Implementing attacks for modbus/TCP protocol in a real-time cyber physical system test bed

Article · June 2015

DOI: 10.1109/CQR.2015.7129084

5 authors, including:

Bo Chen
Argonne National Laboratory
50 PUBLICATIONS **950** CITATIONS
SEE PROFILE

Ana Elisa P. Goulart
Texas A&M University
52 PUBLICATIONS **222** CITATIONS
SEE PROFILE

K.L. Butler-Purry
Texas A&M University
163 PUBLICATIONS **3,440** CITATIONS
SEE PROFILE

Deepa Kundur
University of Toronto
255 PUBLICATIONS **7,741** CITATIONS
SEE PROFILE

Implementing Attacks for Modbus/TCP Protocol in a Real-Time Cyber Physical System Test Bed

Bo Chen
ECE Department Texas A&M University
College Station, USA
bchen@tamu.edu

Nishant Pattanaik
CSE Department Texas A&M University
College Station, USA
neoindian@tamu.edu

Ana Goulart
ETID Department Texas A&M University
College Station, USA
goulart@tamu.edu

Karen L. Butler-Purry
ECE Department Texas A&M University
College Station, USA
klbutler@tamu.edu

Deepa Kundur ECE Department
University of Toronto
Toronto, ON, Canada
dkundur@utoronto.ca

***Abstract*—To understand security vulnerabilities of communication protocols used in power systems, a real-time framework can be developed to conduct vulnerability studies. The framework should implement protection mechanisms against vulnerabilities and study their effectiveness. In this paper, a real-time cyber-physical framework or test bed is presented. It integrates a real-time power system simulator and a communication system simulator to study the cyber and physical system vulnerabilities in smart power grids. The power system simulation is implemented using the Real-Time Digital Simulator (RTDS®) power grid simulator, with LabVIEW and PXI modules that simulate the supervisory control and data acquisition (SCADA) system and intelligent electronic devices (IEDs). The communication system simulation is implemented using Opnet's System-in-the-Loop (SITL) simulator and open source Linux tools and servers. Results of two cyber-attacks on the Modbus/TCP protocol are discussed and improvements to the test bed for protocol attack detection and mitigation are proposed.**

Keywords—SCADA, Modbus/TCP, RTDS, LabVIEW, Opnet, MITM, DoS, cyber-attacks, test bed.

I. INTRODUCTION

Smart grid is a cyber-physical system that includes power system components, communication systems, sensors, and controllers. The interoperability between them makes it possible for a smart grid to operate smartly [1]. Most smart grid technologies communicate data in a duplex manner, where measurements and control commands can be sent among the power system components. The information flow in a smart grid architecture should be supported by independent and dedicated communication networks comprising of various communication media, protocols, and devices [2]. An important concern for the planning and implementation of smart grid applications are the cyber security issues arising because of the numerous access points that make them vulnerable to various cyber attacks [3]. Recent research has shown that power system stability and the economics of operation can be significantly affected by dedicated and coordinated cyber attacks [4, 5]. Therefore, a cyber-security impact analysis and mitigation framework is essential to plan for reliable and secure operation of smart grid applications.

Research on different aspects of smart grid cyber security has been conducted to address the cyber security issues, including framework development [6], vulnerability assessment [7, 8], impact analysis and detection of cyber attacks [9, 10], and mitigation strategies [11, 12], as well as the increasing interest in development of cyber physical test bed [13-17]. The work in this paper focuses on the security aspects for smart grid protocols. Examples of smart grid protocols include Modbus, Distributed Network Protocol (DNP3), IEC 61850, ICCP, ZigBee, C37.118, and C12.22. These protocols enable the communication between supervisory control and data acquisition (SCADA) systems and intelligent electronic devices (IEDs) over the Internet and local substation networks.

