INL/CON-22-66594-Revision-0

Moving Target Defense Routing for SDN-enabled Smart Grid

July 2022

Moataz Abdelkhalek, Burhan Hyder, Manimaran Govindarasu, Craig G Rieger

DISCLAIMER

This information was prepared as an account of work sponsored by an agency of the U.S. Government. Neither the U.S. Government nor any agency thereof, nor any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness, of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the U.S. Government or any agency thereof.

INL/CON-22-66594-Revision-0

Moving Target Defense Routing for SDN-enabled Smart Grid

Moataz Abdelkhalek, Burhan Hyder, Manimaran Govindarasu, Craig G Rieger

July 2022

**Idaho National Laboratory
Idaho Falls, Idaho 83415**

http://www.inl.gov

**Prepared for the
U.S. Department of Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517**

Moving Target Defense Routing for SDN-enabled Smart Grid

Moataz Abdelkhalek
Dept. of Electrical and Computer Engineering
Iowa State University
Email: moataz@iastate.edu

Burhan Hyder
Dept. of Electrical and Computer Engineering
Iowa State University
Email: bhyder@iastate.edu

Manimaran Govindarasu
Dept. of Electrical and Computer Engineering
Iowa State University
Email: gmani@iastate.edu

Craig G Rieger
Idaho National Laboratory (INL)
Email: craig.rieger@inl.gov

***Abstract*—The increasing attack surface area in the smart grid communication networks is making the grid more susceptible to cyber attacks that can lead to instability of the grid and even blackouts. While there are multiple types of cyber attacks that can impact the grid, Denial of Service (DoS) attacks are relatively easier to inject as they require lesser knowledge about the system as compared to data integrity attacks. Various research works showcase methods to prevent or mitigate the impacts of DoS attacks in the smart grid but the research still lacks in demonstrating the feasibility and efficacy of the solutions in a real-world environment. In this paper, we propose a Moving Target Defense (MTD)-enabled Software Defined Network (SDN) for the Smart Grid communication implemented on a Hardware-in-the-Loop (HIL) Testbed. We showcase the implementation of the proposed architecture of MTD-enabled SDN using Mininet 2.3.0 which enables communication between the physical grid and the control center. The results show the advantages of using MTD based on SDN for the wide-area network (WAN) with much lower packet drop percentages in the case of MTD-based routing in the SDN WAN.**

***Index Terms*—SDN, MTD, Smart Grid Communication, DoS, HIL Testbed**

I. Introduction

The smart grid is growing and adapting to the advancements in technologies everyday making it a complex Cyber-Physical System (CPS). The cyber and the physical components usually communicate with each other over a Wide-Area Network (WAN) which traditionally consists of static routing of communication between the physical and the cyber layer [1]. The static nature of this WAN makes the grid susceptible to cyber attacks which can target specific data flowing over the communication channels. Specifically, Denial of Service (DoS) attacks can prevent communication between the cyber and the physical layer of the smart grid leading to instability of the system and loss of situational awareness of the power grid [2].

Software Defined Networking (SDN) is an effective method for enabling programmability in the smart grid WAN [3]. Using SDN-based WAN, the data flows between the cyber and physical layer can be dynamically modified as per the circumstances. For example, in case of congestion on the WAN, critical data that is time-sensitive can be specifically routed through higher bandwidth channels, while low priority data can be rerouted through the congested channels, allowing the high priority data to reach its destination on time. SDN decouples the control of the network (control plane) from the devices that forward the network traffic (data plane). This allows for dynamic programmability for more reliable, efficient, and scalable operation of the communication networks. Apart from these advantages, SDN can also help in thwarting network attacks by filtering or blocking data packets at the first point of entry into the SDN-based WAN.

One of the effective methods to mitigate the impacts of DoS attacks is Moving Target Defense (MTD). Specifically, route mutation or switching in communication networks can significantly reduce the impacts of DoS attacks. Implementation of this type of MTD in WAN is achievable using SDN [4]. Such an implementation architecture with MTD-enabled SDN combines the advantages of both the dynamic programmability of SDN and the randomness of MTD for cyber attack prevention and mitigation in the smart grid.

