Service-Based, Segmented, 5G Network-Based Architecture for Securing Distributed Energy Resources

Preprint

Daniel Bennett, Adarsh Hasandka, MD Touhiduzzaman, and Evan Vaughan

National Renewable Energy Laboratory

Presented at the 2021 IEEE Power & Energy Society General Meeting
July 25-29, 2021

NREL is a national laboratory of the U.S. Department of Energy
Office of Energy Efficiency & Renewable Energy
Operated by the Alliance for Sustainable Energy, LLC

This report is available at no cost from the National Renewable Energy Laboratory (NREL) at www.nrel.gov/publications.

Contract No. DE-AC36-08GO28308

Conference Paper
NREL/CP-5R00-78055
February 2021

Service-Based, Segmented, 5G Network-Based Architecture for Securing Distributed Energy Resources

Preprint

Daniel Bennett, Adarsh Hasandka, MD Touhiduzzaman, and Evan Vaughan

National Renewable Energy Laboratory

Suggested Citation
Bennett, Daniel, Adarsh Hasandka, MD Touhiduzzaman, and Evan Vaughan. 2021. *Service-Based, Segmented, 5G Network-Based Architecture for Securing Distributed Energy Resources: Preprint*. Golden, CO: National Renewable Energy Laboratory. NREL/CP-5R00-78055. https://www.nrel.gov/docs/fy21osti/78055.pdf.

NREL is a national laboratory of the U.S. Department of Energy
Office of Energy Efficiency & Renewable Energy
Operated by the Alliance for Sustainable Energy, LLC

This report is available at no cost from the National Renewable Energy Laboratory (NREL) at www.nrel.gov/publications.

Contract No. DE-AC36-08GO28308

Conference Paper
NREL/CP-5R00-78055
February 2021

National Renewable Energy Laboratory
15013 Denver West Parkway
Golden, CO 80401
303-275-3000 • www.nrel.gov

NOTICE

This work was authored by the National Renewable Energy Laboratory, operated by Alliance for Sustainable Energy, LLC, for the U.S. Department of Energy (DOE) under Contract No. DE-AC36-08GO28308. This work was supported by the Laboratory Directed Research and Development (LDRD) Program at NREL. The views expressed herein do not necessarily represent the views of the DOE or the U.S. Government.

Cover Photos by Dennis Schroeder: (clockwise, left to right) NREL 51934, NREL 45897, NREL 42160, NREL 45891, NREL 48097, NREL 46526.

NREL prints on paper that contains recycled content.

Service-Based, Segmented, 5G Network-Based Architecture for Securing Distributed Energy Resources

Daniel Bennett, *Senior Member, IEEE*, Adarsh Hasandka, *Member, IEEE*, MD Touhiduzzaman, *Member, IEEE*, Evan Vaughan

***Abstract*-- As the number of connected devices in the energy grid increases exponentially, particularly facilitated by modern communications standards such as 5G and beyond, so too does the cyberattack surface. However, 5G also includes features that can help mitigate certain cybersecurity risks. This paper proposes a new service-based network architecture implementing network-slicing capabilities for connected systems and devices to improve performance, availability, security, and reliability of grid devices and services. It considers the quality-of-service requirements and criticality of services needed for securely monitoring, operating, and securing distributed energy resource devices. From developed use cases, network slicing is implemented based on these requirements and resource allocations. This work then highlights examples of how slicing can help prevent standard existing attack methods, such as a denial-of-service or similar attack, which limit resource availability and network bandwidth to the service, and thus inhibit the attack's ability to affect other services. The designed network architecture use case was tested on the National Renewable Energy Laboratory's Cyber-Energy Emulation Platform (CEEP) to verify secure operation and availability of services. Using hardware-in-the-loop devices and systems on CEEP, this fully segmented, secure network may be realized and evaluated. Finally, this paper presents the results of this testing.**

