# Programmable Intrusion Detection for Distributed Energy Resources in Cyber-Physical Networked Microgrids

Shuyang Ma[a], Yan Li[a,*], Liang Du[b], Jianzhong Wu[c], Yue Zhou[c], Yichen Zhang[d], Tao Xu[e]

[a]*Department of Electrical Engineering, The Pennsylvania State University, University Park, PA, 16802 USA*
[b]*Department of Electrical Engineering, Temple University, Philadelphia, PA, 19122 USA*
[c]*School of Engineering, Cardiff University, Cardiff Wales CF24 3AA UK*
[d]*Argonne National Laboratory, Lemont, IL, 60439 USA*
[e]*School of Electrical and Information Engineering, Tianjin University, Tianjin, 300072 China*

**Abstract**

A programmable intrusion detection method is presented to identify the malicious attacks to distributed energy resources (DERs) in the cyber-physical networked microgrids. The proposed method injects small programmable signals into the system and uses the response to identify abnormal conditions. Because of the low or even zero inertia induced by integrations of DER power-electronic-interfaces, microgrids have very limited resilience capability; and thus, being sensitive to attacks. One microgrid's malfunction caused by attacks can easily propagate to its neighboring systems when several microgrids are connected, leading to catastrophic electricity supply failures. Through the presented method, malicious intrusions can be effectively detected, located, and defended for securing microgrids. Theoretical derivations are provided to define the programmable detection rules. The detection rule is easy and flexible to update, making it difficult for attack actors to gain the knowledge of the detection rules, in order to avoid being detected. Numerical results on a cyber-physical networked microgrids system show that the proposed method is effective and efficient in precisely locating intrusion attacks to the microgrids system.

*Corresponding author
*Email address:* yql5925@psu.edu (Yan Li)

*Keywords:*
Programmable intrusion detection, attack, proactive detection, distributed energy resources (DERs), power-electronics interface, microgrids.

## 1. Introduction

Energy sustainability has become one of the major concerns in power engineering [1, 2]. To seek an edge toward energy sustainability, microgrids have been deployed and built worldwide in recent years [3, 4]. A microgrid is defined as a group of interconnected loads and distributed energy resources (DERs), such as photovoltaic and wind generation, within clearly defined electrical boundaries that can act as a single controllable entity [5, 6]. It can connect to or disconnect from the bulk power grid to enable it to operate in either grid-connected or island operational mode [7, 8].

DERs are usually integrated into microgrids through power-electronic interfaces [9], such as inverters. For one thing, the power-electronic interfaces enable flexible system control and operations [10]; and thus, microgrids can provide local green energy generation and delivery to facilitate the sustainable development of power grids [4, 11]. For another, the adoption of power-electronic interfaces makes microgrids vulnerable to attacks [12], because the distributed system configuration offers malicious actors opportunities to access the system locally or remotely [13] or even manipulate the whole power grid in a bottom-up manner. Several power grids attacks, including the first known devastating cyber-attack on Ukraine's power grid in 2015 [14] and the first U.S. 'denial of service' attack launched by remote hacker into the western power grid in March 2019, remind us of this issue as a global challenge. Meanwhile, attacks on power utilities are growing in numbers. Such disastrous attacks would not only take down a large-scale power system but could also result in catastrophic regional or national effects on public health or safety, economic security, or national security. In system operations, the communication network is playing an important role in transmitting measurement data and control signals between physical layer and the control center. A cyber-physical microgrid system is given

in Figure 1 [15], illustrating how signals flow in the system. Therefore, one fundamental question of employing microgrids to promote energy sustainability is: *How to efficiently detect attacks to power-electronic interfaces so microgrids can be used as secure and resilient energy transformation towards sustainability?*

