Preprints of the 21st IFAC World Congress (Virtual)
Berlin, Germany, July 12-17, 2020

Denial of Service Attacks on Centralized Controlled DC Microgrids: Vulnerability Assessment and Recommendations

Mahmoud Saleh*, Mohamad El Hariri**

*Department of Electrical and Computer Engineering, Florida Polytechnic University, Lakeland, FL 33805, USA (e-mail: msaleh@floridapoly.edu).
**Department of Electrical and Computer Engineering, University of Utah, Salt Lake City, UT., USA (e-mail: mohamad.elhariri@utah.edu)

Abstract: This paper aims to provide more insight on the impact of Denial of Service (DOS) attacks on centralized controlled DC Microgrids. A mathematical model, which the author previously developed to represent microgrid stability during delays, will be utilized to investigate the impact of DOS attacks. A vulnerability analysis will be conducted to highlight the attack timing and strategy that could jeopardize the microgrid operation.

Keywords: Cyber physical systems, cyber-attacks on microgrids, denial of service attack, microgrid, smart grid.

1. INTRODUCTION

In the envisioned smart grid, power could be viewed as a commodity transported over an energy cyber-physical electric grid, in which cyber processes read physical states and interact with the physical grid by actuating physical devices [1]. Within the context of energy cyber-physical systems, the smart grid is expected to have, among others, the following main features [2-4]:

- Maximized resiliency and self-healing capabilities;
- Increased efficiency and optimized utilization of available resources;
- Easy participation of the consumers in the distribution and transmission levels through demand response, peak shaving, bidding in the future energy market, etc.;
- Scalable real-time monitoring and control over its assets;
- A highly flexible platform to allows for plug and play capabilities for renewable energy resources, electrification of the transportation systems, massive deployment of distributed energy resources (DERs), and accommodation for the new emerging energy resources.

The smart grid, thus, will rely heavily on Information and Communication Technologies (ICT)s to achieve those features [5]. In fact, the use of ICT will also eventually allow the incorporation of numerous other technologies, which are forcing the acceleration of the transition from the conventional to a smarter grid, such as Advanced Metering Infrastructure (AMI), Phasor Measurement Units (PMUs), Electric Vehicles (EVs), introduction of the 5G which is the fifth generation of cellular network technology, and most importantly microgrids that are considered one of the main pillars of the future smart grid.

The CIGRÉ C6.22 Working Group on microgrid evolution roadmap and the Department of Energy (DOE) define microgrids as electricity distribution networks with distinct electric boundaries containing loads and DERs, (such as distributed generators, storage devices, or controllable loads) that can be operated in a controlled, coordinated manner either while connected to the main electric grid or in an islanded mode [6].

The main reasons behind considering the microgrids as the main building blocks for the smart grid is that they: 1) allow for flexible integration of DERs and renewable energy resources while overcoming associated intermittent issues; 2) have the potential to participate in the electric energy market (e.g. ancillary services markets); 3) enhance the grid resiliency and enable self-healing; 4) if properly integrated (e.g. microgrid clustering) could help defer investments in the existing generation and transmission infrastructures. All of these features, among others, enable the future vision of the smart grid.

However, the use of ICT has introduced new sets of cyber threats to the grid that are different in nature from regular power system operation concerns. The largest threat to the smart grid is that the same technology that is advancing the power grid is being abused by adversaries to exploit vulnerabilities in the grid and maliciously tamper with its operation [7]. Therefore, migrating to a reliable and secure smart grid requires a paradigm shift in the design and implementation of power system applications and control to account for cyber security early on in design stages.

Realizing the criticality of the aforementioned, President Barack Obama issued an executive order No. 13636 at February 2013, which states: "It is the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties." Accordingly, The National Institute of Standards and Technology (NIST) was directed to work with stakeholders to develop a voluntary framework for reducing cyber risks to critical infrastructure. One of NIST's missions is to provide an overview of the cybersecurity strategy used to develop the high-level cybersecurity requirements applicable to the future smart grids [8].