***Index Terms*—5G, cybersecurity, Distributed Energy Resources, DER, network slicing**

I. Introduction

The energy grid's center of gravity is evolving toward the grid edge with increased penetration of renewable technologies, storage, connected transportation, smart buildings, smart cities, and essentially any connected device that uses power and invariably touches the grid to some extent. This energy system transformation is dependent on multifaceted communications, and as we see, the IT infrastructure is evolving toward 5G and beyond. The confluence of 5G and grid edge devices, resources, and systems offer tremendous challenges and opportunities. This work seeks to leverage 5G core functions that can further enable secure and resilient integrated distributed energy resource (DER) systems—behind-the-meter solar photovoltaics, batteries, electric vehicles, and many other areas. A key aspect of DERs relates to the information flow and interconnectedness between these devices and their associated electronics that must take place for coordination, control, efficiency, stability, and resilience purposes versus the more traditional, inertially controlled grid. The protocols used by DERs, such as the IEC-61850 communications protocol, require highly reliable and low-latency (delay) connections; traditionally, such critical infrastructures require dedicated communications networks to meet their specific requirements. This approach, though, can be very costly and difficult and not easily deployable or scaled for dynamic environments or for changes in demand requirements (elasticity).

A solution to integrating DERs seamlessly to the grid with 5G is to leverage network slicing, [1] defined as "multiple, virtual networks, so called network slices, on top of one underlying, shared (public) Physical Network (PN)." [2] describes slicing as "incorporating software defined networking (SDN) and network functional virtualization (NFV)." The independent, virtually separate networks created by 5G network slicing can provide for requirements of individual DER systems and minimize costs and configuration overhead [2].

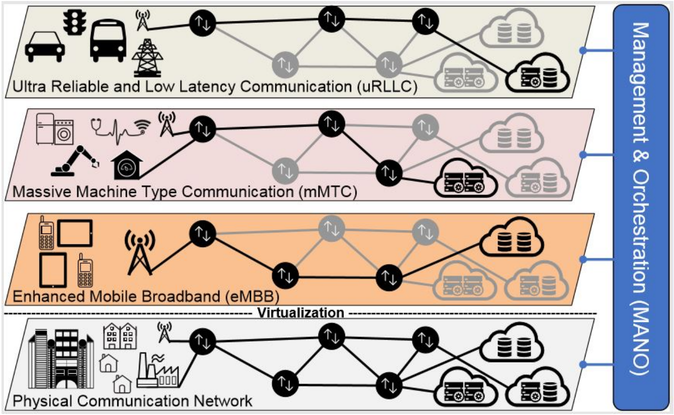

Ultra Reliable and Low Latency Communication (uRLLC)
Massive Machine Type Communication (mMTC)
Enhanced Mobile Broadband (eMBB)
Virtualization
Physical Communication Network
Management & Orchestration (MANO)

Figure 1. 5G slicing characteristics [1], used with permission

For slicing in 5G architectures, the three main categories—enhanced mobile broadband (eMBB), massive machine-type communication (mMTC), and ultra-reliable low-latency communication (uRLLC)—have been defined and are shown in Figure 1 [1]. As shown, a dedicated SDN controller for management and orchestration provides individual slices, which are then managed by their own controller. Slices can then be isolated from one another as shown in [3]. It is noteworthy to mention that the advanced communications technologies and protocols used in DERs are vulnerable to attacks by attempts to intercept, modify, and/or corrupt control signal packets. The National Electric Sector Cybersecurity Organization Resource (NESCOR) working group [4] identified many realistic cybersecurity failure scenarios in the DER domain, which impact distribution grid stability. Some scenarios are related to DER management systems (DERMS) and field DER energy management systems and focus on the disruption of communications technologies. Designing a 5G network architecture in the DER domain must focus on capabilities that help prevent a denial-of-service (DoS) or similar attack by limiting static resource availability and network bandwidth to the service [5].