In this paper, we propose an MTD-enabled SDN-based WAN for the smart grid communication. The SDN-based WAN (SD-WAN) allows the MTD route switching between the physical and cyber layers of the grid in order to mitigate the impacts of a DoS attack on the WAN. We implement this architecture on an HIL Testbed [5] in order to showcase the feasibility and efficacy of such a system in a close to real-world environment. The results from this work show the advantages of using MTD-enabled SDN for smart grid networks with significantly reduced impacts from a DoS attack as compared to a static network. The main contributions and novelties of this paper are:

1) The paper shows feasibility of using SDN-based MTD in the Smart Grid Environment.
2) We implement the proposed architecture on a realistic Hardware In The Loop (HIL) Testbed in order to showcase the practical feasibility and efficacy of such a

978-1-6654-9952-1/22/$31.00 ©2022 IEEE

system in a close to real-world environment.

3) We propose a proactive mitigation technique using SDN-based MTD which is discussed in detail in Section IV-A.

The paper is organized as follows: Section II shows the related work in this area of research, Section III introduces the smart grid and attack model along with the problem statement, Section IV shows the proposed solution, Section V shows the HIL Testbed-based implementation and performance evaluation, and Section VI concludes the work.

II. Related Work

There has been a lot of research on the application of SDN and MTD in the smart grid networks some of which are summarized here. In [6], the authors propose an IP-based SDN communication architecture for distribution systems with high Distributed Energy Resources (DER) penetration. An SDN-based self-recovery wireless communication network for disaster-prone areas is proposed in [7]. The authors in [8] and [9] do an extensive survey of applications and state-of-the-art of SDN in cyber-physical networks and smart grid communications, respectively. A resiliency-aware SDN-based network for Supervisory Control and Data Acquisition (SCADA) System is proposed in [10] for deployment of SDN switches in the smart grid using a Mininet-based environment. The authors in [11] propose a multi-armed bandit approach for link failure detection to ensure reliable and resilient operation of an SDN-based smart grid. [12] proposes an IP-hopping MTD technique for mitigation of static vulnerability exploitation by cyber attackers in a smart grid environment. A hidden MTD technique for preventing false data injection (FDI) attacks in a smart grid environment is proposed in [13]. A similar approach is proposed by the same authors in [14] to prevent FDIs using branch susceptance randomization MTD technique. Another enhanced hidden MTD approach to thwart FDIs in the smart grid is proposed in [15]. An MTD approach to detect stuxnet-like attacks on critical CPSs is proposed in [16]. The authors in [17] propose a game-theory-based MTD to detect and mitigate coordinated cyber-physical attacks on the smart grid. An MTD-based SDN techniques is proposed in [18] to mitigate the impacts of distributed DoS attacks on large-scale internet service providers.

A comprehensive literature survey shows that even though there is plenty of research on the implementation of SDN and MTD in the smart grid network for mitigating and preventing cyber-attacks, the existing research works lack the demonstration of the efficacy and the feasibility in a real-world grid environment. In this paper, we demonstrate the application of MTD-enabled SDN in a smart grid environment for mitigating the impacts of a DoS attack using an HIL Testbed-based implementation and evaluation which represents a close to the real-world environment.

III. System and Adversary model

A. CPS Model of the Smart Grid

Fig. 1 shows the traditional architecture of the overall communications in a typical smart grid network. The physical system which includes generation, transmission, and distribution, consists of: (1) Sensors – that measure voltages, currents, and other parameters of the physical power system; and (2) Actuators – that control various parameters of the physical devices in the grid, e.g., intelligent electronic devices (IEDs or relays) that control the tripping and closing of circuit breakers. The physical system is monitored and controlled by the control center which consists of applications like SCADA and Energy Management Systems (EMS) for real-time control and monitoring of the power system in order to ensure its reliable operation. The control center and the physical power system exchange the measurement and control signals over a wide-area network (WAN) using various communication protocols like DNP3, MODBUS, IEEE C37.118, etc.

