Analyzing Impact of Communication Network Topologies on Reconfiguration of Networked Microgrids

Venkatesh Venkataramanan, YiPeng Zhou, and Anurag Srivastava
School of Electrical Engineering and Computer Science, Washington State University, Pullman, WA 99164.
E-mails: {vvenkata, yzhou, asrivast}@eecs.wsu.edu

***Abstract*—This paper studies the impact of communication network on the performance of reconfiguration of networked microgrids. Various communication network topologies can be used to support the microgrid operation, each offering a set of advantages and disadvantages on the performance of reconfiguration. Network Simulator 3 (NS3) is used for the communication system simulation. A test system with two proximal microgrids based on the CERTS concept is developed in MATLAB, with a few modifications for interconnection and reconfiguration. A reconfiguration algorithm developed in MATLAB aims to supply the maximum amount of load supported by communication network for data exchange. Various case studies with different communication network topologies, loss of communication links and initiating event for microgrid reconfiguration are performed. The simulation results are discussed to analyze the impact of supporting communication network on operational time of the reconfiguration of networked microgrids.**

***Index Terms*—CERTS, communication architectures, microgrids, network simulation, reconfiguration.**

I. Introduction

The power system is increasingly becoming a cyber-physical system, and the impact of cyber system on the power system needs to be analyzed [1]–[3]. The cyber-physical model of power system needs to consider the power system topology and the communication topology [3], [4]. The traditional power system topology has the generation, transmission, and distribution system components. The communication topology consists of the communication medium and various cyber assets such as routers, switches, and network hosts.

Reconfiguration is used to ensure higher reliability and minimizing the amount of load lost after an adverse event [5]. The communication network needs to be reliable and fast for ensuring that the reconfiguration is successful. Several studies have shown that latency in communication of control signals can have adverse effect on the operation of power system in general [6], [7], and also in microgrids [8]. There have been several studies on the communication topologies used in the power grid and their impacts on various power system applications [6], [9]. This paper aims to analyze the impact of the communication network on the performance of reconfiguration for different communication topologies and operating scenarios.

Reconfiguration is more challenging with integration of microgrids in the distribution system. This paper considers two microgrids based on a modified CERTS (Consortium for Electric Reliability Technology Solutions) concept [10]. The various communication topologies that can be used with this network model is developed, and different operating scenarios are simulated to evaluate the impact of the communication network on reconfiguration performance. A reconfiguration algorithm developed by the authors of this paper [11] is implemented at the control center for the distribution system, and the delay in communication is determined to evaluate the impact on the power system. The contribution of this paper is to evaluate different network configurations and study their impact on the reconfiguration, which helps in understanding the operational reliability for the cyber-physical power system. The procedure used here can also be extended to analyze other applications such as stability analysis for the holistic cyber physical model of the power grid.

The rest of the paper is organized as follows. The basics of the communication network simulator and its working has been explained in Section II. The model of the power system and the reconfiguration algorithm is explained in Section III. The communication system modeling is discussed in Section IV. The simulation results for various architectures and discussion are in Section V. The conclusions are provided in Section VI.

II. Network Simulator 3 (ns3)

There are various network simulators and emulators available for modeling of communication networks. Some of them are OMNET++ [12], OPNET [13], NS3 [14], CORE [15], GridStat [16], and DeterLab [17]. In this paper, the network model is simulated using the NS-3 simulator. NS-3 has been previously used for simulating the communication network for the power grid for different applications [18]–[21]. NS-3 has been chosen for its simplicity in creating network models, and accuracy of the simulated communication system.

The scripting of NS-3 can be developed using C++ or Python, and it has several software libraries. By using C++ or Python, the user can build a link with these libraries. There

---

This work is partially supported by the US Department of Energy under Award Number DE-OE0000780. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

