On Using TCBR Against Cyber Switching Attacks on Smart Grids

Hazem Karbouj
Electrical Engineering Department
National Institute of Technology Rourkela
Rourkela, Orissa, India 769008
Email: hazemkarbouj@gmail.com

Somnath Maity
Electrical Engineering Department
National Institute of Technology Rourkela
Rourkela, Orissa, India 769008
Email: : somnatheeiitkgp@gmail.com

***Abstract*—As the conventional power systems turn towards smart grids (SGs) on a fast pace, this transition may create new and significant challenges to the existing electrical network security. Along with many important features of the SGs cyber security has emerged to be a critical issue due to the interconnection of several loads, generators, and renewable resources through the communication network. Cyber-physical attacks (CPAs) are classified as the major threatening of SGs security because it may lead to severe consequences such as large blackout and destruction of infrastructures. Cyber switching attacks (CSAs) (as a part CPAs) start to attract the attention due to its severity and speed in destabilizing the SGs, we present in this paper Thyristor-Controlled Braking Resistor (TCBR) as a solution to mitigate this type of attack. TCBR can enable us to stabilize the target generator in a relatively short time.**

***Index Terms*—Cyber switching attack, SG security and SG stability, thyristor-controlled braking resistor.**

I. Introduction

It is well known that power systems are under the class of hybrid dynamical systems where the system dynamic is continuous for each switch state and shifting from one state to another governed by discontinuous switching event. Switching between two or more stable states does not necessarily lead to a stable system but it might also lead to an unstable one depending on the switching rule [1]. Consequently, it is possible to destabilize the whole system, or a part of it. In literature such kind of destabilizing phenomena is called as a switching attack; in other words, also called as cyber switching attack (CSA) since the cyber layer of SG is the main enabler of implementing it.

CSAs are based on the ability of hacker to get the access (cyber access) to target generator/s's terminals measurements so that the angular speed and rotor angle (i.e. state variables) can be estimated, and to get the authority (cyber or physical authority) to control corrupted switch/s, based on the target generator/s state, driving the target generator/s to instability and isolating it from the network, which might lead in extreme cases (when the attack targets critical generators) to blackout.

The researches have been done so far on CSA can be categorized into two groups. The first group explains and analyzes single and multiple CSAs. While the second group presents a detection and mitigation methods. Researches [4]–[10] present and analyze the methodology of construction single CSA. In [4]–[6] authors reported the principles of constructing single-switch CSA based on sliding mode control (SMC), where the target generator has been simulated as a single machine infinite bus (SMIB) system, and the corrupted breaker was considered as a load breaker. The possibility of constructing CSAs when the opponent (hacker) has a limited knowledge of target generator state (or model parameter error) is studied [5] and [7]. In [8] same authors also investigated the method of constructing single switch CSA on a multi-machine system by considering that the corrupted switch was a line switch. A developed version of CSA has been represented in [9] where the fast-acting energy storage system (ESS) has been used in the attack. Abdullah A et.al. [10] presented an investigation of practical limitation of constructing CSA. The CSAs have been developed in [11], [12] where destabilizing a generator was not the main aim but instead destabilizing the whole network.

On the other hand, some group of researchers presented a power layer based solutions. [16] presents a switching based solution of CSAs, where the SG operator implements a switching signal on a specific power switch in order to oppose the attack signal and drag the system trajectory to stable operating point through specifying a stable sliding surface (SS). The distributed control strategy of fast-acting ESS has been used in [13] to stabilize the SG under CSAs. A game theory based analysis of CSA has been presented in [14], this analysis provided a platform for developing a strategy based on game theory to control the fast-acting ESS in order to mitigate CSAs. It is possible to apply these two solutions technically, but the high cost of ESS is an important obstacle of applying such kind of solutions. [15] presented a CSA detection method based on hidden mode stochastic switched linear systems with unknown inputs, the method success in detecting the switching attack signal during the attack process.

