Practical Limitations of Sliding-Mode Switching Attacks on Smart Grid Systems

Abdallah K. Farraj, Eman M. Hammad, Deepa Kundur, and Karen L. Butler-Purry*
Department of Electrical and Computer Engineering, University of Toronto, Toronto, Ontario, Canada
*Department of Electrical and Computer Engineering, Texas A&M University, College Station, Texas, USA
Email: {abdallah, ehammad, dkundur}@comm.utoronto.ca, klbutler@tamu.edu

***Abstract*—Switching attacks in smart grid systems have gained some recent attention by the research community. Based on understanding the structure of the physical system and accessing the system variables, effective sliding-mode switching attacks can be used to disrupt the normal operation of the power grid. This article investigates the practical limitations of such attacks. Sliding-mode switching attacks on a single-machine infinite-bus system are considered in this work, and the impact of some practical limitations is investigated. These limitations include sampling period, quantization level, signal-to-noise ratio, hysteresis margin and minimum time to switch of a circuit breaker, and communication latency. Results of this work detail the effectiveness of the sliding-mode switching attacks under different practical limitations.**

I. Introduction

Smart grid systems have enjoyed a recent interest from both the academic and industrial communities. By utilizing advanced control, communications, and sensor technologies, smart grid systems improve the efficiency and resilience of the power grid and help utility companies to better manage and control the energy resources and meet the electricity demand. Moreover, the ongoing integration of the renewable energy sources into the power grid accelerates the interest of adopting smart grid technologies. Further, adoption of smart grid systems has enabled various consumers to engage in new applications (for example, demand-response, load-shedding, real-time two-way communications, and time-of-usage pricing) that help consumers control their loads and reduce their energy bill.

As the smart grid applications are getting implemented in various power systems, the security and reliability issues of the cyber assets of the grid have recently surfaced. Cyber assets of the smart grid include the communications and information technology infrastructures, computing systems, and data storage. The introduction of the cyber infrastructure opens the door for potential hacking and cyber attacks on the smart grid; these attacks can yield financial loses for both the consumers and the utility company though compromising the integrity or confidentiality of the consumer data, the stability of the power grid (or part of it), or the availability of critical data for the control centers. Several devices are used in a smart grid to assist in:

- monitoring: for example, phasor measurements units (PMUs), phasor data concentrators (PDCs), and remote terminal units (RTUs);
- communications: for example, advanced metering infrastructure (AMI) and smart meters; and
- control: for example, supervisory control and data acquisition (SCADA) systems and programmable logic controllers (PLCs).

Variable-structure systems, specifically the sliding-mode switching systems [1], are nonlinear control systems that are characterized by discontinuous dynamics. In this case, the dynamics of the system are changed by a control signal that pushes the control system to slide along a switching surface. Utilizing the concept of variable-structure control, a recent work in [2]–[6] investigated the effect of sliding-mode switching attacks on the stability of power systems. The proposed attacks made use of load switching in a power grid to create a sliding-mode control system in the power grid and consequently to create system instability. The attacker must be able to intercept the system measurements, must know the local system model, and has control over specified circuit breakers in order to run a successful attack.

This article investigates the practical limitations of sliding-mode switching attacks in single-machine infinite-bus (SMIB) systems. The works of [2]–[6] assumed perfect conditions for the cyber assets of the system; for example, communication delay and the presence of noise were not taken into account when developing the switching attacks. This work considers the case when the attacker does not have perfect conditions and studies the impact of having such practical limitations on the switching attacks. The effect of the following cases on the planned switching attacks is considered in this work:

1) communication latency between the sensors and the attacker;
2) the sampling time of the sensors (i.e., the duration between the sensor consecutive readings);
3) level of signal quantization;
4) level of signal-to-noise ratio (SNR) at the sensor;
5) circuit breaker's minimum switching time; and
6) circuit breaker's hysteresis margin.