Therefore, one of the key challenges in realizing and accelerating the transition to smart grids is cybersecurity especially with the recent attacks that are being reported on the electric power grid, such as the one reported by the DOE on the NYC distribution grid. This attack left the independent system operator blind for ten hours from the utility side (i.e. distribution side).

As such, and in order to better understand the cyber vulnerabilities of the smart grid, it seems reasonable to investigate the impact of cyberattacks on a small-scale power system, such as the microgrid, especially since it's one of the key enablers of the smart grid. Therefore, in this paper we will try to asses and investigate the vulnerabilities of the microgrid during cyberattacks.

2. Investigated DC Microgrid System

The block diagram of the DC microgrid model used to investigate the impact of DoS is shown in Fig. 1. The details of this model can be found in [9-10]. The solar panels are connected via a DC/DC boost converter, which is controlled using Maximum Power Point Tracking (MPPT), to the DC bus. The battery system is interfaced to the DC bus through a bi-directional converter to charge/discharge the batteries. The whole microgrid is connected to the grid via a bidirectional inverter, which is controlled to regulate the DC bus voltage to 300 V.

During Normal operation (i.e. grid connected mode), the DC/DC boost converter is MPPT-controlled using the observe and perturb method, the bidirectional converter is current controlled to charge/discharge the batteries, and the inverter is regulating the DC bus voltage to 300 V. The microgrid is controlled by a MicroGrid Central Controller (MGCC), as shown in Fig 2.

The stability of DC microgrids is associated with the regulation of their DC bus voltage, which is analogous to inertia in AC systems. During severe cases, such as microgrid islanding, one of the other converters' controller within the microgrid must regulate the DC bus voltage to maintain its stability and safety, as shown in Fig. 3. Usually the MGCC, according to a predefined control logic, selects the converter that is connected to the biggest energy storage to maintain the DC bus voltage, since it has the flexibility to inject/receive sufficient amount of energy.

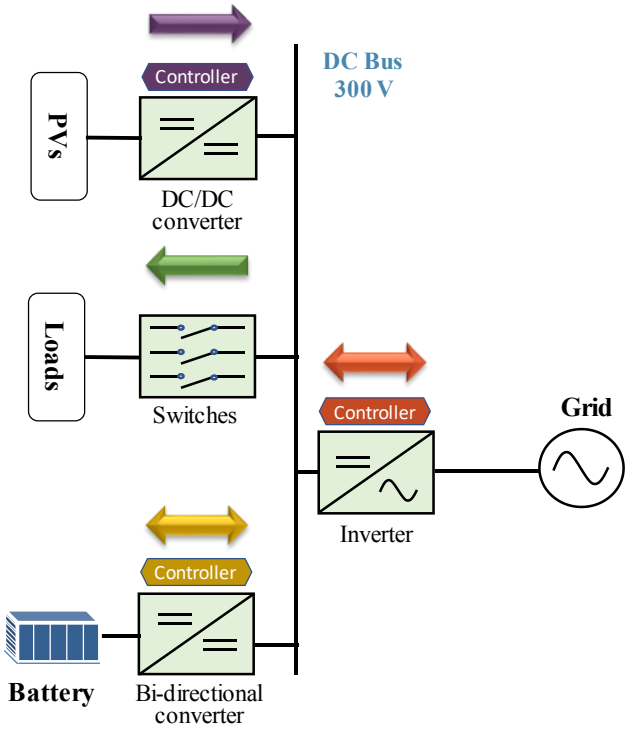

Fig 1. Block diagram of the DC microgrid model understudy.

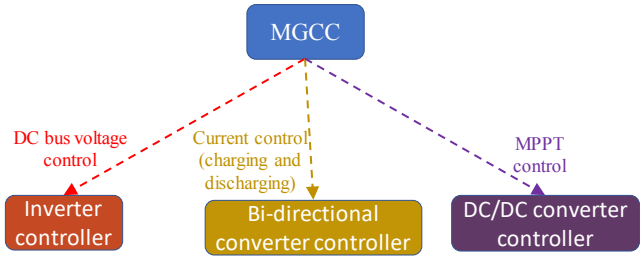

Fig 2. Microgrid control scheme during normal operation.