A microgrid is a small network that consists of multiple components such as a microgrid controller, load controller, and other DER components. Microgrids perform different respective functionalities, primarily for monitoring, diagnosis, and operations. 5G network slicing characteristics help microgrid networks to generate corresponding virtual network topologies and a series of virtual network function sets for each corresponding functionality. Although 5G network slicing in microgrids brings potential benefits from an operational perspective, it is difficult to accurately quantify the potential economic benefit. In this work, we have focused on the operational perspective of 5G network slicing characteristics in the DER domain.

This paper proposes certain DER use cases by incorporating 5G core technology, and then based on those use cases, segmenting the distribution grid network through network slicing. Various security architectures are enabled by this technology; one investigated specifically in this work is mitigation of DoS attacks [6]. This experiment will demonstrate how slicing can address challenging problems such as a DoS attack on a DER system. We have utilized the National Renewable Energy Laboratory's Cyber-Energy Emulation Platform (CEEP) [7] to model the slice isolation based on different scenarios and to proactively mitigate a DoS attack. The main contributions of this paper are: (1) introducing DER use cases that incorporate 5G characteristics (Section II); (2) creating efficient network slicing through the complete separation of host mission-critical devices or priority loads between slices (Section III); (3) mitigating network latency during a DoS attack and guaranteeing end-to-end delay requirements (Section IV); and (4) successfully validating the 5G characteristics by implementing test cases in CEEP (Section III).

II. 5G-RELATED USE CASES IN DER

5G has the capability to dynamically allocate network resources to facilitate fine-tuned control across the DER environment. Moreover, 5G network slicing characteristics are not only capable to meet specific DER characteristics but can also provide resilience in the distribution grid by creating isolated islands and micro networks. It also enables providers to offer various options as a service, particularly, security as a service (SaaS). A proper example of use cases helps to explain how the DER system should behave within a 5G network perimeter.

The use case models presented here catalog DER characteristics relative to the operation and control of DER 5G communications infrastructure and cover all three groups of 5G categories. The description of a use case will identify one or more DER applications that the 5G SDN platform will perform to accomplish its objectives. Figure 2 shows the high-level overview of integrating DER use cases to 5G network slicing characteristics with a possible slice alignment strategy as shown. Below, we discuss DER use case scenarios that can be enabled by 5G network slicing.

A. Distributed control for DER

For utility stakeholders, a distributed energy management system (DERMS) monitors advanced distribution management systems by controlling the DER. A DERMS actively sends control signal requests or commands to DER devices for procuring flexible services and achieving stability in a larger grid scenario in case of emergency action. To mitigate the larger grid impact, the DER communications network requires maintaining a low-latency characteristic for controlling voltage/reactive power and adjusting active power. Additionally, this communications network needs access to up to tens of millions of DER terminals. In a nutshell, this DER controlling use case depicts 5G as a potentially ubiquitous connectivity enabler, matching the requirements for massive volumes of connection points through an uplink mMTC, and controlling the DER devices for utility stakeholders to assure adequate quality of service (QoS) and reliability through downlink uRLCC.

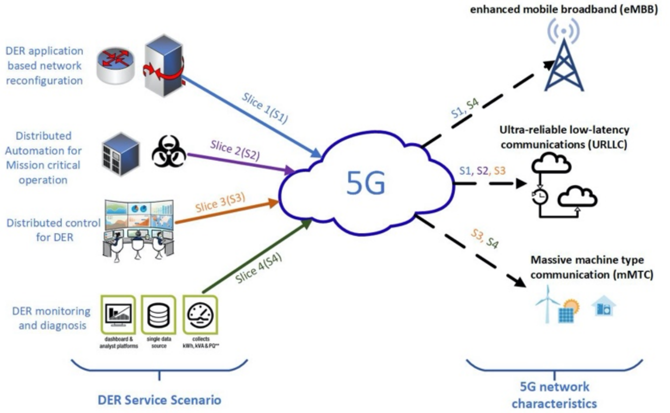

enhanced mobile broadband (eMBB)
DER application based network reconfiguration
Slice 1(S1)
S1, S4
Distributed Automation for Mission critical operation
Slice 2(S2)
Ultra-reliable low-latency communications (URLLC)
5G
S1, S2, S3
Distributed control for DER
Slice 3(S3)
S3, S4
Slice 4(S4)
Massive machine type communication (mMTC)
DER monitoring and diagnosis
dashboard & analyst platforms
single data source
collects kWh, kVA & PQ**
DER Service Scenario
5G network characteristics