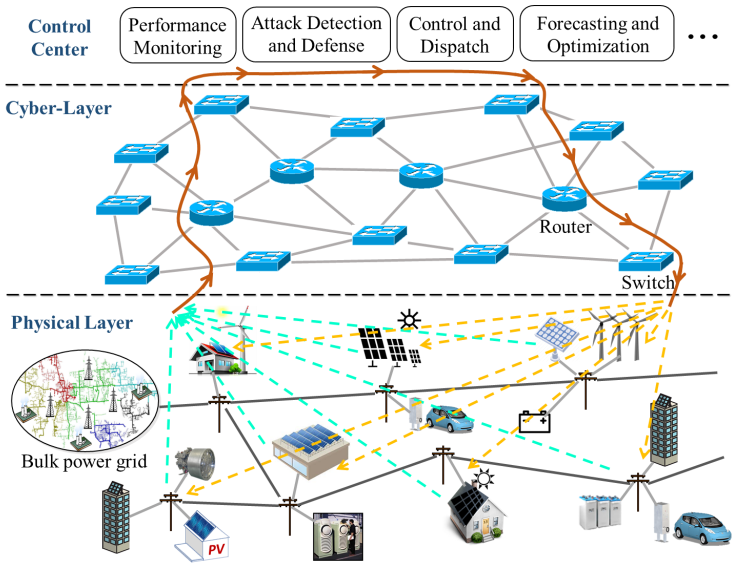



Figure 1: Illustration of cyber-physical microgrids

Among the possible attacks to power-electronic interfaces [16, 17], e.g., denial-of-service, data integrity attacks, intrusions are attracting extensive attention, because they are easy to carry out but hard to detect. The frequent information exchange between DERs also provide several opportunities for malicious actors to manipulate the power-electronic interfaces, such as planting malware [18]. In recent years, intrusion detection has been growing in the computer science field [19, 20]. Intrusion detection is based on software or hardware that can automatically monitor events occurring in the computer system or other networks through analyzing system behaviors for signs of security problems [21, 22]. There broadly exist two main categories of intrusion detection systems [23], namely, Signature-based Intrusion Detection Systems (SIDS) and Anomaly-based Intrusion Detection Systems (AIDS). SIDS, also known as knowledge-based detection or misuse detection, are based on pattern matching

techniques to identify a known attack. When an intrusion signature matches with the signature of an existing intrusion in the database, an alarm signal will be triggered. So, it can accurately detect the previously known intrusions; however, it is difficult to detect unknown attacks since no matching signature exists in the database. Therefore, the effectiveness of SIDS is progressively reduced as new attacks arise, and thus, preventing its applications. AIDS develops a normal model of the system for capturing the significant deviations between the observed behavior and the model. It can be used to identify new attacks because recognizing abnormal activities does not rely on the signature database. However, the recognition highly depends upon accurately building the normal model, which is usually difficult and computationally expensive. Although it is effective in detecting acute intrusions, it is impotent to trigger alarms for attacks which are mild at beginning but can abruptly cause severe damage.

To bridge the knowledge gap, based on AIDS, a Programmable Intrusion Detection method is presented to effectively detect intrusions into microgrids with DERs. The novelties of the presented method are stated below.

- It offers an efficient detection approach for real-time monitoring, which can be used to quickly and accurately identify and locate intrusions to DERs including mild attacks. It identifies attacks when they occur rather than severe damages have been caused by attacks.

- The detection rule is programmable, which can be flexibly renewed when necessary. So, it can avoid the rule being learned by hackers and will significantly increase the cost of hackers. Thus, the system can be secured in a cost-effective way.

- It is a lightweight method which does not impact the normal operations of the system. So, it provides a suitable method to detect anomaly actions in the complicated dynamic systems such as power grids or airplanes.

The remainder of this paper is organized as follows: Section 2 introduces the intrusion detection strategy and its application to the microgrid system. Section 3 presents the programmable detection method and discusses the corresponding changes of detection rules when detection signals are updated. In Section 4,

tests on a networked microgrid system verify the feasibility and effectiveness of the presented method. Conclusions are drawn in Section 5.