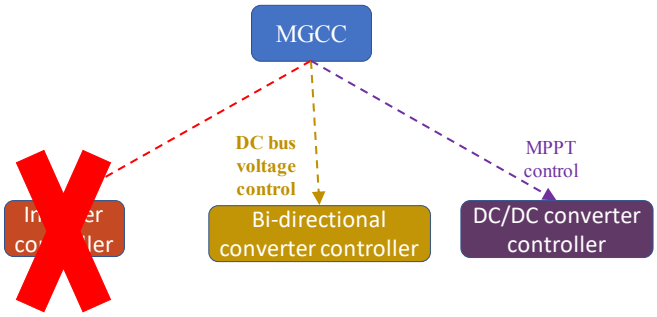

Fig 3. Microgrid control scheme during islanding mode.

3. Mathematical Model to study impact of DoS Attacks

In this paper, we will utilize the mathematical model developed in [11] to investigate the impact of DOS attack on the aforementioned microgrid system during islanding and provide a vulnerability assessment on the subject matter.

Equations (1) and (2) from [11] provide the DC bus voltage behaviour during an imposed delay between the MGCC and the converter that is supposed to regulate the DC bus voltage during islanding:

Equation (1) representing the total supplied current within the microgrid right after islanding:

$$I_G|_{t_{0+}} \approx \begin{cases} \sum_{j=1}^{m} I_{bi-j}|_{t_{0-}} + \sum_{i=1}^{n} I_{bo-i}|_{t_{0-}} + \sum_{\substack{j=1 \\ j\neq x}}^{n} \Delta I_{bi-j}|_{t_{0+}} + \sum_{i=1}^{n} \Delta I_{bo-i}|_{t_{0+}} & , Condition\ 1 \\ \sum_{j=1}^{m} I_{bi-j}|_{t_{0-}} + \sum_{i=1}^{n} I_{bo-i}|_{t_{0-}} + \sum_{\substack{j=1 \\ j\neq y}}^{n} \Delta I_{bi-j}|_{t_{0+}} + \sum_{\substack{i=1 \\ i\neq y}}^{n} \Delta I_{bo-i}|_{t_{0+}} & , Condition\ 2 \end{cases} \quad (1)$$

Where y is the DC/DC boost converter that has the highest capacitance, and x is the DC/DC bidirectional chargers that has the highest capacitance. *condition 1* is:

$$\exists j \left[\begin{array}{c} \left(\forall i \left(C_{bi-j} \geq C_{bo-i}\right)\right) \wedge \\ \left(l = \{1, 2, \dots m\} \left(l \neq j \rightarrow C_{bi-j} \geq C_{bi-l}\right)\right) \end{array} \right] \quad (1a)$$

And *condition 2* is

$$\exists i \left[\begin{array}{c} \left(\forall j \left(C_{bo-i} > C_{bi-j}\right)\right) \wedge \\ \left(l = \{1, 2, \dots n\} (l \neq i \rightarrow C_{bo-i} > C_{bo-l})\right) \end{array} \right] \quad (1b)$$

Equation 2 represents the deviation behaviours of the DC bus voltage during islanding while no converter is regulating it :

$$V_{bus}(t) \approx \begin{cases} I_G|_{t_{0+}} \times \left(\sum_{i=1}^{k} 1/R_{load-i}\right)^{-1} + \left(V_{DC}^{(0-)} - I_G|_{t_{0+}} \times \left(\sum_{i=1}^{k} 1/R_{load-i}\right)^{-1}\right) \times e^{\frac{-\alpha}{\left(\sum_{i=1}^{k} 1/R_{load-i}\right)^{-1} \times C_{bi-x}}} & , Condition\ 1 \\ I_G|_{t_{0+}} \times \left(\sum_{i=1}^{k} 1/R_{load-i}\right)^{-1} + \left(V_{DC}^{(0-)} - I_G|_{t_{0+}} \times \left(\sum_{i=1}^{k} 1/R_{load-i}\right)^{-1}\right) \times e^{\frac{-\alpha}{\left(\sum_{i=1}^{k} 1/R_{load-i}\right)^{-1} \times C_{bo-y}}} & , Condition\ 2 \end{cases} \quad (2)$$