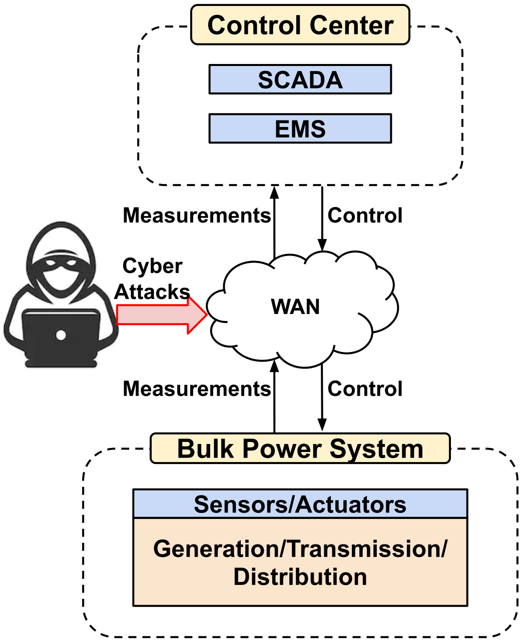

Fig. 1. Traditional CPS Model of the Smart Grid

B. Attack Model and Problem Statement

Since the physical system and the control center are usually geographically remotely located, the WAN often shares most of the infrastructure with the internet. Cyber adversaries leverage this connectivity of the grid to the internet as a point of intrusion in the smart grid. The attackers from such intrusions can manipulate the measurement and control signals which can impact the integrity of the data and subsequently lead to inaccurate operation of the grid, destabilize the grid, or even lead to blackouts. Another form of attack that can have a significant impact on the grid is a denial of service (DoS) attack. In this case, the measurement or the control signals are not delivered to the respective destinations on time leading to poor situational awareness at the control center or grid instability, respectively.

Fig. 2 shows an attack where *Host-1* (which can be considered as the control center) is communicating with *Host-2* (which can be considered as the physical grid) over a

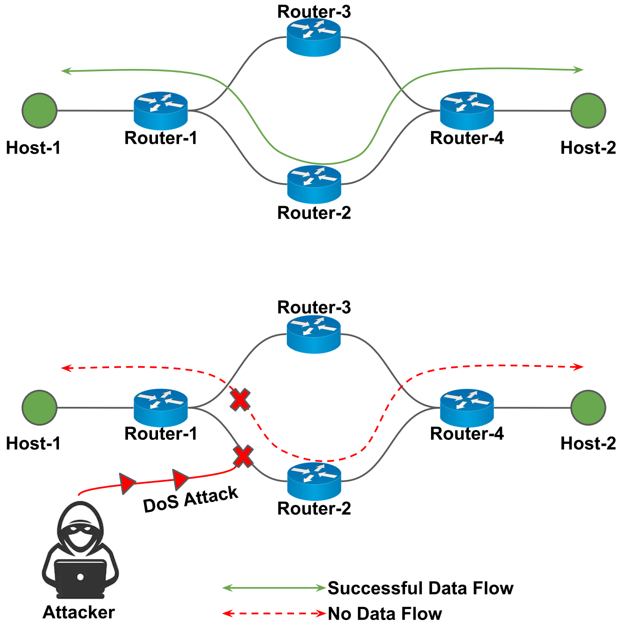

Fig. 2. DoS Attack Impact on Static Network Routing

single channel. This channel is represented by "$Host-1 \rightarrow Router-1 \rightarrow Router-2 \rightarrow Router-4 \rightarrow Host-2$". A DoS attack on this channel blocks any communication between *Host-1* and *Host-2* leading to the failure of data flow between the two hosts. Since the routers have static route tables, the data flow between *Host-1* and *Host-2* cannot be rerouted through the other available channel "$Host-1 \rightarrow Router-1 \rightarrow Router-3 \rightarrow Router-4 \rightarrow Host-2$". This causes a 100% data loss between *Host-1* and *Host-2* wherein only the removal of the attack can bring the system back to normal operation.

Attack Model Assumptions: (1) In this paper, we have considered an adversary capable of carrying out a DoS attack on only one of the communication channels between the substations and the control center causing a loss of communication between these two entities. Distributed Denial of Service (DDoS) type attacks are out of the scope of this paper. (2) We have not considered attacks on nodes/links that result in single points of failure in the system like *Router-1* and *Router-4* in Fig. 2 as the proposed methodology of MTD requires multi-path routing redundancy for efficient functionality.

IV. Proposed Solution

Fig. 3 shows the proposed architecture of the CPS Smart Grid wherein the traditional WAN is replaced by the SDN-enabled WAN (SD-WAN). The SD-WAN consists of routers and switches which are capable of being reprogrammed dynamically with respect to the routing tables and flow rules. The dynamic programmability is enabled by the *Network Control* located in the control center. The *Network Control* consists of an SDN Controller and flow control links to the SDN devices. The SDN controller works as the brain of the SD-WAN. The controller sends the network control signals to all the SDN devices in the SD-WAN in order to change the flows in the network according to a pre-programmed logic. At the same time, the controller receives status information of all the SDN devices in the network to monitor the state of the SD-WAN. The SD-WAN controlled by the SDN controller enables the implementation of Moving Target Defense (MTD) in the network which significantly reduces the impact of DoS attacks on the WAN. This is discussed further in Section IV-A.

