Published article:

T. R. B. Kushal, Z. Gao, J. Wang, and M. S. Illindala, "Causal Chain of Time Delay Attack on Synchronous Generator Control," in *2020 IEEE Power & Energy Society General Meeting (PESGM)*, Aug. 2020, pp. 1–5, doi: 10.1109/PESGM41954.2020.9281666.

Causal Chain of Time Delay Attack on Synchronous Generator Control

Tazim Ridwan Billah Kushal, Ziran Gao, Jiankang Wang, and Mahesh S. Illindala
Department of Electrical and Computer Engineering
The Ohio State University
Columbus, Ohio 43210
Email: kushal.1@osu.edu

***Abstract*—Wide integration of information and communication technology (ICT) in modern power grids has brought many benefits as well as the risk of cyber attacks. A critical step towards defending grid cyber security is to understand the cyber-physical causal chain, which describes the progression of intrusion in cyber-space leading to the formation of consequences on the physical power grid. In this paper, we develop an attack vector for a time delay attack at load frequency control in the power grid. Distinct from existing works, which are separately focused on cyber intrusion, grid response, or testbed validation, the proposed attack vector for the first time provides a full cyber-physical causal chain. It targets specific vulnerabilities in the protocols, performs a denial-of-service (DoS) attack, induces the delays in control loop, and destabilizes grid frequency. The proposed attack vector is proved in theory, presented as an attack tree, and validated in an experimental environment. The results will provide valuable insights to develop security measures and robust controls against time delay attacks.**

***Index Terms*—Cyber-physical systems, cyber security, SCADA systems, time delay.**

I. Introduction

Modernization of power grid is characterized by the integration and advancement of its communication infrastructure, which enables fast data transmission over wide areas. While it has brought many benefits, such as reliable and robust operation, economic decisions, and end-user convenience, it also creates risks of cyber attacks due to two reasons.

First, communications of power grid has become increasingly reliant on open communication protocols, such as the ubiquitous Internet Protocol (IP) [1]. While open communication can fulfill the requirement of high volume data transmission, it does not provide the 'closed environment' as the proprietary protocols and channels, which have been traditionally adopted for control and monitoring in the power grid. Secondly, security solutions for information and communications technology (ICT) systems may not be applicable in power systems [1]. On the one hand, the power grid, as a cyber-physical system (CPS), prioritizes time-critical operation reliability and therefore seeks to minimize latency [2]. On the other hand, specialized protocols, such as DNP3 and Modbus, are adopted in Supervisory Control and Data Acquisition (SCADA) systems [3]. These protocols were developed without security features and are not natively compatible with most ICT security measures [4].

A critical step to defend power grid cyber security is to understand the cyber-physical causal chain of attacks: how the initial cyber intrusion penetrates through the communication infrastructure, induces physical grid responses, and finally inflicts consequences on the power grid. In literature, attack vectors have been studied in attempts to reveal the causal chain in the cyber infrastructure. In [5], an information-based security model evaluates the viability of cyber attack paths. Anomaly-based detection of cyber attacks on SCADA is studied in [6]. However, these studies equate cyber security of CPS to ICT systems by neglecting or simplifying the formation of attack consequences on the physical grid. Since reliability standards make the physical grid robust to disturbances such as measurement errors, many cyber-side intrusions may not inflict any consequences, thus studying their causal chain is trivial.

Complimentary to the studies on cyber intrusion, many studies focus on the impact analysis of attacks on the physical grid. The authors of [7] implemented a DoS cyber attack, which caused a delay in the tripping signal reaching a circuit breaker. Data integrity attacks by modification of network packets in substation communication were studied in [8]. In [9], the concept of reachability was used to study the impact of cyber attacks on Automatic Generation Control (AGC) of the grid. While showing the attack consequences, these works assume successful penetration of the cyber infrastructure without providing a valid rigorous methodology.

Distinct from existing works, this paper proposes a complete cyber-physical causal chain. In particular, we focus on the Time Delay Attack (TDA). Time delays in the power system controllers may adversely affect dynamic stability in applications such as load frequency control (LFC) [10]. While natural delays induced in communications over a Wide Area Network (WAN) can be dealt with by designing controllers that dampen oscillations [11], TDAs could cause more severe consequences and be more difficult to prevent, because (1) devices that use open communication protocols can be targeted by DoS attacks that prevent timely exchange of information such as measurement data and control commands [12], and (2) SCADA is vulnerable to cyber-attacks because latency concerns may prevent installation of firewalls and application range of encryption [4], [13].