The research reported in this paper aims to develop a real-time cyber physical test bed that not only simulates communication system and power system simultaneously, but also models and emulates various smart grid communication protocols. Its current implementation supports Modbus and IEC 61850 protocols. Multiple substation networks and attack PCs can be connected to the test bed, making the test bed flexible to simulate complicated communication systems. Furthermore, the test bed can perform various cyber attacks toward any substations or IEDs. The impact of cyber attacks can be observed and quantified conveniently from the test bed. Another research goal when developing this cyber physical test bed was to integrate commercial tools (such as RTDS and Opnet) with open source tools, so that other researchers can easily replicate our test bed model to further study cyber security in smart grids. Vulnerability assessment can be performed on the proposed test bed by simulating real world cyber attack scenarios such as denial-of-service (DoS) attack and man-in-the-middle (MITM) attack. The work done in [13] was extended to create the proposed test bed and the test bed capabilities was demonstrated by performing two cyber attacks on the Modbus/TCP protocol. Impact of cyber attacks on power system was studied.

The paper is organized as follows. Section II introduces the layout of the proposed real-time cyber physical test bed. Comparison with other cyber physical test beds is presented in section III. Two case studies are presented in Section IV. MITM attack and DoS attack were carried out to justify the effectiveness of the test bed. Finally, conclusions and future work are discussed in section V.

II. PROPOSED REAL-TIME CYBER PHYSICAL TEST BED

The general capabilities of the proposed real-time cyber physical test bed have been discussed in [13]. The work in this paper extends the work done in [13] by implementing the following capabilities:

978-1-4799-8575-3/15/$31.00 ©2015 IEEE

- Models and updates various components and parameters of communication networks.
- Connects to real world networks and IEDs.
- Carries out various attack taxonomies with minimal changes.
- Tests Modbus protocol vulnerabilities.
- Operates with off-the-shelf hardware and software.

In this section, the elements and the architecture of the proposed test bed are introduced. The power system modeled in the test bed is also discussed.

A. Test Bed Elements

The test bed consists of various power system components, cyber components, and physical network devices. These are the physical and software components used in the test bed:

1. Real-Time Digital Simulator (RTDS) [18]: Time domain electromagnetic simulator for power systems. The real-time simulation data can be easily exported as analogue and digital signals. All the simulation data can be displayed through its user interface RSCAD. The data generated by RTDS can be treated as practical data of real power system.
2. Opnet Modeler [19]: A commercial software used to analyze realistic simulated networks to compare the impact of different technology designs. Opnet is suitable for operating with RTDS due to its SITL feature.
3. LabVIEW and PXI Module [20]: LabVIEW is a system-design platform and development environment for a visual programming language from National Instruments. PXI module is an open, PC-based platform for test, measurement, and control. PXI modules can be remotely programmed by LavVIEW to support data streaming through various communication protocols.
4. Fast Ethernet Switches: 10/100Mbps with 16 ports.
5. Attack PC: Ubuntu 12.04 TLS Linux Operating System is installed on the attack PC.
6. Ettercap [21]: Open source tool with a graphical user interface to carry out MITM attacks. This tool runs on the attack PC mentioned above.
7. Libmodbus [22]: Open source freely distributed library used to create spurious Modbus protocol messages to carry out the MITM attack.

B. Modbus/TCP Protocol

The Modbus/TCP protocol was used as the reference protocol to display the effectiveness of the test bed in carrying out cyber attacks on a power system protocol. Modbus/TCP was chosen specifically for these reasons:

- Modbus is still widely used in power systems.
- Modbus/TCP is simple and easy to implement.
- Modbus protocol libraries are freely available for utilities to implement smart grid applications.

To model the TCP/IP network, Opnet was used to create multiple subnets connected by a wide area network or Internet cloud. The power system components were modeled in RTDS and the Modbus components were modeled in LabVIEW and PXI. Because of our strict requirement of having these physical components experience real world traffic situations, the System-In-The-Loop (SITL) feature of Opnet was used to interface the simulated and the real world components. Thus, the security attacks on the command and control portion of the Modbus/TCP protocol can be easily carried out.

C. Test Bed Architecture

The architecture of the test bed is displayed in Fig. 1. RTDS simulates power systems in real time and communicates pre-selected measurement values and control commands with LabVIEW PXI through its analogue and digital ports. NI PXI/LabVIEW Real-Time Module bridges the RTDS and Opnet in real time. The PXI/Modbus Master is modeled in the LabVIEW PC. It interfaces with the Modbus Backend Interface component simulated in LabVIEW PXI, which is connected to RTDS through analogue/digital input/output ports. Fast Ethernet Switch (10/100Mbps) enables to add a real physical attack node, or attack PC, into the test bed and perform real world security attacks. Ettercap and Libmodbus are installed on the attack PC, which has Ubuntu 12.04 TLS Linux Operating System. The attack PC performs the MITM and TCP flood attacks on the simulation. Opnet simulates an IP network and allows emulating the Modbus client and server as separate sub networks. The SITL ports interface the physical network devices and the simulated networking environment. LabVIEW PXI is also used to develop the Modbus client application, shown at the PC located in the bottom of Fig. 1.