By adopting these equations to the system shown in Fig. 1, these equations could be simplified to (3) and (4):

$$I_G|_{t_{0+}} \approx \begin{cases} I_{bi}|_{t_{0-}} + I_{bo}|_{t_{0-}} + \Delta I_{bo}|_{t_{0+}} & , C_{bi} \geq C_{bo} \\ I_{bi}|_{t_{0-}} + I_{bo}|_{t_{0-}} + \Delta I_{bi}|_{t_{0+}} & , C_{bi} < C_{bo} \end{cases} \quad (3)$$

$$V_{bus}(t) \approx \begin{cases} I_G|_{t_{0+}} * R_{load} + \left(V_{DC}{}^{(0-)} - I_G|_{t_{0+}} * R_{load}\right) * e^{\frac{-\alpha}{R_{load} * C_{bi}}} & , C_{bi} \geq C_{bo} \\ I_G|_{t_{0+}} * R_{load} + \left(V_{DC}{}^{(0-)} - I_G|_{t_{0+}} * R_{load}\right) * e^{\frac{-\alpha}{R_{load} * C_{bo}}} & , C_{bi} < C_{bo} \end{cases} \quad (4)$$

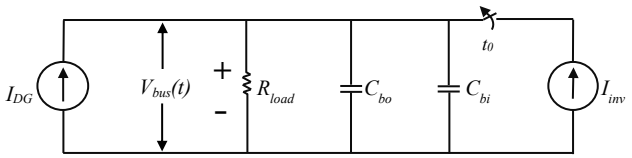

Fig. 4. The DC MG equivalent circuit during normal operation.

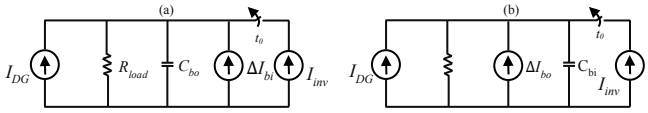

Fig. 5. DC MG equivalent circuit during islanding in case of: (a) $C_{bi} < C_{bo}$ and (b) $C_{bi} \geq C_{bo}$.

The variables' definitions are shown in Appendix A. The electric circuits representing the microgrid understudy during normal operation and islanding mode are shown in Figs. 4, and 5, respectively.

The mathematical model represented by (3) and (4) could be utilized to predict the stability of the DC microgrid during a cyberattack that imposes a delay in the communication with the MGCC and highlight the vulnerabilities as shown in Fig. 6.

In the following section we will demonstrate the utilization of (4) to examine the vulnerabilities of microgrids during a cyber-attack.

