20th International Conference on Renewable Energies and Power Quality (ICREPQ'22)
Vigo (Spain), 27th to 29th July 2022
Renewable Energy and Power Quality Journal (RE&PQJ)
ISSN 2172-038 X, Volume No.20, September 2022

Resilient Smart Grid Under Cyber Switching Attacks Using Distributed Energy Storage Systems

M. Badawi El Najjar[1], M. El Hassan, and C. Gebran

[1] Department of Electrical Engineering
University of Balamand
Kelhat – Al Kurah, (Lebanon)
Phone:+961 6 930250, e-mail: **maged.najjar@balamand.edu.lb**, **moustapha.elhassan@balamand.edu.lb**

Abstract. Throughout the fourth industrial revolution, power systems are evolving into smart grids including intelligent communication networks and smart meters to operate a new "two-way power and information flows". One of the main new concerns of the smart grid is its cyber-security to prevent cyber-attacks. These attacks, such as the switching attacks, can cause physical disturbances and blackouts targeting a generator in the power system destabilizing it. The energy storage systems implemented to improve the reliability of the power grid are also used to achieve the switching attacks and drive the corresponding generator out of stability. The impact of such an attack is simulated on the IEEE 39-Bus system using Power World Simulator and MATLAB. Based on the evaluation of the results and the attacker signature, different counterattack schemes are studied and performed using the available distributed energy storage systems. This is to enhance the performance of the system and to maintain its stability and reliable operation.

Key words. Smart Grid, Energy Storage System, Stability, Switching Attack, Counterattack.

1. Introduction

During the industrial revolutions, traditional power systems were invented and were based on generating electricity from centralized generator utilities and then delivering it to different consumers [9]. A grid defines a system that has "electricity generation", "electricity transmission", "electricity distribution" and "electricity control". These four operations can be implemented through various means but the main purpose of the overall system is to produce power and transfer it to the users [2]. This basic system is radial by having a common source of energy directly connected to a group of consumers and it is in need for new technologies to dramatically raise its efficiency and reduce its role in global warming [11].

Nevertheless, the currently evolving fourth industrial revolution is not based on any new energy resource. Instead, it is based on the Internet. A new virtual world controls the physical world where the factories interact with each other through the Cloud, Data Analysis and smart technologies [13]. Thus, the smart grid concept appeared to upgrade the power system and operate it intelligently. The smart grid embodies a "two-way flow" of power and data i.e. the energy network works from plant to consumer and vice versa using different sustainable sources like the renewable energy resources (RES) and the energy storages systems (ESS). The information is also exchanged between the utilities and the end users to enhance the operation [2].

Hence, the smart grid uses advanced communication and technologies to fulfill its purpose. It combines the physical components with the virtual world using the communication networks and data exchanges. However, cyber security has been the main concern of the electricity sectors for countries and the research community. Thus, the potential of physical disturbances, faults, and virtual attacks have increased, threatening system stability even further. It is crucial to understand the cyber vulnerabilities of the smart grid in order to operate it adequately. One of the most important attacks studied is the switching attacks that control certain circuit breakers connected to a load, or a storage device destabilizing a target generator by driving its rotor speed and angle out of stability [25]. The energy storage systems are introduced into the system to increase reliability, and to achieve load leveling and fast frequency regulations [1]. However, they are also used as a source of disturbance to the system [3].

In this paper, the switching attack using energy storage systems is considered, and new techniques are proposed to protect the system and enhance its performance. Section II will present the methodology followed to execute the switching attack, and section III shows the scenarios taken into consideration to implement the attack. Section IV determines the steps towards counterattacking the effects of the attack, and section V includes different approaches used to maintain the stability of the system with their detailed results. A summary is presented in the conclusion along with some future considerations.

2. Switching attack methodology

The switching attack requires gathering the information about the state variables of the system in real-time such as the rotor speed and angle of the generator while having control over the switching of a circuit breaker. The hacker has a determined aim to provide a physical disturbance in the system by conducting the attack on the spot based on the information obtained. This can be done by hacking the communication network of the breaker or its control system (SCADA or control centers) [8].