Figure 2. Integrating DER use cases to 5G slicing characteristics

B. Distributed automation

A recent study identified that the U.S. Department of Defense's (DOD's) microgrid investments are expected to reach $1.4 billion a year by 2026 [8]. As DERs can produce and operate electricity independently and without interfering with the larger power grid, a greater number of DERs are deployed in DOD's facilities to bolster energy security and resilience. Additionally, DERs have increased significantly in distribution networks. Whether DERs are in mission-critical sites or not, they need to coordinate with the utility control center to reduce line congestion and power quality issues. The uRLCC characteristic in a 5G network can effectively protect information transfer from the DER to distribution automation devices and help to achieve millisecond-level precise discrimination of a line fault. This ultra-fast fault detection enables the rapid self-healing capability in a mission-critical operation. uRLCC also guarantees ultra-high reliability in distribution automation devices by maintaining them in real time and online.

C. DER monitoring and diagnosis

DERMS collect, process, and monitor large amounts of DER data in real time. The tremendous amount of DER data analysis will help to achieve DER objectives, such as voltage management of the grid, local grid load management, and monitoring of abnormal DER measurements. 5G network characteristics can play a crucial role in DER monitoring and diagnosis applications by accommodating large numbers of DER devices and increasing QoS during real-time and quasi-real-time data reporting. These types of application services require 5G mMTC and eMBB. In developing these particular use cases, we have taken a more generalized approach where most of the DERs are considered noncritical, along with their monitoring and diagnosis services, which are performed by the DERMS platform. Even though DERMS is vital to ensure that grids can manage the changing and dynamic demand of DERs, it does not directly impact grid operation.

D. DER application-based network reconfiguration

In traditional distribution systems, network reconfiguration helps to reduce power loss, isolate faults, and restore the system during an emergency. Traditional distribution system capabilities have been changed drastically by rapidly introducing new DER technologies. Recently, this network configuration in distribution systems has been enhanced by incorporating distributed generation in the solution process. However, this process relies on the variability of output power and application of renewable distributed generation. This network reconfiguration requires high bandwidth for distribution grid inspection and high-speed control to isolate the distribution system. Table 1 is a high-level overview of DER use case application requirements in terms of latency and availability, which can be facilitated by 5G network slicing.

III. USE CASE IMPLEMENTATION IN CEEP TEST BED

A. Test case description

In this work, the test cases are designed to investigate the impacts of DER service operation during a disruptive situation (e.g., cyberattack, weather-based contingency) in a low-inertia microgrid. This type of microgrid was chosen because even the slightest network change can create system instability. The use case incorporates realistic modeling of heterogeneous and multiprotocol communications over the same backhaul network. This results in congestion and increases communications delays of measurement and control messages. The proposed microgrid shown in Figure 3 is designed based on an obfuscated, representative model of a partner microgrid. The microgrid has the following features that will help to analyze the DER service scenarios:

- 16 MW of total load
- 7.8 MW of critical load and 8 MW of noncritical load
- 3.65 MVA of existing diesel generators
- 3.25 MVA of backup diesel generators
- 3.2 + 2.4 MW of natural gas generators
- Three 100-kW solar arrays
- Three automated isolation/ segmenting switches.

The test case will create different network slices through network virtualization that guarantee different types of DER services with different requirements for network operators. Here, three experimental scenarios have been created within the proposed microgrid architecture (Figure 3) by considering 5G use case service classes and network slicing.