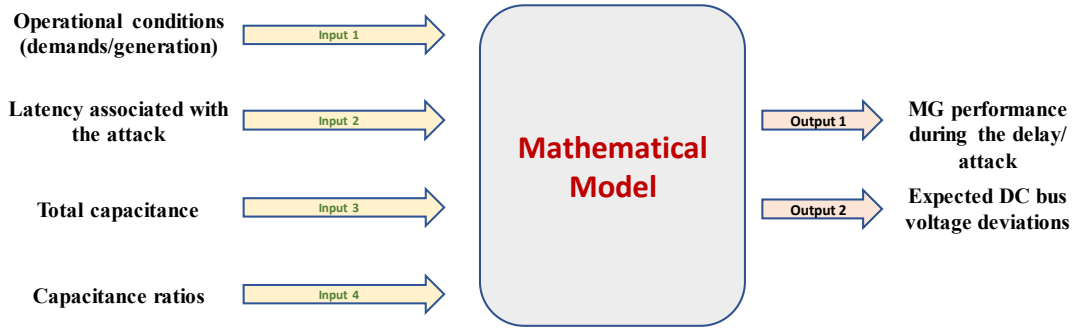

Fig. 6. The mathematical model's inputs and outputs

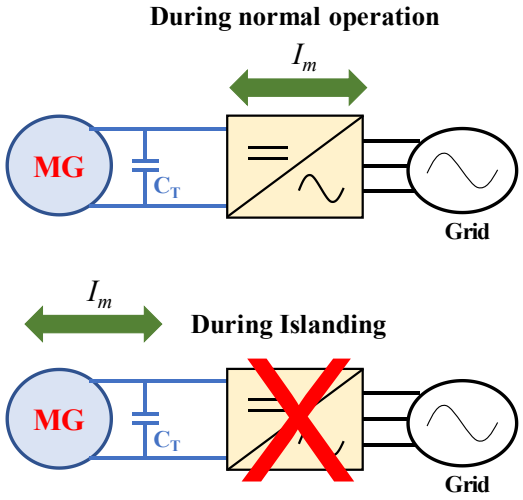

Fig. 7. Demonstration of the I_m current.

4. Results and Discussions

In this section, it is assumed that an attacker is able to successfully initiate an islanding to the microgrid system shown in Fig. 1 by sending a fake signal to open the circuit breaker at the point of common coupling. Then, the attacker performs a denial of service attack to prevent the MGCC from communicating with the bidirectional controller to regulate the DC bus voltage.

Equation (4) represents the DC bus voltage during the DoS attack. Fig. 8 shows the variation of the DC bus voltage on the z-axis, the mismatch current, I, on the x-axis (i.e. current that was drawn from or injected into the microgrid by the main grid at the moment of islanding, as shown in Fig. 7), and the delay, α, on the y-axis. I_m varies from -20 to 20 A and α varies from 0 to 100 msec.

By examining Fig. 8, it can be noticed that at $I_m = 0$ A (the MG was selfsustained by its DERs), no matter how long the DoS lasts, $V_{bus}(t)$ remains at 300 V, which verifies (4) theoretically. Also, it can be seen that at $\alpha = 0$, $V_{bus}(t)$ stays at 300 V, which again verifies (4). By further inspecting Fig. 8 at $\alpha = 100$ msec and $I_m = 20$ A (i.e. the MG was injecting 20 A to the grid at the moment of islanding), $V_{bus}(t)$ could reach up to 500 V. Also, at $\alpha = 100$ msec and $I_m = -20$ A (i.e. the MG was receiving 20 A from the grid), $V_{bus}(t)$ could go down to 100 V. In both cases, the over voltage and under voltage will trip the protection system and lead to a total blackout. Therefore, if an attacker is monitoring the MG, the best time to initiate this attack is when the inverter is operating at its rated capacity (i.e. I_m is maximum). Consequently, the inverter measurements should be highly secured as it is the most vulnerable point in the MG during a cyberattack that could lead a total shutdown.

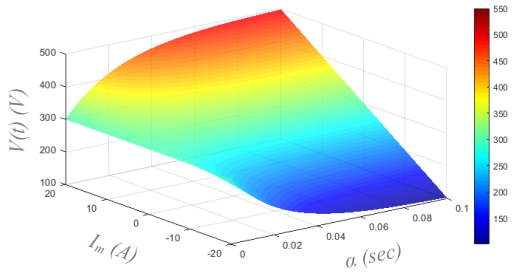

Fig. 8. Represents the variation of the DC bus voltage with I_m and α at $C_T = 2*1200$ μF and C_{bi}:C_{bo} = 1:1.

