Letters

Active Synchronous Detection of Deception Attacks in Microgrid Control Systems

Yan Li, *Student Member, IEEE*, Peng Zhang, *Senior Member, IEEE*, Liang Zhang, *Member, IEEE*, and Bing Wang, *Member, IEEE*

***Abstract*—An active synchronous detection method (ASDM) is presented to detect deception attacks on inverter controllers in microgrids without impeding system operations. First, microgrid control center generates specified small probing signals and inject them into controllers. The output signals are then obtained and compared with pre-determined values to locate infracted controller components. Test results show that ASDM can quickly and precisely detect various deception attacks in microgrids.**

***Index Terms*—Microgrids, deception attack, inverter controller, active synchronous detection method.**

I. Introduction

CYBER security of microgrids becomes a major concern largely owing to the unprecedented series of distribution grid attacks recently [1]. Among various cyber-attacks [2], deception attacks, which aim to modify the data exchanged between the different microgrid components, are of high risk, low visibility and can cause cascading effects [3]. Nearly all microgrid functions, e.g., islanding operation, power dispatch, frequency/voltage regulation, are performed via inverter controllers. The primary task, therefore, is to detect deception attacks on microgrid inverter controllers.

Detecting deception attacks in microgrids remains an open problem [4]. Fault-tolerant control or robust control has limited capability to detect control anomaly at a cost of either significant changes in control architectures [3] or poor performance under nominal conditions [5].

To bridge the gap, this letter contributes an Active Synchronous Detection Method (ASDM) to detect attacks on microgrid inverters. ASDM is an extremely light weight solution to *real-time* detection of deception attacks, which does not compromise microgrid control performance. In practice, ASDM can be integrated as a part of the higher level control schemes, e.g., secondary control, tertiary control. Besides, the lookup table built for attack detection provides useful information that can be used for various functions, e.g., system identification.

Manuscript received May 18, 2016; revised August 27, 2016; accepted September 21, 2016. Date of publication October 3, 2016; date of current version December 21, 2016. This work was supported by the National Science Foundation under Grant 1611095 and by Eversource Energy Center. Paper no. PESL-00090-2016.

Y. Li, P. Zhang, and L. Zhang are with the Department of Electrical and Computer Engineering, University of Connecticut, Storrs, CT 06269 USA (e-mail: yan.7.li@uconn.edu; peng.zhang@uconn.edu).

B. Wang is with the Department of Computer Science and Engineering, University of Connecticut, Storrs, CT 06269 USA.

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TSG.2016.2614884

II. Active Synchronous Detection Method

The basic idea of ASDM includes that (1) specified small probing signals are generated by microgrid control center and delivered to targets (e.g., inverter controllers) and (2) responses of targets are then demodulated and compared with pre-determined values to identify whether and where the attack occurs. The probing signals and detection rules are adjusted periodically (or aperiodically) to further increase the cost of adversary, which makes ASDM an active defense scheme.

A. Probing Signals for Attack Detection

For real-time probing and detection without causing unnecessary disturbances, a continuous, periodic signal $x(t)$ with small magnitudes in frequency domain is desirable. Mathematically, these can be described as

$$x(t) = x(t + kT) \tag{1}$$

$$|x(\omega)| < \gamma \tag{2}$$

$$\int_{t}^{t+T} x(t)\, dt = 0 \tag{3}$$

where T is the period of $x(t)$, $k \in \boldsymbol{N}$, $|\cdot|$ is the magnitude of harmonic of $x(t)$ at frequency ω, and γ is a small threshold.

B. ASDM for Inverter Controller

Inverter controllers between sensors (measurement system) and actuators (inverters) are most vulnerable to deception attacks because changing the controllers is the most efficient way for the attackers to tamper a microgrid system. As the double loop dq controller is widely adopted for inverters, this letter demonstrates ASDM on this type of controllers (see Fig. 1). In Fig. 1, two probing signals, $x_P(t)$ and $x_Q(t)$, are injected into reference signals for d-axis and q-axis, respectively. Both are generated from upper control schemes (e.g., secondary or tertiary control) and then delivered through communication network. Therefore, these probing signals can

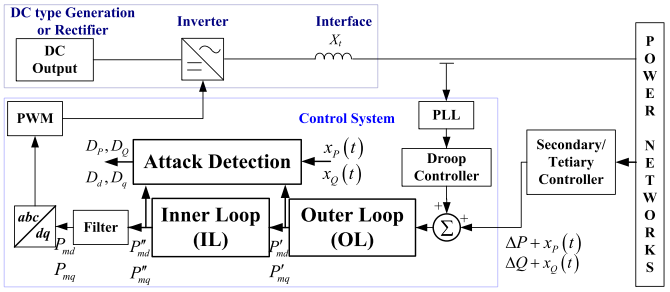

Fig. 1. ASDM for typical double loop controller in an inverter of microgrid.