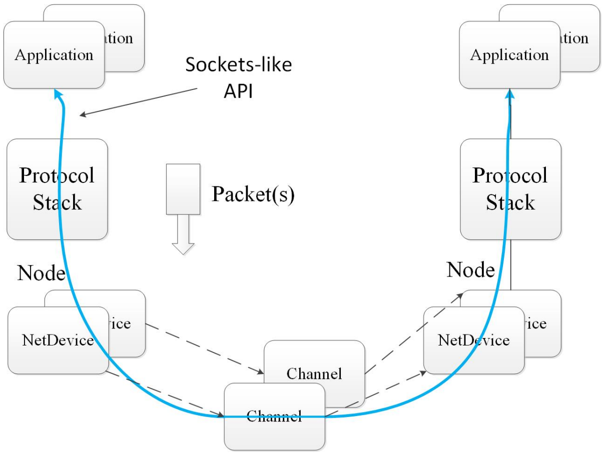

Fig. 1. Basic view of NS3 simulation [22]

is a core library responsible for managing the models and the back end processes of the simulator. A simulator library is defined for declaring events, time objects, and schedulers and a common library will declare the network architecture. Finally, the node and device libraries are taken care of by definition of classes in NS-3. The classes provide a template for which objects can be created and directly used in the simulation. The basic architecture of NS-3 is shown in Fig 1.

The following are some key concepts in a NS-3 simulation:
1. Node: A computing device in a network is called a node.
2. Application: The function of application is to run NS-3 node to drive simulations.
3. Channel: The channel is responsible for connecting node to sub-network objects and managing communication.
4. Net Device: The net device is installed in node in order to help the nodes to communicate with each other through channels. In some case, one node has multiple channels and multiple net devices.
5. Topology Helpers: The function of topology helpers is to arrange the connection between nodes, net devices and channels.

III. MODELING OF MICROGRID SYSTEM

The CERTS microgrid has been used in this work to model the networked microgrid. For the purposes of making the microgrid suitable for reconfiguration, a few modifications have been made as detailed below:

1) There is no substation transformer modeled specifically between main grid and the microgrid,
2) Zone-3 and Zone-4 are three-wired and without neutral,
3) There is no isolation transformer in Zone-5,
4) The PV panel supplies both priority loads and non-priority loads in Zone- 3, 4, and 5, and
5) Additional DER units are added to increase the number of feasible paths.

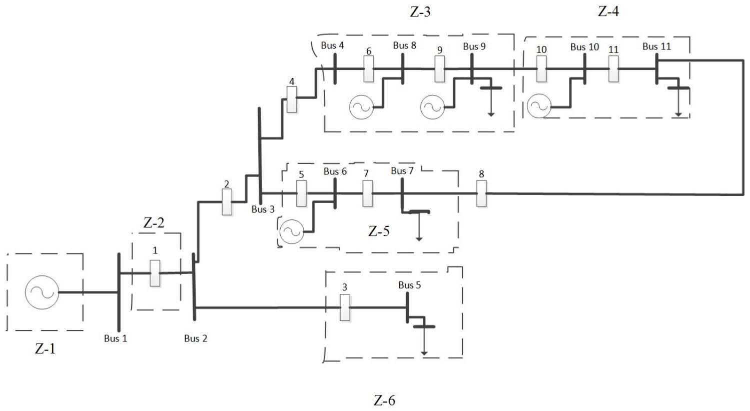

Fig. 2. Modified CERTS Microgrid System

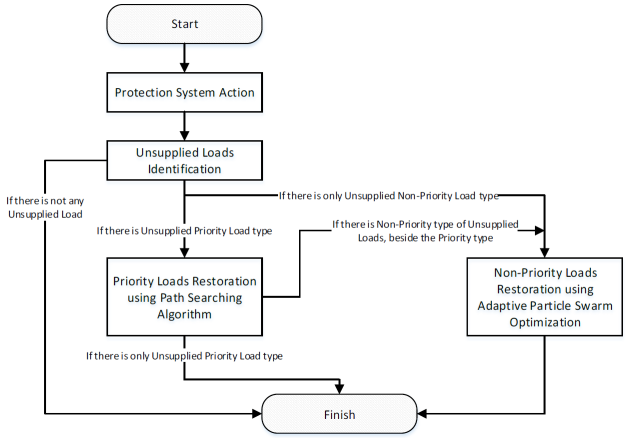

Fig. 4. Reconfiguration Algorithm

The modified model of the microgrid is shown in Fig. 2. In order to provide more options for reconfiguration and also to have a more complex feasible network architecture, two CERTS microgrids have been connected together. The microgrids connect with main grid at the same substation, but have different feeders. In addition, there is a tie line switch between the two individual microgrids, which enables the microgrids to exchange power in cases where the connection through the main grid is unavailable. The overall power system topology is shown in Fig. 3.

