Proceedings of the 2018 Winter Simulation Conference
M. Rabe, A. A. Juan, N. Mustafee, A. Skoogh, S. Jain, and B. Johansson, eds.

VOTNET: HYBRID SIMULATION OF VIRTUAL OPERATIONAL TECHNOLOGY NETWORK FOR CYBERSECURITY ASSESSMENT

Sajal Sarkar
Anand Agrawal
Yong Meng Teo
Ee-Chien Chang

Department of Computer Science
National University of Singapore
Singapore 117417, SINGAPORE

ABSTRACT

Cybersecurity assessment in automation requires a modeling and simulation framework to study the complex relationships between the cyber-based control mechanisms and the power systems. A real power system is not ideal for such an assessment due to potential disruption in operation. In this paper, we propose a simulation model of a virtual operational technology (OT) network in power system automation for cybersecurity assessment. The proposed simulation model is modularized with key components including power system and process, communication, automation, and enterprise network. We discuss Virtual OT Network (VOTNet), a specific instance of the model, in terms of simulated and emulated systems such as programmable logic controller, computing systems, control centers, and software. We evaluate VOTNet under two use cases: different attack scenarios and scalability vs. attack surface to study the impacts of cyber attacks. Particularly, unauthorized access, data manipulation in PLC, and denial of service in SCADA communication are demonstrated.

1 INTRODUCTION

Recently, integrated large-scale generation and distribution in power systems faces new challenges such as load balancing, observability, availability, and stability of the power grid. Although the usage of Industrial Control Systems (ICSs) for automation in OT networks enables us to do load balancing, observability, integration of diverse resources, among others, it depends on Information Technology (IT) which introduces cyber risks. As a result, an OT network is also prone to cyber risks. Further, a number of sophisticated cyberattacks recently targeted OT networks. Therefore, realistic hands-on and experimental research is required to understand and explore cyber challenges in OT networks (Cebula and Young 2010). However, operational systems are not ideal and available for such research due to potential impacts in operations (Hahn et al. 2013). On the other hand, software-based simulations are unable to reflect the potential system states due to oversimplified assumptions. Therefore, research to design a cyber-resilient power grid depends on the availability of infrastructure facilities like virtual OT networks with the computing resources, IEDs, control software, etc., where current cybersecurity challenges, future scopes, and ideas can be evaluated.

Hence, laboratory-based OT networks have become a key platform for cybersecurity research in industrial automation. The development of such a network is an expensive and time-intensive activity that must balance a range of design considerations, such as hardware diversity, scalability, and cybersecurity (Green et al. 2017). Although a few works have been done on such design considerations and their implications to overcome typical drawbacks, most of the works have been done on physical or semi-virtual systems.

In this paper, we propose a hybrid simulation and model for virtual OT networks of power systems automation. The proposed hybrid simulation model incorporates both real and virtual components all possible functionalities of the power system. We present VOTNet, an instance of the proposed simulation framework, and its implementation that integrate computing systems, simulated PLC, emulated communication network, simulated power system, software, and tools. Virtualization is used to address the scalability of VOTNet and to reduce the cost of the VOTNet testbed. To demonstrate the use of VOTNet, we set up an emulated communication network of routers to represent a WAN and model different attack scenarios. Power simulation is performed using the PowerWorld simulator. The main contributions of our work are:

1. We provide a hybrid simulation and modeling framework for OT networks of power system automation consisting of computing systems, emulated communication networks, simulated Modbus PLC, SCADA system and different software.
2. Our hybrid simulation model provides some degree of generality through modularizing the power system as well as process, communication, automation, and enterprise network. We demonstrate this in the VOTNet, an instance of the model, in terms of simulated and emulated instances of different devices such as PLC, network devices, computing systems, software, and tools.
3. We evaluate two use cases, viz., *different attack scenarios* and *scalability vs. attack surface*. Our simulation study stressed the tolerance level of the system by increasing the volume of attack traffic to reach the SCADA system breakdown point. We also discussed the problems associated with scalability of OT networks in general, and what-if analyses after scaling up the VOTNet.

The remainder of the paper is organized as follows. Related work is presented in Section 2, whereas Section 3 presents the background of our work. We discuss VOTNet in Section 4. In Section 5, we evaluate VOTNet in different attack scenarios. Finally, we conclude our work with future directions in Section 6.

2 RELATED WORK

In a power grid, substations are being managed and operated through an IP network from a centralized control center (CC) with several cybersecurity challenges. Thus, power grid automation IP networks have been given a huge attention for their resiliency, efficiency, availability, reliability, and cybersecurity. A number of steps are being taken to make them more resilient, transparent, and observable. While doing this brings a more sustainable power grid, it also opens up new interdependencies and cyber risks. Integrating IT is essential for building an IP network for power systems, but it is even more important to devise effective strategies for cyber risks in power systems' control networks. In the past years, a number of cybersecurity testbeds have been proposed to study cybersecurity issues in power systems automation.

A cybersecurity testbed was developed for a SCADA system in a power grid as well as a mock chemical mixing setup to test wireless and physical security (INL 2016). The intrusion detection systems, firewalls, and encryption links for communication have also been deployed to make it capable and expert in control system applications and cybersecurity. A Virtual Control System Environment (VCSE) is built to investigate SCADA vulnerabilities of energy systems and to conduct operator training, evaluation activities, and mitigation (McDonald et al. 2008). Here, an OPNET system-in-the-loop emulation is used to integrate physical devices with the simulated network where network traffic is monitored using Wireshark. The CRUTIAL project has developed testbeds to explore impacts from various attack scenarios (Dondossola et al. 2009). In (Mallouhi et al. 2011), the Testbed Analyzing Security of SCADA Control System (TASSCS) focused on securing and protecting SCADA systems against a wide range of cyberattacks to evaluate anomaly-based intrusion detection system and its effectiveness. The DIgSILENT power system simulator and substation automation is used for intrusion and defense to feature a cyber-power testbed for providing an environment to both identify attacks and evaluate physical impact (Hong et al. 2011). Here, the authors considered two control centers and two substations in the testbed and they have used ICCP and DNP 3.0 protocols for communication between substation devices and control centers.