The rest of this article is organized as follows. Sliding-mode switching is introduced in Section II. Single-machine infinite-bus system model is shown in Section III. Section IV investigates the performance of the switching attacks under practical system limitations. Conclusions and final remarks are shown in Section V.

978-1-4799-6415-4/14/$31.00 ©2014 IEEE

II. Sliding-Mode Switching

Sliding-mode systems (or in general variable-structure systems) are nonlinear systems characterized by ordinary differential equations with discontinuous state functions [7]. Such systems are found useful in modeling and analyzing the behavior of smart grid systems. For example, a variable-structure system can be modelled as

$$\dot{x} = \begin{cases} f_1(x,t), & s(x) > 0 \\ f_2(x,t), & s(x) \leq 0\,, \end{cases} \tag{1}$$

where $\dot{x}$ denotes the derivative of x with respect to time, t is the time variable, and x (sometimes denoted as $x(t)$ to emphasize its time dependence) is the system state variable. Moreover, $f_1(x,t)$ is the system dynamics when $s(x) > 0$, and $f_2(x,t)$ is the system dynamics when $s(x) \leq 0$. Further, $s(x)$ is a state-dependent switching signal, and $s(x) = 0$ represents the switching surface (often termed as the sliding surface). The trajectory of the system often refers to the evolution of x in time through state space. This equation, as it models a dynamical change between two physical systems, can be useful to model and analyze a power system when a circuit breaker switches between two states.

To shed light on a potential application of sliding-mode control systems for a smart grid application, an attacker is assumed to be interested in destabilizing part of the power grid by switching a circuit breaker back-and-forth. However, in order to successfully accomplish this mission, the attacker needs to have a physical or cyber access to the circuit breaker, have an access to the system state information (i.e., x), and have a working knowledge of the system model of the smart grid depending on the state of the circuit breaker. Using these conditions, the attacker can build a variable-structure system model, design the switching signal (i.e., $s(x)$) accordingly, and switch the circuit breaker back-and-forth depending on the value of $s(x)$.

For a sliding mode to exist, both $s(x)$ and $\dot{s}(x)$ should have opposite signs in the vicinity of the sliding surface; in other words [7, Section 1.4]

$$\begin{aligned} \lim_{s(x)\to 0^-} \dot{s}(x) > 0 \\ \lim_{s(x)\to 0^+} \dot{s}(x) < 0\,, \end{aligned} \tag{2}$$

where $\dot{s}(x)$ is the derivative of $s(x)$ with respect to time. In other words, if $s(x)\,\dot{s}(x) < 0$ for $s(x) \neq 0$ is satisfied, then the sliding mode existence condition is satisfied. However, if in the vicinity of sliding surface the trajectory vectors of $f_1(x,t)$ and $f_2(x,t)$ point toward the sliding surface in opposite directions and away from the origin, the sliding mode is an unstable one. This condition will ensure that the state trajectory of the switched system will be driven to the sliding surface, continue to stay within a neighborhood of it, and move away from the origin to cause system instability [2].

To construct a sliding-mode switching attack on the smart grid, the attacker has to:

1) determine the system state variable;
2) model the power grid under attack as a switched system (i.e., find $f_1(x,t)$ and $f_2(x,t)$);
3) determine the phase portrait of each subsystem and overlap them on the same plot;
4) search for an unstable sliding surface using the phase portrait;
5) control the status of the switch depending on the value of $s(x)$; and
6) drive the system state variable outside the stability region.

The theme of the attack is to trap the system inside the sliding surface by conducting calculated back-and-forth switchings, and then guide the system state variable outside the stability boundary of one of the two switched systems; once that happens, switching can stop and the power system becomes unstable.

Theoretical sliding-mode switching systems can exhibit high-frequency oscillations in the state variable; this phenomenon is called chattering [7], which is unrealistic for real-life circuit breakers that display practical delays and hysteresis between consecutive switchings. Consequently, to overcome such issue for practical sliding-mode switching attacks, a boundary layer, known as the hysteresis margin and termed as $\epsilon > 0$, is employed. Accordingly, to implement a sliding-mode switching attack, the system is switched inside the sliding surface according to

$$\dot{x} = \begin{cases} f_1(x,t), & s(x) > -\epsilon \\ f_2(x,t), & s(x) \leq \epsilon\,. \end{cases} \tag{3}$$

This means that switching between the two subsystems occurs when $s(x)$ crosses the boundary between the lines of ϵ and $-\epsilon$.