The Opnet network model in Fig. 1 emulated two sub networks in different geographical locations and the traffic flowed through the emulated Opnet simulation in real time. The Modbus query consists of the Modbus application data unit (ADU) containing the unit identifier and the function code indicating the type of service requested from the Modbus server. The Modbus Server then replies back with the Modbus response. The Modbus queries were triggered from the TX (Transmission) sub net, then it flew through the Opnet SITL Wide Area Network (WAN). Then, the query went through the SITL interface and the switch, and arrived at the Modbus Master.

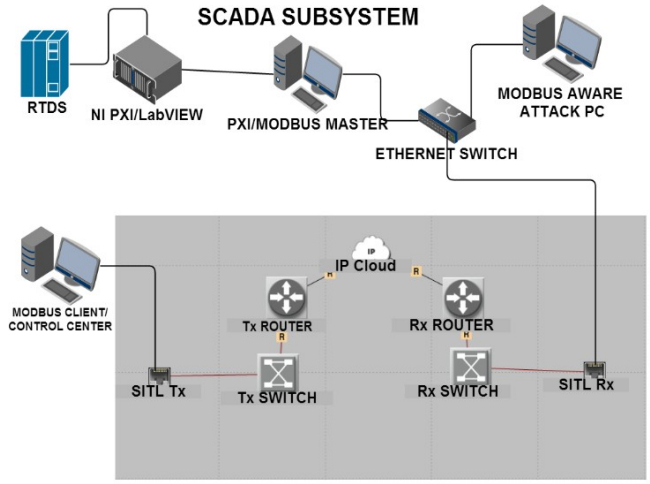

Fig. 1. Proposed Real-Time Cyber Physical Test Bed.

TABLE I. CYBER PHSYICAL TEST BEDS IN THE LITERATURE

Test Bed		Real Time	Smart Grid Protocol Supported	Components		Comments
Name	*Year*			*Commercial*	*In-House*	
[13]	2014	Yes	IEC 61850	RTDS, LabVIEW, OPNET	N/A	Replay attack was simulated and its impact on transient stability was studied.
[14]	2013	Yes	DNP3, IEC 61850, MMS	RTDS, DIgSILENT	ISEAGE	A wide range of protocols are supported. DoS and MITM attacks were performed to show the effectiveness of the test bed.
[15]	2011	Yes	Modbus/TCP	PowerWorld, OPNET, Modbus RSim	N/A	Modbus attacks were outlined in detail and various attacks were carried out.
[16]	2008	Yes	Modbus/TCP	OPNET, PXI, RTU	UMR	Several types of cyber attacks were performed on the test bed.
[17]	2006	Yes	Modbus/TCP	PowerWorld	RINSE	DoS attack was simulated and overloaded a transmission line.

The Modbus Master interfaced with the RTDS which emulated the IED slaves. The Modbus Master read the register or voltage values and formulated the Modbus replies. The replies were then sent back to the Modbus Client in the reverse direction. The Modbus Master emulated two logical Modbus masters, each controlling a single slave. Modbus Master 1 operated on Modbus TCP port 502 and Modbus Master 2 controlling slave 2 operated on TCP port 501.

It is worth noting that the two subnetworks can be used for modeling the SCADA system for two power system substations. The test bed allows multiple substations to be connected to one or more Modbus clients. Multiple attack PCs can be located all over the network to sniff the un-encrypted Modbus packets and carry out attacks, by simply adding SITL ports in Opnet. However, current test bed is limited to one substation and one attack PC due to the high cost of RTDS and PXI.