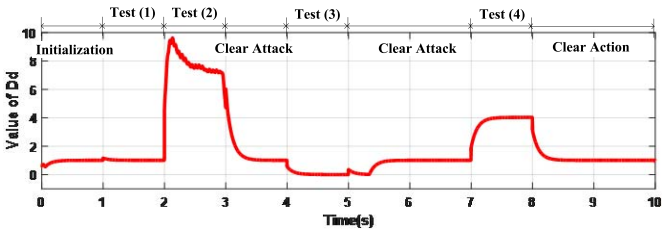

Fig. 2. Detection results of D_d under attacks ($\omega_P = 200$ Hz).

TABLE I
STEADY STATE OF DETECTOR SIGNALS UNDER NORMAL OPERATION

D_P	D_Q	D_d	D_q
$\frac{\beta_P^2 K_P}{2}$	$\frac{\beta_Q^2 K_Q}{2}$	$\frac{\beta_P^2 K_d K_P\left(T_d T_P \omega_P^2 - 1\right)}{2T_d T_P \omega_P^2}$	$\frac{\beta_Q^2 K_q K_Q\left(T_q T_Q \omega_Q^2 - 1\right)}{2T_q T_Q \omega_Q^2}$

be adjusted whenever necessary. The attack detection function can be a shifting window average as follows [6]

$$D = \frac{1}{T}\int_t^{t+T} x(t)\, P'_m dt \tag{4}$$

For the specific system in Fig. 1, $x(t)$ refers to $x_P(t)$ or $x_Q(t)$; P'_m corresponds to $P'_{md}, P'_{mq}, P''_{md}$, or P''_{mq}; D represents the attack detector signals for the double loop controller, i.e., D_P, D_Q, D_d, D_q, which are discussed in detail in the next section.

C. Detection Criteria

We define three types of deception attacks:

(i) Inputs of controllers are attacked and modified;
(ii) Parameters in the controller are overwritten by attacker;
(iii) Combinations of attacks (i) and (ii).

Taking the system in Fig. 1 as an example, two sinusoidal signals are introduced to detect attacks, i.e., $x_P(t) = \beta_P \sin(\omega_P t)$, $x_Q(t) = \beta_Q \sin(\omega_Q t)$. If the system is not attacked, the steady-state values of the detector signals should be identical to the values listed in Table I. Otherwise, if the system is attacked, the detector signals will deviate from the values in Table I. By checking those abnormal outputs against Table II.[1] One can identify the type and location of a specific attack.

As seen from Tables I and II, when the frequencies of probing signals (ω_P and ω_Q) are set high, ASDM is more sensitive to changes in proportional parameters of outer loop (OL) or inner loop (IL). Whereas, if the frequencies are set low, ASDM becomes more sensitive to the integration loop.

[1]Definitions of parameters in Tables I and II can be found in [7].

TABLE II
STEADY STATE OF DETECTOR SIGNALS UNDER ATTACKS

	Attack (i)			*Attack (iii)*	
	OL	IL	OL & IL	Attack (i) on OL, Attack (ii) on IL	Attack (i) on IL, Attack (ii) on OL
D_P	0	$\beta_P^2 K_P / 2$	0	0	$\beta_P^2 \tilde{K}_P / 2$
D_Q	0	$\beta_Q^2 K_Q / 2$	0	0	$\beta_Q^2 \tilde{K}_Q / 2$
D_d	0	0	0	0	0
D_q	0	0	0	0	0
	Attack (ii)				
	OL		IL		
D_P	$\beta_P^2 \tilde{K}_P / 2$		$\beta_P^2 K_P / 2$		
D_Q	$\beta_Q^2 \tilde{K}_Q / 2$		$\beta_Q^2 K_Q / 2$		
D_d	$\frac{\beta_P^2 K_d \tilde{K}_P\left(T_d \tilde{T}_P \omega_P^2 - 1\right)}{2T_d \tilde{T}_P \omega_P^2}$		$\frac{\beta_P^2 \tilde{K}_d K_P\left(\tilde{T}_d T_P \omega_P^2 - 1\right)}{2\tilde{T}_d T_P \omega_P^2}$		
D_q	$\frac{\beta_Q^2 K_q \tilde{K}_Q\left(T_q \tilde{T}_Q \omega_Q^2 - 1\right)}{2T_q \tilde{T}_Q \omega_Q^2}$		$\frac{\beta_Q^2 \tilde{K}_q K_Q\left(\tilde{T}_q T_Q \omega_Q^2 - 1\right)}{2\tilde{T}_q T_Q \omega_Q^2}$		
	Attack (ii) on OL & IL				
D_P	$\beta_P^2 \tilde{K}_P / 2$				
D_Q	$\beta_Q^2 \tilde{K}_Q / 2$				
D_d	$\beta_P^2 \tilde{K}_d \tilde{K}_P\left(\tilde{T}_d \tilde{T}_P \omega_P^2 - 1\right) / \left(2\tilde{T}_d \tilde{T}_P \omega_P^2\right)$				
D_q	$\beta_Q^2 \tilde{K}_q \tilde{K}_Q\left(\tilde{T}_q \tilde{T}_Q \omega_Q^2 - 1\right) / \left(2\tilde{T}_q \tilde{T}_Q \omega_Q^2\right)$				