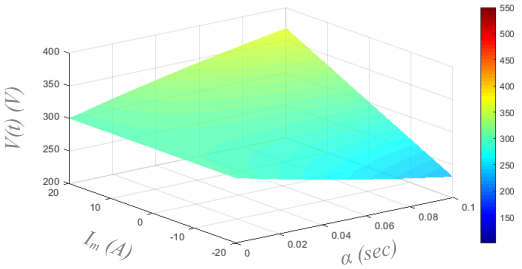

Fig. 9. Represents the variation of the DC bus voltage with I_m and α at $C_T = 20*1200$ μF and C_{bi}:C_{bo} = 1:1

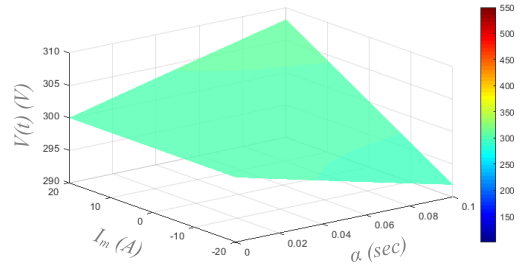

Fig. 10. Represents the variation of the DC bus voltage with I_m and α at $C_T = 200*1200$ μF and C_{bi}:C_{bo} = 1:1

Figs. 9 and 10 show similar representations to (4) but with higher values of C_T. It can be seen that as the total capacitance increases, $V_{bus}(t)$ does not reach extreme values as in Fig. 8. The main reason is that as the capacitance connected to the DC bus increases, it has the potential to hold the charges longer. Therefore, if an attacker were to perform such an attack on a group of connected MGs (i.e. microgrid clustering), the attacker would initiate the attack on the MG that has the least capacitance. So, that the voltage deviates quickly, which will draw higher currents from the neighbour MGs and might cause all the MGs to collapse. Consequently, any information regarding the total capacitance connected to the DC bus should not be publicly available. All the previous results and the next ones were generated at C_{bi}:C_{bo} = 1:1 since the mathematical model is most accurate at this ratio as explained in [11].

One of the key aspects that need to be further explored is the variation of the rate change of the DC bus voltage during a cyberattack. This could be achieved by differentiating (4) with respect to α, which will yield (5):

$$\frac{dV_{bus}(t)}{d\alpha} \approx \begin{cases} \frac{\alpha}{C_{bi}} * \left(I_G|_{t_{0+}} - \frac{{V_{DC}}^{(0-)}}{R_{load}} \right) * \\ e^{\frac{-\alpha}{R_{load} * C_{bi}}} & , C_{bi} \geq C_{bo} \\ \frac{\alpha}{C_{bo}} * \left(I_G|_{t_{0+}} - \frac{{V_{DC}}^{(0-)}}{R_{load}} \right) * \\ e^{\frac{-\alpha}{R_{load} * C_{bo}}} & , C_{bi} < C_{bo} \end{cases} \quad (5)$$

Fig. 11 is similar to Fig. 8, except that it shows the variation of the rate of change of the DC bus voltage on the z-axis. It can be noticed that at I_m = 0 A $(dV_{bus}(t))/d\alpha$ = 0, which goes back to what was explained earlier (i.e. the DERs within the MG were supplying the loads without the need of the grid).

At the moment of islanding I_m gets suddenly imposed on the capacitors connected to the DC bus. Looking at it from a circuit perspective $dv/dt = i_c/c$. Inspecting Fig. 10, it can be seen that dv/dα is maximum when I_m is at either of its extremums (i.e. -20 or 20). The sudden change of current within the MG from 0 to 20 or -20 A causes a sudden change in the voltage. Then, dv/dα tends to be zero as the DoS attack continues, since the capacitor tends to reach the final value exponentially. In other words, if the MG was sending extra 5 A to the grid, then a sudden islanding occurs and no controller is regulating the DC bus voltage, these 5 Amps will tend to increase the DC bus voltage. Assuming a resistive load of a value 10 ohms was connected to the DC bus, then a sharp change in the voltage is expected by 5A * 10 ohms = 50 V. However, since there are capacitors connected to the DC bus, this increase will be exponentially with a sharp change in the beginning and tends to stabilize toward the final value. Accordingly, if you were an attacker, the best time to initiate an attack is during the extreme operational conditions of the microgrid, as mentioned earlier. This can be noticed in Fig. 8, where the voltage increased from 300 V to ~420 V (i.e. 40% increase in voltage) in the first 10 msec, then increased slowly from 420 to 500 V in 90 msec. In terms of a cyber-attack that means that msec of a DoS could cause MG failure.