B. Experiment scenario description

The 5G communications architecture can be emulated by utilizing the CEEP test bed. CEEP is leveraged to orchestrate the desired test cases by hosting an intricate virtual testing environment. The environment features co-simulated network and power capabilities by utilizing SDN, host virtualization through kernel-based virtualization, and distributed system simulation with OpenDSS. The SDN design in CEEP's dedicated virtual testing environment enables dynamic segmentation of network communications through host network interface manipulation and virtual area network tagging, which allows the system to emulate the 5G network slicing functions. Additionally, the traffic control command is used to throttle the switch's interface throughput for emulating realistic 5G network characteristics such as bandwidth and latency. For instance, one slice is dedicated to critical loads for the mission-critical operation; one slice is dedicated to store and forward all the DER sensor data to DERMS or the microgrid center controller; and a final slice is dedicated to DER control and automation for performing volt-var control, voltage ride

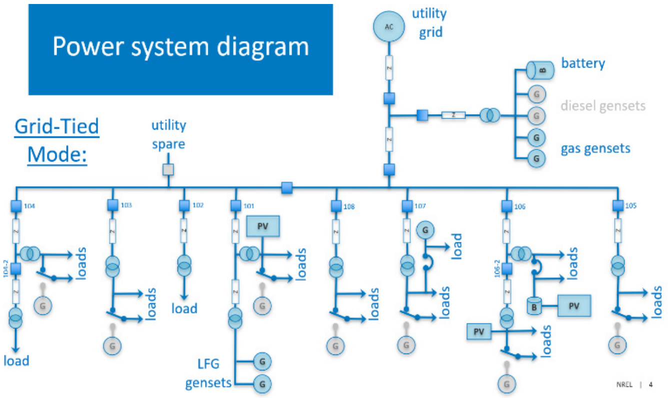


Figure 3. Microgrid architecture

Table 1. 5G Use Cases for Distributed Energy Resources

Slice	DER use cases	5G service class	DER Services	Latency	Availability	Bandwidth
1	Distributed automation for mission critical operation	uRLCC	Automated outage response	Low	High	Low
2	Distributed Control	uRLCC, mMTC	Volt-var control, voltage ride through	Low	High	Low
3	DER Monitoring and Diagnosis	mMTC, eMBB	DER Orchestration (Situational awareness)	High	Low	High
4	DER application-based network reconfiguration	uRLCC, eMBB	UFLS	Low	Low	High

through, etc. Our end goal is to demonstrate efficient slice creation during adversarial conditions in the proposed microgrid and guarantee that traffic from one slice will not interfere with another slice. The tool used to assess bandwidth changes in all scenarios is the Iperf3 network performance analyzer. Iperf3 is a server-client utility, which sits on both the monitoring and control NFV communications streams to make precise bandwidth measurements on each. Initially, the test system operates in a "storm-ready" mode and is deployed in CEEP.

Critical load and priority load in the microgrid are still grid connected and are interconnected with each other via a switch. At t = 1 second, an upstream outage prompts the microgrid to fully separate from the system through the opening of a switch to maintain operation of the system's critical loads.

To evaluate the 5G network slice isolation for DER use cases, three types of scenarios are introduced and implemented in CEEP. Those scenarios are merged with distributed automation for mission-critical operation and distributed monitoring and diagnosis use cases. The three scenarios under consideration for this experiment are described below and shown in Figure 4:

1. A baseline identifies normal network traffic latencies when both the monitoring service and control communications share the same physical and logical network.
2. An upstream outage is introduced inside of the emulated microgrid via a DoS attack on the microgrid's backup generator following the outage, resulting in network congestion and prevention of grid service restoration.
3. 5G technology is implemented. When the attack is observed, previous work in [9] is leveraged, and network slicing is implemented to allow for restoration of power as well as resumed monitoring, despite the attack.