A. Variable Structure System Model and Sliding Mode

The switching mode is governed by the variable structure systems theory that models the cyber-physical system as continuous and discrete cases. The variable structure systems consist of subsystems and rules that determine the switching between them as shown in Fig. 1. A hybrid dynamical system presents the model of different cases of the power system based on a switching signal directly related to the state variables i.e. this is a state-dependent switching. For instance, each action based on the decision-making controller of a circuit breaker indicates a new state of the power system, thus a new subsystem [7].

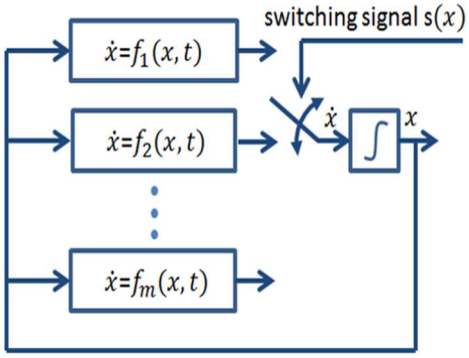

Fig. 1. Variable Structure System Model [7].

Hence, the cyber-physical system is described using state space models where each function is determined according to the state of the system under such condition. The parameters of a hybrid system in Fig. 1 are the following:

- x is the state vector dependent on time t
- f_i is the dynamical function of x and t for the subsystem i
- s(x) is the switching signal function of x
- s(x) = 0 is the switching surface or sliding surface.

The sliding mode is based on choosing a switching signal for which the trajectory of the state vector i.e. the change in x versus time is attracted to the sliding surface to stay on it and causing a stable behavior [8]. However, there is an unstable sliding mode when the trajectories of each subsystem go toward the sliding surface but in opposite directions and move away from the origin, causing instability. Therefore, to conduct a sliding mode switching attack, the attacker has to specify the state variables, find the variable structure model for the system, overlap the phase portraits plots of the subsystems (the axes are the state variables), and choose an unstable sliding surface thus the switching signal. Once the model is determined, the hacker controls the switching according to the signal, moves the system out of its stability region and guides its target to instability. Nonetheless, circuit breakers have delays, hysteresis and complexity for consecutive switching. The hysteresis margin ϵ for the switching signal takes into consideration this problem and the sliding mode system for two subsystems example becomes as discussed by Farraj *et al* [4].

B. Transient Stability of Synchronous Machines

The voltage stability, the frequency stability and the rotor angle stability are complementary but each case respectively corresponds to the particular observed parameter: the buses' voltages levels, the frequency of the electrical signals, and the rotor angle and speed for synchronism. The transient stability of the power system is based on maintaining synchronism through the rotor speed and the phase angle cohesiveness. The transient period occurs after a disturbance that changes the equilibrium of the system. This dynamical behavior is represented using the swing equation of the synchronous generators that generate the power in the system. This model is used because it relates the rotor speed and angle through two differential equations per generator forming a non-linear state space model. This model applies the equilibrium principle between the mechanical input power and the electrical output power [5].

Equation (1) is the swing equation for a generator i in any system.

$$\begin{aligned} \dot{\delta}_i &= \omega_i \\ M_i\dot{\omega}_i &= -D_i\,\omega_i + Pm_i - Pe_i \end{aligned} \tag{1}$$

Where:

$\omega_i = \frac{\omega_i{}^{actual} - \omega^{nominal}}{\omega^{nominal}}$: relative rotor speed in rad/s

$\omega^{nominal}$: nominal frequency in rad/s

δ_i: rotor angle in rad

Pm_i: mechanical input power in p.u.

Pe_i: electrical output power in p.u.

$M_i = \frac{H_i}{\pi f}$: inertia of the generator in MJ.s/rad

D_i: damping coefficient of the generator in seconds.