In this paper we introduce using TCBR as a cheap and efficient solution to mitigate CSA on SMIB system.

The rest parts of this paper are organized as follow. We address in Section II the problem by explaining and analyzing the studied system, CSA is constructed and applied in this part. Using TCBR to mitigate CSAs is presented in section III. finally, in section IV the paper is concluded.

II. Cyber Switching Attack: principle and analysis

A. Hybrid Systems Stability

As the SG under CSA is considered as a hybrid system we introduce a brief discussion on its stability criteria. The system which contains both continuous and discrete states that influence the dynamic behavior is called Hybrid system or switched system [2], such type of system has its own stability rules, where the stability of all system continuous states is necessary condition but not sufficient to ensure that this system is stable.Let us take the hybrid system shown in Fig. 1, the system has N continuous states, where $A_1, ..., A_k \in \mathbb{R}^{n\times n}$ are the states matrices, $B_1, ..., B_k \in \mathbb{R}^{n\times m}$ are the input matrices, $C \in \mathbb{R}^{p\times n}$ is the output matrix, $D \in \mathbb{R}^{p\times m}$ is the feedforward matrix, and $u \in \mathbb{R}^m$, $x \in \mathbb{R}^n$ and $y \in \mathbb{R}^p$ are the input, state and output vectors respectively, n,m and p denote the number of state variables, inputs and output respectively. The switching decision is taken by switching rule block to switch to state Ψ_i, where i is an integer $i \in [1{-}N]$, based on the state vector and it might be based on output vector. Here we have many methods of controlling the hybrid system such as finite time switched control, time average control and SMC. In this paper, we are more interested in studying SMC because it is the control scheme which is used to control corrupted switch in CSA. SMC is based on designing a SS $S(x)$ force the controlled system trajectory to follow its direction reaching to the desired operating point. To make the mission of designing $S(x)$ easier, we choose $S(x)$ as a linear combination of weighted state variables which is given by $S(x) = \sum_{i=1}^{N} a_i x_i$ where a_i represent sliding coefficients. SMC problem is summed up by designing these coefficients in such a way that three conditions — hitting, existence and stability are simultaneously fulfilled [3]. Hitting condition ensures that the control action will drive the system trajectory toward $S(x)$ or it's vicinity ε regardless it's initial condition, where ε represents the hysteresis band. the following inequality guarantees this condition

$$S\frac{dS}{dt} < 0. \tag{1}$$

Existence condition ensures that the system trajectory after hitting the SS it will keep tracking its manifold. Mathematically this condition is represented by:

$$\lim_{S\to 0^+} \frac{dS}{dt} < 0 \quad \text{and} \quad \lim_{S\to 0^-} \frac{dS}{dt} > 0. \tag{2}$$

While stability condition ensures that SS not only drives system trajectory toward the equilibrium point but also it stop this trajectory at the vicinity of this equilibrium point. After designing SS according to previous conditions, the control signal will be given to the switch or the system to move from one state to another.

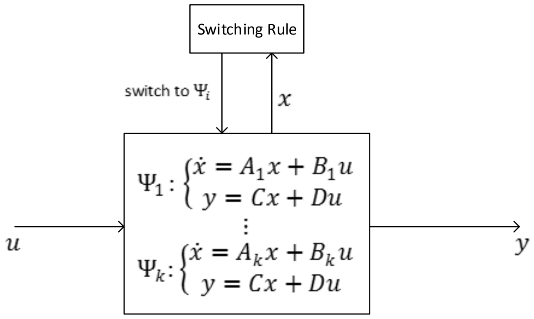

Switching Rule
switch to Ψ_i
x
u
$\Psi_1: \begin{cases} \dot{x} = A_1 x + B_1 u \\ y = Cx + Du \end{cases}$
$\vdots$
$\Psi_k: \begin{cases} \dot{x} = A_k x + B_k u \\ y = Cx + Du \end{cases}$
y