Recently, TDA against power grid has gained more atten-

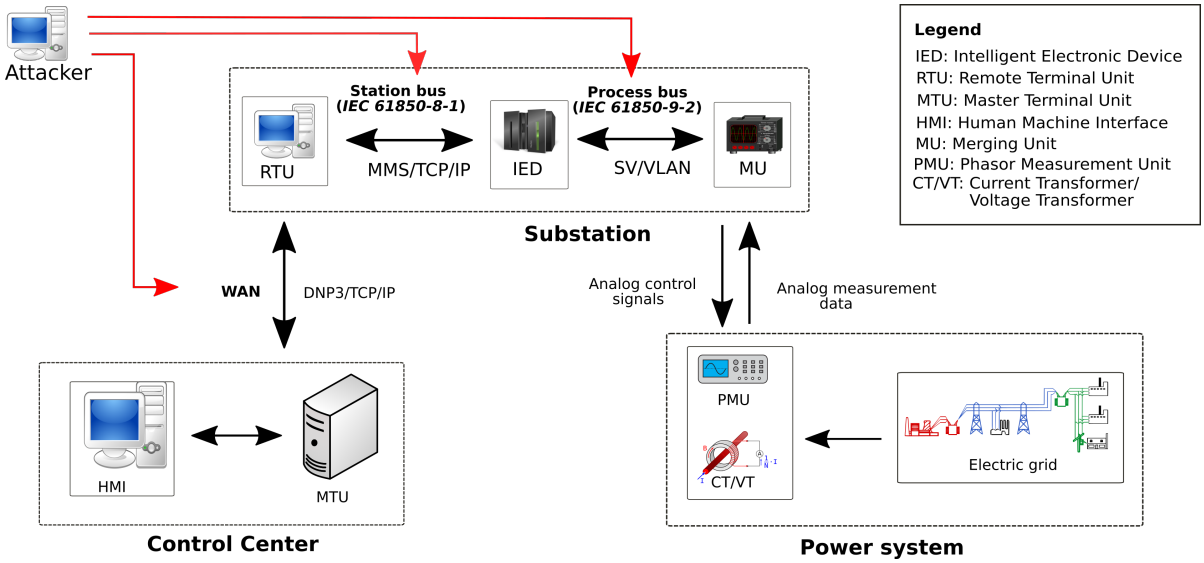

Fig. 1. Overview of SCADA system focused on DNP3 and IEC 61850 communication.

tion. The destabilizing effect of TDA on the LFC of a two-area power system is studied in [14] using a state-space model. The analysis of TDAs in [15] showed that causing delays above a certain margin leads to unstable dynamics. However, despite the assumption that these delays originate from cyber intrusion, only the physical causal chain is described in these works. On the contrary, testbeds have been used to simulate DoS attacks on power system communications that lead to time delays. For example, DoS attacks were observed to cause delays in the sending of tripping commands to circuit breakers [7], [16] and receiving measurements from smart meters [17]. Those works, nevertheless, are difficult to be reproduced on the real-system scale due to negligence of implementation details in grid communication infrastructure or control responses.

To address these deficiencies, this paper develops an attack vector for a time delay attack at load frequency control in the power grid. It targets specific vulnerabilities in the protocols, performs a denial-of-service (DoS) attack, induces the delays in control loop, and destabilizes grid frequency. In particular, Section II provides an overview of the communication protocols used in the grid operation that can be exploited by a TDA. Section III describes the system vulnerabilities and success conditions from the attacker's perspective. The exploited attack vector is validated in Section IV. Finally, Section V concludes the paper. The results in this paper will provide valuable insights to develop security measures and robust controls against time delay attacks.

