Journal of Network Computing and Applications (2019) 4: 14-20
Clausius Scientific Press, Canada

DOI: 10.23977/jnca.2019.41003
EISSN 2371-9214

Research on Coordinated Attack Protection Method Based on Global Time Synchronization System of Intelligent Substation

Shaomin Zhang[a,*], Pengzhi Cheng[b], Baoyi Wang[c], Xia Zhou

*Department of Control and Computer, North China Electric Power University, Huadian Road,
Baoding, China
zhangshaomin@126.com, cpzybhh@foxmail.com,wangbaoyi@126.com*

Keywords: coordinated attack, differentiated time management design, intelligent substation automation system, power outage accident

Abstract: Aiming at the coordinated attack based on time problem in the network attack of intelligent substation automation system, leading to large scale power outages, coordinated attack model called ENFTA is proposed. The scheme adds a differentiated time management design and time anti-correction design of the dispatcher based on the time synchronization system of the smart substation. The former is used to differentiate the synchronization time of substation and thus stagger the trigger time initiated by the coordinated attack software. In the latter, the information of the global synchronization time between the dispatcher and the station is marked, and anti-correcting the differentiated time and the reverse differentiated time are adjusted. In the unified reference time, to operate monitoring and the fault analysis after the accident. Relevant experiment results show that the method is effective to avoid the large number of substations losing voltage due to aggressive actions, and significantly reduce the harm caused by the coordinated attack of substations.

1. Introduction

On December 23, 2015, the Ukrainian power grid was hit by a coordinated network attack, which resulted in the loss of load of the power physical system and even the chain failure, This event is a typical case of a system failure caused by a network attack on the power secondary system, it is considered as a milestone event that information security affects the operation of the power system [1]-[2]. It is also thought to be the first blackout caused by network attacks. After this incident, governments gradually pay more attention to the impact of network attacks on power systems and conduct self-inspection on network security through simulating attacks [3]. Network attacks are easy to achieve multiple substation coordinated attacks, such as penetration invasion of malicious software at the same time in many 220kv substations and above voltage grade of tripping attack, maybe to trigger 3 level and above large blackout accident risk [4]-[5].

The existing papers on coordinated attack are mainly about modelling and detection methods. The definition of network coordination attack for power system is given in [1]. Paper [6] proposes modeling and analysis of network coordinated attacks based on enhanced attack tree and tree finite state automata model. Unfortunately, this model cannot predict some new network coordinated attack behaviors. The author in paper [7] proposes the coordinated attack strategy of firepower/net warfare system is not very effective for the network attack algorithm. The mathematical model of the accused network has a certain gap with the real situation and cannot be used in practice. In paper [8], decomposes the detection into timing-based and space-based action-based host actions detection. In paper [9], puts forward iteration method for multiple optimization and used for some protection of greedy heuristic algorithm is used to solve the current coordinated attack protection problems that may occur.

2. Related Technology

Modern electric power system widely uses BDS or GPS global clock synchronization system, such as access to global synchronization time [10], this protocol can print global synchronization time sequence of events within the station tag [11]. Substations are equipped with a public time synchronization system [12].Once malicious software invades the substation automation system, it only needs to set the attack time in advance, and can perform coordinated attacks based on the global synchronous clock of the plant station where there is no communication. The Diagram of coordinated attack principle based on time is shown in figure 1.