III. SMIB System Model

The SMIB model is an approximation of a power grid where a generator has a small inertia compared to the rest of the grid. A schematic of an SMIB system is shown in Fig. 1 where a local load and a local generator with a relatively small inertia are connected to the system. The load is connected to the grid through a circuit breaker.

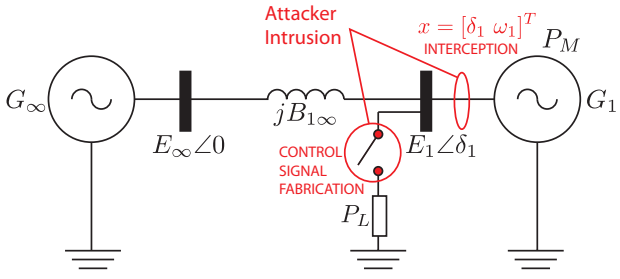

Fig. 1. Single-machine infinite-bus system model

Let G_1 and B_1 represent the local generator and bus, respectively, and let G_∞ and B_∞ represent the SMIB generator and the infinite bus, respectively. The parameters of the power system are explained in the Table I.

Parameter	Description
δ_1	the deviation of the rotor angle of G_1
ω_1	the deviation of the rotor speed of G_1
$B_{1\infty}$	the transfer susceptance of the line between B_1 and B_∞
D_1	the damping coefficient of G_1
E_∞	the voltage at the infinite bus
E_1	the internal voltage of G_1
G_{11}	the equivalent shunt conductance of G_1
M_1	the moment of inertia of G_1
P_L	the local load at B_1
P_M	the mechanical power of G_1
s_L	the status of the load switch

TABLE I
SYSTEM PARAMETERS

The swing equation can be used to study the transient stability of a power system; it links the system parameters in a differential equation. Further, during the attack duration, the system parameters can be considered constant. Consequently, a swing equation with time-invariant parameters can be used to model the power system dynamics during the sliding-mode attack. The swing equation of the local generator when connected to the SMIB system is expressed as [8]

$$\begin{aligned} \dot{\delta}_1 = \;& \omega_1 \\ M_1\,\dot{\omega}_1 = \;& P_M - E_1^2\,G_{11} - s_L\,P_L \\ & -E_1\,E_\infty\,B_{1\infty}\,\sin\delta_1 - D_1\,\omega_1\,. \end{aligned} \tag{4}$$

Let $P_1 = P_M - E_1^2\,G_{11} - s_L\,P_L$ and $C_1 = E_1\,E_\infty\,B_{1\infty}$, then the swing equation of G_1 is simplified into

$$\begin{aligned} \dot{\delta}_1 = \;& \omega_1 \\ \dot{\omega}_1 = \;& \tfrac{P_1}{M_1} - \tfrac{C_1}{M_1}\,\sin\delta_1 - \tfrac{D_1}{M_1}\,\omega_1\,. \end{aligned} \tag{5}$$

Let the state of G_1 be represented as $x = [\delta_1\,,\,\omega_1]^T$, where $[\cdot]^T$ is the transpose operator. Moreover, $s_L = 1$ if the load is connected, and $s_L = 0$ if the load is not connected. For a practical case, and using per-unit (pu) values, let $C_1 = 1$, $D_1 = 0.1$, and $M_1 = 0.1$; in addition, let $P_1 = 0$ for $s_L = 1$ and $P_1 = 0.9$ for $s_L = 0$ (i.e., $P_M - E_1^2\,G_{11} = 0.9$). Consequently, the swing equation of G_1 becomes

$$\begin{cases} \dot{\delta}_1 = \;\omega_1 \\ \dot{\omega}_1 = \;-10\,\sin\delta_1 - \omega_1\,, \end{cases} \quad s_L = 1 \qquad \begin{cases} \dot{\delta}_1 = \;\omega_1 \\ \dot{\omega}_1 = \;9 - 10\,\sin\delta_1 - \omega_1\,, \end{cases} \quad s_L = 0 \tag{6}$$