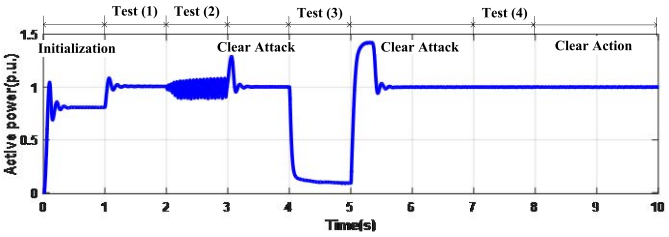

Fig. 3. Active power output of Battery1.

III. TEST RESULTS

A microgrid consisting of three photovoltaic units, three batteries and two microturbines [7] is used to validate ASDM. Four tests are performed, including: (1) Power output of Battery1 is adjusted from 0.8 p.u. to 1.0 p.u. at 1s; (2) A type (ii) attack occurs on OL from 2s through 3s, where K_P is modified from 0.5 to 3.75; (3) A type (i) attack occurs on IL from 4s through 5s; (4) The amplitude of the probing signal $x_P(t)$ is adjusted online from 0.02 to 0.04 from 7s through 8s. Due to limited space, only detection results D_d and Battery1's active power output are shown in Fig. 2 and Fig. 3.

Fig. 2 and Fig. 3 offer the following insights:

1) Test 1 shows ASDM can distinguish normal control operations from attacks (here, battery power output variation does not change detecting results), meaning ASDM is *secure* (does not trigger alarm for non-attacks);
2) Tests 2 and 3 shows ASDM precisely indicates the type and location of attacks online, meaning ASDM is *dependable*;
3) Test 4 demonstrates that the active adjustment of probing signal ($x_P(t)$) does not affect microgrid operations, meaning ASDM has *zero footprint* on the secured systems.

IV. Conclusion

ASDM is introduced to detect deception attacks. The general procedures are substantiated through an application to securing microgrid inverter controllers. Analyses and tests have confirmed the security and dependability of ASDM. ASDM uses trusted footprint in the form of small signals and does not impede system operations. It is a scalable method which can be effectively combined with advanced control schemes.

References

[1] J. Yoon, S. Dunlap, J. Butts, M. Rice, and B. Ramsey, "Evaluating the readiness of cyber first responders responsible for critical infrastructure protection," *Int. J. Critical Infrastruct. Protect.*, vol. 13, pp. 19–27, Jun. 2016.

[2] X. Liu and Z. Li, "Trilevel modeling of cyber attacks on transmission lines," *IEEE Trans. Smart Grid*, to be published, doi: 10.1109/TSG.2015.2475701.

[3] F. Skopik and P. D. Smith, Eds., *Smart Grid Security: Innovative Solutions for a Modernized Grid*. Waltham, MA, USA: Syngress, 2015.

[4] C. K. Veitch, J. M. Henry, B. T. Richardson, and D. H. Hart, "Microgrid cyber security reference architecture," Sandia Nat. Lab., Albuquerque, NM, USA, Tech. Rep. SAND2013-5472, 2013.

[5] R. J. Patton, "Fault-tolerant control," in *Encyclopedia of Systems and Control*, London. U.K.: Springer, 2015, pp. 422–428.

[6] M. T. Ravichandran, "Resilient monitoring and control systems: Design, analysis, and performance evaluation," Ph.D. dissertation, Elect. Eng. Syst., Univ. Michigan, Ann Arbor, MI, USA, 2015.

[7] C. Wang *et al.*, "Coordinated optimal design of inverter controllers in a micro-grid with multiple distributed generation units," *IEEE Trans. Power Syst.*, vol. 28, no. 3, pp. 2679–2687, Aug. 2013.