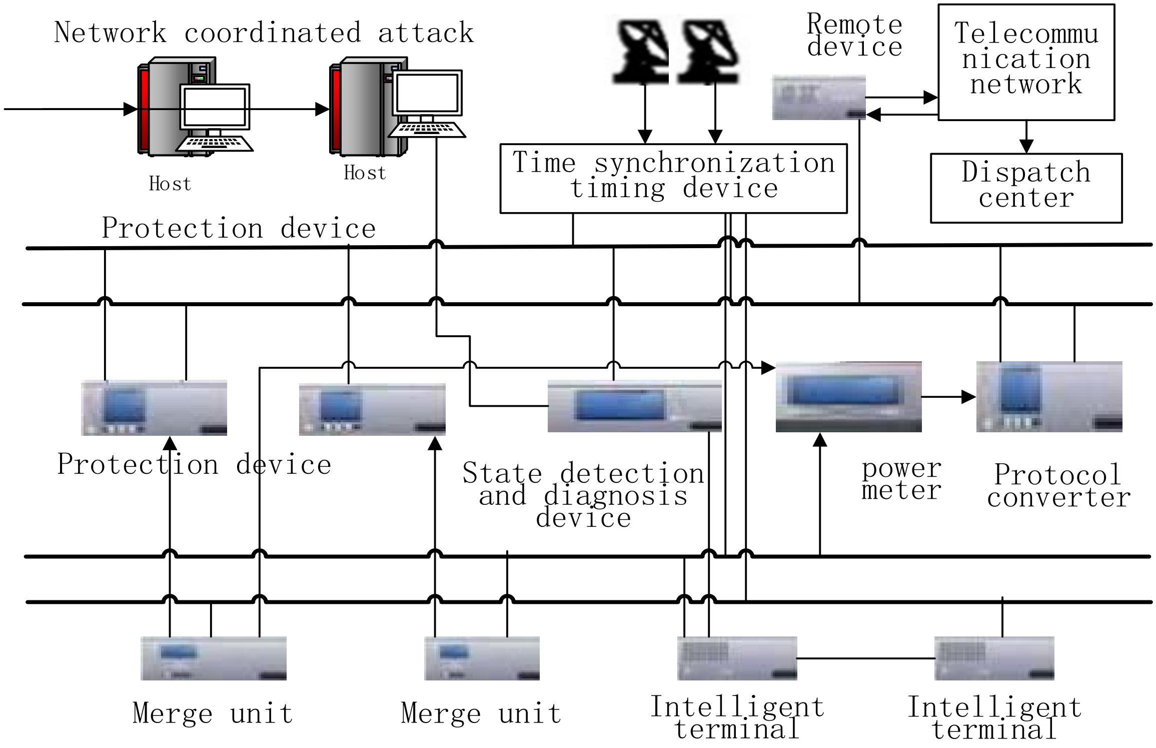

Figure 1: Coordinated Attack Principle Based on Time.

3. Coordinated Attack Based on Time Protection Scheme Design

3.1. Design Ideas

Globally synchronized clocks may become a powerful tool for substation directed attacks against malicious software to initiate coordinated attacks [13]-[14].

Time differentiation management can be carried out in the global synchronous clock system of intelligent substation, different substations for different synchronous clock adjustment, so that each substation synchronization clock staggers the global synchronization time, in the scheduling side of the information containing time sequence anti-correction design to obtain the global synchronous time before substation differentiation, when a directional attack malware that invades a substation automation system initiates a synchronous attack according to a predetermined time, only a single substation will be attacked, and the resulting loss will be significantly lower than the simultaneous loss of voltage at multiple substations.

3.2. Differentiated Time Management Design

The time compensating device of the global synchronous clock system of the smart substation is shown in figure 2. In this scheme, time management is differentiated by software.

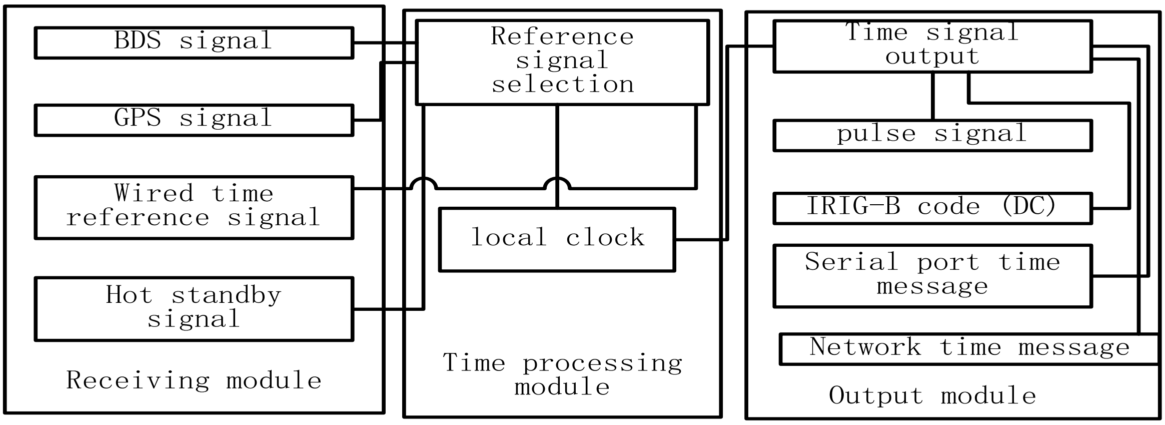

Figure 2: Basic composition of time synchronization device.