The following assumptions about the power system are used in this article:

1) the load is initially disconnected from the grid (i.e., $s_L = 0$);
2) the model of the local generator does not include an exciter nor a governor control; and
3) the attacker uses $s = \delta_1 + \omega_1$ to calculate the value of the switching signal.

By trapping the power system inside the sliding surface, the sliding-mode switching attack is conducted in the following steps:

1) the attacker switches the circuit breaker to connect the load to the grid (i.e., $s_L = 1$);
2) when $s(\delta_1, \omega_1) = \delta_1 + \omega_1 < -\epsilon$, the attacker switches the circuit breaker to disconnect the load;
3) when $s(\delta_1, \omega_1) > \epsilon$, the attacker switches the circuit breaker to connect the load;
4) the attacker repeats 2) and 3) until the $x = [\delta_1\,,\,\omega_1]^T$ is outside the attraction region of $f_1(x, t)$; and finally
5) the attacker permanently switches the circuit breaker to disconnect the load.

As a result, the dynamics of the switched system inside the sliding surface, taking into account the hysteresis margin, are displayed as

$$\begin{aligned} \dot{\delta}_1 = \;& \omega_1 \\ \dot{\omega}_1 = \;& \begin{cases} -10\,\sin\delta_1 - \omega_1 & s(\delta_1, \omega_1) > -\epsilon \\ 9 - 10\,\sin\delta_1 - \omega_1 & s(\delta_1, \omega_1) \le \epsilon\,. \end{cases} \end{aligned} \tag{7}$$

The system trajectory during and after the sliding-mode switching attack is shown in Fig 2. It is noted that the phase and frequency of the local generator fluctuate during the attack; the attack stops when the system state is outside the boundary region, then the generator's frequency and phase become unbounded after that. Consequently, the generator becomes unstable and the sliding-mode switching attack is said to be successful.

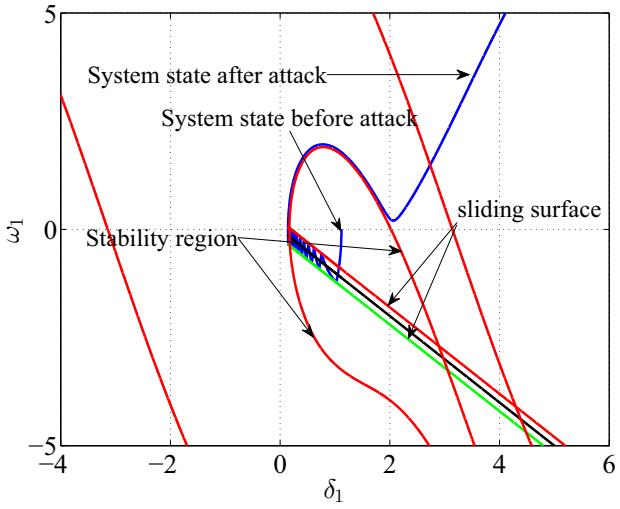

Fig. 2. System trajectory

IV. PRACTICAL CYBER LIMITATIONS

Analysis in Section III demonstrated the development and effectiveness of the sliding-mode switching attack in causing instability in an SMIB system. However, the development of the attack assumed no imperfections in the cyber assets of the system. The impact of having practical cyber limitations on the switching attacks is considered in this section. The investigated limitations include the communications latency between the sensors and the attacker, the sampling period of the sensors, signal quantization, signal-to-noise ratio, circuit

breaker's minimum time to switch, and circuit breaker's hysteresis margin.