## 2. Intrusion Detection

### *2.1. Intrusion Detection Idea*

The essential idea of intrusion detection is to proactively introduce a detection signal $f_s(t)$ to the physical system, and then analyze the response of the system under that detection signal to see whether intrusions into the system occur [24]. There are several detection rules to analyze the response of the system. The following integration function is given as an example, as it is efficient to implement and suitable for programming under different scenarios.

$$\mathcal{H}(t) = \int_0^t \langle r(t), f_s(t) \rangle dt, \tag{1}$$

where $\mathcal{H}(t)$ is the detection result; $f_s(t)$ is the detection signal that will be discussed in Section 3; $r(t)$ represents the response of the testing system; $\langle \cdot, \cdot \rangle$ represents the inner product; and $t$ is the time under investigation.

In order to perform a real-time detection, $f_s(t)$ is usually designed as a periodical signal and it should be small enough compared to the real signals in the testing system; otherwise, it is going to impact the system's normal operation. Additionally, $f_s(t)$ must meet the following requirement to avoid introducing unintended consequences to the monitored system.

$$\frac{1}{T} \int_\tau^{\tau+T} f_s(t) dt = 0, \tag{2}$$

where $\tau$ is the beginning time of monitoring and $T$ is the period of the detection signal $f_s(t)$.

### *2.2. Intrusion Detection in Cyber-Physical Microgrids*

Most of microgrid functions, such as island operation and smoothing DER fluctuations, are realized through controlling DER power-electronic interfaces. As those interfaces are operated through controllers, intrusions into those controllers would provide malicious actors an easy way to malfunction the power-electronic interfaces; and eventually manipulate the overall microgrid system.

So, intrusions to the controllers of DER power-electronic interfaces is analyzed in this paper. Figure 2 shows a typical double loop controller of the DER power-electronic interfaces [25].

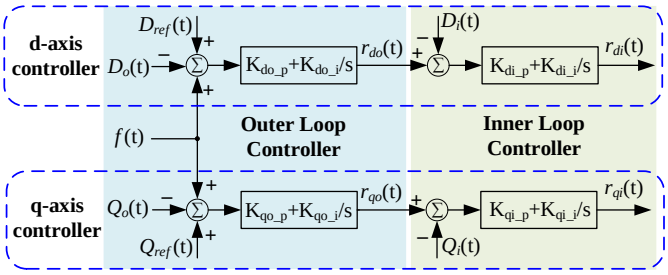



Figure 2: A typical double loop controller

In Figure 2, $D_{ref}(t)$ and $Q_{ref}(t)$ are reference signals for the dispatchable DERs. Those signals are usually generated in a control center in the centralized control strategy and sent to DERs through the communication network. The detection signal $f(t)$ is also generated in the control center and added to the reference signals. Then those signals are transmitted to DERs through communication network. $D_o(t)$ and $Q_o(t)$ are the outer loop measurement signals. $r_{do}(t)$ and $r_{qo}(t)$ are the outer loop output signals. $D_i(t)$ and $Q_i(t)$ are the inner loop measurement signals. $r_{di}(t)$ and $r_{qi}(t)$ are the inner loop output signals. Their responses under the detection signal are analyzed below.

## 3. Programmable Intrusion Detection

The detection signal $f_s(t)$ is playing an essential role in identifying malicious behaviors in the DER power-electronic interfaces and guaranteeing their integrity. If malicious actors gain the knowledge of $f_s(t)$ and then make up fake responses to emulate normal operations, the intrusion detection rule given in (1) will fail to detect attacks. So, in order to make it difficult for malicious actors to always know $f_s(t)$ and increase the attack cost of adversary, the detection signal $f_s(t)$ will be designed as a programmable signal, i.e., programmable intrusion detection.

Several periodic signals can be used to design the detection signal, e.g., square signal and sinusoidal signal, etc. Those fundamental signals must meet the condition given in (2). When necessary, those signals will be combined to create a hybrid detection signal, which makes it harder for hackers to exactly know the detection signal.

### *3.1. Square Detection Signal*

Taking square signal as an example, the programmable detection rule is analyzed below. Assume the square signal is expressed by,

$$f_1(t) = \begin{cases} \varphi_1 & kT_1 \le t < (k+1/2)T_1 \\ -\varphi_1 & (1/2+k)T_1 \le t < (k+1)T_1, \end{cases} \tag{3}$$

where $f_1(t)$ represents $f_s(t)$ in (1), $\varphi_1$ is the amplitude of the square wave, $T_1$ is the period of the detection signal, and $k = 0, 1, 2, \cdots, n$.