II. Background of Communication Protocols in Power Grids

Power grid communication adopts specialized protocols for industrial control systems, *i.e.,* SCADA. Fig. 1 shows the communication structure of SCADA as well as the potential cyber-attack entry points. We describe the SCADA communication structure using the seven-layer Open Systems Interconnection (OSI) model [18]. For convenience, the top three layers (application, presentation, and session) are collectively referred to as the application layer. The application, transport, and network layers are of interest in this study. On the application layer, there are two main protocols. Distributed Network Protocol 3.0 (DNP3) was originally developed for SCADA and updated for control and protection within substations and among substations and control centers. IEC 61850 standard was recently proposed by International Electrotechnical Commission (IEC) for substation automation. While DNP3 is more widely used, IEC 61850 will gain more extensive use and potentially replace DNP3 in the future [2]. On the transport layer, Transmission Control Protocol (TCP) is supported by DNP3 and IEC 61850. In addition, the latter could also use User Datagram Protocol (UDP). Unlike TCP, UDP does not guarantee proper delivery of all packets. However, UDP is favored when high throughput is prioritized and missing data packets can be tolerated. IP is used at the network layer.

III. Development of Attack Vector

The cyber-physical causal chain for TDA against LFC, as depicted in Fig. 2, consists of two parts: how initial cyber intrusion leads to delaying packets of control commands, and how the delayed control signal destabilizes power grid through LFC. Each node represents an action of the attacker or a state of the system. There are two types of nodes: AND nodes and OR nodes. While the former requires *all* child nodes to be true for the parent node to be true, the latter requires at least one node to be true for the parent node to be true. The root node represents the ultimate objective (grid destabilization) and the leaves represent initial attacker actions.

A. Cyber-side Intrusion

DoS attacks generally aim to disrupt services by wasting system resources that would be otherwise allocated to those

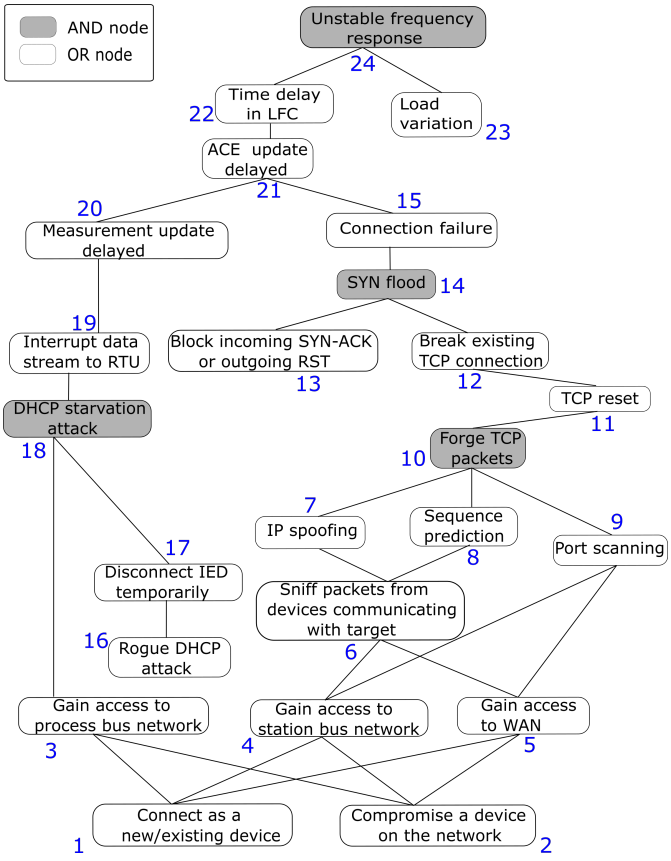

Fig. 2. Attack tree for causing unstable frequency response through DoS attack.

services. This can be achieved in several ways depending on the type of network, what protocols are used by the end nodes, and whether data transfer occurs through a connection. The adversary can select one or more attack vectors and apply them continuously as long as they are viable, in order to destabilize the system. The system in Fig. 1 has two types of networks exposed to potential cyber attacks: TCP/IP and Virtual Local Area Network (VLAN). In channels that use TCP, one way to cause DoS is to exploit a vulnerability in the method used to establish a server-client connection. On VLAN, where no such dedicated connections are formed, service interruption can be caused by preventing devices from properly using the network. A detailed explanation of the vulnerabilities and methods of exploiting them is given below.