The reconfiguration algorithm developed by the authors of this paper [11] for multiple microgrids has two stages. A simplified algorithm is shown in Fig. 4. After protection system action, the unsupplied load identification will find out which loads are unsupplied. If there is no unsupplied load, the algorithm will not lead to any control action. If there is unsupplied load, the algorithm will consider the classification of priority and non-priority load. The process begins with fast restoration of priority load followed by optimal restoration of non-priority load. The priority load is restored using a fast path search algorithm which focuses on timing rather than finding an optimal path. For the non-priority load, a particle swarm optimization based technique is used which attempts to find an optimal path to supply the non-priority load.

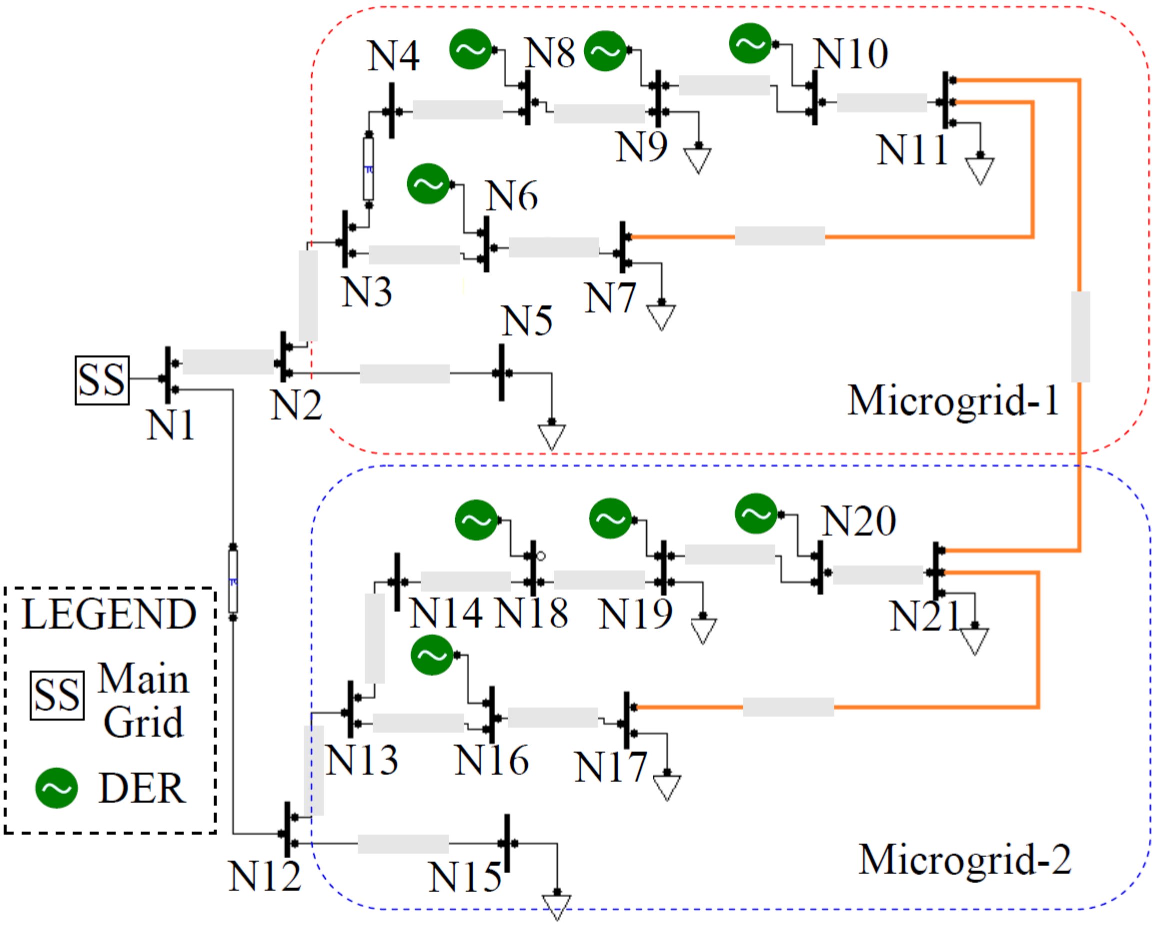

Fig. 3. Multiple Microgrid System

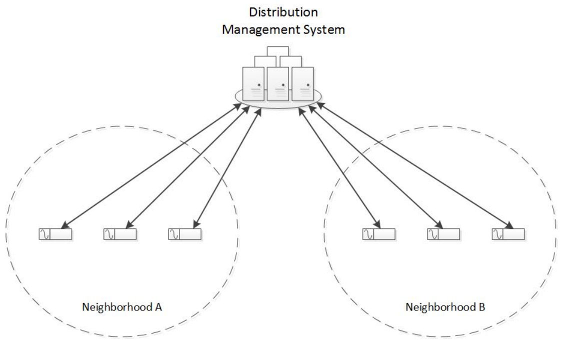

Fig. 5. Point to Point Network

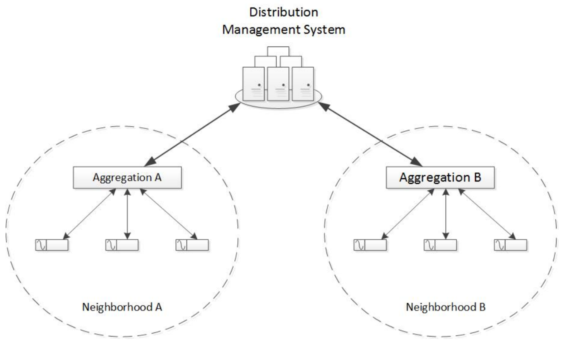

Fig. 6. Aggregated Network

IV. MODELING OF COMMUNICATION SYSTEM

Some of the various commmon network architectures that can be used for this test system are:

1. Point to point network model (P2P) - Fig. 5,
2. Aggregated substation network model (AGG) - Fig. 6, and
3. Meshed network model (MESH) - Fig. 7.

For the communication model, each node of the microgrid is modeled as a node in NS3. The DMS (Distribution Management System) is at the control center, and this is where the reconfiguration algorithm is implemented. For point to point network topology, there are no aggregators in the communication model, and each node is assumed to be directly connected to the control center. The mesh and aggregated networks require an aggregator to be present between the nodes and the control center. In this case, each of the aggregator can be considered as a substation, while the reconfiguration is implemented at the control center with DMS. The key difference between the