SCADASim (Queiroz et al. 2011) is an emulated communication network to analyze and study the impact of cyber attacks in the performance of SCADA protocols. A cyber-physical testbed is presented by Morris et al. (2011) for critical infrastructures in industrial control networks. Here, cybersecurity vulnerabilities and forensic studies are performed using Modbus and DNP3 protocols. Virtual Power System Testbed (VPST) is developed to combine both simulation and physical elements together (Bergman et al. 2009) by leveraging the cyberattack capability of DETERLab (Mirkovic and Benzel 2012). VPST used PowerWorld simulator and Real-Time Immersive Network Simulation Environment (RINSE) where physical devices and industry-standard software are integrated to develop a realistic control environment. This testbed is also facilitated to integrate other testbeds across the country to analyze the nature of cyber attacks on a large-scale system. A Network Intrusion Detection System (NIDS) was developed by Koutsandria et al. (2015) for ICSs. An HIL and cyber-in-the-loop Matlab/Simulink environment is considered for the Modbus protocol, which is developed using open source libmodbus. A set of intrusion detection rules is also implemented to check abnormality relying on a packet sequence and the time gap.

The PowerCyber testbed, one of the most comprehensive smart grid testbeds, is developed to support information and communication technology (ICT) and cybersecurity research (Mahnke et al. 2009; Hahn et al. 2013). The testbed is emulating a WAN using Internet-Scale Event and Attack Generation Environment (ISEAGE). RTDS and DigSilent power system simulators are used for power system modeling, where IEDs and PLCs are integrated as hardware components. Cyber-Physical System Testbed is established using RTDS, LabVIEW PXI modules and an OPNET for working with various industrial protocols and technologies (Chen et al. 2014; Chen et al. 2015). Here, researchers can evaluate the performance of the virtual network and physical devices in real time under a comprised scenario of the network. A comprehensive cyber-physical system testbed is implemented with RTDS and a network simulator incorporating actual remote terminal units (RTUs), phasor measurement units (PMUs), and PDC (Vellaithurai et al. 2017; Biswas et al. 2013). In this testbed, a virtual IEEE 14bus system is implemented to investigate wide-area situational awareness, cybersecurity, and network communications. A Wide Area Measurement System (WAMS) testbed is developed by Chakrabortty and Xin (2013) and Weiss et al. (2013) to test remote accessibility. The main focus of the testbed is wide area situational awareness and network communications. VOLTTRON, an intelligent agent platform is developed for coordination of PEV charging with home energy utilization (Haack et al. 2013) to provide platform services such as resource management, authentication, and cryptographic agent code verification for interaction with smart and legacy devices.

3 BACKGROUND

A cybersecurity research and education platform, DeterLab, has been built for cybersecurity experimentation (Mirkovic and Benzel 2012). The DeterLab consists of computing nodes and hardware devices. A set of tools is also deployed in the DeterLab. Users across the globe utilize the platform through a Web-based interface. Similar to DeterLab, the National cybersecurity research and development laboratory (NCL) is built at the National University of Singapore. NCL, a national shared infrastructure, provides computing resources and application services to the local cybersecurity research communities. NCL has used DeterLab software for building its infrastructure, which consists of 200 computing nodes and is capable of providing a wide range of provisioning mechanisms, virtual networks, security data, and security services for cybersecurity research and analysis. Beside different services, NCL carries out research on virtual OT networks for cybersecurity assessment, development of vulnerable environments, etc.

An OT network consists of hardware devices and software that monitors hardware devices and control operations of hardware devices. Unlike IT, OT used for operations and controls in ICSs is isolated as most of those OT network tools for monitoring and operations are mechanical and proprietary in nature. Nowadays, however, OT consists of smart devices to monitor, operate, and control equipment used in power stations, water treatment plants, etc. Therefore, there is an increasing trend to integrate IT in OT systems. Integration of IT with OT enables to make not only systems interconnected, but also to operate and control devices remotely by adopting standard industrial communications protocols (e.g., DNP3, Modbus,

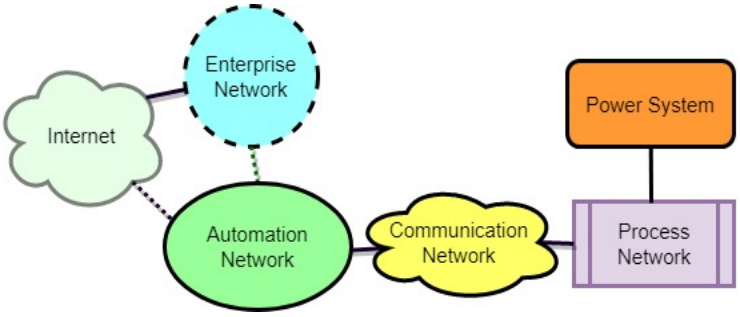

Figure 1: Simulation model of virtual OT network.

Profibus). As a result, there is a drastic reduction in OT system security (Cebula and Young 2010). Hence, the interconnectivity in OT systems brings a number of cybersecurity challenges such as DoS attacks, access control, threats of malware, identity management, vendor dependency, etc.