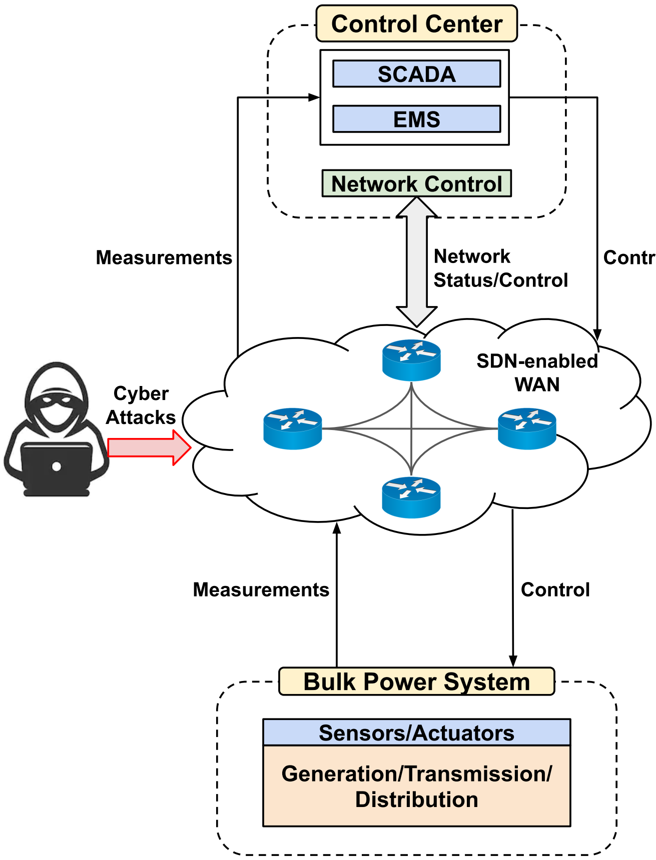

Fig. 3. SDN-enabled CPS Model of the Smart Grid

A. MTD-based Route Switching

Fig. 4 shows a system wherein *Host-1* and *Host-2* are exchanging data over an SDN-enabled network. The initial communication is taking place on the channel "$Host-1 \rightarrow Router-1 \rightarrow Router-2 \rightarrow Router-4 \rightarrow Host-2$". Subsequently, this channel undergoes a DoS attack from an adversary which blocks all the data flow on this channel. The SDN controller senses the blocking of the communication path and switches the data flow to the other available channel "$Host-1 \rightarrow Router-1 \rightarrow Router-3 \rightarrow Router-4 \rightarrow Host-2$" by changing the routing tables of *Router-1, Router-2, Router-3*, and *Router-4*. This allows the hosts to exchange the data successfully without any impacts due to the DoS attack. This type of route mutation or switching is a type of MTD wherein the attacked channel (or target) is switched to a healthy or unaffected communication path.

With respect to route switching, there can be two types of MTDs: (1) Reactive MTD - In this type of route switching, the controller switches the path after it detects the injected attack in the network; and (2) Proactive MTD - In this case, the route switching is always turned on, that is, the communication path between the hosts keeps switching continuously whether the attack is present or not. Even though Reactive MTD can show better performance as compared to proactive MTD in this example, the overheads associated with reactive MTD are much higher in terms of detecting the injection and removal of attack. In this work, we have considered proactive MTD-based route switching only.

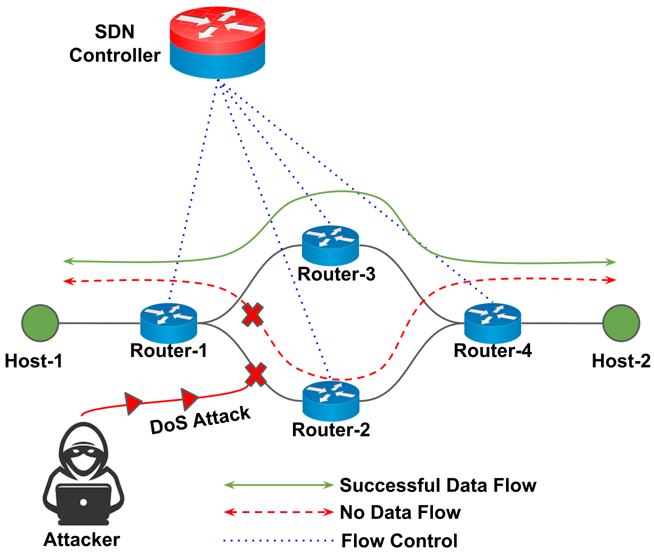

Fig. 4. DoS Attack Impact on SDN-enabled MTD Routing

B. MTD Performance Parameters

The performance of the MTD for different environments is dependent on the following parameters:

1) Diversity or Redundancy: Depending on the number of options available for randomization, the performance of the MTD can vary. This means that if there are, for example, only a limited set of redundant communication channels that can act as alternate channels for the same communication, the attacker can eventually figure out switching targets as the alternate paths keep repeating over time.

2) Randomness: The amount of randomness used in designing the MTD determines how difficult it will be for the attacker to compromise the MTD technique. If the MTD repeats itself more often and there is not enough randomness, the attacker after multiple attempts can figure out the MTD patterns and exploit the repetition of the configurations.

3) Switching Frequency: One of the important aspects of MTD is how often should the targets be moved, which can be called the switching frequency of the MTD. If the switching frequency is too high, the performance of the system can go down as the communication protocol overheads may increase in this case, that is, the protocols require a specific minimum amount of time for successful communication, e.g., TCP handshake. On the other hand, if the switching frequency is too low, then the attack vectors can have higher impacts on the performance of the system.

4) Peer-to-peer vs Centralized: The configuration control of the entities on which MTD is being implemented can be either decentralized (peer-to-peer) or centralized. In the case of decentralized configuration control, the MTD agents decide locally as to what their respective configurations are going to be in the next cycle or when to change the configurations. Whereas in the centralized case, all the MTD agents (or entities) communicate with a central decision making logic which sends the configurations to all the entities for every switching cycle. The decentralized MTD is more robust as the failure of one component will not affect the whole system whereas the centralized MTD has a single point of failure, the central controller, which in case of a failure will lead to the whole system getting affected. SDN implements the centralized type of MTD wherein the SDN controller is the single point of failure. Although this limitation can be overcome by having redundant central controllers.

V. Experimental Evaluation

A. Mininet-based Testbed Architecture

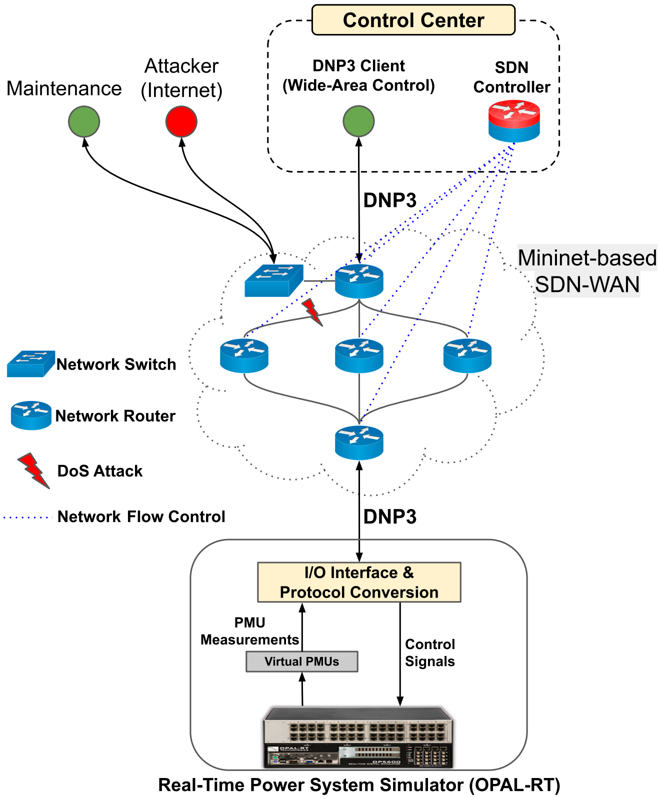

Fig. 5. HIL Testbed-based Implementation Architecture

Fig. 5 shows the Hardware-in-the-Loop (HIL) testbed-based implementation architecture of the MTD-enabled SDN routing for a smart grid environment in the testbed located at the Iowa State University [5], [19]. The implementation consists of: (1) Real-time power system simulator (OPAL-RT): The OPAL-RT implements the physical models of the grid in real-time along with the communication interfaces with the network; (2)