D. Power System Test System

An eleven-bus 230KV power system was modeled in the test bed. The single line diagram is shown in Fig. 2. Two generators, Gen1 and Gen2, are connected to bus 6 and bus 9, respectively. Three lumped loads are connected to bus 2, bus 3, and bus 4. Two breakers, BRK1 and BRK2, are responsible for tripping the transmission line between bus7 and bus 10, when an abnormal condition on the transmission line is detected by the protective relays, which have built-in memories to store various setting parameters. These parameters can be set remotely using different power system protocols (e.g., DNP3, Modbus/TCP, IEC 61850). In addition, the control center can trip or reclose BRK1 and BRK2 remotely, by sending a tripping or a reclosing signal to the breaker controllers. The test bed measures the status and the three-phase current of BRK1 and BRK2 through the communication network modeled in Opnet using Modbus/TCP protocol. Tripping or reclosing a breaker will introduce a big disturbance to power system stability, since the suddenly changed network topology will re-dispatch the power flow, which will initiate the transient process [23]. Usually the system will settle down in a new steady state in a short duration. However, recent research has shown that the power system dynamic stability can be collapsed if the breakers are compromised by malicious attacks [24].

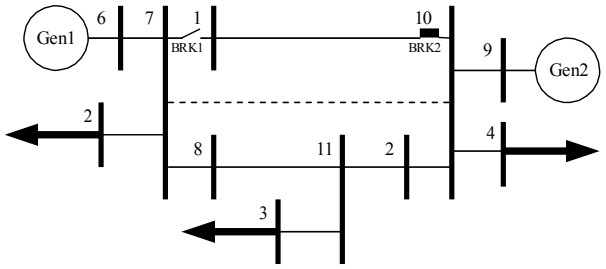

Fig. 2. Power System Modeled in the Test Bed.

III. RELATED WORK

Although current efforts on cyber physical test bed development are limited, some work has been done in this area to analyze smart grid protocols. Table I summarizes test beds in the literature that focus on cyber security of smart grid. We have outlined the commercial and in-house components of the test bed. Test beds with in-house components can be difficult to replicate.

IV. CASE STUDIES

The Modbus protocol attack taxonomies have been studied in detail in [25] and were used as reference for the two case studies presented in this section. The MITM attack and the DoS attack were performed on the Modbus/TCP protocol to testify the effectiveness of the test bed

In the proposed cyber physical test bed, the eleven-bus test system and its communication network were modeled in RTDS and Opnet. The parameters of the test system can be found in [26]. The controllers of BRK1 and BRK2 were modeled in LabVIEW PXI, and Modbus/TCP protocol was chosen to transfer measurement values (e.g., breaker status, three phase current magnitudes) from breaker controllers (i.e., Modbus master) to control center (i.e., Modbus client), then transfer control commands (e.g., tripping and reclosing signals) from control center to breaker controllers.

For both case studies, the network traffic was monitored by Wireshark [27], and the power system quantities were measured by RSCAD and LabVIEW. The impact of both cyber attacks on network traffic and power system dynamic stability is presented in this section.

A. MITM Attack

MITM attack happens when an untrusted PC gains access to the communication between two peers without the peers being aware of such an attack being in progress [28]. In order for a successful MITM attack to be carried out, the attacker should be in the same subnet as the target PC and it should be able to poison the Address Resolution Protocol (ARP) caches of the victims. Thus, the attacker can receive the traffic from both victims and act as the router forwarding the received traffic. In the test bed, the attack PC in the same subnet was used as the target (Fig. 1). In order to carry out the attack, the attacker poisoned the ARP caches of the Rx Router in Fig. 1 and the Modbus Master. This was done by using the open source MITM attack tool called Ettercap [21]. After poisoning the ARP caches of the Rx Router and the PXI Modbus Master, the attacker was able to see the Modbus Query and Modbus Response packets being exchanged by the use of Wireshark, which acted both as a packet analyzer and sniffer. Once the attacker had the knowledge of the server and the slave IP addresses, attacker emulated the Modbus client and was able to send a Modbus command to trip the slave IED.

B. Impact of MITM Attack

The Modbus traffic and the general traffic in the MITM attack PC are shown in Fig. 3. The attacker received the Modbus traffic by acting as a hidden router between master and client. The graph from time t=0 seconds to t=100 seconds shows the general traffic being received on the attack PC. During this time, there is no Modbus traffic being received on the attack PC as the MITM attack was not yet executed. Hence, only one line graph during this time interval can be observed. Approximately at time t=110 seconds, the MITM was carried out successfully and the attack PC started receiving all traffic to and from the Modbus client and the Modbus master. The top line shows all the traffic being received on the attack PC, and the lower line shows the Modbus traffic being received on the attack PC when the MITM attack is in progress. Note that the Modbus traffic is smaller compared to the overall data packets being received on the attack PC.