Security of OT networks has previously relied almost entirely on the standalone nature of OT installations. Nowadays, OT is powered by IT for the corporate goal of widening an organization's ability to monitor, operate, and control its OT systems, whose components are often built without basic cybersecurity requirements (Cole 2017; Cleveland 2012). Therefore, an OT network is no longer air-gapped and there are many security challenges (i.e., DoS attack). An IT network is generally designed considering security aspects in the order of confidentiality, integrity, availability; whereas an OT network requires security aspects in reversed order, viz., availability, integrity, confidentiality. Hence, the previously used traditional cybersecurity approaches in regular IT networks need to be replaced and redesigned to align with the OT network's cybersecurity requirements. Also, an OT system needs highest priorities for protection with enhanced cybersecurity measured, as OT plays an important role in monitoring, operating, and controlling industrial processes in National Critical Infrastructures.

4 APPROACH

4.1 Hybrid Simulation Model

Simulation modeling of a power system automation includes creation of a digital power system automation prototype to analyze and predict its performance. A simulation model helps to understand the system's functionality and behavior under different conditions. In a simulation model, cybersecurity issues in power system automation can also be investigated to study cyber-physical impacts by applying simulation tools.

Figure 1 shows a hybrid simulation model of an OT network with the power system connected directly to a process network, where industrial control protocols aggregate data from field devices. The process network interacts with an automation network through a communication network. The automation network is a power system control network that connects to the Internet for online patch management of deployed computing systems, cybersecurity systems, and others. Most automation networks today are connected to the enterprise network for widening an organization's ability to monitor, operate, and control power systems. We discuss details about the model as part of our VOTNet testbed in the following Section 4.2.

4.2 VOTNet Simulation Testbed

The development of an OT testbed depends on IT deployments to support communication and control functions. Unfortunately, this dependency expands cyber risk in the OT. Designing systems with adequate cybersecurity depends on the availability of testbeds. A testbed is a platform for conducting rigorous, transparent, and replicable testing of scientific theories, computational tools, and new technologies. A testbed can be developed physically using real hardware as well as using virtual systems. A physical testbed can reflect the actual purpose of the testbed, but installation cost and time, manpower, computing,

and hardware resources are main constraints to build a physical testbed. On the other hand, a virtual testbed can be built with less time and cost as well as taking care of different constraints. Therefore, we develop a hybrid virtual OT network testbed of power systems for cybersecurity assessment on a NCL cluster.

A block diagram of the VOTNet testbed is shown in Figure 2. Its key components are a WECC 9bus power system, a substation control center, a communication network and the centralized control center. VOTNet's capabilities include visualization and visualized simulation of the power system, control of the simulated power system's signal and emulated communication network topology, attack scenarios in different components etc. We discuss details of our testbed's components in the following subsections.

4.2.1 WECC/IEEE 9Bus Power System

The 9bus power system of Western Electricity Coordinating Council (WECC) (Hahn et al. 2013) is used as a reference system in our testbed. Figure 3 shows a single-line diagram of a three machine and 9bus power system with three generators (G1-G3), with built-in voltage and speed-regulators, transformers (T1-T3) and loads (D1-D3), as well as 6 (TL1-TL6) transmission lines. Generator G1 is connected to slack bus 1, whereas generators G2 and G3 are connected to PV-bus 2 and 3. Each generator is represented as a voltage source. Loads D1, D2, and D3 are connected with bus bars 8, 5, and 6 respectively.

4.2.2 Substation Control Center

A substation control center is also known as local control center. From this local control center, operators generally control and operate field devices locally. The field devices are connected with the control system (e.g., HMI) via intelligent electronic devices (e.g., PLC).

In VOTNet, the substation control center consists of a network switch, the router-cum firewall (RCF), HMI, simulated PLCs, and the power systems simulator. A simple network diagram of our substation