Mininet-based SD-WAN: The SDN-enabled WAN is implemented using the open source software Mininet 2.3.0 which enables emulation of SDN routers and switches as well as the SDN Controller; (3) Control Center: The control center hosts the wide-area control system (WACS) application that controls the power grid in OPAL-RT for reliable operation; and (4) External Nodes: These consist of the cyber attacker who injects DoS attack in the SD-WAN and a maintenance node which can send legitimate data to the grid and the control center. The grid communicates with the WACS using the DNP3 protocol at a rate of 1 data packet per second, sending different measurements to the WACS (which acts as a DNP3 client) and in turn receiving control signals for stable operation of the grid. The measurements are converted from IEEE C37.118 to DNP3 using the I/O interface and protocol conversion module within the OPAL-RT. The DNP3 protocol-based communication is facilitated by the Mininet-based SD-WAN. The SD-WAN consists of three parallel channels over which the WACS and the grid can communicate. The attacker and the maintenance node act as external hosts which are connected to the SD-WAN using a switch.

B. Results and Evaluation

The attacker carries out a DoS attack on one of the communication channels as shown by the red bolt in Fig. 5. The attacked channel (left-most path) is considered as the default path for the data exchange between the the control center and the grid. We have made the assumption that the attacker has the capacity to completely block only one of the channels using a DoS attack. The attack vectors used for the DoS attack are shown in Table I. The attack volume is defined in terms of number of TCP SYN packets injected per second and various percentages of the maximum attack volume (1000 packets/sec) are used as the attack vectors for various test cases.

TABLE I
DoS Attack Vectors: Attack Volume

Attack Volume Percentage	TCP SYN packets/sec
100%	1000
75%	750
50%	500
25%	250
0%	0

As mentioned in Section IV, we have considered proactive MTD as the defense mechanism to mitigate the impacts of the DoS attack. With respect to the parameters of MTD that are mentioned in Section IV-B, the proposed implementation of the MTD has the following parameters:

1) Diversity or Redundancy: Three parallel communication channels connecting control center with the grid.

2) Randomness: The switching between the three channels is randomly chosen using random number generator.

3) Switching Frequency: The switching between the three channels for proactive MTD is done at various timings starting from 0.1 seconds to 15 seconds for each channel.

4) Peer-to-peer vs centralized: Since the proposed implementation is based on SDN, the MTD is centralized.

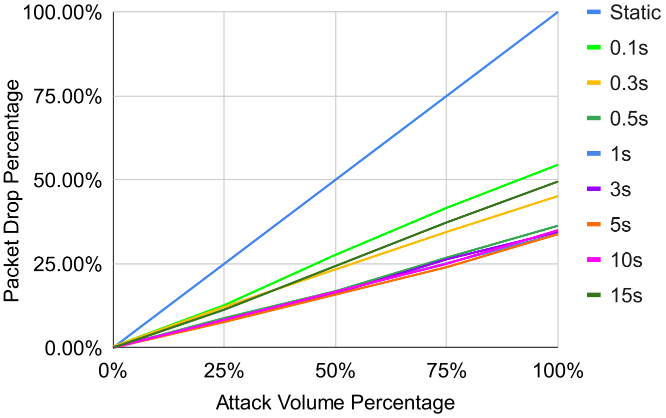

Fig. 6. Percentage Packet Drop vs Attack Volume Percentage for Various MTD Switching Times

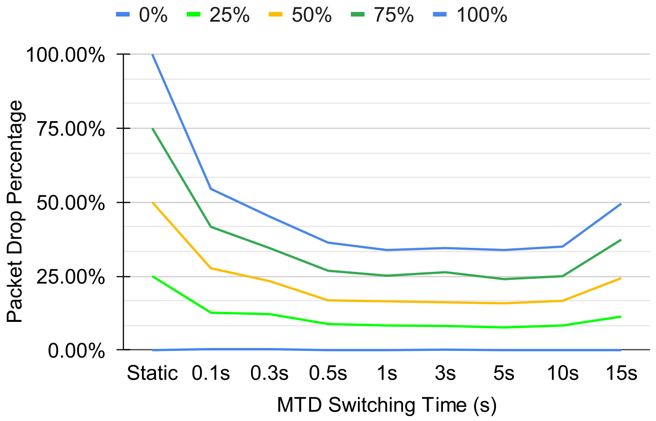

Fig. 7. Percentage Packet Drop vs MTD Switching Time for Various Attack Volume Percentages

Figs. 6 and 7 show the average DNP3 packet drop percentage between the control center and the OPAL-RT for varying attack volume percentages and MTD switching times, respectively. Figs. 8 and 9 show the average DNP3 packet round trip time (RTT) between the control center and the grid (OPAL-RT) for varying attack volume percentages and MTD switching times, respectively.