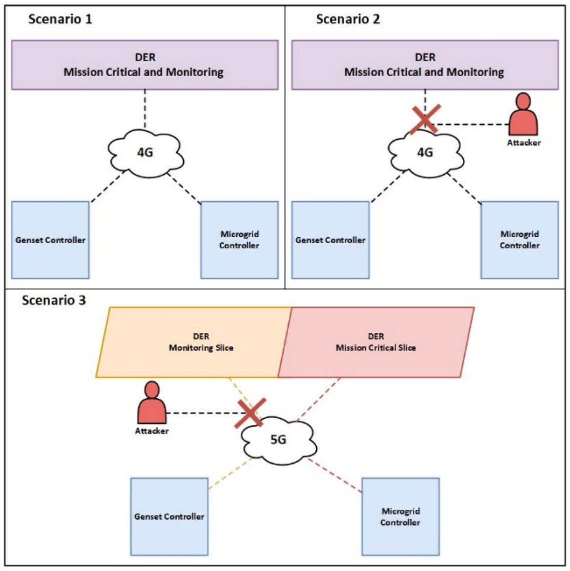


Figure 4. Scenario description

IV. Simulation Result

Each of these scenarios was deployed in CEEP with normal grid monitoring communications acting as background traffic in the network. Minimega was used to orchestrate and deploy the experiment within the CEEP environment. 4G LTE network characteristics of bandwidth and latency were emulated, based on characteristics defined in previous research [10]. The metrics used to define and measure this network performance are bandwidth (speed) and round-trip time (RTT) latency. The performance shown here, representative of 4G communications, is ~16-Mbps speed and ~90-ms latency. Similarly, 5G communications (low-band or mid-band, not mmWave) are shown to perform at 50-Mbps speed and ~30-ms RTT latency [11, 12, 13]. For this work, the attack facilitated on the backup generator was manually triggered inside of the cyber-energy environment, simulating an internal attacker. During normal operation, a Kali Linux virtual machine, established as the primary attack vector, executes an hping3, synchronizing flood command for ~100 seconds on the backup generator following the upstream outage. This DoS attack successfully floods the generator's network interface and thus restricts corrective measures. As shown in Scenario 2 below, the microgrid fails to stabilize because of the attack. Further, the same attack method is used in Scenario 3, but the 5G preventive network slicing is successful in restoring the microgrid.

A. *First scenario:*

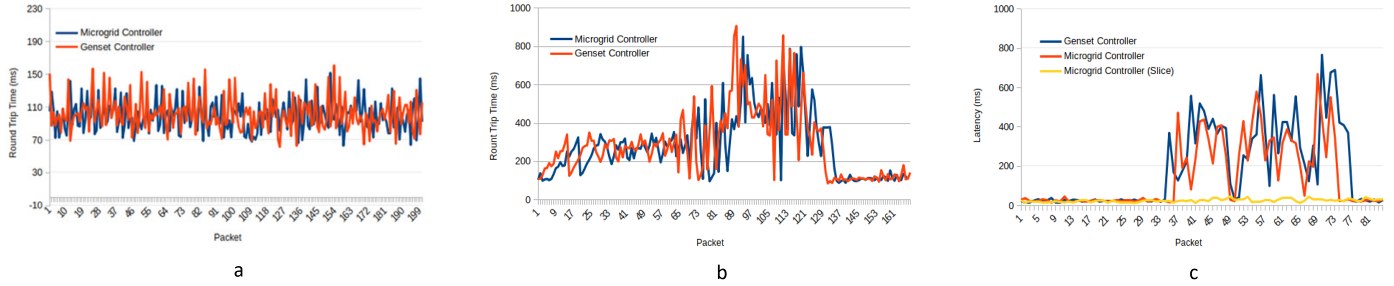
In the first scenario, the microgrid operates normally with no anomalies introduced during this data aggregation period. Figures 5a and 6a, showing latency and network bandwidth, respectively, provide expected baseline values of ~110-ms latency and ~15-Mbps bandwidth.