#### *3.1.1. Outer Loop*

Taking the d-axis as an example, the output of the outer loop, $r_{do}(t)$, is expressed as:

$$\begin{aligned} r_{do}(t) &= \big(D_{ref}(t) + f_s(t) - D_o(t)\big)\big(K_{do\_p} + \frac{K_{do\_i}}{s}\big) \\ &= K_{do\_p}\big(D_{ref}(t) + f_s(t) - D_o(t)\big) + \int_0^t K_{do\_i}\big(D_{ref}(t) + f_s(t) - D_o(t)\big)\, dt. \end{aligned} \tag{4}$$

Then, based on (1), (3), and (4), the attack detection rule of the outer loop controller is derived as follows:

$$\begin{aligned} \mathcal{H}_{1,Do}(t) &= \int_0^t \langle r_{do}(t), f_1(t)\rangle\, dt \\ &= \int_0^t \langle K_{do\_p}\big(D_{ref}(t) + f_1(t) - D_o(t)\big), f_1(t)\rangle\, dt \\ &\quad + \int_0^t \langle \int_0^t K_{do\_i}\big(D_{ref}(t) + f_1(t) - D_o(t)\big)\, dt, f_1(t)\rangle\, dt \\ &= A + B, \end{aligned} \tag{5}$$

where $\int_0^t \langle K_{do\_p}\big(D_{ref}(t) + f_1(t) - D_o(t)\big), f_1(t)\rangle\, dt$ is defined as $A$, and $\int_0^t \langle \int_0^t K_{do\_i}\big(D_{ref}(t) + f_1(t) - D_o(t)\big)\, dt, f_1(t)\rangle\, dt$ is defined as $B$ to simply the analysis of programmable detection in Sections 3.1.3 and 3.1.4.

*3.1.2. Inner Loop*

The d-axis inner loop is also analyzed as an example. According to Figure 2, the output of the inner loop, $r_{di}(t)$, is expressed as:

$$\begin{aligned} r_{di}(t) &= \big(r_{do}(t) - D_i(t)\big)\big(K_{di\_p} + \frac{K_{di\_i}}{s}\big) \\ &= K_{di\_p}\big(r_{do}(t) - D_i(t)\big) + \int_0^t K_{di\_i}\big(r_{do}(t) - D_i(t)\big)\ dt. \end{aligned} \tag{6}$$

Then, based on (1), (3), and (6), the attack detection rule of the inner loop controller is derived as follows:

$$\begin{aligned} &\mathcal{H}_{1,Di}(t) = \int_0^t \langle r_{di}(t), f_1(t)\rangle\ dt \\ &= \int_0^t \langle K_{di\_p}\big(r_{do}(t) - D_i(t)\big), f_1(t)\rangle\ dt + \int_0^t \langle \int_0^t K_{di\_i}\big(r_{do}(t) - D_i(t)\big)\ dt, f_1(t)\rangle\ dt \\ &= C + D, \end{aligned} \tag{7}$$

where $\int_0^t \langle K_{di\_p}\big(r_{do}(t) - D_i(t)\big), f_1(t)\rangle\ dt$ is defined as $C$, and $\int_0^t \langle \int_0^t K_{di\_i}\big(r_{do}(t) - D_i(t)\big)\ dt, f_1(t)\rangle\ dt$ is defined as $D$.

Depending on how to adjust the amplitude and frequency of the detection signal $f_1(t)$, the detection rules given in (5) and (7) will have the following two different detection results.

*3.1.3. Program the amplitude of the detection signal*

When the frequency of the detection signal is set at a very high value, e.g., a few kHz, the detection rule will depend on the amplitude change of the detection signal. Note that the detection signal $f_1(t)$ is very small. When $f_1(t)$ is a periodical signal and meets the condition given in (2), the following findings can be obtained from analyzing (5) and (7).