The state variables are the rotor angle and speed of the generator. Their trajectory as a function of time is observed to assess the stability of the system. Moreover, the system is reduced to present only the generators available. For this purpose, Kron reduction technique is used in order to reduce the interconnections and highlight the coupling between the generators and their dynamical behavior. Hence, equation (2) defines the electrical power based on the reduction process

$$Pe_i = \sum_{k=1}^{N} |E_i||E_k|\,[G_{ik}\cos(\delta_i - \delta_k) + B_{ik}\sin(\delta_i - \delta_k)\,] \tag{2}$$

Where:

N: number of generators

E_i: internal voltage in p.u. behind the direct axis transient reactance X'_{di} in p.u.

Pa_i: accelerating power in p.u.

G_{ik} and B_{ik}: Kron-reduced conductance and susceptance between the generators [21].

Sometimes, the transient stability means returning to the previous steady state operation or to a new acceptable steady state operation. Several methods have been used to determine the stability of the machines, but observing the plots of the rotor angles and the rotor velocities is the fundamental one. A Transient Stability Index (TSI) is defined to indicate stability and its margin. However, this needs more or less complicated techniques to determine it.

Furthermore, other mathematical approaches have been made such as the controlling unstable equilibrium point method, the structure preserving approach, the potential energy surface (PEBS) methods and the Lyapunuv's stability theory [12]. This theory defines the system with a stable equilibrium point for its state vector for which there is an attraction region. This region means that if the state vector is inside this region, it can converge to the stable state, but if it is outside this region, it diverges and goes to instability after the fault. The boundary of this region is called the energy function and the limit of attraction is the critical value of this function [12]. The switching attacks determine their commands based on the stability regions for each subsystem of the target generator in order to have the maximum possible impact.

C. Platform Study

The IEEE Benchmark New England 10-machine 39-bus system is considered as platform study. The system's data for the buses, the transmission lines, and the synchronous generators are presented in the analysis by Pai [12]. The system model is shown in Fig 2. Besides the available data, the damping coefficients D for all the generators are constants equal to 0.02 seconds. The governors and the excitation systems for the synchronous generators are neglected due to their slow response time compared to the fast switching strategy [3].

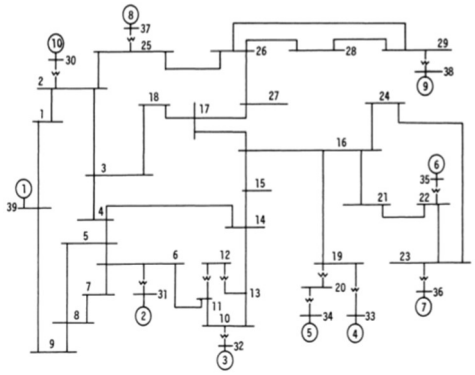

Fig.2. New England System [12].

This test system is represented as a multi-agent framework. Each agent consist of a synchronous generator, a fast acting energy storage unit, sensors to measure the rotor speed and angle, Phasor Measurement Unit (PMU), and intelligent controllers that use the measurements of all the agents for decision-making. This models a cyber-physical system where the physical system is the New England system with all its components, and the cyber system is the communication network connecting the different sensors and controllers between the agents. The physical to cyber interface is with the sensors that digitalize the measurements, and the cyber to physical interface is with the controllers that changes the physical system based on the information measured [5].

The switching attack scenario consists of attacking Generator 9 in this system which is connected to bus 38. The Storage unit is considered to have a capacity of 10% of the mechanical input power corresponding to this generator i.e. 10% from the 830 MW. The mechanical power is equal to the electrical power of a generator during steady state [3]. The 39-bus system is reduced to the 10-machine model described by the swing equations of the generators as in equation (3).

This swing equation for generator "i" includes the effect of the storage units added in the agent where:

σ_i is the control signal for the ESS which determines whether it absorbs power from the system as a load ($\sigma_i = -1$), or it injects power into the system as a source ($\sigma_i = 1$), or it is not connected to the system ($\sigma_i = 0$),

U_i is the value of the real power in p.u. absorbed or injected by the storage unit.