Fig. 1: Hybrid system architecture

B. Cyber Switching Attack on SMIB

The system we are going to study is shown in Fig. 2. G_t represents target generator, it is connected to infinite bus by transmission line which is represented by reactance, a local load is connected to G_t through circuit breaker. The obstacles which face the hacker to implement CSAs can be divided to cyber and physical obstacles, in cyber obstacles the opponent has to access cyber layer to get both target generator G_t measurements and authority to control the corrupted switch. On the other hand opponent needs to get the local network model around G_t and also able to estimate states variables affecting stability, e.g., the rotor angle and frequency, from which measurements can be collected. We assume that the hacker is able to cross all these difficulties to concentrate on analyzing CSA. Normally, successful CSA depends on choosing the right control rule to drive the system dynamic to instability. However, SMC is used to control the corrupted switch in switching attacks, but before talking about the attack construction we have to study the system dynamic. The generator rotor angle δ and its rotor speed ω represent the main state variables that describe the system stability, they linked to the mechanical power input P_m, electrical active power output P_e and generator parameters by swing equation (3).

$$\frac{d\delta}{dt} = \Delta\omega \quad \text{and} \quad M\frac{d^2\delta}{dt^2} = P_m - P_e - P_d \tag{3}$$

where $\Delta\omega = \omega - \omega_s$ represents rotor speed deviation from synchronous speed, $P_d = D\frac{d\delta}{dt}$ is the damping power, D and M represent damping factor and inertia coefficient

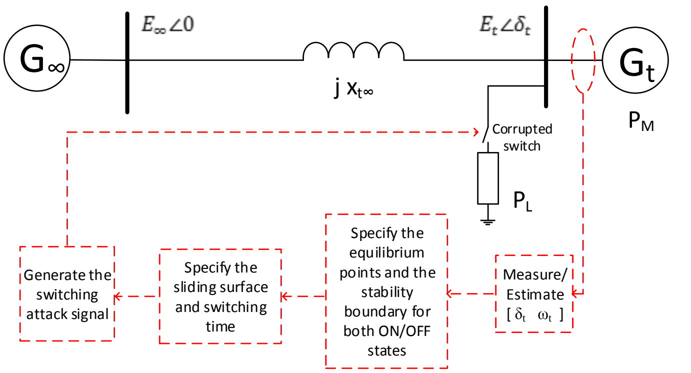

G_∞
$E_\infty \angle 0$
$j\,X_{t\infty}$
$E_t \angle \delta_t$
G_t
P_M
Corrupted switch
P_L
Generate the switching attack signal
Specify the sliding surface and switching time
Specify the equilibrium points and the stability boundary for both ON/OFF states
Measure/ Estimate $[\delta_t \;\; \omega_t]$

Fig. 2: CSA construction steps on SMIB system

respectively. The electrical power drawn from target generator G_t can be divided into two parts, electrical power consumed by local load P_L which is assumed as resistive load, and $\acute{P_e}(\delta_t)$ includes active power losses in G_t and the active power sent through transmission line, it can be mathematically written as,

$$P_e = P_L + \acute{P_e}(\delta_t) = P_L + E_t^2 g_t - \frac{E_t E_\infty}{x_{t\infty}} \sin(\delta_t) \quad (4)$$

Where E_t and E_∞ represent the magnitude of internal voltage of target generator G_t and the voltage of infinite bus G_∞, x_t compounds all reactances between E_t and E_∞, i.e. transmission line reactance and transient reactance of G_t, g_t is the equivalent shunt conductance of G_t. By substituting (4) in (3), and including the load breaker status σ in the equation, where $\sigma = 1$ when the load is connected and $\sigma = 0$ when it is not.

$$\begin{cases} \dot{\delta_t} = \Delta\omega_t \\ \Delta\dot{\omega_t} = \dfrac{1}{M_t}[P_M - \acute{P_e}(\delta_t) - \sigma P_{load} - D_t \Delta\omega_t] \end{cases} \quad (5)$$

Based on the status of corrupted switch σ, the dynamic performance of target generator G_t changes.