TABLE I
RECONFIGURATION ALGORITHM RESULT

Simulation case	Unsupplied load	Final Reconfiguration (Switch Number)	No. of Switching	Restored Load (Bus No.)	Load Not Supplied (Bus No.)
One microgrid is islanded after fault	21	Closed Switch: 1, 3, 4, 5, 6, 7, 8, 9, 10, 11, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22 Opened Switch: 2, 12, 23	4	21	-
A fault within a microgrid leading to load loss	9, 11	Closed Switch: 1, 2, 3, 4, 5, 6, 8, 9, 14, 15, 16, 17, 18, 19, 21, 22, 23 Opened Switch: 7, 10, 11, 12, 13, 20	1	11	9
A fault within a microgrid when two microgrids are islanded	15, 16	Closed Switch: 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 16, 18, 19, 20, 21, 22, 23, 24, 25, 26, 28, 29, 30, 31, 32, 33 Opened Switch: 1, 2, 11, 14, 15, 17, 27	2	15	16

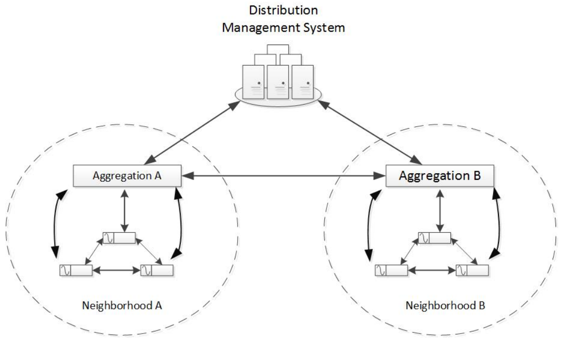

Fig. 7. Meshed Network

mesh and the aggregated communication architectures is that the mesh network also has connections between the various nodes in the system, while in the aggregated architecture the nodes are only connected to the aggregator. In the mesh architecture, more redundancy can also be built in, such as a connection between the node and the DMS directly similar to the point to point configuration for some critical nodes. The planning engineer needs to study the cost-reliability ratio and determine the redundancy required for the system. The microgrid is simulated with all of the above architectures and the performance of the network for various cases is examined in the next section. For all the cases, TCP protocol has been used for simulation. Various application level protocols can be used, but since the focus of the paper is on the communication architecture and not the substation protocols, the application level protocols are not discussed here.