Inspecting Figs 12 and 13, it can be seen that dv/dα tends to decrease as C_T increases. Also, the shape tends to be like linear plane instead of exponential since bigger capacitance tends to hold the charges longer.

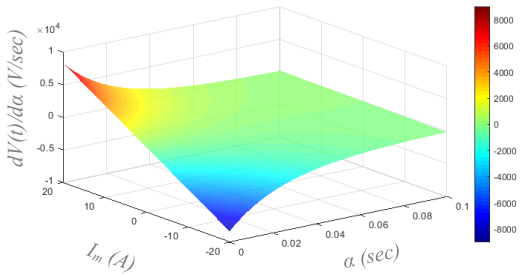

Fig. 11. Represents the variation of the rate of change of the DC bus voltage with I_m and α at C_T = 2*1200 µF and C_{bi}:C_{bo} = 1:1.

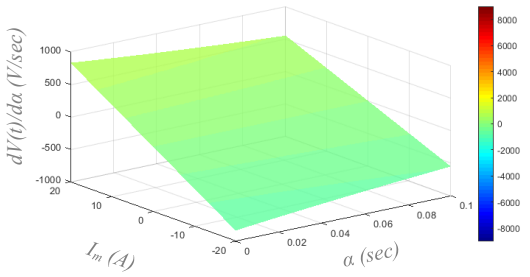

Fig. 12. Represents the variation of the rate of change of the DC bus voltage with I_m and α at C_T = 2*1200 µF and C_{bi}:C_{bo} = 1:1.

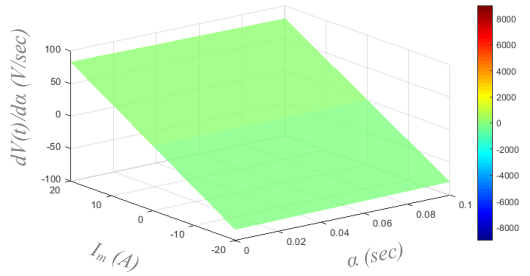

Fig. 13. Represents the variation of the rate of change of the DC bus voltage with I_m and α at C_T = 2*1200 µF and C_{bi}:C_{bo} = 1:1.

Finally by inspecting (5), it can be noticed that if the term $\left(I_G|_{t_{0+}} - \frac{{V_{DC}}^{(0-)}}{R_{load}} \right)$ has the highest value, then dv/dα becomes maximum. ${V_{DC}}^{(0-)}/R_{load}$ is basically the demand current right before islanding that depends on the MG loading. Therefore, another attack strategy could be performed if the attacker has full observability over the MG measurements. The attacker could wait till the MG is receiving maximum current (i.e. I_m is maximum) and tamper the current reference of the bidirectional converter to force it to charge the batteries with maximum current, this will lead to a catastrophic dv/dα. Fig. 14 reflects this impact. It shows the variation of dv/dα with I_{bi} and α when the MG was sending 20 A (i.e. I_m = -20 A) and C_T = 2*1200 µF. It can be seen that when the batteries were charging with 20 A, that led to drastic deviation in dv/dα.

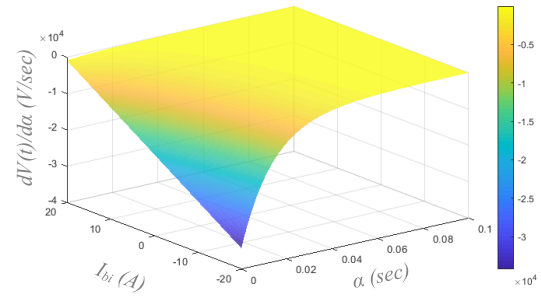

Fig. 14. Represents the variation of the rate of change of the DC bus voltage with I_{bi} and α at: I_m = -20 A, C_T = 2*1200, and C_{bi}:C_{bo} = 1:1.