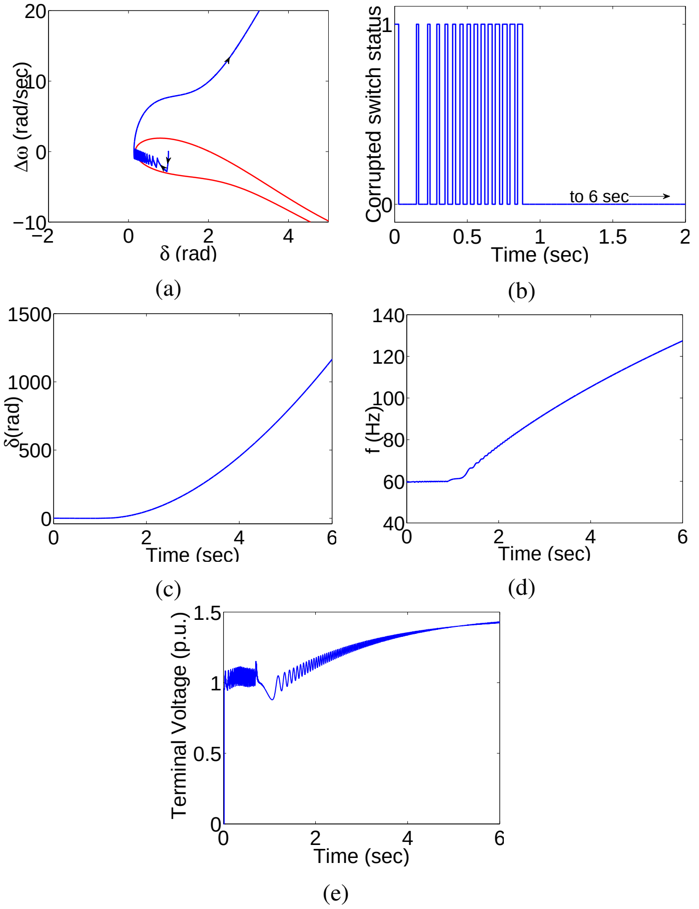
C. Attack Analysis and Discussion

The aim of hacking the cyber-layer is to get the required measurements and detect the initial conditions. The following step of implementing CSA is to study the dynamical behavior of the system, and detect all equilibrium points and stability boundaries for both breaker status ($\sigma = 1$ and $\sigma = 0$), depending on σ status (5) can be rewritten as

$$\begin{aligned} &\dot{\delta_t} = \Delta\omega_t \qquad \forall\ \sigma \in (0,1) \\ &\sigma = 0 \left\{ \Delta\dot{\omega_t} \right. = \tfrac{1}{M_t}\left[P_M - \acute{P_e}(\delta_t) - D_t \Delta\omega_t \right] \\ &\sigma = 1 \left\{ \Delta\dot{\omega_t} \right. = \tfrac{1}{M_t}\left[P_M - \acute{P_e}(\delta_t) - P_{load} - D_t \Delta\omega_t \right] \quad (6) \end{aligned}$$

The following step is to construct the switching rule by designing proper SS $S(\delta_t, \Delta\omega_t)$, this can be done by drawing the space of sliding parameters based on hitting and existence conditions (1) and (1), and then choose the SS parameters from this space. Here we have to note that the hacker aims to destabilize G_t, consequently, the stability condition is not going to be satisfied. After ensuring that the system trajectory will follow the desired SS, it is driven to cross the stability boundary and then force the system dynamic to follow the system dynamic that the crossed boundary belongs to.The simulation results of implementing CSA on target generator G_t are shown in Fig. 3, the target generator parameters are introduced in table 1, this generator is connected to an infinite bus through transmission line has been modeled by inductor with 0.014H, The generator is loaded by an ohmic load, $P_L = 32.4MW$.