3.3. Differentiated Time Adjustment Method

Considering various factors to determine the differential time T, including the existing time for the substation network attack detection to identify the network attack C, the dispatch side sends out control information to each substation to adjust the substation response attack time M and the repaired substation repair time F, so there is a difference in time: T=C+M+F. Among them, C, M, and F are limited by different grid environments and some objective reasons. In different regions, time T naturally varies.

3.4. Time Anti-correction Design of the Dispatcher

The SCADA in the power dispatching automation system receives the data sent by each substation remote control terminal through the data transmission network [15]. Before the SCADA acquisition, the hardware time adjustment module is added, including the differential time. The anti-collation and control information adjustment module with time stamps sent to the substation by the dispatch to solve the synchronization problem between the time scales of the substation and the global synchronous clock and the dispatch for the substation Control information time difference.

4. Experiment Analysis

4.1. Multiple Substation Combinatorial Simulation Analysis

Simulation experiment analysis of IEEE 14 node system as shown in figure 3 is applied. Nodes 5 and 6 and nodes 4, 7, 8, and 9 are deconstructed from a single substation.

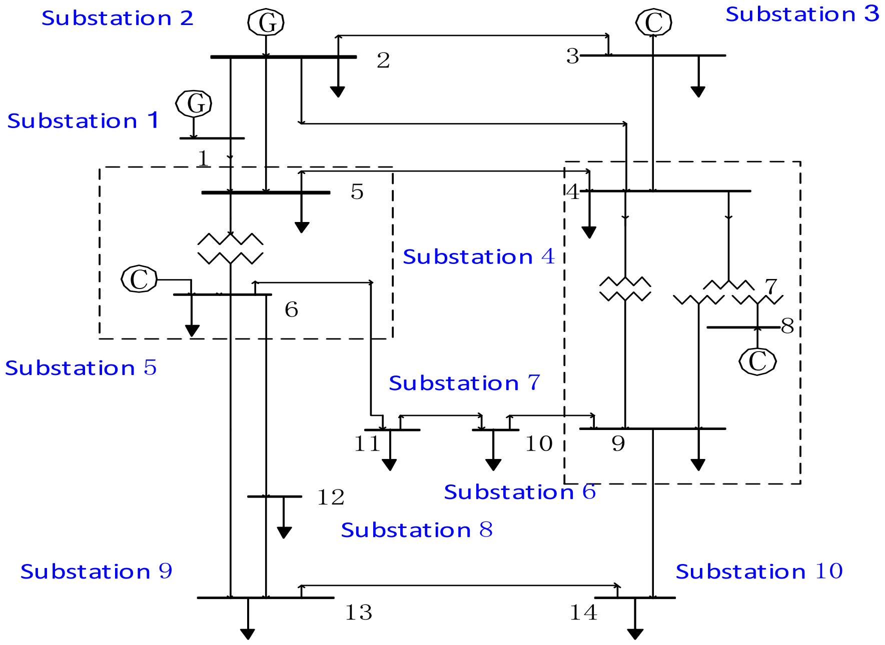

Figure 3: Combination diagram of the substation of the IEEE 14-node system.

The IEEE 14-node system is simulated in Matpower and the total active power of the system is 272.39 MW and the load is 259 MW. Refer to paper [16] for specific parameter settings.

Using Matpower to carry out the simulation calculation single substation which was fully stopped, the load loss of all substations is shown in Table 1. The average loss load is 25.9MW when a single substation suffers complete loss of voltage. The standard deviation of loss load is 30.8219MW.

Table 1: The total stop loss load of a single transformer station.

Substation number	1	2	3	4	5	6	7	8	9	10
Loss of load(MW)	0	21.7	94.2	77.3	18.8	9	3.5	6.1	13.5	14.9

As the number of fully-stopped substations increases, the possible combination for attack increases, and the loss load at the time of shutdown of multiple substations will increase significantly. In order to simplify the analysis, only the combination of all three stop substations is selected for simulation analysis. There are 120 kinds of all substation completely shutdown combinations for the three substations.

After the simulation of the substation attacked combination scene is completed, the loss load data is plotted as shown in figure 4. Among them, the vertical axis represents the number of losses, and the horizontal axis represents the corresponding combination number of the substation. The cylinder identifies the substation's load loss under the corresponding attack combination. The substation complete shutdown loss is identified by a blue fold line, and the turning point is the corresponding substation loss load.

After the synchronization time of each substation is adjusted, each attack only causes a single completely shutdown of the substation, and the load loss is significantly lower than that of the multi-station combination scenario.