$$\dot{\delta}_i = \omega_i$$

$$M_i\dot{\omega}_i = \begin{cases} f_{i,0}(x,t) = -D_i\,\omega_i + Pa_i; \\ \sigma_i = 0 \\ f_{i,1}(x,t) = -D_i\,\omega_i + Pa_i + U_i; \\ \sigma_i = 1 \\ f_{i,2}(x,t) = -D_i\,\omega_i + Pa_i - U_i; \\ \sigma_i = -1 \end{cases} \quad (3)$$

$$s(x) = s(\delta_9, \omega_9) = \omega_9 \quad (4)$$

The target is generator 9, so the variable structure model will be used to represent the different states of the generator during the attack. The storage unit at generator 9 has three statuses. All the other storages are considered to be disconnected from the grid i.e. their swing equation is one and does not change as in $f_{i,0}(x,t)$.When the breaker of the storage unit switches between these three statuses, the function of the subsystem changes and the dynamical behavior of the system varies [3]. The switching signal for this switching attack is based on the rotor's relative speed of generator 9 as in equation (4), and the hysteresis margin is considered as ϵ=0.1 to take into account the effect of the breaker's time delay [3].

As for the stability regions, there are three subsystems and each subsystem has a corresponding swing equation i.e. a corresponding energy function and an attraction region. This attack does not change the physical structure of the system but it changes the power flow at the terminal of the generator. This means that the real power of the storage alters the energy function in the potential energy component and more specifically in the mechanical power and self-conductance components. Moreover, the conductance of each line is not neglected.

D. Switching Attack Algorithm

For this attack, there are three subsystems, and the switching among them is not a simple alternation between two cases since there are three stability regions. Consequently, the attack algorithm is more complex and has two different switching cases. Several assumptions have been made in order to conduct this attack [3]:

1. The attacker has access to the circuit breaker of the ESS and to the measurement data of the rotor speed and angle of generator 9.
2. The attacker is able to model the system as the variable structure model and find the stability regions for the three cases with the stable equilibrium points.

3. The synchronous generators do not have governor or exciter control.
4. The storage unit of the target generator, which is generator 9, in this case, is disconnected initially.
5. The generator is supposed to be unstable if its state variables' trajectory is outside the stability region for the first case where the storage is disconnected.

The attack algorithm in [3] is then as follows:

1. The attacker switches the circuit breaker of the storage unit to the absorb status.
2. The attacker tracks the system trajectory until the rotor speed ω_9 is greater than 0.1.
3. If the state vector is inside the stability region of $f_{9,1}$, the attacker switches the storage to inject or disconnect statuses.
4. The attacker again tracks the trajectory of the state variable until ω_9 is less than - 0.1.
5. If the state vector is inside the stability region of $f_{9,2}$, the attacker switches the storage to absorb or disconnect statuses
6. The attacker repeats this process until the state vector is outside the stability region of $f_{9,0}$.
7. Then, the attacker permanently disconnects the storage unit from the system.

The trajectory of the state variables is the key for this type of attack since the attacker must always track it to determine its value for the switching signal and the stability regions. Once the rotor speed and angle are outside the attraction region for the disconnected storage, they cannot return to equilibrium if the system is switched back to the respective disconnected subsystem function. The attacker makes use of this fact and destabilizes the target generator (generator 9) within seconds.

3. Switching attack scenarios

The IEEE benchmark has 10 generators but only the generator 9 is targeted for the switching attacks. Three test cases are considered in [3] to implement the attack algorithm previously developed and to determine its effectiveness in destabilizing the system. As a first approach (Case 1), the governor control is considered slow compared to the attack, and only the rotor angle and speed of generator 9 are changing due to the attack. This implies that the state variables for the other generators are fixed but the swing equation 9 varies. Then (Case 2), all the generators are affected by the switching attack on generator 9 and their rotor angle and speed are shifting.

One important aspect of the system equations is that the rank is not N but N-1 because the swing equations and the stable points depend on the difference between the rotor angles rather than on each rotor angle alone. Therefore, a reference machine needs to be chosen, its state variables set to the stable point values, and the rest of the equations are solved to find the rest of the angles. The reference may be chosen as the synchronous machine with the highest inertia to facilitate the computations [10]. For the purpose of this attack, the swing machine (generator 2) is selected as the reference machine i.e. its rotor angle will stay fixed compared to the other generators.