1) WAN and Station Bus: The IEC 61850 station bus enables bidirectional communication between the substation RTU and various IEDs using the Manufacturing Message Specification (MMS) protocol over TCP/IP. Communication between the RTU and the MTU in the control center occurs over a Wide Area Network (WAN) using DNP3 over TCP/IP. The MTU houses AGC functionality and interacts with human operators through the human-machine interface (HMI). To establish a reliable server-client connection, TCP uses the three-way handshake protocol. First, a client wishing to connect sends a SYN packet to the server. The server

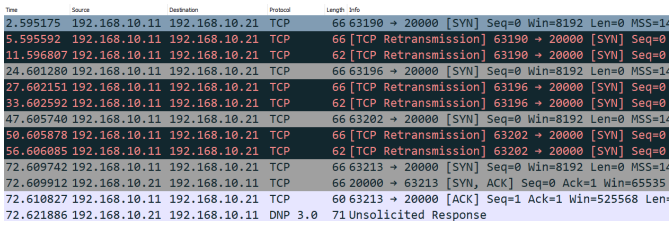

Fig. 3. Client-server connection interrupted by SYN flood attack, shown by captured packets in Wireshark/Npcap.

responds with a SYN-ACK message, creating a half-open connection over which it can receive data but not send. Normally the client responds with an ACK, completing the connection and enabling bidirectional data exchange. Failure to receive an ACK reply causes the server to retransmit the SYN-ACK packet, increasing the timeouts between successive retransmissions. The half-open connection is terminated after a certain number of retransmissions. The server can only have a fixed number of half-open connections in its buffer. An attacker may perform a SYN flood attack, bombarding the server with SYN without the final ACK replies, resulting in numerous half-open connections [20]. This can lead to buffer overflow, causing client SYN packets to be discarded and preventing connections.

This entry point is represented by nodes 4–15 of the attack tree in Fig. 2. Although TCP SYN flood attacks on the grid have been tested before, previous works in the literature such as [7], [17] leave out certain practical details. In a realistic scenario, an intruder is likely to find an existing server-client connection which must be disrupted before initiating the SYN flood (node 12). To force a reconnection attempt, the attacker sends an RST (reset) message to the server while impersonating the client. This forged TCP packet must contain the right source IP address, port numbers and sequence number to be considered legitimate by the server. This information can be obtained by sniffing packets in the network traffic between the server and the client (node 6). Port scanning can identify whether certain TCP ports on the server are active (node 9), which is useful information because the server will reject attacker SYN requests sent to an inactive port. The attacker must also ensure that the server does not receive an RST response to its SYN-ACK (node 13), which would terminate the half-open connection immediately. This can be achieved in two ways. If the attacker uses spoofed IP addresses that do not belong to actual devices, the SYN-ACKs do not go anywhere and no reply is received. Using a real IP address will cause the arrival of SYN-ACKs, which must then be ignored or the outgoing RST reply blocked.

2) Process Bus: Measurement data from CTs, VTs, and PMUs are communicated to IEDs over the process bus in the Sampled Values (SV) format. A merging unit (MU) is a device that transforms the analog data into SV and transfers it over the process bus as shown in Fig. 1. The process bus follows a connectionless publish-subscribe pattern, sending data via multicast over the data link layer to any listening devices.

	Time	Source	Destination	Protocol	Info
✗	0.000000000	0.0.0.0	255.255.255.255	DHCP	DHCP Discover
	1.001677904	192.168.110.5	192.168.110.7	DHCP	DHCP Offer
✗	2.001739692	0.0.0.0	255.255.255.255	DHCP	DHCP Discover
	2.001919261	192.168.110.5	192.168.110.7	DHCP	DHCP Offer
✗	4.003724673	0.0.0.0	255.255.255.255	DHCP	DHCP Discover
	4.003904593	192.168.110.5	192.168.110.7	DHCP	DHCP Offer
✗	6.005881674	0.0.0.0	255.255.255.255	DHCP	DHCP Discover
✗	8.008806574	0.0.0.0	255.255.255.255	DHCP	DHCP Discover
✗	10.011240467	0.0.0.0	255.255.255.255	DHCP	DHCP Discover
✗	12.013437337	0.0.0.0	255.255.255.255	DHCP	DHCP Discover
✗	14.015902599	0.0.0.0	255.255.255.255	DHCP	DHCP Discover
✗	16.018195909	0.0.0.0	255.255.255.255	DHCP	DHCP Discover
✗	18.021143460	0.0.0.0	255.255.255.255	DHCP	DHCP Discover
✓	19.268165297	0.0.0.0	255.255.255.255	DHCP	DHCP Discover
✗	21.269134619	0.0.0.0	255.255.255.255	DHCP	DHCP Discover
✓	22.064752271	0.0.0.0	255.255.255.255	DHCP	DHCP Discover
	59.305230382	192.168.110.5	192.168.110.7	DHCP	DHCP Offer
✓	59.305429162	0.0.0.0	255.255.255.255	DHCP	DHCP Request
	59.378853282	192.168.110.5	192.168.110.7	DHCP	DHCP ACK

Fig. 4. DHCP starvation attack, shown by captured packets in Wireshark/Npcap. Malicious packets are marked by red crosses.