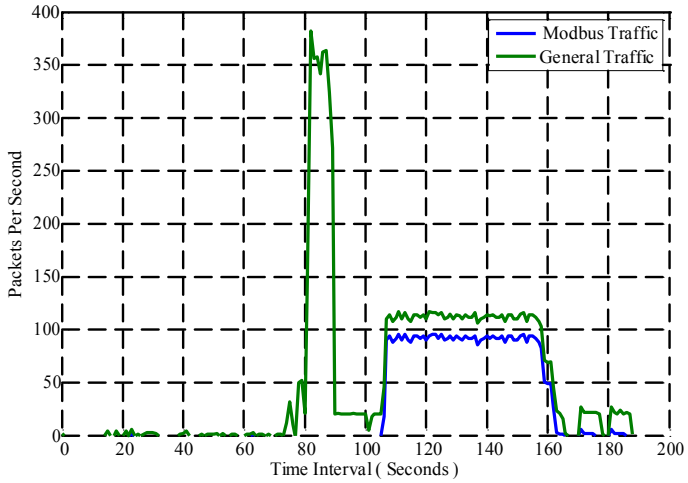

Fig. 3. Modbus Traffic Visible in the MITM attack PC.

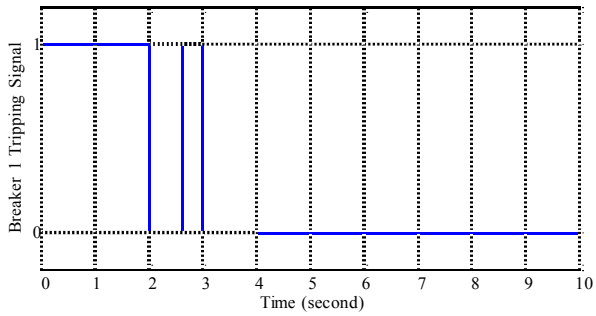

Fig. 4. Fake BRK1 Tripping Signal Sent by the Attacker.

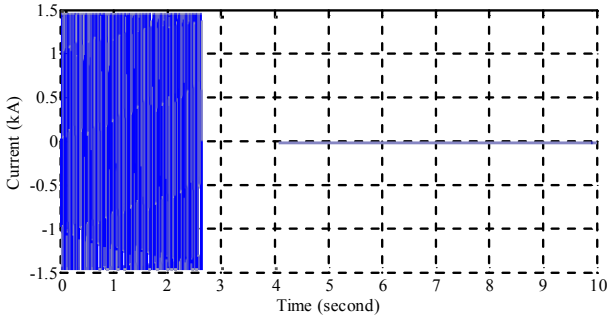

Fig. 5. Phase A Current Measurement of BRK1 at Bus 7.

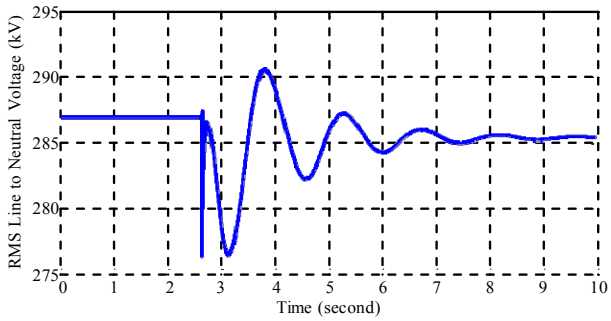

Fig. 6. RMS Voltage Measurement at Bus 7.

The spoofed or fake Modbus "write register" messages were then generated using libmodbus library towards the Modbus Master and was used to trip one of the slave IEDs. Because of the MITM attack, the attacker was able to observe the Modbus traffic between the master and the client when the attack was in progress.