In all cases, the rotor angle and speed of generator 9 in Fig 3 and 4 are increasing indefinitely after a 5 second switching attack. The state variables exit the stability regions and cannot converge back to the stability point, and the synchronous generator becomes unstable. Even though the governor controls are activated, the state variables of generator 9 require 20 seconds to reach stability.

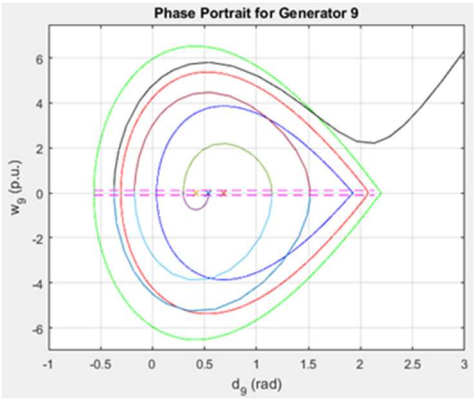

Fig.3. Phase of Generator 9 Under Switching Attack (Case 1).

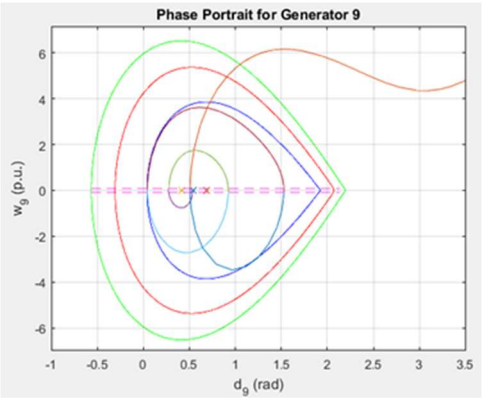

Fig.4. Phase of Generator 9 (Case 2).

The rest of the generators, except generator 2, behave like generator 9 in Case 2 and 3 i.e. their respective state variables take the same paths as the state variables of generator 9. Once the switching attack is studied, its effects are to be eliminated in order to preserve the stability of the generators and improve the resiliency of the power system.

4. Counterattack strategy

In order to execute the switching attack and counterattack, several assumptions and considerations are taken.

1. The switching attack algorithm is considered fixed and the attacker does not change it during the hacking process.
2. Primarily, the attack lasts for 5 seconds but then takes as much time as needed to reach its end.
3. Both the attacker and the control center have access to the state variables of the generators and the stability regions of generator 9.
4. The detection system positively identifies the type of switching attack.
5. The counterstrike is executed according to the time needed to identify the attack.

6. The governor control is modeled as a simple linear proportional control, but the time taken to adjust the mechanical input power is varied to demonstrate the effect of its response time during the attack.
7. The fast acting ESS power is constant because each ESS connection mode lasts a maximum of 1 to 2 seconds. Thus the power value does not change.
8. The purpose of the counterattack is to maintain the stability of generator 9 and improve its performance and resilience to this attack as much as possible.

The strategy of the counterattack is based on multiple approaches to prevent losing the operation of generator 9. These approaches identify the techniques used to conduct a defense mechanism against the attacker. It consists of:

1. Using already available resources in the system without adding any additional components. The ESS of each generator having the 10% capacity of the mechanical input power of its corresponding generator and the governor controls are from these components that are used.
2. Using breakers and components not connected to generator 9 in order to be certain that the control center has access to them.
3. Using the neighbor generators to help compensate the change that is occurring at generator 9.
4. Trying to use the algorithm of the attacker against its purpose and counterattack accordingly.
5. Expanding the stability regions for generator 9 to be able to converge back to a stable point after the algorithm is completed.

The motive behind the counterattack is to be able to lead the state variables of generator 9 back to their stable point after the hacker has finished their attack and enhance the performance of the machine to stay resilient. The algorithm only stops when the trajectory of the rotor speed and phase is outside the stability region of the disconnected mode and the ESS is disconnected. Therefore, after the last switch, normally generator 9 cannot return to stability. However, if the system changed, the stability region of generator 9 would change which will give the opportunity to bring it back to stability. It can be deduced from the three stability regions that when the power increases i.e. more real power injected into the system, the stability regions gets smaller, but when more power is absorbed, the stability region grows. Hence, in order to increase the region, more loads should be added or the mechanical input power should be decreased.