5. Conclusion

This paper presented the impact of Denial of Service attack on centrally controlled DC microgrids. A mathematical model representing the behaviour of the MG during the attack was utilized to provide a vulnerability assessment. The results showed that the inverter size and the total capacitance connected to the DC bus, which are design parameters, should not be publicly available. Also, the inverter measurements should be secured, since an attacker could imitate a deadly attack based on the inverter measurements and cause an MG total shutdown. Also, at least portion of the MG measurements should be secured, such that it would be difficult for the attacker to perform some arithmetic operation and figure out the inverter measurements (i.e. privacy is a main concern). Moreover, it is highly recommended that once an islanding of a microgrid is initiated, an out-of-band secure communication network is utilized. Besides, adding strict security measures, such as authentication and encryption to ensure data integrity and privacy, within the controllers before executing the control is necessary to make sure its not a false attack.

References

[1] R. Akella; H. Tang; B. M. McMillin; "Analysis of information flow security in cyber–physical systems," *International Journal of Critical Infrastructure Protection*, Volume 3, Issues 3–4, December 2010, Pages 157-173, ISSN 1874-5482.

[2] Smart Grid Communications. Available online: https://www.nist.gov/programs-projects/smart-grid-communications-0 (accessed on 17 July 2019).

[3] Greer, C.; Wollman, D.A.; Prochaska, D.E.; Boynton, P.A.; Mazer, J.A.; Nguyen, C.T.; FitzPatrick, G.J.; Nelson, T.L.; Koepke, G.H.; Hefner, A.R., Jr.; et al. Nist Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0; US National Institute of Standards and Technology: Gaithersburg, MD, USA, 2014.

[4] F.F. Wu ; K. Moslehi ; A. Bose, "Power System Control Centers: Past, Present, and Future," *Proceedings of the IEEE*, Volume: 93 , Issue: 11 , Nov. 2005.

[5] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey,"*Computer Netwo*rk, vol. 54, no. 15, pp. 2787–2805, 2010.

[6] Microgrid Definitions. Accessed on: Nov. 17, 2019. [Online]. Available: https://building-microgrid.lbl.gov/microgrid-definitions

[7] Kelly Zieglar, "Grid, PhD: The Smart Grid,Cyber Security, and the Future of Keeping the Lights On", 19th USENIX Security Symposium, Washington, DC, August 11-13, 2010.

[8] The Evolving Smart Grid: What's New in the NIST Framework and Roadmap. Accessed on: Nov. 17, 2019. [Online]. Available: https://www.nist.gov/sites/default/files/documents/smartgrid/SG-Webinar-20140502-VER-2.pdf

[9] M. Saleh, Y. Esa, A. Moahmed "Design and Implementation of CCNY DC Microgrid Testbed," *IAS, IEEE*, October 2016, Portland, OR.

[10] M. Saleh, Y. Esa and A. Mohamed, "Hardware Based Testing of Communication Based Control for DC Microgrid," *International Conference on Renewable Energy Research and Applications (ICRERA)*, San Diego, 2017.

[11] M. Saleh, Y. Esa, and A. Moahmed, "Impact of Communication Latency on the Bus Voltage of Centrally Controlled DC Microgrid during Islanding," *IEEE Transactions on Sustainable Energy*, 2019.

Appendix

t_0 is the moment at which the islanding is initiated.

$I_{bo-i}|_{t_{0-}}$ the boost current right before the islanding.

$I_{bi-j}|_{t_{0-}}$ the bidirectional current right before the islanding.

$I_G|_{t_{0-}}$ the total generated current right before the islanding.

I_m is the inverter current at the moment of islanding = $I_{inv}|_{t_0}$

$V_{DC}{}^{(0-)}$ the DC bus voltage during normal operation (300 V).

R_{load} the connected load to the DC bus.

α the delay imposed by the DoS attack.

C_{bi} the output capacitance of the bidirectional converter.

C_{bo} the output capacitance of the boost converter.

C_T is the aggregation of all the capacitance connected to the DC bus (i.e. $C_{bi} + C_{bo}$).