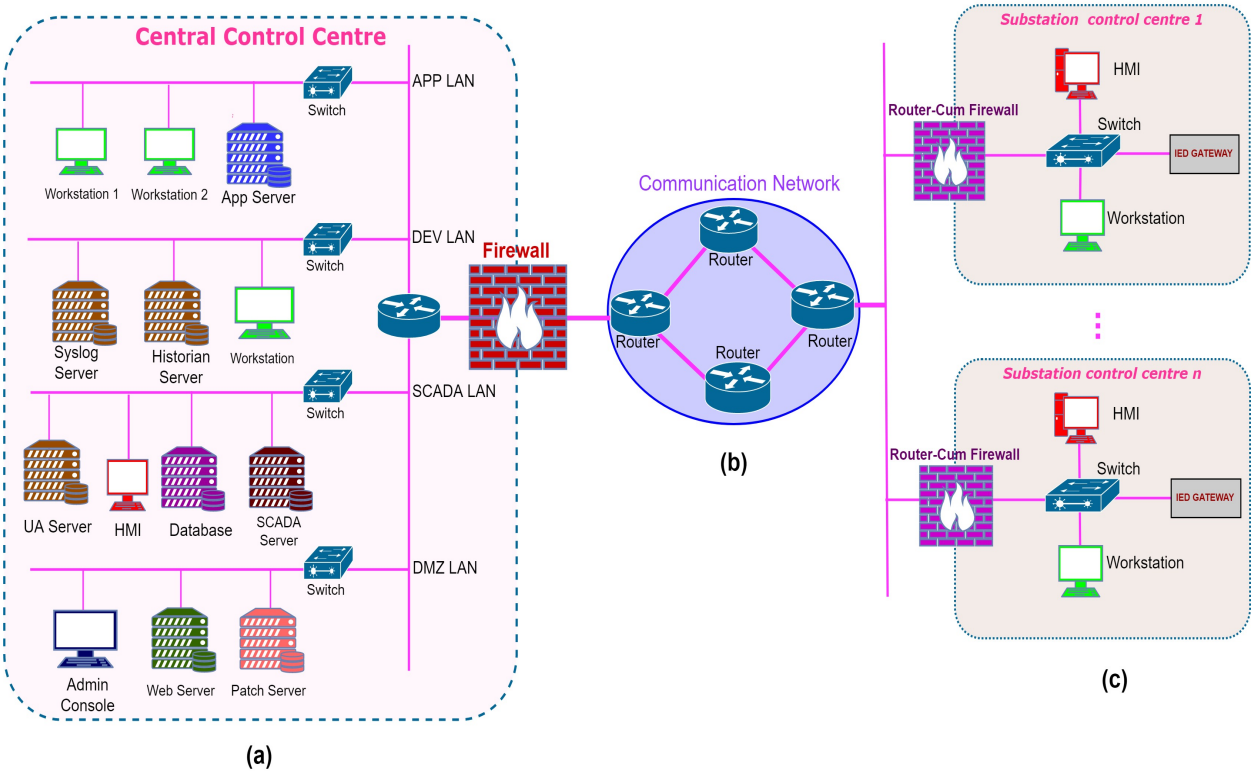

Figure 2: VOTNet hybrid simulation testbed.

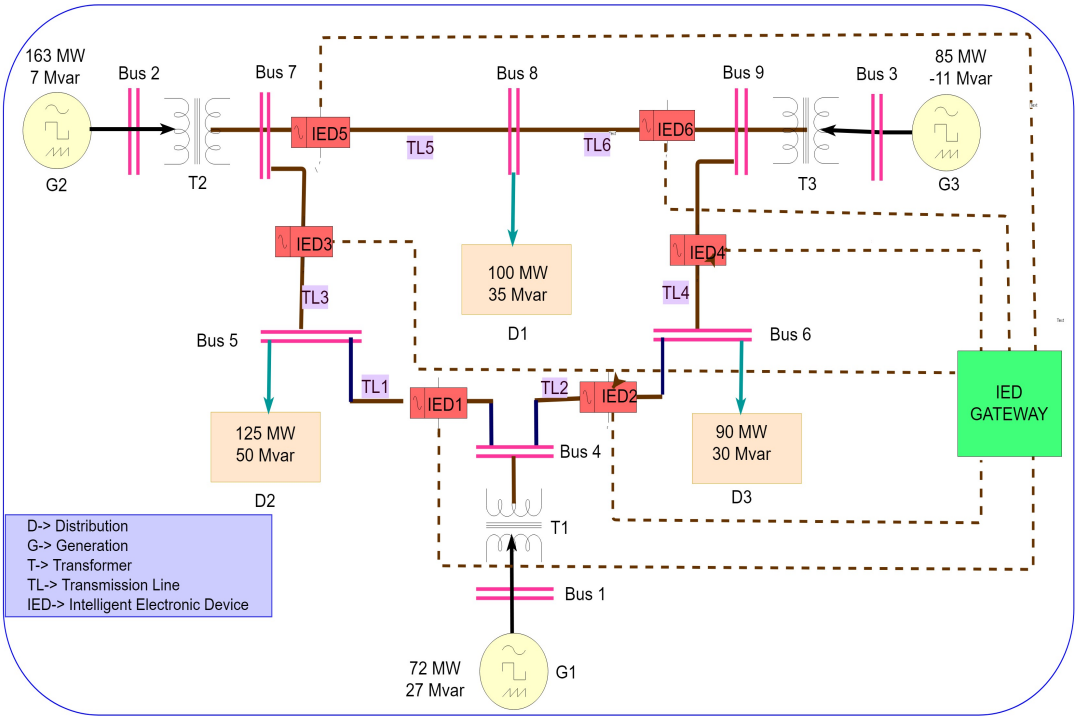

Figure 3: WECC/IEEE 9bus system.

control center is shown in Figure 2(c). The figure shows that the IED gateway is connected with a switch, which is nothing but a virtual machine (VM) installed with Windows 7. The PowerWorld simulator and simulated Modbus PLC is installed in the VM. An HMI is also connected with the switch. The switch is connected with a RCF which passes data to the communication network. The simulated PLC fetches data from the 9bus power system simulated in PowerWorld. The PLC aggregates data from the power system simulator and transmits them to HMI and also to the CC. The PLCs within the substation control center are configured to monitor the status and detect the fault of systems. The local control center's functions include human-in-the-loop control and protection schemes for the field devices. A number of protection schemes can be configured in physical PLCs for transmitting their status and detected faults.

4.2.3 Communication Network

A communication network (CN) consists generally of a network and different network protocols. CN for power system's automation consist of local area network (LAN), wide area network (WAN), industrial communication, and traditional networking protocols. The CN of VOTNet is shown in Figure 2(b), where there are four routers virtually configured on four physical NCL nodes. One end of the network is connected with (CC) through a firewall and the other end of the CN is connected with the substation control center via a RCF. A SCADA protocol, Modbus TCP/IP performs the communication between CC and substation PLCs. Modbus TCP/IP operates to enable routable networks with the scale and exposure properties of a real WAN. The real scale and exposure of the WAN can be utilized to perform various attack studies (DoS, BGP flooding, etc) on availability, redundancy, and resiliency of the network. Communication between CC and substation PLCs is normally in public networks and may be exposed to different kinds of attacks.