Let the communications latency between the sensor and the attacker be represented as δ, the sampling period be termed as τ, the number of quantization levels be represented as σ, the SNR be termed as ψ, the minimum switching time be represented as ζ, and the hysteresis margin be termed as ϵ. For the following numerical results, except the last table, the value of ϵ is set to 0.2. For each considered case, the number of switchings and the total switching time needed to destabilize the SMIB system are shown.

A. Latency

The communication latency occurs due to time to sample and quantize, encryption delay, propagation delay, and queueing delay. Latency can be variable or fixed for each data transmission; The case of fixed latency is considered, this means all data packets between the sensor and the attacker experience the same amount of delay.

Table II shows the results of the sliding-mode switching attack versus the communications latency. When there is no delay (i.e., $\delta = 0$), the attacker needs 18 switchings in 2.006 sec to successfully carry the attack. It is noted that as the latency increases, the attacker needs less switchings in more time. For example, if the delay is 45 ms, the attacker needs 10 switchings in 2.008 sec; on the other hand, if the latency is 90 ms, the attacker will still need the 10 switchings but in 2.889 sec. However, if the communications delay is greater than 97 ms, the sliding-mode switching attack will not succeed.

δ (ms)	Number of Switchings	Switching Time (sec)
0	18	2.006
10	16	2.182
20	14	2.207
30	12	2.101
35	12	2.253
40	12	2.402
45	10	2.008
50	10	2.119
55	10	2.227
60	10	2.332
65	10	2.434
70	10	2.532
75	10	2.626
80	10	2.717
85	10	2.804
90	10	2.889
94	10	2.955
95	10	2.971
96	10	2.987

TABLE II
EFFECT OF COMMUNICATIONS LATENCY

B. Sampling Period

For the sensor readings (i.e., δ_1 and ω_1) to be sent over the channel, the measurements have to be sampled at a certain sampling frequency named f_s. Consequently, the sampling period $\tau = \frac{1}{f_s}$. Higher values of f_s (i.e., lower values of τ) mean that the sensor is measuring the system parameters more frequently. Consequently, as τ becomes lower, the attacker gets more frequent updates of the system parameters.

Table III displays the switching attack results versus the sampling period. It is noted that as τ increases, the time needed for a successful attack increases while the number of switchings decreases. However, if the sampling period is greater than 140 ms, the sliding-mode switching attack will not succeed; Accordingly, if the sampling frequency of the sensors is less than 7.14 Hz, the attacker will not get the readings in a timely manner and so will not be able to construct a successful attack.

τ (ms)	Number of Switchings	Switching Time (sec)
1	18	2.05
10	16	2.07
20	16	2.44
30	14	2.31
40	14	2.52
50	14	2.75
60	14	3.24
70	14	3.92
80	14	3.44
90	12	3.24
100	12	3.70
110	10	3.19
120	10	3.36
130	10	3.38

TABLE III
EFFECT OF SAMPLING PERIOD

C. Quantization

Quantization process is the next step after signal sampling. The goal of the quantization process is to discretize a measurement before converting it into bits. As the number of quantization levels increases, the quantization noise decreases.

Table IV shows the effect of the number of quantization levels on the switching attack. If the number of quantization bits is less than 5, the attack will not succeed. In this case, the quantization noise is high to an extent that prevents the attacker from building a clear picture of the system variables and consequently constructing a successful switching attack.

σ	Number of Switchings	Switching Time (sec)
6	14	1.712
7	16	1.819
8	18	2.064
9	18	2.025
10	18	2.019
11	18	2.009
12	18	2.004
13	18	2.005
14	18	2.004

TABLE IV
EFFECT OF QUANTIZATION

D. Signal-to-Noise Ratio

SNR value is a measure of the quality of the received signal at the attacker's side. A higher value of SNR indicates that the received signal is less corrupted with noise; consequently, it is

more favorable for the attacker to intercept x at a high value of ψ.

Table V details the relation between the SNR values and the time and number of switchings needed to run a sliding-mode attack that destabilizes the local generator. If the SNR value is less than 30 dB, the attacker will not be able to construct a successful sliding-mode switching attack.