B. *Second scenario:*

Scenario 2 operates with the same 4G communications specifications as scenario 1; however, this time a DoS attack is introduced at packet (p)=3 in the latency plot of Figure 5b and p=66s in the respective bandwidth plot shown in Figure 6b. The attack persists for 100 seconds until network 7 levels reach equilibrium, and the system operation returns to normal. As shown, both the critical and monitoring connection bandwidths dropped to zero, which restricts the microgrid communications from reaching the generator, delaying restoration of the grid.

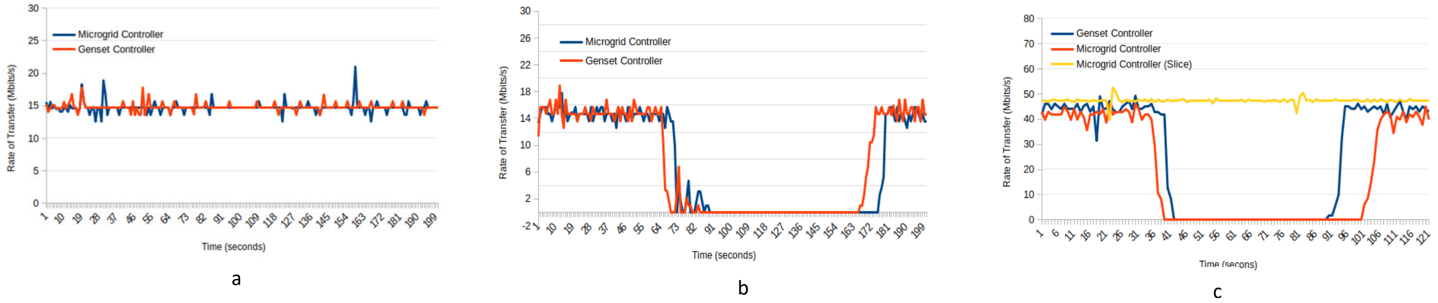
C. *Third scenario:*

Finally, in scenario 3, a few variables are introduced. As for scenarios 1 and 2, Figures 5c and 6c represent the network latency and bandwidth, respectively, of the operating network. The operating network in this scenario resembles 5G characteristics with ~30-ms latency and ~45-Mbps bandwidth. These figures also contain an additional yellow line, indicating the sliced network utilized by the microgrid controller and backup generator in the event of anomalous activity occurring, as detected and responded to, given previous work in [8]. During the attack introduced at p=35 in the latency plot (Figure 5c) and p=36s in the respective bandwidth plot (Figure 6c), the generator and microgrid controller were issued commands to shift to the critical load network slice. Due to the logical separation of the monitoring and critical load network slices, the critical load slice remained unaffected, allowing quick restoration to the microgrid, as displayed in Figures 5c and 6c. Like scenario 2, an attack in scenario 3 is made on the



a b c

Figure 5. (a) Latency of normal operation with 4G communication, (b) operation during cyberattack, and (c) 5G operation during cyberattack



a b c

Figure 6. (a) Bandwidth of normal operation with 4G communication, (b) operation during cyberattack, and (c) 5G operation during cyberattack

microgrid's backup generator following an outage, resulting in network congestion. By slicing and segmenting the microgrid's communications with the backup generator, Figures 5c and 6c demonstrate that the latency and bandwidth are preserved, enabling the critical load to restore power to the grid.

V. Conclusions and Future Work

This work provides a high-level overview of protecting, monitoring, and controlling DERs connected to a power grid using emerging 5G capabilities. In this work, 5G network slicing characteristics have been used to reduce the impact of a DoS attack on DER mission-critical services. By analyzing network latency and bandwidth, we observed that the complete slice isolation in DER mission-critical services provides a strong mitigation mechanism during this cyberattack. This solution was evaluated by implementing use case scenarios in the CEEP emulation test bed. Finally, this work concludes that 5G network isolation characteristics provide better control, protection, and monitoring capabilities over the trade-off between security, availability, and resource utilization. Future work will primarily focus on incorporating a more mathematical, parameterized approach to addressing some of the cybersecurity concerns outlined in Section IIB of this work.