The application sends the payload (SV data) directly to the data link layer without going through transport and network. Devices on the process bus are grouped at the data link layer on a VLAN as specified by the IEEE 802.1Q standard, allowing them to behave as if they are physically connected to the same network switch. Due to the inherent limitations of the original IEC 61850 architecture with regard to scalability and bandwidth utilization, the modernized standard also allows SV packets to be transferred between VLANs through IP multicasting [19].

The attack on the process bus is represented by the branch of nodes 3 and 16–20 in Fig. 2. Lack of authentication and dedicated channels make eavesdropping and interruption of network traffic easier, exposing the network to DoS and man-in-the-middle (MITM) attacks [21]. One way to cause DoS in the VLAN is to target the Dynamic Host Configuration Protocol (DHCP), which dynamically assigns IP addresses to each device with a data link layer Media Access Control (MAC) address to allow them to use the network [22]. Upon receiving a DHCPDISCOVER broadcast message from a client looking to connect, the DHCP server sends a DHCPOFFER back to indicate that it has an available IP address. The client responds with a DHCPREQUEST for the IP address, to which the server replies with DHCPACK to finalize the IP address assignment. The IP address is allocated to the client for a certain amount of time, called the lease time, and must be periodically renewed. To disrupt this process, the attacker first sets up a rogue DHCP server that sends the wrong configuration to the client. Then a DHCP starvation attack is launched, flooding the legitimate server with DHCPDISCOVER messages from spoofed MAC addresses and "starving" the network of IP address by depleting the available pool [22], rendering the client temporarily unable to send data.

B. Attack Consequences in Physical Grid

The target of the TDA is secondary control of system frequency, which depends on remote communication, unlike localized primary control. A proportional-integral (PI) controller adjusts the generator active power output based on the Area Control Error (ACE). The ACE signal calculated by the AGC is the difference between the actual and scheduled power output and is sent every 4 seconds from the control center to the substation. For a single-area system, the ACE calculation is based on Δf, the deviation of the system frequency from the nominal value, as shown in Fig. 5. The total change in active power output is the sum of the adjustments from the primary and secondary control loops, *i.e.,* $\Delta P = \Delta P_1 + \Delta P_2$. The system frequency is estimated from the time intervals between voltage zero crossings. A delay in measurement data reaching the control center or control commands reaching the generator could potentially cause instability in the frequency response, as shown in the analysis of the LFC state-space model in [15]. Since the model uses an output feedback controller, delays in either measurement or control would have this destabilizing effect.

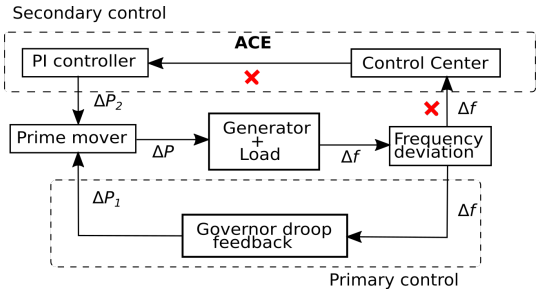

Fig. 5. Load frequency control diagram, with attack locations marked by red crosses.

IV. Simulation Results

To simulate TDAs caused by DoS attacks in the cyber domain, a testbed based on Fig. 1 was used. DNP3 and IEC 61850 communications were implemented using open-source libraries: *opendnp3* is an implementation of DNP3 in C++ and *libIEC61850* provides a C library for MMS and SV protocols in IEC61850. SYN flooding attack was performed by *hping3*, a network penetration testing tool capable of sending any number of customizable TCP/IP packets over a network. DHCP starvation attack was simulated by running the *dhcpstarv* program on the LAN. A synchronous generator and its controls were implemented in MATLAB/Simulink to simulate single-area LFC. Network packets were captured by Wireshark/Npcap to show the effect of the attacks on the communication channels. Three different entry points for the TDA are considered, as shown in Fig. 1, with the same ultimate effect of causing a delay in the update of the feedback control input in the synchronous generator.