Fig. 3a presents a phase plan of target generator rotor angle and rotor speed deviation. It is assumed that the system was working for a long period while the switch was opened, consequently the initial conditions $[1.098\ 0]^T$ are calculated based on this assumption. The system has two types of equilibrium points for each switch status, stable focus points at $(2n\pi + 1.1198, 0)$ and $(2n\pi$,0) for opened and closed switch respectively, and saddle nodes at $(2n\pi + 2.0218, 0)$ for opened switch and $(2n\pi + \pi$;0) for closed one. we can notice how the system trajectory in Fig. 3a starts from the initial condition, following the SS until it crosses the stability boundary of the opened switch state and then going to infinity with the passage of time which means the system becomes unstable and the protection relays will disconnect it from the network. The stability boundary is drawn in Fig. 3a is for an opened switch position. Driving the operation point of target generator in very fast manner to make big difference between the input mechanical power and the output electrical power is the main reason behind destabilizing the target generator under CSA. The SS $S = \delta_t + 0.45\Delta\omega_t$ is used to generate the switching



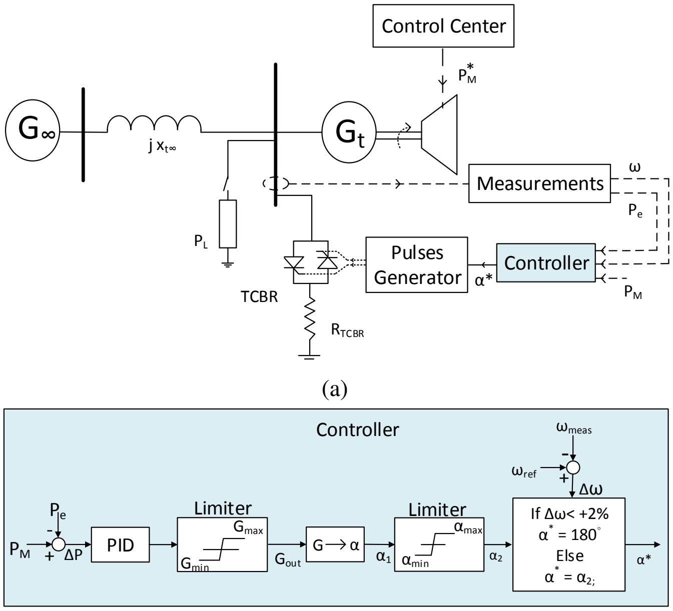
(a) (b) (c) (d) (e)

Fig. 3: CSA on G_t: (a) phase plan, (b) switching signal, (c) rotor angle of G_t, (d) frequency of G_t, and (e) terminal voltage of G_t, respectively.

TABLE I: Target generator parameters. $P_{\text{base}} = 100\text{MVA}$ [6]

Parameter	V_{rated}	P_g	Power factor	f
Value	13.8 kV	36 MW	0.8	60 Hz
x_d	$\acute{x_d}$	x_q	H	$\acute{T_{do}}$
1.55 p.u	0.22 p.u	0.76 p.u.	0.5 sec	8.95 sec

signal shown in Fig. 3b, with noticing that the switching process stops at $t = 0.9sec$ due to cross the border of stability. The reader who is interested to know more about constructing this attack is advised to read [6] because this case study has been taken from it. Fig. 3c, 3d and 3ey show the target generator rotor angle and frequency respectively.



(a)

(b)

Fig. 4: Proposed TCBR based control scheme to mitigate CSA: (a) closed loop control of TCBR, (b) the controller structure.