4.2.4 Centralized Control Center

The centralized control center of VOTNet is configured for SCADA functionality, which includes collecting data and reading system status from the simulated power system, forwarding data to the SCADA server,

Table 1: LAN and computing system.

LAN	Systems
DMZ LAN	Admin Console-1, Web Server-1, Patch Management Server-1
SCADA LAN	SCADA Server-1, Database, User Authentication Server-1, HMI-1
DEV Server	Historian Server-1, Syslog Server-1. Workstation-1
APP LAN	Application Server-1, Workstation-1, Workstation-2

forwarding operator's commands, and managing historical data of the SCADA system, etc. Most of these functions are being implemented and practiced in industry standards such as SCADA server, HMIs, data replica server, and historian server. The CC network diagram of VOTNet is shown in Figure 2(a). CC networks consist of systems such as DMZ LAN, SCADA LAN, Development (DEV) LAN, and Application (APP) LAN. Each LAN has a few systems for specific requirements. All CC systems are listed in Table 1.

Control operations and monitoring within a CC is similar as within a local control center. However, a CC is a global perspective of control operations and monitoring of the field devices deployed in different substations, and SCADA data are passing from different substations' PLCs to the SCADA server. This is because the SCADA server collects various data, reads status of the devices in every second and displays the collected data and devices' status on the operator's HMI. Based on these information, an operator at the CC can monitor the status of the devices and send commands to the substation for operating the systems.

4.3 Scalability

Modeling a power grid system and studying its scalability is not only difficult due to its existence in various geographical locations, but also real systems are not ideal and available for such a study (Bergman et al. 2009). But, it is an essential requirement to model such systems considering scalability and cybersecurity to study and analyze. Hence, in this work we study and analyze the scalability of VOTNet. The scalability of VOTNet is studied in form of functionality that VOTNet supports and scaling up VOTNet by adding various components (process network, PLCs, VMs, etc.).

Particularly, we have integrated two Modbus PLC simulation systems on two different VMs running on different physical nodes in two substations. The PLCs are connected and configured with local HMI of the respective substation control center and also with the SCADA server (refer Figure 2) installed in the CC. ScadaBR software is installed in the SCADA server as remote control system. It may be noted that in VOTNet we consider two instances of PLCs in two substations, but in order to accommodate a huge number of events generated from substations, it can be extended to further PLCs. It may also be noted that an event is an occurrence that can be monitored. It can be asynchronous and pushed from the PLC to the ScadaBR application. Examples of events could be *start-up PLC*, *PLC operating in steady state*, etc. An event is different from an alarm. An event does not require an operator attention as it does not have a degree of criticality associated with it.

Scaling up a system is a requirement which may invite additional risk. Therefore, scaling up VOTNet inherently increases the attacker surfaces. Thus, in the following sections we describe how different attacks can be launched in increased attack surfaces with the scalability of VOTNet.

4.4 Attack Surface

An attack surface measures the total security risk exposure of a system. It aggregates all known, unknown, reachable, and potentially exploitable weaknesses and vulnerabilities of the system. To successfully defend the system from any possible attack or exploitation, there is a need to understand how attackers can attack the systems (Cole 2017). So, attack modeling is a very efficient way to understand the system's attack surface. An attack model is a set of diagrams and descriptions of how attackers can attack a system whereas an attack surface is a list of system inputs that an attacker can use to compromise a system. Therefore, it

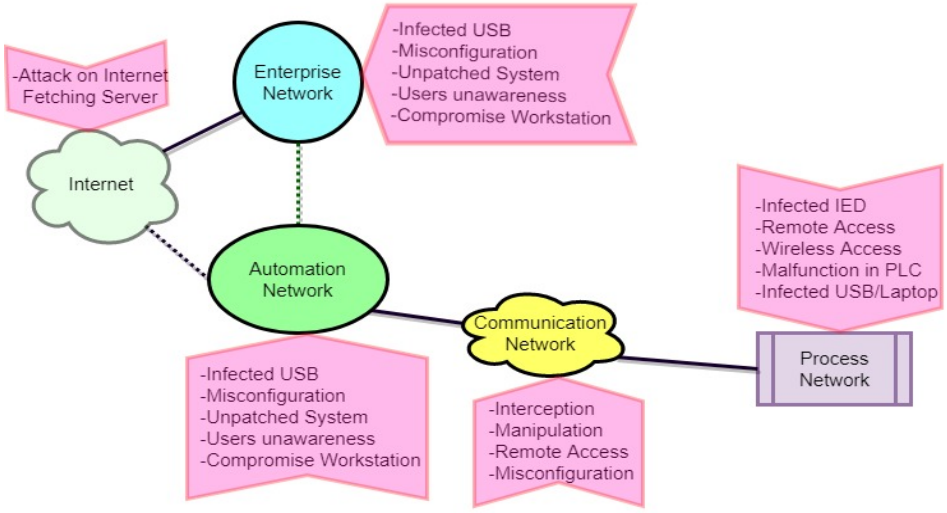

Figure 4: Attack model and surface of OT network.

is obvious that if the attack surface is small, the chance of attack or exploitation is lower. An attack model with corresponding attack surface of our VOTNet is shown in Figure 4. There are four identified attack surfaces associated with the communication network of VOTNet. Similarly, the process, automation, and enterprise network has five identified attack surfaces. To demonstrate the attack scenarios in VOTNet, we exploit the attack surfaces, viz., the communication interface and misconfiguration in the SCADA server.