Results of the TCP SYN flood are shown in Fig. 3 through data packets in the network. After receiving no reply for the first SYN message, the client retransmits it twice, 3 and 9 seconds after the first, before dropping the attempt. This behavior is characteristic of the Windows operating system, on which the programs were run, and both the timeouts and number of retransmissions would be different for Linux or

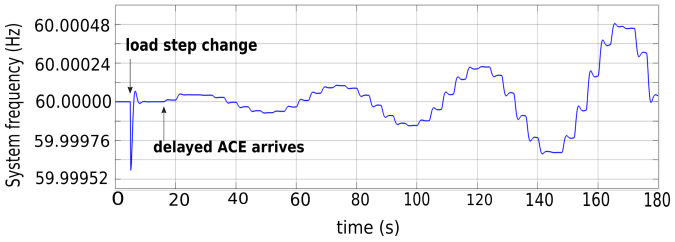

Fig. 6. Frequency response of the synchronous generator for a delay of 10 seconds.

BSD systems [20]. When a server-client connection does not exist or has been broken by a TCP reset attack, a successful SYN flood will prevent data exchange since the three-way handshake cannot be completed until the flood stops. Fig. 4 shows the packets captured during a DHCP starvation attack, where malicious DHCPDISCOVER messages are marked by red crosses and messages from legitimate clients are indicated by green tick marks. The DHCP server initially offers an available IP address to the spoofed MAC addresses. However, when flooded with DHCPDISCOVER messages, the server becomes unresponsive to both attacker and client messages as the pool of IP addresses is exhausted. The client can obtain an IP address only after the starvation attack has ceased.

Fig. 6 shows the frequency response of the system for the first three minutes with a delay of 10 seconds in the loop. At $t = 5\,s$, at 20% step change in load occurs, causing the dip followed by restoration of the nominal frequency by the primary droop feedback. However, the brief frequency deviation also generates an ACE that arrives at $t = 15\,s$ and leads to an unstable response. As reported in [15], the delay margin needs to be large enough to cause instability. Delays that are too small may have no effect or cause decaying oscillations. For the system tested in the simulation, a delay of 10 seconds was observed to cause the oscillations to increase in magnitude over time.

V. Conclusion

A critical step towards defending grid cyber security is to understand the cyber-physical causal chain. In this paper, we develop an attack vector for a Time Delay Attack at load frequency control in the power grid. The contribution of this paper is twofold: (1) It proposes a TDA attack vector, which for the first time reveals the full cyber-physical causal chain of TDA on the power grid. It targets specific vulnerabilities in the protocols, performs a denial-of-service (DoS) attack, induces the delays in control loop, and destabilizes grid frequency. (2) The proposed attack vector is reproducible at the real-system scale. It defines the specific sequence of steps to induce delays in LFC parameters. A testbed was constructed for the validation purpose. Test results demonstrate that in a grid with centralized LFC, it is possible to launch TDAs to destabilize frequency during changing system conditions such as load variation. The results will provide valuable insights to develop security measures and robust controls against time delay attacks.

References

[1] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, and A. Hahn, "Guide to Industrial Control Systems (ICS) Security," Nat. Inst. of Standards and Technology, SP 800-82 Rev. 2, Gaithersburg, MD, Jun. 2015.

[2] W. Wang and Z. Lu, "Cyber security in the Smart Grid: Survey and challenges," *Comput. Networks*, vol. 57, no. 5, pp. 1344–1371, 2013.

[3] M. H. Cintuglu, O. A. Mohammed, K. Akkaya, and A. S. Uluagac, "A Survey on Smart Grid Cyber-Physical System Testbeds," *IEEE Commun. Surv. Tutorials*, vol. 19, no. 1, pp. 446–464, 2017.

[4] C. C. Sun, A. Hahn, and C. C. Liu, "Cyber security of a power grid: State-of-the-art," *Int. J. Elect. Power Energy Syst.*, vol. 99. Elsevier, pp. 45–56, 01-Jul-2018.