III. Using TCBR to Re-Stabilize the Target Generator

TCBR is a member of FACTS controllers family. This controller is used to stabilize the power system by absorbing the excess acceleration electrical energy. Due to its resistive nature, TCBR is widely used to enhance the transient stability, damp low-frequency oscillations, damp subsynchronous resonance and solves many other stability problems [18].Controlling the consumed power from TCBR can be done by controlling the firing angle of thyristors, the relation between the average active power consumed by TCBR P_{TCBR} and firing angle α is given by:

$$P_{TCBR} = V^2\ G_{out} = V^2\ \frac{G_{TCBR}}{\pi}(\pi - \alpha + \frac{1}{2}\sin(2\alpha)) \quad (7)$$

Where V is the rms voltage at the point of TCBR connection, G_{TCBR} is the conductance of braking resistor i.e. $G_{TCBR} = \frac{1}{R_{TCBR}}$, and α has a range of variation $[0, \pi]$. The power consumed by TCBR is at maximum value when $\alpha = 0$ and then decreases with increasing α till reaching zero at $\alpha = \pi$. Our proposed method of mitigating CSA is based on fixing TCBR at the target generator terminals, the objectives of TCBR is to absorb the accelerating active/additional power that produced by CSA which is the main reason of destabilizing the target generator as it is mentioned in the previous section.

Fig. 4a shows the proposed method, the generator frequency and electric output power are fed to the controller, the controller specifies the appropriate firing angle based on the required energy to be absorbed by TCBR. Firing angle α is fed to pulses generator which in turn trigger TCBR thyristors. After adding TCBR to the system the system dynamic can be represented by:

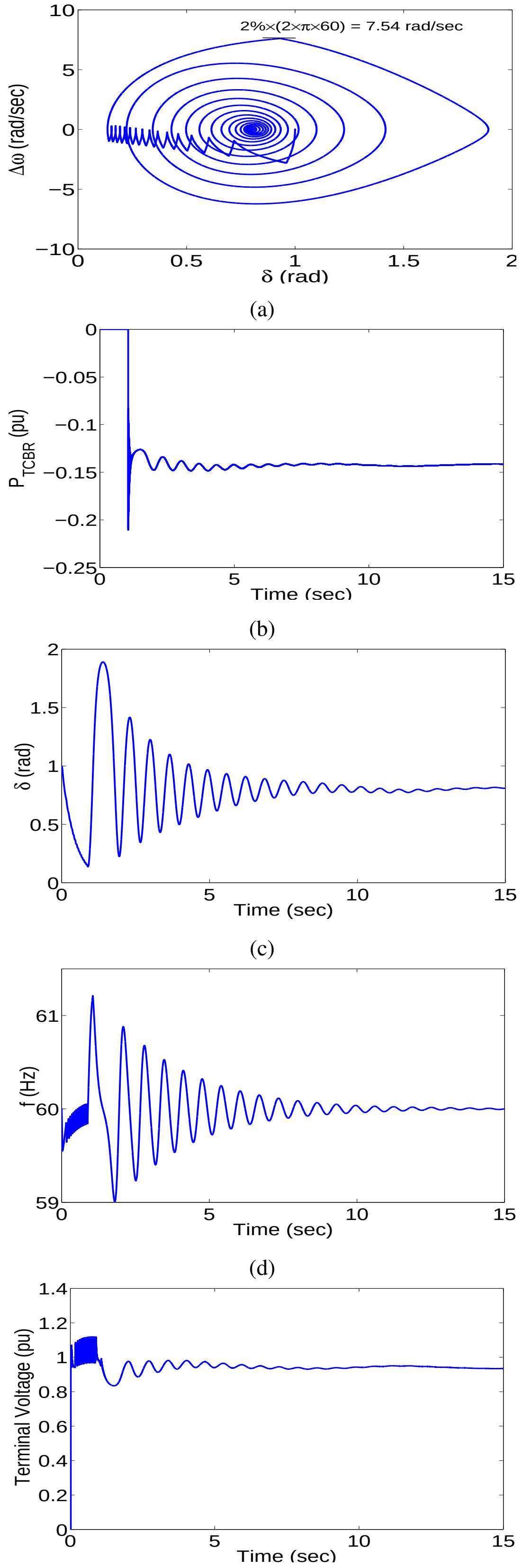
$$\frac{d\delta}{dt} = \Delta\omega \quad \text{and} \quad M\frac{d^2\delta}{dt^2} = P_m - P_e - P_d - P_{\text{TCBR}} \quad (8)$$