- When microgrids reach the steady state, the result of $A$ depends on $\int_0^t \langle K_{do\_p} f_1(t), f_1(t)\rangle\ dt$ and the result of $C$ depends on $\int_0^t \langle K_{do\_p} K_{di\_p} f(t), f(t)\rangle\ dt$.
- The result of $\int_0^t K_{do\_i}\big(D_{ref}(t) + f_1(t) - D_o(t)\big)\ dt$ and $\int_0^t K_{di\_i}\big(r_{do}(t) - D_i(t)\big)\ dt$ are small periodical triangle signals and meet the condition given in (2).

- The result of $B$ and $D$ are small periodical signals, which can be negligible when monitoring the detection results.

Therefore, the result of (5) mainly depends on $A$, and the result of (7) mainly depends on $C$. Then, the detection results of the outer and inner loop controllers can be calculated through the following two functions.

$$\mathcal{H}_{1,Do}(t) = \int_0^t \langle K_{do\_p} f_1(t), f_1(t) \rangle \, dt = K_{do\_p} \varphi^2 t. \tag{8}$$

$$\mathcal{H}_{1,Di}(t) = \int_0^t \langle K_{do\_p} K_{di\_p} f_1(t), f_1(t) \rangle \, dt = K_{do\_p} K_{di\_p} \varphi^2 t. \tag{9}$$

It can be seen from (8) and (9) that the detection results are proportional to the time $t$ and the amplitude square of the detection signal $f_1(t)$.

*3.1.4. Program the frequency of the detection signal*

When the amplitude of the detection signal is fixed and the frequency of the detection signal is relatively small (e.g., a few Hz to hundreds of Hz) and adjustable, the detection rule will depend on the frequency change of the detection signal. The following findings can be obtained from analyzing (5) and (7).

- The result of $\int_0^t K_{do\_i}\big(D_{ref}(t) + f_1(t) - D_o(t)\big) \, dt$ and $\int_0^t K_{di\_i}\big(r_{do}(t) - D_i(t)\big) \, dt$ are periodical signals.
- When microgrids reach the steady state, the result of $A$ depends on $\int_0^t \langle K_{do\_p} f_1(t), f_1(t) \rangle \, dt$ and the result of $C$ depends on $\int_0^t \langle K_{do\_p} K_{di\_p} f_1(t), f_1(t) \rangle \, dt$.
- The impacts of $A$ and $C$ on the detection results are negligible.

Therefore, the result of (5) mainly depends on $B$, and the result of (7) mainly depends on $D$. The detection results of the outer and inner loop controllers can be calculated through the following two functions.

$$\begin{aligned} \mathcal{H}_{1,Do}(t) &= \int_0^t \langle \int_0^t K_{do\_i}\big(D_{ref}(t) + f_1(t) - D_o(t)\big) \, dt, f_1(t) \rangle \, dt \\ &= K_{do\_i} \int_0^t \langle \int_0^t f_1(t) \, dt, f_1(t) \rangle \, dt. \end{aligned} \tag{10}$$

$$\begin{aligned}\mathcal{H}_{1,Di}(t) &= \int_0^t \langle \int_0^t K_{di\_i}\big(r_{do}(t) - D_i(t)\big)\ dt, f_1(t)\rangle\ dt \\ &= K_{do\_i}K_{di\_i}\int_0^t \langle \int_0^t f_1(t)\ dt, f_1(t)\rangle\ dt.\end{aligned} \tag{11}$$

*3.2. Sinusoidal Detection Signal*

Sinusoidal wave is another example that can be used as a detion signal. The corresponding programmable detection rule is analyzed below. Assume a sinusoidal signal is expressed by,

$$f_2(t) = \varphi_2 \sin(\omega_2 t + \theta_2), \tag{12}$$

where $f_2(t)$ represents $f_s(t)$ in (1), $\varphi_2$ is the amplitude of the sinusoidal wave, $\omega_2 = 2\pi/T_2$ is the angular frequency, and $\theta_2$ is the initial angle.