The effect of communication medium is also considered; both fiber optic links and Wi-Fi medium are studied. In distribution communication network, fiber optic cables are usually used between the RTU (Remote Terminal Unit) and DMS. Fiber optic provides lowest network latency and these cables are usually laid with electrical lines. The bandwidth can approach 26 Tbit/s for 50 km and 171 Gbit/s for 240 km [23]. On the other hand, wireless communication makes real-time monitoring of distribution automation more easy in a dispersed area. But it would be costly to build, and hard to maintain and monitor the wireless infrastructure compared to the fiber optic cables. The 802.11a/b/g standards [23] have been widely implemented in various fields with the rapid development of wireless Local Area Network (LAN) technology. The data transmission rate of IEEE 802.11a ranges from 6 Mbps to 54 Mbps at 5 GHz. But for some devices using 802.11b/g standards, the 5 GHz bandwidth does not work as these devices work in the 2.4 GHz bandwidth range. Thus, in this case the 802.11a keeps the same transmission rate of 54 Mbps but operates at 2.4 GHz in order to be compatible with devices using 802.11b/g standards.

V. SIMULATION RESULTS AND DISCUSSION

For determining the impact of communication system on the microgrid reconfiguration performance, several case studies are performed. The case studies examine the network latency for the different models explained in the previous section. Network latency of packets is defined as the delay from the time of the start of packet transmission at the sender host to the packet reception at the receiver host.

The reconfiguration algorithm is run for three scenarios:

1) One microgrid is islanded after fault,
2) A fault within a microgrid leading to load loss, and
3) A fault within a microgrid when two microgrids are islanded.

The result from the reconfiguration algorithm for the cases are provided in Table I. Three case studies have been examined in this paper.

1) Network performance for various communication architectures,
2) Network performance with loss of link, and
3) Network performance with loss of two links

Case A: Network performance for various communication architectures

In this case, the various communication architectures that have been described in Section III are simulated and the time taken for the data to flow through the network is determined. This is a base case, considering that all the nodes and links are working properly. This case is useful to evaluate the base performance of all the configurations. The results are provided in Table II.

1. Point to point: In this architecture, the RTU connects with the DMS directly. It is very simple but suffers from low

TABLE II
Network performance for various communication architectures

Medium	Configuration	Case A (ms)	Case B (ms)	Case C (ms)
Fiber Optic	P2P	10.1	10.14	10.1
	AGG	11.4	11.37	12.5
	MESH	11.4	11.37	12.5
Wi-Fi	P2P	10.1	10.14	10.1
	AGG	38.7	38.742	38.742
	MESH	38.7	38.742	38.742

reliability, which means that the DMS will lose control and monitoring of an area when communication with the RTU in that area fails.

2. Local Access Aggregators: This architecture is more complex than the direct connection between the RTU and the DMS. The addition of the aggregator in this system reduces the connections to the DMS, and helps control the data flow to the DMS. This will be an advantage when considering bigger systems or more frequent data. However, it does not improve the reliability of the network as a single communication failure can still stop information from that area. The addition of the aggregators make it more vulnerable that a single failure will isolate a bigger area instead of the status of a single RTU. The trip time is slightly higher when compared to the point to point model, but for the purposes of reconfiguration, this is acceptable.

3. Meshed Network: This architecture takes care of the disadvantages of the aggregator model by creating more redundant connections that ensures reliability in communication. It also takes care of the single failure problem from the other two network architectures. The trip times are comparable to the aggregated network model, but still within acceptable range for reconfiguration. However, the increased time might be of concern for bigger systems and applications with more demanding time requirements. The cost also becomes a factor as the number of redundant connections is increased. Finding the balance between cost and performance is a process unique to each microgrid system, and even the initial design might not be optimum solution throughout the lifetime of the microgrid, and might need to be updated at regular intervals.