[5] A. Hahn and M. Govindarasu, "Cyber attack exposure evaluation framework for the smart grid," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 835–843, Dec. 2011.

[6] M. Mallouhi, Y. Al-Nashif, D. Cox, T. Chadaga, and S. Hariri, "A testbed for analyzing security of SCADA control systems (TASSCS)," in *IEEE PES Innovative Smart Grid Technologies 2011*, Anaheim, CA, 2011.

[7] B. Chen, N. Pattanaik, A. Goulart, K. L. Butler-Purry, and D. Kundur, "Implementing attacks for modbus/TCP protocol in a real-time cyber physical system test bed," in *Proc. 2015 IEEE Int. Workshop Tech. Committee Commun. Qual. Rel.*, Charleston, SC, USA, 2015, pp. 1–6.

[8] C. C. Sun, J. Hong, and C. C. Liu, "A co-simulation environment for integrated cyber and power systems," in *2015 IEEE International Conference on Smart Grid Communications*, 2015, pp. 133–138.

[9] P. Mohajerin Esfahani, M. Vrakopoulou, K. Margellos, J. Lygeros, and G. Andersson, "Cyber attack in a two-area power system: Impact identification using reachability," in *2010 American Control Conf.*, 2010, pp. 962–967.

[10] C. K. Zhang, L. Jiang, Q. H. Wu, Y. He, and M. Wu, "Delay-dependent robust load frequency control for time delay power systems," *IEEE Trans. Power Syst.*, vol. 28, no. 3, pp. 2192–2201, 2013.

[11] I. Kamwa, R. Grondin, and Y. Hébert, "Wide-area measurement based stabilizing control of large power systems - A decentralized/hierarchical approach," *IEEE Trans. Power Syst.*, vol. 16, no. 1, pp. 136–153, Feb. 2001.

[12] S. Amin, A. A. Cárdenas, and S. S. Sastry, "Safe and secure networked control systems under denial-of-service attacks," in *12th Int. Conf. Hybrid Systems: Computation and Control*, 2009, vol. 5469, pp. 31–45.

[13] M. Kezunovic and T. Popovic. (2012, Oct. 26). *Wide Area Monitoring, Protection, and Control Systems (WAMPAC): Standards for Cyber Security Requirements* [Online]. Available: http://smartgrid.epri.com/doc/ESRFSD.pdf

[14] A. Sargolzaei, K. Yen, and M. N. Abdelghani, "Delayed inputs attack on load frequency control in smart grid," in *2014 IEEE PES Innovative Smart Grid Technol. Conf.*, 2014, pp. 1–5.

[15] J. K. Wang and C. Peng, "Analysis of time delay attacks against power grid stability," in *2017 2nd Workshop on Cyber-Physical Security and Resilience in Smart Grids*, 2017, pp. 67–72.

[16] G. Dondossola, G. Garrone, J. Szanto, G. Deconinck, T. Loix, and H. Beitollahi, "ICT resilience of power control systems: Experimental results from the CRUTIAL testbeds," in *Proc. Int. Conf. Dependable Systems and Networks*, 2009, pp. 554–559.

[17] C. Queiroz, A. Mahmood, and Z. Tari, "SCADASim – A framework for building SCADA simulations," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 589–597, Dec. 2011.

[18] J. D. Day and H. Zimmermann, "The OSI Reference Model," *Proc. IEEE*, vol. 71, no. 12, pp. 1334–1340, 1983.

[19] M. Kanabar, M. G. Adamiak, and J. Rodrigues, "Optimizing wide area measurement system architectures with advancements in phasor data concentrators (PDCs)," in *IEEE Power and Energy Society General Meeting*, Vancouver, Canada, 2013.

[20] R. K. C. Chang, "Defending against flooding-based distributed denial-of-service attacks: A tutorial," *IEEE Commun. Mag.*, vol. 40, no. 10, pp. 42–51, Oct. 2002.

[21] S. A. Rouiller, "Virtual LAN Security: Weaknesses and Countermeasures," 2006. [Online]. Available: https://www.sans.org/reading-room/whitepapers/networkdevs/paper/1090. [Accessed: 18-Oct-2019].

[22] H. Mukhtar, K. Salah, and Y. Iraqi, "Mitigation of DHCP starvation attack," *Comput. Electr. Eng.*, vol. 38, no. 5, pp. 1115–1128, 2012.