The counterattack is studied to determine its effectiveness and the strategy to use the ESSs of the system. The time to start the defense after detecting the attack is also evaluated to identify how the speed of the detection system affects the performance, the outcome of the counterattack and if it hinders or extends the time needed for the completion of the attack. In addition, the speed of the governor controls is also studied to figure out how a fast governor can help prevent the failures due to such an attack.

5. Simulation and Results

The same switching attack is targeting generator 9 of the system. The detection systems is considered to determine the attack during different switching states and the counterattack begins at the next switch. The different techniques used to eliminate the effects of the attack are: connecting all or some ESSs to absorb power only, connecting all or some ESSs to absorb and inject power alternatively according to the switching of the attack, connecting a group of ESSs to charge and another group to discharge at the same time and vice versa according to the switching of the attack, or connecting all or some ESSs to absorb and inject power alternatively according to stable switching.

1) Counterattack the Effects on Generator 9 (Case 1)

To force the trajectory of the state variables of generator 9 to return to the stable point, more load should be inserted into the grid in order to expand its stability region when its ESS is disconnected. The ESS of the other generators can be connected in charging mode in order to absorb power from the grid. All the ESSs of the other generators can be used but it is not efficient to use all the resources when a more optimized approach is available. Therefore, generator 8 supplies power with generator 9, which can help it overcome the switching attack. The ESS of generator 8 is also 10% of the 540 MW mechanical input power. In addition, generator 10 supplies power alongside generator 8 with 250 MW mechanical input power. Both can be used to support generator 9 and force it back to stability.

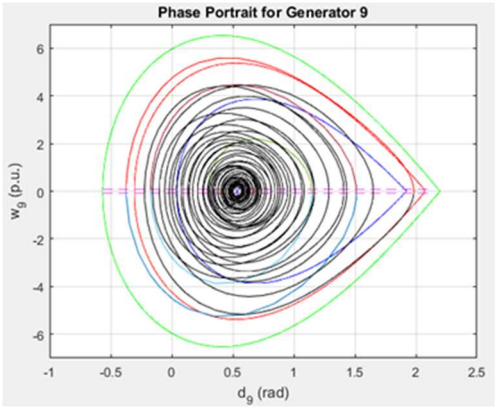

Fig.5. Last Switch Counterattack with ESS 8 and 10 (Case 1).

If the attack was only determined before the last switch where the state variables are outside the stability region, then the ESS 8 and 10 are connected to charge with last switch to disconnect ESS 9. The phase portrait in Fig 5 shows that generator 9 is able to return to its stable region with the additional switch until the ω reaches -0.1. Afterward, all the ESSs are disconnected and generator 9 resumes to its stable point as in Fig 6 and the black curve in Fig 5. The blue curve in Fig 6 corresponds to the rotor angle, which settles near its value around 40 seconds with small oscillations without surpassing the 2 rad value and the rotor speed in the red curve takes longer, about 60 seconds, to reach near 0 p.u. The oscillations decrease without any type of controller.

Another method to achieve the purpose of the counterattack is to decrease the number of the ESSs in a way that the oscillations are more damped, the performance is better, and the ESSs' real power value stays constant. The attacker switches on ESS 9, forcing it to alternate between charging

and discharging modes according to the location of the trajectory.

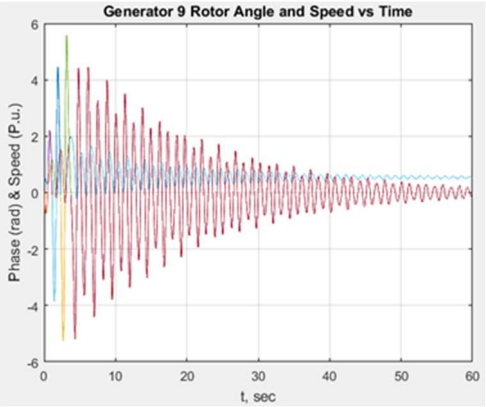

Fig.6. Rotor Speed and Angle of Generator 9 with Last Switch Counterattack (Case 1).