Once again, taking the d-axis as an example, based on (1), (4), and (12), the attack detection function of the outer loop controller is derived as follows:

$$\begin{aligned}\mathcal{H}_{2,Do}(t) &= \int_0^t \langle r_{do}(t), f_2(t)\rangle\ dt \\ &= \int_0^t \langle K_{do\_p}\Big(D_{ref}(t) + f_2(t) - D_o(t)\Big), f_2(t)\rangle\ dt.\end{aligned} \tag{13}$$

Based on (1), (6), and (12), the attack detection function of the inner loop controller is derived in (14).

$$\begin{aligned}\mathcal{H}_{2,Di}(t) &= \int_0^t \langle r_{di}(t), f_2(t)\rangle\ dt \\ &= \int_0^t \langle K_{di\_p}\big(r_{do}(t) - D_i(t)\big), f_2(t)\rangle\ dt.\end{aligned} \tag{14}$$

Similar to the derivation and analysis in Section 3.1.3, the detection results of inverter controllers are calculated through the following two functions.

$$\mathcal{H}_{2,Do}(t) = \int_0^t \langle K_{do\_p} f_2(t), f_2(t)\rangle\ dt = \frac{K_{do\_p}}{2}\varphi_2^2 t. \tag{15}$$

$$\mathcal{H}_{2,Di}(t) = \int_0^t \langle K_{do\_p}K_{di\_p} f_2(t), f_2(t)\rangle\ dt = \frac{K_{do\_p}K_{di\_p}}{2}\varphi_2^2 t. \tag{16}$$

When the frequency of the sinusoidal wave is adjustable, the detection results of the outer and inner loop controllers are calculated below.

$$\begin{aligned}\mathcal{H}_{2,Do}(t) &= \int_0^t \langle \int_0^t K_{do\_i}\big(D_{ref}(t) + f_2(t) - D_o(t)\big)\, dt, f_2(t)\rangle\, dt \\ &= K_{do\_i} \int_0^t \langle \int_0^t f_2(t)\, dt, f_2(t)\rangle\, dt.\end{aligned} \tag{17}$$

$$\begin{aligned}\mathcal{H}_{2,Di}(t) &= \int_0^t \langle \int_0^t K_{di\_i}\big(r_{do}(t) - D_i(t)\big)\, dt, f_2(t)\rangle\, dt \\ &= K_{do\_i}K_{di\_i} \int_0^t \langle \int_0^t f_2(t)\, dt, f_2(t)\rangle\, dt.\end{aligned} \tag{18}$$

*3.3. Programmable Hybrid Detection Signal*

To further increase the cost of adversary, the detection signal can be defined as a combination of signals, such as the aforementioned two basic signals. This detection signal is programmed at the microgrid coordination center; and thus, it can be modified over time. The programmable detection signal is expressed in (19), where the same period $T$ is used in the two signals as an example.

$$\begin{aligned} f_s(t) &= \alpha_1 f_1(t) + \alpha_2 f_2(t) \\ &= \begin{cases} -\alpha_1\varphi_1 + \alpha_2\varphi_2 \sin(\omega_2 t + \theta_2) & kT \le t < (k+1/2)T \\ \alpha_1\varphi_1 + \alpha_2\varphi_2 \sin(\omega_2 t + \theta_2) & (1/2+k)T \le t < (k+1)T, \end{cases} \end{aligned} \tag{19}$$

where $f_1$ and $f_2$ are the signals discussed in the previous section, $\alpha_1$ and $\alpha_2$ are impact factors that can be adjusted in the microgrid coordination center.