The controller structure is shown in fig. 4b. The difference between the input mechanical power P_m and the output electrical power is calculated and feed it to PID controller, which in turn produce the required conductance of TCBR G_{out} to absorb the acceleration active power. The required conductance is limited between zero and nominal conductance value G_{TCBR}, (7) is used to calculate the required firing angle which is limited in the range of $[0, \pi]$. TCBR controller works only when the generator accelerates and its speed deviation cross 2% of the nominal speed, otherwise TCBR does not consume any power i.e. $\alpha = \pi$.

We use Matlab/Simulink to check the efficiency of proposed method in mitigating CSA, the attack implemented in the previous section is applied to the system with simulation time 15 sec with same SS and switching time. The rated conductance of TCBR is $G_{TCBR} = 0.15pu$ with $P_{\text{base}} =$ 100MVA and $V_{\text{base}} = 13.8$kV. The conduction and switching losses in TCBR's thyristors are neglected compared with the power consumed by the braking resistor. Fig. 5a shows the phase portrait of target generator dynamic, the generator was attacked by CSA and trajectory started to diverge away from the equilibrium point. When $\Delta\omega$ crosses the specified limit i.e. $\Delta\omega = 2\% * 120\pi = 7.54\ rad/sec$, TCBR intervenes and starts to consume the excess acceleration power specified from the difference between P_m and P_e, the consumed power by TCBR is shown in Fig. 5b. We can notice from Fig (5a) that the intervention of TCBR restore the system stability and draw the system trajectory to new equilibrium point, the location of this equilibrium point can be specified by (8) and can be controlled by changing P_{TCBR}. The rotor angle ,terminal voltage, and frequency of the target generator are shown in Figs (5c)—(5e), respectively. We can notice from both rotor angle and frequency curves that the system recaptures the stability in less than 10 seconds after the CSA. The time of stability can be minimized by increasing the rated power of TCBR, but practically it is not efficient action due to the increase of TCBR cost.

IV. Conclusion and Future Work

In this paper, we have introduced TCBR as a solution to mitigate CSA on SG. The TCBR's controller has been designed so that the braking resistor absorbs the acceleration power which produced after CSA. The results have shown that the attack can be mitigated and the target machine has captured the stability again after the attack in less than 10 seconds. The suggested solution is cheaper than the solution



(a)

(b)

(c)

(d)

(e)

Fig. 5: Simulation results of SMIB system under CSA in the presence of TCBR. (a) System phase plan. (b) Active power consumed by TCBR P_{TCBR}. (c) Frequency of G_t. (d) Rotor angle of G_t. (e) Terminal voltage of G_t.

in [13], [14] which are using ESS to mitigate the same type of attacks. Future work will focus on extending the usage of TCBR to protect the SG from multi-switch CSA. We will find the optimal place and the rated power of TCBR so that SG can be protected from the most severe attack scenario.

References

[1] D. Liberzon, *”Switching in Systems and Control”*. Boston: Birkhauser,2003.

[2] S. Pettersson and B. Lennartson, *”Hybrid system stability and robustness verification using linear matrix inequalities*, Inter.J. Control, vol. 75, no. 16-17, pp. 1335-1355, 2002.

[3] S.-C. Tan, Y.-M. Lai, and C. K. Tse, *”Sliding Mode Control of Switching Power Converters”*. Boca Raton, FL, USA: CRC Press, 2011.

[4] S. Liu, X. Feng, D. Kundur, T. Zourntos, and K. Butler-Purry, *”Switched system models for coordinated cyber-physical attack construction and simulation”*, In First IEEE International Workshop on Smart Grid Modeling and Simulation, Brussels, Belgium, October 2011, pp. 49-54.