5 EXPERIMENTAL EVALUATION

5.1 Experimental Setup

Our experimental setup consists of 10 physical nodes. Each node is of the following configuration: 2 Intel Xeon 2.40GHz Processor, 64GB memory, 4TB HDD, and 4 Gigabit Ethernet Interfaces. All physical nodes are installed with Ubuntu 1604-64-STD by default. The network topology of VOTNet is created using an ns-file by provisioning the physical machine. Virtual Machines are installed and configured on top of physical nodes with different OS such as Windows 7, Ubuntu, and Kali Linux, etc., and industrial software like PLCs, PowerWorld simulator, SCADA software, application software, and tools. PLCs and different components of SCADA are communicating using the Modbus TCP/IP protocol.

5.2 Use Case 1: Attack Scenarios

This section presents attack scenarios such as *unauthorized access to the SCADA control server*, *data manipulation attack in PLC*, and *denial of service (DoS) attack* to demonstrate SCADA system behaviors in terms of bandwidth utilization by SCADA communication. All three attack scenarios are shown in Table 2. It can be seen from the following result that while bandwidth utilization is about 2Mbps, the SCADA communication is unable to exchange system data in VOTNet. Although the bandwidth utilization graphs under considered attack scenarios can be presented and discussed, we have only presented and discussed the bandwidth utilization graph under a DoS attack to study the SCADA system behavior.

Attack 1: Denial of Service (DoS): The DoS attack is demonstrated on the SCADA communication interface (the Ethernet interface of the PLC) of the Modbus/TCP protocol through which data are passing to HMI and the SCADA control server. The PLC aggregates and fetches data from the PowerWorld simulator. We used Ping of Death (PoD) and hping3 for a DoS attack to the interface. Upon launching

Table 2: Attack scenarios.

Attack	DoS: PoD, hping3	Data manipulation	IP-Hijacking & Password Cracking
Source	Outside network	Inside Network	Outside Network
Tool	CLI & Zabbix	Python	Nmap/Kali Linux
Target	Router/Switch	PLC	SCADA Server
Result	Non-availability	Malfunction	Malfunction

the attacks, the SCADA server generates a huge number of alarms, which will not be possible to study in a standalone fashion. On the other hand, the communication between the PLC and the SCADA control server was disconnected. The reason of this incident is explained in Figure 5. The graph shows the length of attack and throughput of the SCADA protocol for every 5 seconds. Obviously, while the attack length increases, the throughput of the SCADA protocol decreases. Specifically, the throughput of the SCADA protocol decreases at 2 Mbps once the length of attack reached at 10 seconds with 30 Mbps. At this point (breakdown point which is marked with a bold red line) the protocol is unable to exchange data between the PLC and the central control center. As a result, the control server begins to obtain a decreasing number of SCADA events and device status, which are essential to take a decision and to estimate the state of the physical system, and accordingly the system goes into a non-functioning state.

Attack 2: Data Manipulation: The objective of this attack is to exploit the Modbus TCP protocol conducting the communication between the PLC and the SCADA Server, and to inject a malicious value in the register to manipulate data and to disrupt the normal VOTNet functionality. Generally, the PLC keeps on sending data to the server in real time. The protocol is configured in a way that it tracks and stores four different data, namely, *coil status, input status, holding register*, and *input register*. We manipulated the holding register value before it has reached the server. By launching this attack, the server is under the impression that the system is in a safe state, which is not the case, and if data manipulation is done on smaller scale, it becomes even harder for the server to detect. By performing this attack, we were not able to get a quantifiable result. Nevertheless, we understand that the operator was unable to take the right decision due to faulty values of the register.

Attack 3: IP-Hijacking and password cracking: This attack is performed on the SCADA server. The objective of the attack is to get unauthorized access to the sever. Firstly, we have identified the IP address of the SCADA server and then we have looked for open ports associated with the server. Finally, the default password of the control software was cracked using brute force. After getting the password, we were able to login to the SCADA server, from where unwanted commands had been sent to the PLC.

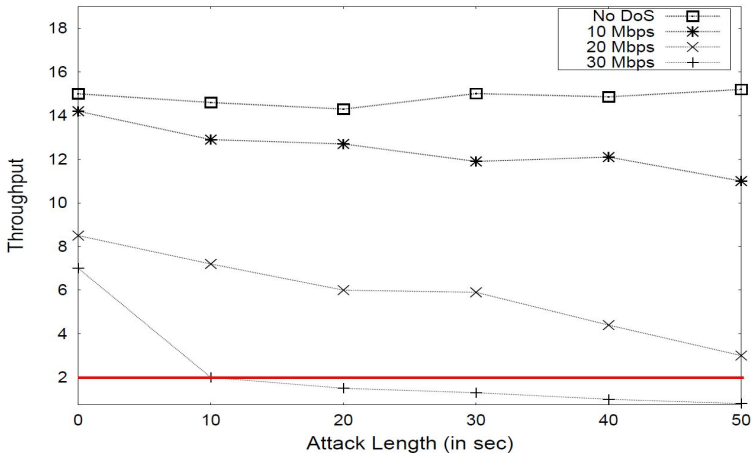

Figure 5: DoS attack impact on SCADA communication.

Table 3: Scalability vs. attack surfaces.

Component	Internet				COM Network				P/A/E Network			
Scale	1	2	3	4	1	2	3	4	1	2	3	4
A_s	1				4				5			
Total A_s	1	2	3	4	4	8	12	16	5	10	15	20

5.3 Use Case 2: Scalability vs. Attack Surface

The scalability of VOTNet is evaluated considering the identified components in the testbed without simulation. It can be seen from Figure 4 that the identified components of the testbed are process (P) network, communication network (COM), automation network (A), enterprise network (E), and the Internet. The corresponding identified attack surfaces of the respective components are also shown in Figure 4. It may noted that in real scenarios, the size (number of attack vectors/applicable inputs) of the identified attack surfaces may vary. But, to make our study simple we assume that all the attack surfaces for all the components are equivalent. The relationships between the component, scalability, and attack surface are given in Table 3, where A_s means attack surface. It can be seen from this table that the attack surface increases when scaling up the components in VOTNet. Particularly, if Internet connection is increased, then the attack surface is also increased proportionally, whereas the attack surface for the COM is increased by four times as it has four attack surfaces. On the other hand, the attack surface for process, automation, and enterprize network is increased by five times for adding one of each components with VOTNet, because each of the process, automation, and enterprize network components has five attack surfaces.