2) Counterattack the Effects on all Generators (Case 2)

If the same technique is used, then some ESSs are connected in charging mode when ESS 9 is charging and vice versa. This means that the counterattack uses the same pattern of the attack. As for choosing the right ESSs to use, ESS 8 and 10 are already proven to help generator 9 but in this case, their power is not enough to maintain all the other generators so generator 1 is added to them. Generators 4, 5, 6, and 7 injects power into the system that meets the power flow of generator 8 and 9 at bus 17. These generators are closer to generator 9 than the others, and the ESSs used are 6 and 7 because the performance will be enhanced in the same way if 4 and 5 are used. By introducing the ESSs 1, 6, 7, 8, and 10, the response of generator 9 is improved as compared to the previous attempt.

Fig 7 displays the plots for the rotor angle and speed of generator 9. The rotor speed (angle) maximums are 4.45 and -5.31 p.u. (2.07 and -0.39 rad). The oscillations start to settle at around 60 seconds, which is an improvement. All the generators reach their stable points faster using this approach, and only five ESSs are used while charging and discharging them so that the real power values remain fixed. However, the last step is to connect all the storages as loads to force the system back to stability for only 0.5 seconds and disconnect them. This will help the generators to surely regain stability. In addition, if the detection system is quicker, the same counterattack is applied but the response of all generators will be more improved.

The rotor speed and angle oscillations in Fig 8 are more damped and the generator reaches stability faster after 50 seconds.

Hence, the switching of the ESSs next to other generators in the system helps to stabilize an unstable generator under switching attack. This is done according to the strategy applied to switch the storages to charging and discharging modes in order to improve the performance.

There are different techniques to maintain the stability of generator 9 and the other generators. It is better to use a lesser number of ESSs when possible, and to obtain the lowest oscillations with the shortest settling time. These are the main criteria to choose the best counterattack to apply according to the power system. For each case, there is the most beneficial method and the ones that obstruct the effect of the attack as long as the hacker keeps on trying to execute their algorithm.

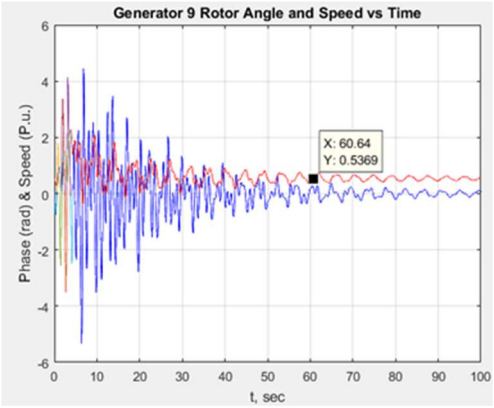

Fig.7. Rotor Speed/Angle of Generator 9 with ESS Charging/Discharging from 4th Switch (Case 2).

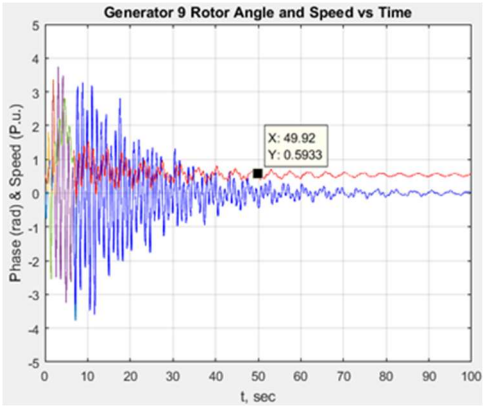

Fig. 8. Rotor Speed/Angle of Generator 9 with Stable ESSs Switching from 3rd Switch (Case 2).