VI. Acknowledgment

This work was authored by NREL, operated by Alliance for Sustainable Energy, LLC, for the U.S. Department of Energy (DOE) under Contract No. DE-AC36-08GO28308. The views expressed in the article do not necessarily represent the views of the DOE or the U.S. Government. The U.S. Government retains and the publisher, by accepting the article for publication, acknowledges that the U.S. Government retains a nonexclusive, paid-up, irrevocable, worldwide license to publish or reproduce the published form of this work, or allow others to do so, for U.S. Government purposes.

VII. References

[1] F. Kurtz, C. Bektas, N. Dorsch, C. Wietfeld, "Network Slicing for Critical Communications in Shared 5G Infrastructures – An Empirical Evaluation," *2018 4th IEEE Conference on Network Softwarization and Workshops (NetSoft)*, 2018, 393-399.

[2] J. Ordonez-Lucena, P. Ameigeiras, D. Lopez, J.J. Ramos-Munoz, J. Lorca, J. Folgueira, "Network Slicing for 5G with SDN/NFV: Concepts, Architectures, and Challenges," *IEEE Communications Magazine*, May 2017, pp. 80-87.

[3] D. Sattar, A. Matrawy, "Towards Secure Slicing: Using Slice Isolation to Mitigate DDoS Attacks on 5G Core Network Slices," *2019 IEEE Conference on Communications and Network Security (CNS)*, Washington DC, DC, USA, 2019, pp. 82-90.

[4] National Electric Sector Cybersecurity Organization Resource, Electric 749 Sector Failure Scenarios Common Vulnerabilities and Mitigations Mapping Version 1, Elect. Power Res. Inst., Palo Alto, CA, Jun. 2014.

[5] M. Lourenço, L. Marinos, "ENISA Threat Landscape For 5g Networks" ENISA, Nov 2019.

[6] J. Yao, Z. Han, M. Sohail, L. Wang, "A Robust Security Architecture for SDN-based 5G Networks," *Future Internet*, 11(4), 2019, p. 85.

[7] A. Hasandka, J. Rivera, J. Van Natta. 2020. NREL's Cyber-Energy Emulation Platform for Research and System Visualization. Golden, CO: National Renewable Energy Laboratory. 2020.

[8] P. Asmus, Lawrence M., "Military Microgrid," Navigant, 2017.

[9] V. K. Singh, E. Vaughan, J. Rivera and A. Hasandka, "HIDES: Hybrid Intrusion Detector for Energy Systems," *2020 IEEE Texas Power and Energy Conference (TPEC)*, College Station, TX, USA, 2020, pp. 1-6.

[10] J. Zhang, A. Hasandka, S. M. S. Alam, T. Elgindy, A. R. Florita and B. Hodge, "Analysis of Hybrid Smart Grid Communication Network Designs for Distributed Energy Resources Coordination," *2019 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, Washington, DC, USA, 2019, pp. 1-5.

[11] R. Trivisonno, R. Guerzoni, I. Vaishnavi, D. Soldani, "Towards Zero Latency Software Defined 5G Networks," *2015 IEEE International Conference on Communication Workshop (ICCW)*, London, 2015, pp. 2566-2571.

[12] E. Pateromichelakis, M. Fabrizio, C. Mannweiler, P. Arnold, M. Shariat, M. Einhaus, Q. Wei, Ö. Bulakci, A. De Domenico, "End-to-End Data Analytics Framework for 5G Architecture," *IEEE Access (2019)*, pp. 40295-40312.

[13] R. Solozabal, A. Sanchoyerto, E. Atxutegi, B. Blanco, J.O. Fajardo, F. Liberal, "Exploitation of Mobile Edge Computing in 5G Distributed Mission-Critical Push-to-Talk Service Deployment," *IEEE Access*, Vol. 6, 2018, pp. 37665-37675.