[5] S. Liu, X. Feng, D. Kundur, T. Zourntos, and K. L. Butler-Purry, *”A Class of Cyber-Physical Switching Attacks for Power System Disruption”*, in Cyber Security and Information Intelligence Research Workshop (CSIIRW), pp. 1-4, 2011.

[6] S. Liu, S. Mashayekh, D. Kundur, T. Zourntos, and K. Butler-Purry, *”A framework for modeling cyber-physical switching attacks in smart grid”*, IEEE Trans. Emerging Topics Comput., vol. 1, no. 2, pp.273-285, 2013.

[7] S. Liu, D. Kundur, T. Zourntos, and K. L. Butler-Purry, *”Coordinated Variable Structure Switching Attack in the Presence of Model Error and State Estimation”*, in IEEE International Conference on Smart Grid Communications (SmartGridComm), pp.318-323, 2012.

[8] S. Liu, S. Mashayekh, D. Kundur, T. Zourntos, and K. L. Butler-Purry, *”A Smart Grid Vulnerability Analysis Framework for Coordinated Variable Structure Switching Attacks”*, in IEEE Power and Energy Society General Meeting, pp. 1-6, 2012.

[9] A. Farraj and D. Kundur,*”On Using Energy Storage Systems in Switching Attacks That Destabilize Smart Grid Systems”*, in IEEE PES Conference on Innovative Smart Grid Technologies (ISGT), pp. 1-5, February 2015.

[10] A. Farraj, E. Hammad, D. Kundur, and K. Bulter-Purry,*”Practical Limitations of Sliding-Mode Switching Attacks on Smart Grid Systems”*, in IEEE Power and Energy Society General Meeting, pp. 1-5, July 2014.

[11] S. Liu, B. Chen, T. Zourntos, D. Kundur, and K. Butler-Purry, *”Progressive switching attacks for instigating cascading failures in smart grid”*, in IEEE PES General Meeting, pp. 1-5, 2013.

[12] S. Liu, B. Chen, T. Zourntos, D. Kundur, and K. Butler-Purry, *”A coordinated multi-switch attack for cascading failures in smart grid”*, IEEE Trans. Smart Grid, vol. 5, no. 3, pp. 1183-1195, May 2014.

[13] A. Farraj, E. Hammad, and D. Kundur, *”On Using Distributed Control Schemes to Mitigate Switching Attacks in Smart Grids”*, in IEEE 28th Canadian Conference on Electrical and Computer Engineering (CCECE), pp. 1578-1582, May 2015.

[14] A. Farraj, E. Hammad, A. Al Daoud, and D. Kundur, *” A game theoretic analysis of cyber switching attacks and mitigation in smart grid systems”*, IEEE Trans. Smart Grid, 2015.

[15] S.Z. Yong, M. Zhu, and E. Frazzoli, *”Resilient state estimation against switching attacks on stochastic cyber-physical systems”*, in IEEE International Conference on Decision and Control. 2015.

[16] S. Liu, D. Kundur, T. Zourntos, and K. Butler-Purry, *”Coordinated variable structure switching in smart power systems: Attacks and mitigation”*, in 1st International Conference on High Confidence Networked Systems, China, April 2012.

[17] J. Machowski, J. Bialek, and J. Bumby, *”Power System Dynamics: Stability and Control”*, 2nd ed. NJ, US: John Wiley & Sons, Inc. 2008.

[18] N. G. Hingorani and L. Gyugyi, Understanding FACTS: *”Concepts and Technology of Flexible AC Transmission Systems”*, New York: IEEE Press, 2000.

[19] A. H. M. A. Rahim and D. A. H. Alamgir,*”A closed-loop quasi-optimal dynamic braking resistor and shunt reactor control strategy for transient stability”*, IEEE Trans. Power Syst., vol. 3, no. 3, pp. 879-886, Aug. 1988.

[20] W. Wang and Z. Lu, *”Cyber security in the smart grid: Survey and challenges”*, Comput. Netw., vol. 57, no. 5, pp. 1344-1371, 2013.