Case B: Network performance with loss of link

In this case, a network link between the RTU and the aggregator is considered to be lost. This case does not consider the point to point model, as the loss of the communication link means that the DMS cannot communicate with the host. The aggregated model loses a link, and might result in a loss of an additional load if the loss occurs at a different place. The mesh architecture is not really affected by the loss of a link as there is enough redundancy in the network. For the simulated case, the network latency remains the same. The results are provided in the Table III.

TABLE III
Network performance with loss of link

Medium	Configuration	Case A (ms)	Case B (ms)	Case C (ms)
Fiber Optic	MESH	11.7	11.638	12.8
	AGG	11.7	11.6	12.8
Wi-Fi	MESH	54.3	54.41	54.3
	AGG	54.3	54.41	54.3

TABLE IV
Network performance with loss of two links

Medium	Configuration	Case a (ms)	Case b (ms)	Case c (ms)
Fiber Optic	MESH	11.9	11.91	13
Wi-Fi	MESH	70	70.09	70

Case C: Network performance with loss of node (loss of two links)

In this case, two network links are considered to be lost. This affects the aggregated model more than the mesh model, as the aggregated model loses upto a whole neighborhood if the aggregator is lost. The results are provided in Table IV. This case shows that even for the loss of two links, the meshed architecture is most resilient and the DMS retains control over all the breakers through the redundant links and does not need to shed any load due to loss of communication link. However, it is important to notice that for certain cases, such as the loss of the aggregator, the neighborhood can still be lost if enough redundancy is not built in. This shows that redundancy is more important for the nodes higher in the hierarchy such as the aggregator and the DMS. This will ensure that even if a node in the lower level is lost, the effect is localized.

D. Results Discussion

The results show that the mesh architecture is the most resilient and minimize the impact on performance of reconfiguration. However, more factors need to be considered before deciding on the communication architecture for any system. As previously discussed, cost is an important factor. Having redundancy for non-priority loads will first increase the cost of cables for these redundant connections, but the rest of the communication devices such as switches and routers might also need to be upgraded to deal with the additional data. Another factor to consider is that the increased redundant connections might also increase the attack surface, which needs to be determined by using cyber attack exposure evaluation framework such as [24]. While the point to point architecture certainly has some disadvantages, it might be sufficient for a smaller geographical area without many obstructions. In most cases, it will be to the advantage of the microgrid operator to do a thorough planning study and adopt a hybrid architecture depending on the number of priority and non-priority loads. The study performed in this paper provides a method to analyze a test system for reconfiguration, which can also be used for other applications such as stability studies.

VI. CONCLUSIONS

This paper examines the various communication architectures to support the networked microgrid configuration. The paper addresses the modeling of the microgrid, implmentation of a reconfiguration algorithm for different scenarios, and the communication network latency for all these cases. The effect of communication medium and architecture in terms of implementation is also considered. It has been determined that the meshed communication model is most resilient when considering the loss of communication links as the other architectures result in shedding load due to loss of control over the breaker. The contribution of this paper is to provide a framework to analyze impact of cyber system on the microgrid reconfiguration performance in quantitative manner.

ACKNOWLEDGMENT

The authors gratefully acknowledge the financial support provided by the National Science Foundation (NSF) for this research.

REFERENCES

[1] G. Brown, M. Carlyle, J. Salmerón, and K. Wood, "Defending critical infrastructure," *Interfaces*, vol. 36, no. 6, pp. 530–544, 2006.

[2] G. N. Ericsson, "Cyber security and power system communicationessential parts of a smart grid infrastructure," *Power Delivery, IEEE Trans.*, vol. 25, no. 3, pp. 1501–1507, 2010.

[3] R. R. Rajkumar, I. Lee, L. Sha, and J. Stankovic, "Cyber-physical systems: the next computing revolution," in *Proceedings of the 47th Design Automation Conference*. ACM, 2010, pp. 731–736.

[4] S. Karnouskos, "Cyber-physical systems in the smartgrid," in *Industrial Informatics (INDIN), 2011 9th IEEE International Conference on*. IEEE, 2011, pp. 20–23.