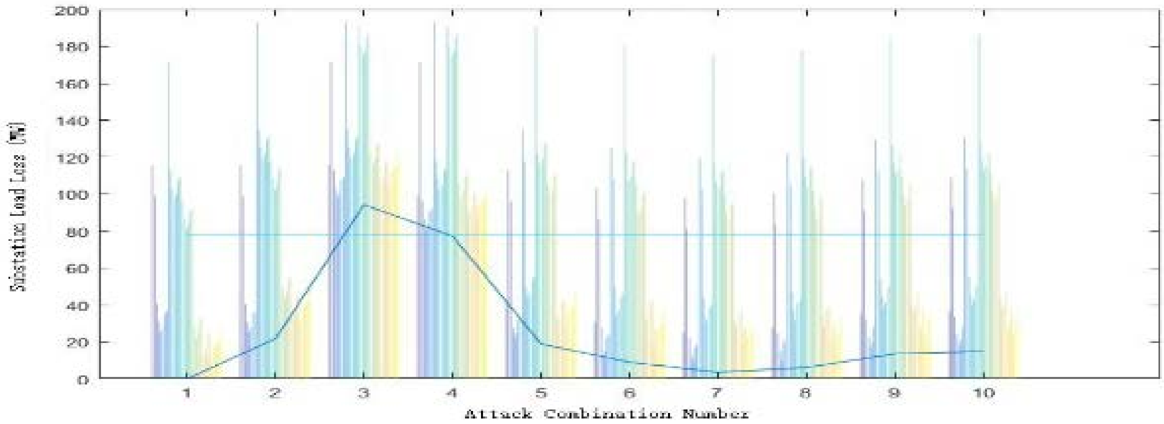

Figure 4: Substation coordinated attack loss load.

4.2. Selectively Differentiated Time Management Substation Combination Attack Protection Simulation Analysis

The No.3 and No.4 substations with the highest load loss are selected for differential adjustment of the in-station synchronization clock so that the two substations could not be combined with the other 8 substations. At this time, the number of attack combinations of the substations is 56.According to the same method of simulation, the loss of load data is plotted in figure 5.

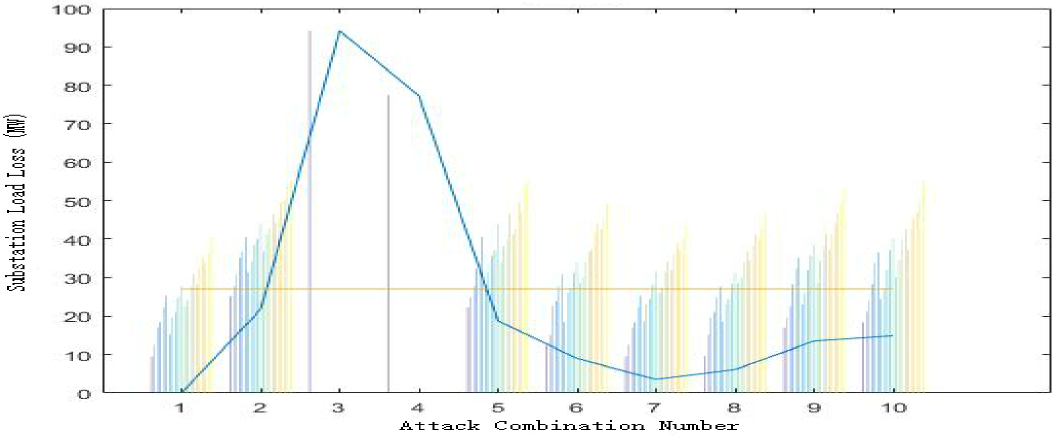

Figure 5: Selective to differentiate time management substation combination attack's load loss.

Compare the loss load of the unadjusted clock, the selective adjustment clock, and the all substation adjusted clock as shown in Table 2.

Table 2: Comparison of Loss Loads

plan Load evaluation	Unadjusted clock	Some substations adjust clocks	All substations adjust the clock
Average loss load (MW)	77.7	27.0667	25.9
Loss of load standard deviation (MW)	47.0812	16.9395	30.8219
Maximum loss load (MW)	193.2	94.2	94.2

Substations No.3 and No.4 do not perform attack combinations with other substations. The losses of the corresponding attack combination and single station completely shutdown loss are 94.2MW and 77.3MW. The self-access load is large, and the No.3 substation can also guarantee the overall structure of the power grid. Therefore, the number of losses under other combinations of attacks is significantly lower. The maximum loss load for the combined attack was 94.2 MW, the average loss load was 16.9395 MW, and the standard deviation for the loss load was 27.0667 MW. Compared with the system without synchronous clock differential management in Figure 4, after the selective management of synchronous clock selectivity, the maximum loss load decreased from 193.2MW to 94.2MW, the loss load decreased by 51.2%, and the average loss load dropped from 77.7 MW to 27.0667 MW, which reduced the average loss load by 65.2%, and the protective effect is close to the clock adjustment of all substations which average loss load of 25.9MW.