The status of BRK1 is shown in Fig. 4. When the MITM attack was in progress, BRK1 was originally closed, i.e., the status equaled to 1. At 2.5 second, the attack injected a fake Modbus packet through the MITM PC by modifying the register value within the packet from 1 to 0. The breaker controller received and parsed this packet, then tripped the breaker, since the register value was changed. Hence the status of BRK1 changed from 1 to 0, meaning the breaker was tripped in response to the fake tripping signal. The instantaneous current of phase A at BRK1 became zero since the breaker was tripped, as shown in Fig. 5.

The root-mean-square (RMS) voltage at bus 7 is shown in Fig. 6. When BRK1 was tripped at 2.5 second, the power that was flowing through BRK1 was disconnected, resulting in a dip

in the bus voltage. Then, the power flow was re-dispatched. Gen1 and Gen2 adjusted their power output to approach a new steady state. The voltage was eventually dampened down within 8 seconds.

Initially, the power system was running in normal condition, since the current and the voltage profile was stable before BRK1 was tripped. Tripping BRK1 under normal conditions will shrink the system stability margin, and may result in stability and economic problems. The transient process will also affect the functionalities of other protective relays in the system, and may cause cascading failures. The system will collapse if multiple transmission lines are tripped by the attacker, then the customers will experience a power outage.

C. TCP SYN Flood DoS Attack

In order to check the delay sensitive nature of Modbus TCP, TCP SYN flood attack methodology was used to flood the Modbus Master. A TCP SYN Flood Attack takes advantage of the TCP three-way connection handshake mechanism to establish a reliable session between a sender and a receiver [29]. TCP SYN flood attack floods the Modbus Master with TCP connection requests from potential Modbus clients with spoofed source IP addresses and random destination TCP ports towards the Modbus master. The Hping tool [30] was used to trigger spurious TCP SYN requests towards the Modbus master.

Fig. 7 shows the Modbus traffic between the control center and BRK1. The TCP SYN flood attack started at 15 seconds, and ended around 70 seconds. When the attack was in progress, it can be observed in Fig. 7 that approximately 120 spoofed TCP SYN packets per second were received on the Modbus master.

Two experiments were performed. First, during the attack, a Modbus tripping command was sent to BRK1. Then, after the attack, another Modbus tripping command was sent to BRK1. The time difference between command and status messages for both cases are depicted in Fig. 8 and Fig. 9. Please note that the sampled time spans in Fig. 8 and Fig. 9 are at different time intervals. In Fig. 8, the tripping signal was sent at 32 seconds, and the sampled time span was from 30 second to 40 second. In Fig. 9, the tripping signal was sent at 83.7 seconds, and the sampled time span was from 80 second to 90 second. When the TCP SYN flood attack was in progress, it can be observed in Fig. 8 that the Modbus client or the control center received the status with approximately 3 seconds delay. The response was delayed from the Modbus server because the server was busy handling the spurious TCP SYN requests being generated from the attackers. When the attack was stopped, by terminating the Hping tool on the attack PC, the Modbus Master was able to discard the spurious TCP SYN requests. This freed the system resources and the clients were able to get the status of the IED's, approximately with a 300 millisecond delay, as shown in Fig. 9.

When the DoS attack is in progress, the control center will receive delayed information from IEDs. If the measurement is blocked by the DoS attack, the control center will not have an accurate picture of the system. Smart grid applications in the control center that rely on the information provided by the IEDs will malfunction.

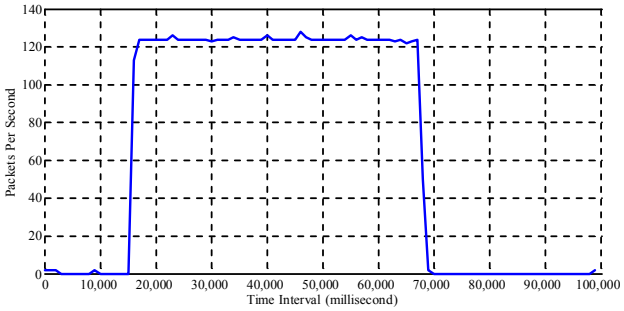

Fig. 7. Number of spoofed TCP SYN packets being received on the Modbus Master when TCP SYN Flood attack is in progress.

