korean power grid[J]. Physica A: Statistical Mechanics and its Applications, 2017, 465: 13-24.
- [3] Xiang Y, Wang L, Liu N. Coordinated attacks on electric power systems in a cyber-physical environment[J]. Electric Power Systems Research, 2017, 149: 156-168.
- [4] Langill, J T. Defending against the Dragonfly cyber security attacks. Retrieved 2014, 11, 2015.

- [5] SANS and Electricity Information Sharing and Analysis Center (E-ISAC). Analysis of the cyber attack on the Ukrainian power grid; Mar. 18, 2016.
- [6] Ficco M, Choraś M, Kozik R. Simulation platform for cyber-security and vulnerability analysis of critical infrastructures[J]. Journal of computational science, 2017, 22: 179-186.
- [7] Zhao L, Ni M, Tong H, et al. Design and application of distributed co - simulation platform for cyber physical power system based on the concepts of software bus and middleware[J]. IET Cyber - Physical Systems: Theory & Applications, 2020, 5(1): 71-79.
- [8] Zhang L, Li L, Wihl L, et al. Cybersecurity Study of Power System Utilizing Advanced CPS Simulation Tools[C]//Proceedings of the 2019 PAC World Americas Conference, Raleigh, NC, USA. 2019: 19-22.
- [9] Liu R, Srivastava A. Integrated simulation to analyze the impact of cyber-attacks on the power grid[C]//2015 Workshop on Modeling and Simulation of Cyber-Physical Energy Systems (MSPES). IEEE, 2015: 1-6.
- [10] Le T D, Anwar A, Loke S W, et al. GridAttackSim: A cyber attack simulation framework for smart grids[J]. Electronics, 2020, 9(8): 1218.



Xiang Gao received the BS degree in Mechatronical Engineering from Beijing Institute of Technology in 2014, and the MS and Ph.D. degrees from Beijing Institute of Technology in 2016 and 2021. His research interests include network simulation and emulation, wireless communication and the next generation wireless systems such as MIMO, Cognitive radio and so on.



Peng Gong received the BS degree in Mechatronical Engineering from Beijing Institute of Technology, Beijing, China, in 2004, and the MS and Ph.D. degrees from the Inha University, Korea, in 2006 and 2010, respectively. In July 2010, he joined the School of Mechatronical Engineering, Beijing Institute of Technology, China. His research interests include link/system level performance evaluation and radio resource management in wireless systems, information security, and the next generation wireless systems such as 3GPP LTE, UWB, MIMO, Cognitive radio and so on.



Zijiao Zhou received the BS degree in Mechatronical Engineering from Beijing Institute of Technology in 2020, and now she is a MS candidate in School of Mechatronical Engineering, Beijing Institute of Technology. Her research interests include wireless network simulation and emulation, information security, wireless communication and so on.



Haowei Yang received the BS degree in Mechatronical Engineering from Beijing Institute of Technology in 2015, and then he received the MS degree in Beijing Institute of Technology in 2018. Now he is a DS candidate in School of Mechatronical Engineering, Beijing Institute of Technology. His research interests include network simulation and emulation, VANET and so on.



Huiibo Li received the BS degree in Mechatronical Engineering from Beijing Institute of Technology in 2016, and then she received the MS degree in Beijing Institute of Technology in 2019. Now she is a DS candidate in School of Mechatronical Engineering, Beijing Institute of Technology. Her research interests include wireless network simulation and emulation, resource management in wireless systems and development of secure network protocols for wireless networks.



Jihao Zhang received the BS degree in Mechatronical Engineering from Beijing Institute of Technology in 2018, and then he received the MS degree in Beijing Institute of Technology in 2021. Now he is a DS candidate in School of Mechatronical Engineering, Beijing Institute of Technology. He research interests include wireless network simulation and emulation, wireless communication and so on.



Siqi Li received the BS degree in Electronic Information Engineering from Beijing Institute of Technology, Beijing, China, in 2018. And in 2021 she received the MS degree in Beijing Institute of Technology. Now she is a DS candidate in School of Mechatronical Engineering, Beijing Institute of Technology. Her research interests include wireless network simulation and emulation, resource management in wireless systems and so on.