Therefore, the attack surfaces increase with higher chances of attacks while the OT network scales up. This can be explained as follows. Additional substation integration with an automation network adds one more process network. Adding a process network in an automation network means adding more field devices, computing systems, switches, HMIs, etc. As a process network has few attack surfaces, the scaling of a process network increases the chance of attacks in the automation network. Similarly, there may be a situation where one power system automation network needs to have multiple central control centers which in turn might be connected with respective regional enterprise networks. Therefore, the interconnected components of the automation network increase the attack surfaces. Hence, the chance of attacks increases with increasing attack surfaces while scaling up different components in the system.

It is worth to mention that a study on scalability and attack surface in terms of size (i.e., number of attack vectors/applicable inputs) can also be done pertaining to newly added devices, generated events from the devices, and functionality in the OT network. But, we have left this study as future work.

5.4 Mitigation

To mitigate a DoS attack, an anti-DoS system can be deployed. Placing this security measure requires additional functionality in each networking device (i.e., firewall, router) and ICS (e.g., PLC) to not only detect and alter attack traffic but also to send the push notification to upstream networking devices.

The second demonstrated attack, data manipulation in Modbus PLC, is trivial and to mitigate such attack requires a good understanding of the SCADA network. To avoid this attack, PLCs should be placed behind the firewall with strict firewall rules. In order to achieve better security, more-secured protocols like DNP3 and secure Modbus need to be used, and attacks on the PLC's logic manipulation in the form of a logic bomb can be controlled by providing a centralized logic store mechanism.

IP-Hijacking and password cracking involve stealing an IP address of system or network devices either accidentally or purposefully. The mitigation of this attack is difficult as it is difficult to trace back. Mitigating IP hijacking requires proper routing filter mechanisms or digitally sign routing updates and storing a list of originating autonomous systems which are unauthenticated. To mitigate password cracking, default

passwords of the systems and devices need to be replaced with a complex and strong password, which also needs to be changed periodically.

Finally, security is a continuous approach comprising of processes, people, and technology. Therefore, the deployed security measure needs to be upgraded over time and also the deployed systems in the OT network and its generated events should be monitored on a real-time basis.

6 CONCLUSION AND FUTURE WORK

To advance the study of cyber-based control mechanisms requires a new approach to analyze the complex relationships of OT networks consisting of power systems and processes as well as enterprise and automation networks. This paper proposed a simulation model of an OT network for cybersecurity assessment and what-if analysis of cyberattacks. We designed and developed VOTNet, a virtual OT network for cybersecurity assessment, with the following key components: The PowerWorld simulator feeds data to PLCs that bridge the physical process with the substation control center, an underlying communication network, along with the SCADA workstation and the centralized control center to assess cybersecurity. In contrast with state-of-the-art approaches, providing either a physically or semi-virtual model for power system automation, VOTNet is a hybrid approach incorporating real devices with a simulation framework. To validate the use of VOTNet, we studied and discussed two use-cases, viz., *attack scenarios* and *scalability vs. attack surface* by integrating the control output produced by the PLC, operated from the control server. The first use case advances our understanding of the impact of different attacks and the corresponding SCADA system behaviors in power system automation, while the second use case exposes the problems associated in scaling the OT network. Future effort focuses on analyzing the impacts of sophisticated coordinated attacks along with various impact mitigation efforts for a large-scale automation system.

ACKNOWLEDGEMENT

This research is supported by the National Research Foundation, Prime Ministers Office, Singapore under its National Cybersecurity R&D Program (Award No. NRF2015-NCRNCR002-001) and administered by the National Cybersecurity R&D Directorate.

REFERENCES

Bergman, D. C., D. Jin, D. M. Nicol, and T. Yardley. 2009. "The Virtual Power System Testbed and Inter-testbed Integration". In *Proceedings of 2nd Workshop Cyber Security Exp. Test*, August 10th–14th, Montreal, QC, Canada, 1–5.

Biswas, S. S., F. Shariatzadeh, R. Beckstrom, and A. K. Srivastava. 2013. "Real time Testing and Validation of Smart Grid Devices and Algorithms". In *Proceedings of IEEE Power Energy Soc. Gen. Meeting (PES)*, July 21st–25th, Vancouver, BC, Canada, 1–5.

Cebula, J. J., and L. R. Young. 2010. "A Taxonomy of Operational Cyber Security Risks". Technical Report No. 14, Carnegie Mellon University Software Engineering Institute (SEI), Institute, Pittsburgh, PA.

Chakrabortty, A., and Y. Xin. 2013. "Hardware-in-the-loop Simulations and Verifications of Smart Power Systems over an Exo-GENI Testbed". In *Proceedings of 2nd GENI Res. Educ. Exper. Workshop (GREE)*, March 20th–22nd, Salt Lake City, UT, USA, 16–19.

Chen, B., K. L. Butler-Purry, A. Goulart, and D. Kundur. 2014. "Implementing a Real-time Cyber-physical System Testbed in RTDS and OPNET". In *Proceedings of North Amer. Power Symp. (NAPS)*, September 7th–9th, Pullman, WA, USA, 171–176.