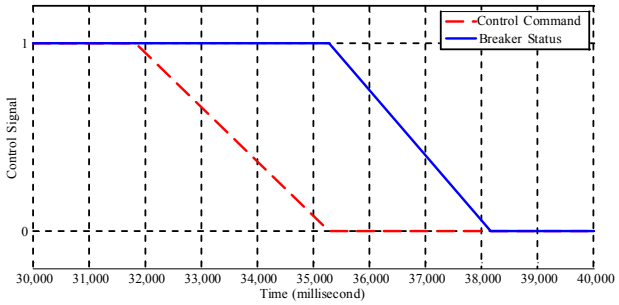

Fig. 8. Time Difference between Control and Status Messages received at Modbus Client of BRK1 when TCP SYN Attack is in progress on Server.

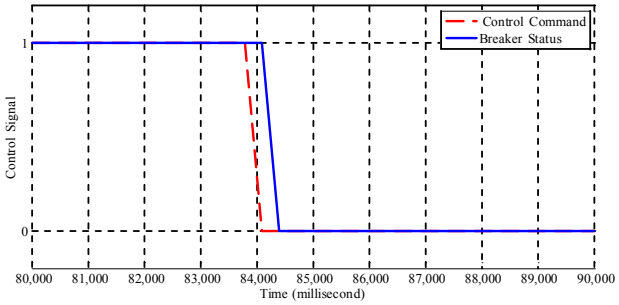

Fig. 9. Time Difference between Control and Status Messages at Modbus Client of BRK1 without TCP SYN Attack on Server.

In conclusion, both the MITM and the DoS attacks can result in severe impact on system operation and stability. The attacker can directly inject false data and control commands to various smart grid applications; hence, the security and the stability of the system will be deteriorated. Case studies highlight the fact that the Modbus protocol is too trusting in nature with no access control lists and no form of trust domain. Any attacker who gets the knowledge of the Modbus master IP can target it.

V. Conclusions And Future Work

In this paper, a real time cyber physical system test bed was presented. The test bed allows studying the power system protocol vulnerabilities and proposing mitigation strategies. The test bed is flexible and can be used to model different kinds of power system protocols and test their security in real time. Furthermore, the proposed cyber physical test bed can be configured to interact with real intelligent electronic devices (IEDs) and communication devices such as switches and routers.

The details of the component interaction and packet flow architecture of the communication system in the test bed were discussed. The effectiveness of the test bed was demonstrated by two case studies and the impacts of MITM attack and DoS attack were discussed. Future work involves extending the test bed by:

- Implementing a timestamp or a cookie field in Modbus protocol data unit (PDU) which will help discard Modbus responses which are delayed beyond a threshold and spurious Modbus messages.
- Introducing IP layer encryption and firewall before the Modbus master to demonstrate the effectiveness of the prevention mechanism.

REFERENCES

[1] A. Ipakchi and F. Albuyeh, "Grid of the future," IEEE Power and Energy Magazine, vol. 7, pp. 52-62, 2009.

[2] M. Govindarasu, A. Hahn, and P. Sauer, "Cyber-Physical Systems Security for Smart Grid," Power Systems Engineering Research CenterMay 2012.

[3] M. Yilin, T. H. J. Kim, K. Brancik, D. Dickinson, L. Heejo, A. Perrig, et al., "Cyber Physical Security of a Smart Grid Infrastructure," Proceedings of the IEEE, vol. 100, pp. 195-209, 2012.

[4] X. Le, M. Yilin, and B. Sinopoli, "Integrity Data Attacks in Power Market Operations," IEEE Transactions on Smart Grid, vol. 2, pp. 659-666, 2011.

[5] B. Chen, S. Mashayekh, K. L. Butler-Purry, and D. Kundur, "Impact of Cyber Attacks on Transient Stability of Smart Grids with Voltage Support Devices," in Proc. 2013 IEEE/PES General Meeting, Vancouver, Canada, 2013.

[6] D. Kundur, F. Xianyong, L. Shan, T. Zourntos, and K. L. Butler-Purry, "Towards a Framework for Cyber Attack Impact Analysis of the Electric Smart Grid," in Proc. 1st IEEE International Conference on Smart Grid Communications, Gaithersburg, pp. 244-249.

[7] T. Chee-Wooi, L. Chen-Ching, and G. Manimaran, "Vulnerability Assessment of Cybersecurity for SCADA Systems," IEEE Transactions on Power Systems, vol. 23, pp. 1836-1846, 2008.