The results show that the packet drop percentage between the control center and the grid decreases initially with the increase in the MTD switching times but then starts to increase as the MTD switching time goes over 5 seconds. As explained in Section IV-B, depending on the polling time between the control center and the grid (1s in this case), the optimal MTD switching time in this case is 5s. The MTD-enabled operation using the SD-WAN always performs better than the static configuration (wherein no switching of channels takes place).

The average RTT for the packets between the control center and the grid does not vary as much with changing MTD switching times and attack volumes with the average RTT ranging between 0.12s to 0.15s in all cases. This implies that the packets that are sent when the channel is being flooded are dropped completely, whereas only the packets that are exchanged when the channel is not flooded are acknowledged

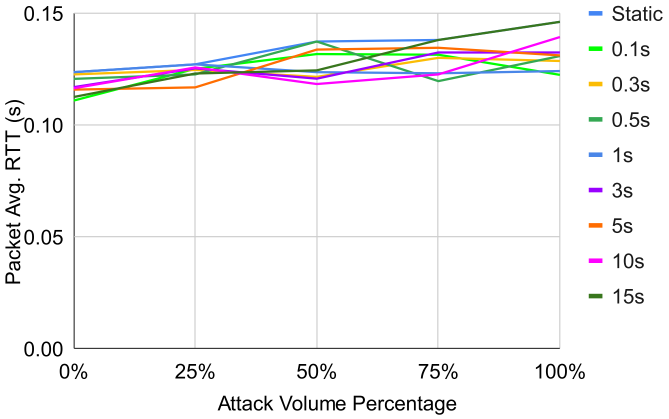

Fig. 8. Packet Average Round Trip Time vs Attack Volume Percentage for Various MTD Switching Times

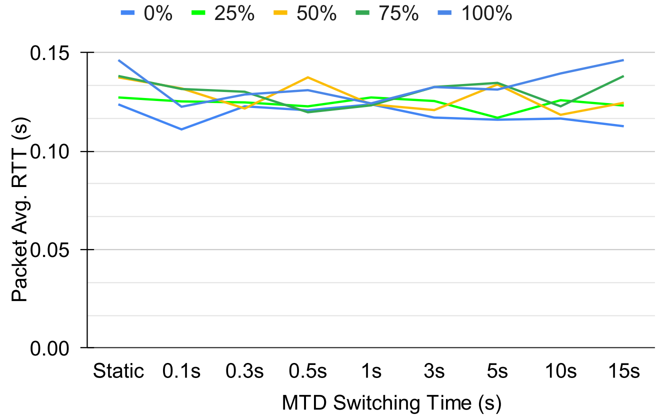

Fig. 9. Packet Average Round Trip Time vs MTD Switching Time for Various Attack Volume Percentages

by either the client or the server.

VI. Conclusion and Future Work

We proposed an MTD-enabled SDN for the Smart Grid communication architecture to mitigate the impacts of DoS attacks on the communication network. We implemented and evaluated the proposed solution on a Hardware-in-the-Loop (HIL) Testbed using Mininet 2.3.0 open source software to facilitate communication between a real-time power system simulator and a wide-area control application over DNP3 protocol. The MTD-enabled SD-WAN allows communication between the physical grid and the control center even when a communication channel is undergoing a DoS attack. The results show the advantages of using MTD based on SDN for the wide-area network (WAN) with much lower packet drop percentages under a DoS attack in the case of MTD-based routing in the SD-WAN. As part of the future work, we are currently working on evaluating the performance of the Wide-Area Control Application under DoS attack by measuring the impact on the grid stability using the voltages and power flows in the grid. We also plan to extend this work to evaluate larger networks, other types of attacks, and different MTD configuration parameters.

Acknowledgment

This work is funded in part by (1) The NSF CPS grant ECCS 1739969 for Moataz Abdelkhalek, Burhan Hyder, and Manimaran Govindarasu; and (2) The Office of Naval Research under grant number N000141812395 and through Department of Energy under U.S. DOE Idaho Operations Office Contract DE-AC07-05ID14517, as part of the Resilient Control and Instrumentation Systems (ReCIS) program of Idaho National Laboratory for Craig G. Rieger.