When the d-axis is taken as an example, based on (1), (4), and (19), the attack detection function of the outer loop controller is expressed as,

$$\mathcal{H}_{s,Do} = \int_0^t \langle\, r_{do}(t), f_s(t)\rangle dt = \int_0^t \langle\, K_{do\_p}\Big(D_{ref}(t) + f_s(t) - D_o(t)\Big), f_s(t)\rangle dt. \tag{20}$$

Based on (1), (6), and (19), the attack detection function of the inner loop controller is derived in (21).

$$\mathcal{H}_{s,Di} = \int_0^t \langle\, r_{di}(t), f_s(t)\rangle dt = \int_0^t \langle\, f_s(t)(K_{do\_p}K_{di\_p}, f_s(t)\rangle dt. \tag{21}$$

*3.3.1. Program the amplitude of the hybrid detection signal*

According to the derivation in Section 3.1.3, the detection results of the outer and inner loop controllers can be calculated through the following two functions, from which we can see they are proportional to the detection time $t$.

$$\mathcal{H}_{s,Do}(t) = \int_0^t \langle K_{do\_p} f_s(t), f_s(t) \rangle \, dt = K_{do\_p}\big(\alpha_1 \varphi_1^2 + \frac{\alpha_2 \varphi_2^2}{2}\big)t. \tag{22}$$

$$\mathcal{H}_{s,Di}(t) = \int_0^t \langle K_{do\_p} K_{di\_p} f_s(t), f_s(t) \rangle \, dt = K_{do\_p} K_{di\_p}\big(\alpha_1 \varphi_1^2 + \frac{\alpha_2 \varphi_2^2}{2}\big)t. \tag{23}$$

*3.3.2. Program the frequency of the hybrid detection signal*

Based on the derivation in Section 3.1.4, the responses of the inverter controllers under the hybrid detection signal are calculated as follows.

$$\begin{aligned} \mathcal{H}_{s,Do}(t) &= \int_0^t \langle \int_0^t K_{do\_i}\big(D_{ref}(t) + f_s(t) - D_o(t)\big) \, dt, f_s(t) \rangle \, dt \\ &= K_{do\_i} \int_0^t \langle \int_0^t f_s(t) \, dt, f_s(t) \rangle \, dt. \end{aligned} \tag{24}$$

$$\begin{aligned} \mathcal{H}_{s,Di}(t) &= \int_0^t \langle \int_0^t K_{di\_i}\big(r_{do}(t) - D_i(t)\big) \, dt, f_s(t) \rangle \, dt \\ &= K_{do\_i} K_{di\_i} \int_0^t \langle \int_0^t f_s(t) \, dt, f_s(t) \rangle \, dt. \end{aligned} \tag{25}$$

It can be seen from (24) and (25) that the detection results are periodical signals and the frequency of the detection results is same with the detection signal's frequency. This conclusion is very straightforward for system operators to analyze the detection results and will be verified in the following Section 4.

Note that only square signals and sinusoidal signals as well as their combination are introduced here as examples. In fact, many other fundamental signals can be used, such as triangle signals, sawtooth signals,etc. The detection signals can be programmed in multiple ways as long as the detection signals meet the requirements given in (2). Programmable means that the detection signals can be flexibly renewed to avoid the detection rule being learned by hackers and increase the cost of hackers because the programmable detection signals can

cause a big difference in the detection results when the signal is renewed. It can be seen from the simulation results in Section 4.

## 4. Numerical Examples

A typical networked microgrids system given in Figure 3 is used to test and validate the feasibility of the programmable intrusion detection method in detecting intrusions into the microgrids system. The programmable intrusion detection method is implemented in a centralized control center. The networked microgrids system and communication network are modeled in Matlab/Simulink. To better show the impact of the intrusion attack to microgrids, the test system operates in the islanded mode, i.e., Circuit Breaker 0 is open. Other circuit breakers are closed at the beginning, and could be open when necessary. More details of the test system can be found in [25].

As mentioned in (19), the programmable detection signals are assumed to have the same period $T$. Ten examples of the programmable signal will be carried out to verify the effectiveness of the method in attack detection.

### *4.1. Validation When Adjusting the Amplitude of the Detection Signal*

The test system is secure before 1.50 s. An intrusion occurs in the power-electronic interface of Fuel Cell 20 at 1.50 s. Specifically, a malware is planted into the outer loop controller of Fuel Cell 20's inverter, causing a significant change to its PI control parameters, so that controller will be malfunctioning. The frequency of the detection signals sets at $3,000$ Hz. The settings of five test cases are summarized in Table 1. Figure 4 demonstrates the corresponding detection results of the system. Figure 5 and Figure 6 show the transient dynamics of the networked microgrids system under the intrusion.