[8] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber Physical System Security for the Electric Power Grid," Proceedings of the IEEE, vol. 100, pp. 210-224, 2012.

[9] B. Chen, K. L. Butler-Purry, S. Nuthalapati, and D. Kundur, "Network Delay Caused by Cyber Attacks on SVC and its Impact on Transient Stability of Smart Grids," in Proc. 2014 IEEE Power and Energy Society General Meeting (PES), 2014, pp. 1-5.

[10] H. Junho, L. Chen-Ching, and M. Govindarasu, "Integrated Anomaly Detection for Cyber Security of the Substations," Smart Grid, IEEE Transactions on, vol. 5, pp. 1643-1653, 2014.

[11] T. T. Kim and H. V. Poor, "Strategic Protection Against Data Injection Attacks on Power Grids," IEEE Transactions on Smart Grid, vol. 2, pp. 326-333, 2011.

[12] S. Zonouz, K. M. Rogers, R. Berthier, R. B. Bobba, W. H. Sanders, and T. J. Overbye, "SCPSE: Security-Oriented Cyber-Physical State Estimation for Power Grid Critical Infrastructures," IEEE Transactions on Smart Grid, vol. 3, pp. 1790-1799, 2012.

[13] B. Chen, K. L. Butler-Purry, A. Goulart, and D. Kundur, "Implementing a real-time cyber-physical system test bed in RTDS and OPNET," in North American Power Symposium (NAPS), 2014, 2014, pp. 1-6.

[14] A. Hahn, A. Ashok, S. Sridhar, and M. Govindarasu, "Cyber-Physical Security Testbeds: Architecture, Application, and Evaluation for Smart Grid," IEEE Trans. on Smart Grid, vol. 4, pp. 847-855, 2013.

[15] M. Mallouhi, Y. Al-Nashif, D. Cox, T. Chadaga, and S. Hariri, "A testbed for analyzing security of SCADA control systems (TASSCS)," in Proc. 2011 IEEE PES Innovative Smart Grid Technologies (ISGT), 2011, pp. 1-7.

[16] M. J. McDonald, G. N. Conrad, T. C. Service, and R. H. Cassidy, "Cyber effects analysis using VCSE: Promoting Control System Reliability," Sandia National Laboratories SAND2008-5954, Sep. 2008.

[17] C. M. Davis, J. E. Tate, H. Okhravi, C. Grier, T. J. Overbye, and D. Nicol, "SCADA Cyber Security Testbed Development," in Proc. 38th North American Power Symposium, 2006, pp. 483-488.

[18] RTDS Technologies. Available: http://www.rtds.com/

[19] Network Simulation (OPNET Modeler Suite). Available: http://www.riverbed.com/products-solutions/products/network-planning-simulation/Network-Simulation.html

[20] LabVIEW Real-Time Module. Available: http://sine.ni.com/nips/cds/view/p/lang/en/nid/209855

[21] Ettercap open source packet sniffer and MITM attack tool Available: http://openmaniak.com/ettercap.php

[22] Libmodbus – A LGPL v2.1+ licensed Modbus TCP implementation. Available: http://libmodbus.org/documentation/

[23] P. Kundur, Power System Stability And Control. New York: McGraw-Hill, 1994.

[24] L. Shan, C. Bo, T. Zourntos, D. Kundur, and K. Butler-Purry, "A Coordinated Multi-Switch Attack for Cascading Failures in Smart Grid," Smart Grid, IEEE Transactions on, vol. 5, pp. 1183-1195, 2014.

[25] P. Huitsing, R. Chandia, M. Papa, and S. Shenoi, "Attack taxonomies for the Modbus protocols," International Journal of Critical Infrastructure Protection, vol. 1, pp. 37-44, 12// 2008.

[26] Powertech Labs Inc., "TSAT User Manual," ed. Canada, 2012.

[27] Wireshark packet analyzer Available: https://www.wireshark.org/

[28] Man-in-the-middle attack. Available: https://www.owasp.org/index.php/Man-in-the-middle_attack

[29] TCP SYN Flooding and IP Spoofing Attacks. Available: http://www.cert.org/historical/advisories/ca-1996-21.cfm?

[30] Hping3 packet generator and analyzer. Available: http://linux.die.net/man/8/hping3