5. Conclusions

This paper gives the principle of collaborative attack based on time to analyze network coordinated attacks. The method proposes a differentiated management method based on synchronous clocks in substations. When directional attack malware that invades multiple substations initiates a coordinated attack based on synchronized clocks, it can only cause a single substation to stop and avoid a blackout. Experimental simulation analysis shows that the application of the proposed method in a few key sites can significantly reduce the loss of multi-station coordinated attacks.

Acknowledgements

The paper is supported by the Fundamental Research Funds for the Central Universities (2018ZD06).

References

[1] Liu Nian, Yu Xinghuo, Zhang Jianhua et al. "Coordinated Cyber-attack:Inference and Thinking of Incident on Ukrainian Power Grid". Automation of Electric Power Systems, 2016, 40(6):144-147.

[2] Liang G, Weller S R, Zhao J, et al. The 2015 Ukraine Blackout: Implications for False Data Injection Attacks[J]. IEEE Transactions on Power Systems, 2016, PP(99):1-1.

[3] Tang Wei, Chen Qian, Li Mengya, et al."Overview on Cyber-attacks Against Cyber Physical Power System". Automation of Electric Power Systems,2016,40(17):59-69.

[4] Li Tian, Su Sheng, Yang Hongming, et al. "Attacks and Cyber Security Defense in Cyber-physical Power System".Automation of Electric Power Systems,2017,(22):162-167.

[5] Guo Qinglai, Xin Yujun, Wang Jianhui, et al. "Comprehensive Security Assessment for a Cyber Physical Energy System:a Lesson from Ukraine Blackout".Automation of Electric Power Systems.2016 40(5):145-147.

[6] Wang Jiang,"Modeling and Analyzing Network Coordinated Attack", thesis.XiDian Uniuersity,2014.

[7] Wang Yuyang, "Research on the Cooperative Attack Decision Algorithm Based on Complex Network", thesis.Wuhan University of Technology,2015.

[8] Xiaochuan, Hu Changzhen, "Tan Huimin. Study of network coordinated attack and its detecting mothod". ComputerApplications,2004(11):25-27.

[9] Xiang Y, Wang L, Liu N. "Coordinated attacks on electric power systems in a cyber-physical environment". Electric Power Systems Research, 2017, 149:156-168.

[10] Li Jungang, Liu Xing, Zhang Aimin, et al. "Research on redundant technology of IEEE1588 clock synchronization system in smart substation". Power System Protection and Control,2015,(20):97-101.

[11] Dominicis C M D, Ferrari P, Flammini A, et al. "On the Use of IEEE 1588 in Existing IEC 61850-Based SASs: Current Behavior and Future Challenges". IEEE Transactions on Instrumentation & Measurement, 2011, 60(9):3070-3081.

[12] Wang K, Hu Y H, Ma H J." Research and design on time synchronization technology of smart substation based on IEEE1588",International Conference on Advanced Power System Automation and Protection. IEEE, 2012:2244-2248.

[13] Huang Xin, Wang Yongfu, Zhang Daoong, et al. "Smart Substation IEC 61588 Time Synchronization System and

Safety Evaluation". Automation of Electric Power Systems. 2012, 36(13):76-80.

[14] Zhao Xuyang, Zhang Daonong. "Research and Analysis on Time Synchronization Online Monitoring Technology of Smart Substation". 2013 Annual Meeting of China Electrical Engineering Society.2013:1-4.

[15] Zheng Zongqiang, Yan Mingyu, Peng Hui, et al. "Architecture and Key Technologies of Distributed SCADA System for Power Dispatching and Control". Automation of Electric Power Systems, 2017,41(5):71-77.

[16] Han Xiaoqing, Xiao Yu, Zhang Haiyan." The application of MATPOWER in the real-time electricity price of the optimal power system". JOURNAL OF TAIYUAN UNIVERSITY OF TECHNOLOGY,2005,(3):242-245.