6. Conclusion

The smart grid offered several benefits for the energy sector such as protecting the environment, decreasing the energy losses in the entire system, and enhancing the efficiency and reliability of the power delivery. It also improves the operation of the entire grid by implementing new technologies, new devices, advanced computational programs, robust control systems, and secure communication networks. However, the cyber-security of the intelligent interconnected system remains the most vulnerable aspect, and it is threatened by attacks like the switching attack. The proposed defense algorithms against this type of attack use the distributed ESSs available for each synchronous generator to help it regain its stability.

These counterattacks force the trajectory of the target generator as well as the other generators back to the stable point after it leaves the stability region. In addition, these techniques enhance the performance of the generators by decreasing the amplitude and the frequency of the transient oscillations, decreasing the time needed to settle at the stability point, thus hindering the effects of the attack by containing the trajectory of the generator inside the stability region no matter how long the attack lasts. These approaches can be developed into a full algorithm, which can be directly implemented once the occurrence of the attack is determined. The counterattacks can be used without any

additional control devices, and they can be developed to continue opposing the effect of the attack if the hacker does not leave and keeps on trying to destabilize a generator every time its trajectory re-enters the stability region. This can also be studied if the ESSs used for the attack are those for the RESs connected to the grid rather than for the synchronous generators as well as studying the switching of the RESs feeders.

Acknowledgment

The authors would like to thank the University of Balamand for supporting this work.

References

[1] Calderaro, V., Galdi, V., Graber, G., Graditi, G., & Lamberti, F. (2014). Impact assessment of energy storage and electric vehicles on smart grids. Electric Power Quality and Supply Reliability Conference (PQ), (pp. 15-18). Retrieved from https://ieeexplore.ieee.org/

[2] Fang, X., Misra, S., Xue, G., & Yang, D. (2012). Smart grid – The New and improved power grid: A survey. IEEE Communications Surveys & Tutorials, 14(4), 944-980.

[3] Farraj, A. K., & Kundur, D. (2015, February). On using energy storage systems in switching attacks that destabilize smart grid systems. In 2015 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT) (pp. 1-5). IEEE.

[4] Farraj, A. K., Hammad, E. M., Kundur, D., & Butler-Purry, K. L. (2014). Practical limitations of sliding-mode switching attacks on smart grid systems. In 2014 IEEE PES General Meeting| Conference & Exposition (pp. 1-5). IEEE.

[5] Farraj, A., Hammad, E., & Kundur, D. (2015). On using distributed energy resources to reshape the dynamics of power systems during transients. In 2015 IEEE International Conference on Smart Grid Communications (SmartGridComm) (pp. 756-761). IEEE.

[6] Line, M. B., Tøndel, I. A., & Jaatun, M. G. (2011). Cyber security challenges in Smart Grids. In 2011 2nd IEEE PES International Conference and Exhibition on Innovative Smart Grid Technologies (pp. 1-8). IEEE.

[7] Liu, S., Kundur, D., Zourntos, T., & Butler-Purry, K. (2012). Coordinated variable structure switching in smart power systems: Attacks and mitigation. In Proceedings of the 1st international conference on High Confidence Networked Systems (pp. 21-30). ACM.

[8] Liu, S., Mashayekh, S., Kundur, D., Zourntos, T., & Butler-Purry, K. L. (2012). A smart grid vulnerability analysis framework for coordinated variable structure switching attacks. In 2012 IEEE Power and Energy Society General Meeting (pp. 1-6). IEEE.

[9] Lo, C. H., & Ansari, N. (2012). The progressive smart grid system from both power and communications aspects. IEEE Communications Surveys & Tutorials, 14(3), 799-821.

[10] Lugtu, R. (1971). Transient stability analysis of power systems using Liapunov's second method. (Restrospective thesis and dissertations, Iowa State University). Retrieved from https://lib.dr.iastate.edu/

[11] Ma, R., Chen, H. H., Huang, Y. R., & Meng, W. (2013). Smart grid communication: Its challenges and opportunities. IEEE Transactions on Smart Grid, 4(1), 36-46.

[12] Pai, M. A. (1989). Energy function analysis for power system stability. Kluwer Academic Publishers. doi:10.1007/978-1-4613-1635-0.

[13] The 4 Industrial Revolutions. (2017, February 23). Retrieved from Sentryo website: https://www.sentryo.net/