Chen, B., N. Pattanaik, A. Goulart, K. L. Butler-Purry, and D. Kundur. 2015. "Implementing Attacks for Modbus/TCP Protocol in a Real-time Cyber Physical System Test bed". In *Proceedings of IEEE Int. Workshop Tech. Committee Commun. Qual. Rel. (CQR)*, May 12th–14th, Charleston, SC, USA.

Cleveland, F. 2012. "IEC 62351 Security Standards for the Power System Information Infrastructure". *IEC TC57 WG15 Security Standards* 14.

Cole, E. 2017. "SANS ICS Attack Surfaces". *SANS Industrial Control System*.

Dondossola, G., G. Deconinck, F. Garrone, and H. Beitollahi. 2009. "Testbeds for Assessing Critical Scenarios in Power Control Systems". In *Critical Information Infrastructure Security*, edited by R. Setola and S. Geretshuber, 223–234. Berlin, Germany: Springer.

Green, B., A. Lee, R. Antrobus, U. Roedig, D. Hutchison, and A. Rashid. 2017. "Pains, Gains and PLCs: Ten Lessons from Building an Industrial Control Systems Testbed for Security Research". In *Proceedings of 10th USENIX Workshop on Cyber Security Experimentation and Test (CSET 17)*, August 14th, Vancouver, BC, Canada.

Haack, J., B. A. Akyol, N. Tenney, B. Carpenter, R. Pratt, and T. Carroll. 2013. "VOLTTRON: An Agent Platform for Integrating Electric Vehicles and Smart grid". In *Proceedings of Int. Conf. Connected Veh. Expo (ICCVE)*, December 2nd–6th, Las Vegas, NV, USA, 81–86.

Hahn, A., A. Ashok, S. Sridhar, and M. Govindarasu. 2013. "Cyberphysical Security Testbeds: Architecture, Application, and Evaluation for Smart Grid". *IEEE Trans. Smart Grid* 4(2):847–855.

Hong, J., S.-S. Wu, A. Stefano, A. Fshosha, C.-C. Liu, P. Gladyshev, and M. Govindarasu. 2011. "An Intrusion and Defense Testbed in a Cyberpower System Environment". In *Proceedings of IEEE Power Energy Soc. Gen. Meet.*, July 24th–29th, San Diego, CA, USA.

INL 2016. "INL Test Range, Protecting Nation's Infrastructure". https://factsheets.inl.gov/FactSheets/idaho-test-range.pdf, accessed March 15th, 2018.

Koutsandria, G., R. Gentz, M. Jamei, S. Peisert, A. Scaglione, and C. McParland. 2015. "A Real-time Testbed Environment for Cyberphysical Security on the Power Grid". In *Proceedings of 1st ACM Workshop Cyber Phys. Syst. Security PrivaCy*, October 16th, Denver, CO, USA, 67–78.

Mahnke, W., S.-H. Leitner, and M. Damm. 2009. *OPC Unified Architecture*. Heidelberg, Germany: Springer.

Mallouhi, M., Y. Al-Nashif, D. Cox, T. Chadaga, and S. Hariri. 2011. "A Testbed for Analyzing Security of SCADA Control Systems (TASSCS)". In *Proceedings of IEEE PES Innov. Smart Grid Technol. (ISGT)*, January 17th–19th, Anaheim, CA, USA, 1–7.

McDonald, M. J., G. N. Conrad, T. C. Service, and R. H. Cassidy. 2008. "Cyber Effects Analysis Using VCSE". Technical Report No. 5954, Sandia Nat. Lab, Albuquerque, NM, USA.

Mirkovic, J., and T. Benzel. 2012. "Teaching Cybersecurity with DeterLab". *IEEE Security Privacy* 10(1):73–76.

Morris, T., A. Srivastava, B. Reaves, W. Gao, K. Pavurapu, and R. Reddia. 2011. "A Control System Testbed to Validate Critical Infrastructure Protection Concepts". *Int. J. Crit. Infrastruct. Protect.* 4(2):88–103.

Queiroz, G., A. Mahmood, and Z. Tari. 2011. "SCADASim-A Framework for Building SCADA Simulations". *IEEE Trans. Smart Grid* 2(4):589–597.

Vellaithurai, C. B., S. S. Biswas, and A. K. Srivastava. 2017. "Development and Application of a Real-time Test bed for Cyber-physical System". *IEEE System Journal* 11(4):2192–2203.

Weiss, M., A. Chakrabortty, and Y. Xin. 2013. "A multi-user Network Testbed for Wide-area Monitoring and Control of Power Systems Using Distributed Synchrophasors". In *Proceedings of 4th Int. Conf. Future Energy Syst.*, May 22nd–24th, Berkeley, CA, USA, 291–292.

AUTHOR BIOGRAPHIES

SAJAL SARKAR is a Research Fellow at the National Cybersecurity R&D Lab, Singapore. His main research interests include cyber security in power systems, IoT and ad-hoc networks. His email address is sajals@ece.iitkgp.ernet.in.

ANAND AGRAWAL is a Software Engineer at the National Cybersecurity R&D Lab, Singapore. His email address is anandag@comp.nus.edu.sg.

YONG MENG TEO is an Associate Professor at the Department of Computer Science at the National University of Singapore (NUS) and an Affiliate Professor at the NUS Business Analytics Center. He heads the Computer Systems Research Group. His email address is teoym@comp.nus.edu.sg.

EE-CHIEN CHANG is an Associate Professor at the Department of Computer Science at the National University of Singapore (NUS). His email address is changec@comp.nus.edu.sg.