ψ (dB)	Number of Switchings	Switching Time (sec)
100	18	2.004
75	18	2.003
60	18	1.996
50	18	1.946
40	24	2.745
35	48	5.626

TABLE V
EFFECT OF SNR

E. Minimum Switching Time

Minimum switching time of the circuit breakers indicates how fast the breaker can switch back-and-forth. A faster circuit breaker enables the attacker to switch the circuit breaker whenever needed (i.e., when the switching signal crosses the sliding surface).

Table VI shows the effect of the circuit breaker's minimum switching time on the switching attack. It takes the attacker more time and number of switchings as the circuit breaker becomes slower. However, if the circuit breaker's minimum switching time is greater than 111 ms, the sliding-mode switching attack will not destabilize the SMIB system.

ζ (ms)	Number of Switchings	Switching Time (sec)
0	18	2.006
10	18	2.006
20	18	2.006
30	18	2.006
40	18	2.006
50	18	2.006
60	18	2.020
70	18	2.171
80	18	2.403
90	18	2.683
100	18	2.917
105	18	3.021
106	18	3.043
107	18	3.064
108	20	3.580
109	20	3.600
110	22	4.118

TABLE VI
EFFECT OF MINIMUM SWITCHING TIME

F. Hysteresis Margin

Practical circuit breakers experience practical delays and hysteresis between consecutive switchings. Hysteresis margin can used as a measure of circuit breakers's practicality where low values of ϵ denote a more ideal circuit breaker.

Table VII detail the relation between the hysteresis margin and the switching attack time and number of switchings. If the hysteresis margin is very small ($\epsilon \leq 0.01$), the attack will not work. As the hysteresis margin decreases, the attacker needs more switchings to construct a successful attack.

ϵ	Number of Switchings	Switching Time (sec)
0.05	66	1.964
0.10	34	1.977
0.15	24	2.072
0.20	18	2.006
0.25	14	1.689
0.30	12	1.876
0.35	10	1.745
0.40	10	2.039
0.45	8	1.687
0.50	8	1.891

TABLE VII
EFFECT OF HYSTERESIS MARGIN

V. CONCLUSIONS

This article investigated the practical limitations of sliding-mode switching attacks in single-machine infinite-bus (SMIB) systems. The investigated limitations include the communications latency the sensors and the attacker, the sampling period of the sensors, signal quantization, signal-to-noise ratio, circuit breaker's minimum switching time, and hysteresis margin.

Results of this work detail the attack's total time and required number of switchings when the attacker is restricted to operate in a non-ideal cyber environment.

ACKNOWLEDGMENT

This work was supported in part by a grant from the National Science Foundation.

REFERENCES

[1] D. Liberzon, *Switching in Systems and Control*. Systems & Control: Foundations & Applications Series, Boston, Massachusetts, USA: Birkhäuser, 2003.

[2] 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.

[3] S. Liu, X. Feng, D. Kundur, T. Zourntos, and K. L. Butler-Purry, "Switched System Models for Coordinated Cyber-Physical Attack Construction and Simulation," in *IEEE International Conference on Smart Grid Communications (SmartGridComm)*, pp. 49–54, 2011.

[4] 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.

[5] S. Liu, D. Kundur, T. Zourntos, and K. L. Butler-Purry, "Coordinated Variable Structure Switching in Smart Power Systems: Attacks and Mitigation," in *International Conference on High Confidence Network Systems (HiCoNS) at Cyber Physical Systems Week (CPSWeek)*, pp. 21–30, 2012.

[6] 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.

[7] A. Sabanovic, L. Fridman, and S. Spurgeon, *Variable Structure Systems: from Principles to Implementation*. IEE Contol Engineering Series 66, London, United Kindom: The Institution of Electrical Engineers, 2004.

[8] P. Kundur, *Power System Stability and Control*. EPRI Power System Engineering Series, McGraw-Hill, 1994.