References

[1] US Department of Energy, “Communications Requirements of Smart Grid Technologies,” 2010. [Online]. Available: https://www.energy.gov/gc/downloads/communications-requirements-smart-grid-technologies

[2] National Institute of Standards and Technology (NIST), “Guidelines for Smart Grid Cybersecurity,” 2014. [Online]. Available: http://dx.doi.org/10.6028/NIST.IR.7628r1

[3] JD Taft (PNNL) and NASPI, “NASPInet 2.0 Architecture Guidance,” 2019. [Online]. Available: https://www.naspi.org/node/746

[4] Cybersecurity of Energy Delivery Systems (CEDS) Research and Development, “Software-defined Networking for Energy Delivery Systems (SDN4EDS): An Architectural Blueprint – Final Report,” 2021. [Online]. Available: https://www.osti.gov/servlets/purl/1840650

[5] G. Ravikumar, B. Hyder, J. R. Babu, K. Khanna, M. Govindarasu, and M. Parashar, “Cps testbed architectures for wampac using industrial substation and control center platforms and attack-defense evaluation,” in *2021 IEEE Power Energy Society General Meeting (PESGM)*, 2021.

[6] S. Rinaldi, F. Bonafini, P. Ferrari, A. Flammini, E. Sisinni, D. D. Cara, N. Panzavecchia, G. Tinè, A. Cataliotti, V. Cosentino, and S. Guaiana, “Characterization of ip-based communication for smart grid using software-defined networking,” *IEEE Transactions on Instrumentation and Measurement*, 2018.

[7] A. Aydeger, N. Saputro, K. Akkaya, and S. Uluagac, “Sdn-enabled recovery for smart grid teleprotection applications in post-disaster scenarios,” *Journal of Network and Computer Applications*, 2019.

[8] E. Molina and E. Jacob, “Software-defined networking in cyber-physical systems: A survey,” *Computers Electrical Engineering*, 2018.

[9] M. H. Rehmani, A. Davy, B. Jennings, and C. Assi, “Software defined networks-based smart grid communication: A comprehensive survey,” *IEEE Communications Surveys Tutorials*, 2019.

[10] A. H. M. Jakaria, M. A. Rahman, and A. Gokhale, “Resiliency-aware deployment of sdn in smart grid scada: A formal synthesis model,” *IEEE Transactions on Network and Service Management*, 2021.

[11] M. H. Rehmani, F. Akhtar, A. Davy, and B. Jennings, “Achieving resilience in sdn-based smart grid: A multi-armed bandit approach,” in *2018 4th IEEE NetSoft*, 2018.

[12] A. C. Pappa, A. Ashok, and M. Govindarasu, “Moving target defense for securing smart grid communications: Architecture, implementation amp; evaluation,” in *2017 IEEE Power Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, 2017.

[13] Z. Zhang, R. Deng, D. K. Y. Yau, P. Cheng, and J. Chen, “On hiddenness of moving target defense against false data injection attacks on power grid,” *ACM Transactions on Cyber-Physical Systems*, 2020.

[14] ——, “Analysis of moving target defense against false data injection attacks on power grid,” *IEEE Transactions on Information Forensics and Security*, 2020.

[15] J. Tian, R. Tan, X. Guan, and T. Liu, “Enhanced hidden moving target defense in smart grids,” *IEEE Transactions on Smart Grid*, 2019.

[16] J. Tian, R. Tan, X. Guan, Z. Xu, and T. Liu, “Moving target defense approach to detecting stuxnet-like attacks,” *IEEE Transactions on Smart Grid*, 2020.

[17] S. Lakshminarayana, E. V. Belmega, and H. V. Poor, “Moving-target defense against cyber-physical attacks in power grids via game theory,” *IEEE Transactions on Smart Grid*, 2021.

[18] J. Steinberger, B. Kuhnert, C. Dietz, L. Ball, A. Sperotto, H. Baier, A. Pras, and G. Dreo, “Ddos defense using mtd and sdn,” in *IEEE/IFIP Network Operations and Management Symposium*, 2018.

[19] G. Ravikumar, B. Hyder, M. Abdelkhalek, and M. Govindarasu, “On-Premise Cloud-based HIL CPS Security Testbed for Smart Grid,” 2020. [Online]. Available: https://powercybertestbed.ece.iastate.edu/