[5] S. Mishra, D. Das, and S. Paul, "A comprehensive review on power distribution network reconfiguration," *Energy Systems*, pp. 1–58, 2016.

[6] P. Kansal and A. Bose, "Bandwidth and latency requirements for smart transmission grid applications," *Smart Grid, IEEE Transactions on*, vol. 3, no. 3, pp. 1344–1352, 2012.

[7] C. P. Nguyen and A. J. Flueck, "Modeling of communication latency in smart grid," in *Power and Energy Society General Meeting, 2011 IEEE*. IEEE, 2011, pp. 1–7.

[8] A. Shapoury, V. Venkataramanan, A. Mallikeswaran, A. Mehrizi-Sani, and M. Lopez, "Study of stability of an islanded microgrid in the presence of communication delays," in *Industrial Electronics Society, IECON 2014-40th Annual Conference of the IEEE*. IEEE, 2014, pp. 5666–5671.

[9] W. Wang, Y. Xu, and M. Khanna, "A survey on the communication architectures in smart grid," *Computer Networks*, vol. 55, no. 15, pp. 3604–3629, 2011.

[10] R. Lasseter, J. Eto, B. Schenkman, J. Stevens, H. Vollkommer, D. Klapp, E. Linton, H. Hurtado, and J. Roy, "CERTS microgrid laboratory test bed," *Power Delivery, IEEE Transactions on*, vol. 26, no. 1, pp. 325–332, Jan 2011.

[11] F. Martina, "Graph theory and particle swarm based reconfiguration of multiple microgrids for grid resiliency," *M.S. Thesis Dissertation, Washington State Univesrity*, December 2014.

[12] A. Varga *et al.*, "The OMNeT++ discrete event simulation system," in *Proceedings of the European simulation multiconference (ESM 2001)*, vol. 9, no. S 185. sn, 2001, p. 65.

[13] X. Chang, "Network simulations with OPNET," in *Proceedings of the 31st conference on Winter simulation: Simulation—A bridge to the future-Volume 1*. ACM, 1999, pp. 307–314.

[14] T. R. Henderson, M. Lacage, G. F. Riley, C. Dowell, and J. Kopena, "Network simulations with the NS-3 simulator," *SIGCOMM demonstration*, vol. 14, 2008.

[15] J. Ahrenholz, "Comparison of CORE network emulation platforms," in *MILCOM, 2010 MILITARY COMMUNICATIONS CONFERENCE*.

[16] H. Gjermundrod, D. E. Bakken, C. H. Hauser, and A. Bose, "GridStat: A flexible qos-managed data dissemination framework for the power grid," *Power Delivery, IEEE Transactions on*, vol. 24, no. 1, pp. 136–143, 2009.

[17] J. Mirkovic and T. Benzel, "Teaching cybersecurity with DeterLab," *Security & Privacy, IEEE*, vol. 10, no. 1, pp. 73–76, 2012.

[18] D. Hartmann, K. Wolter, and T. Krauss, "ICT resilience simulations in small confined smart distribution grids," in *Telecommunications Energy Conference 'Smart Power and Efficiency' (INTELEC), Proceedings of 2013 35th International*, Oct 2013, pp. 1–6.

[19] C. Vellaithurai, S. Biswas, and A. Srivastava, "Development and application of a real-time test bed for cyber physical system," *Systems Journal, IEEE*, vol. PP, no. 99, pp. 1–12, 2015.

[20] B. Kelley, P. Top, S. Smith, C. Woodward, and L. Min, "A federated simulation toolkit for electric power grid and communication network co-simulation," in *Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES), 2015 Workshop on*, April 2015, pp. 1–6.

[21] J. Fuller, S. Ciraci, J. Daily, A. Fisher, and M. Hauer, "Communication simulations for power system applications," in *Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES), 2013 Workshop on*, May 2013, pp. 1–6.

[22] C. Vellaithurai, "Cyber power system analysis using a real time test bed," *M.S. Thesis Dissertation, Washington State Univesrity*, July 2013.

[23] "IEEE draft standard for information technology-telecommunications and information exchange between systems-local and metropolitan networks-specific requirements-part ii: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications-amendment 8: IEEE 802.11 wireless network management," *IEEE P802.11v/D15.0, September 2010*, pp. 1–428, Sept 2010.

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