#### *4.1.1. Case $A_1$: $\alpha_1 = 1$ and $\alpha_2 = 0$*

In Case $A_1$, $\alpha_2 = 0$, according to (19), the detection signal is equivalent to the square signal $f_1$. The amplitude of $f_1(t)$ is set as $5 \times 10^{-4}$. At 1.00 s, the amplitude changes to $1 \times 10^{-3}$, and then changes to $2 \times 10^{-4}$ at 1.25 s, for showing the impact of amplitude on the detection results. Figure 4 (a) and (b) show the outer loop detection results from which it can be observed that:

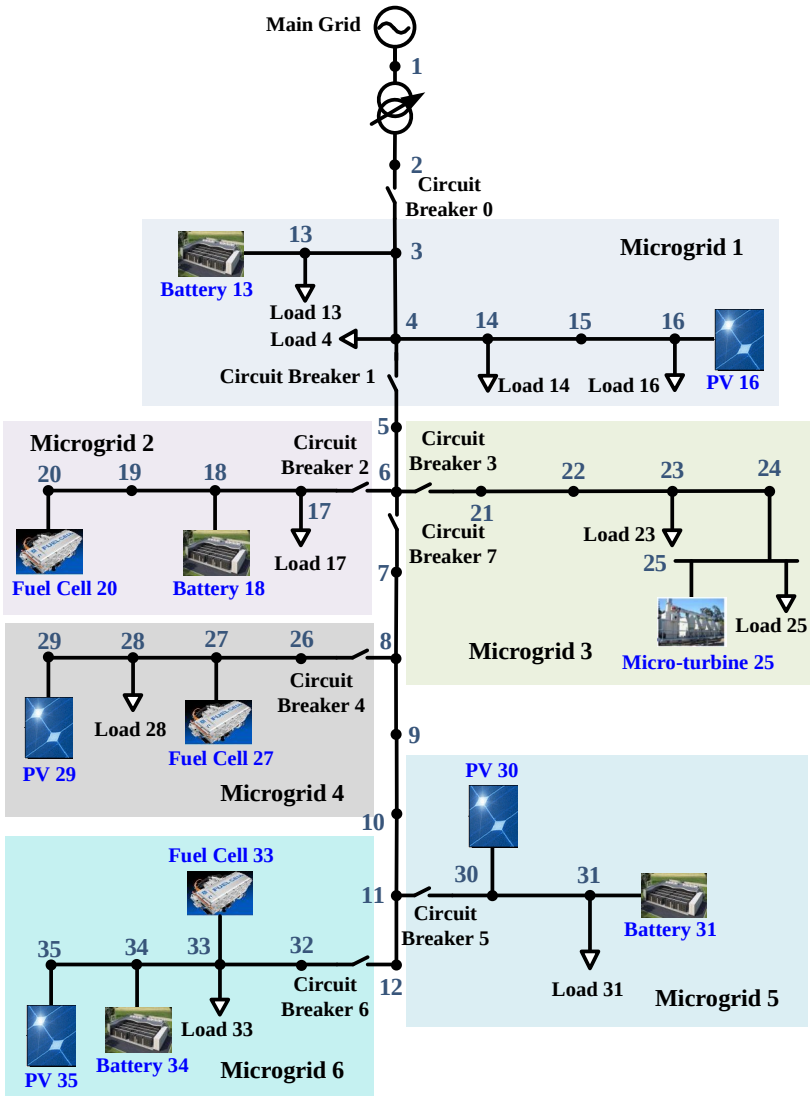



Figure 3: A typical networked microgrids test system

- During normal operations, the detection result is linearly increasing as the time $t$ increases, when the same detection signal is used, as shown by the results during $[0.80s, 1.00s]$ and $[1.00s, 1.25s]$ in Figure 4(b). So, it verifies the detection rule derived in (8).

- When the amplitude of $f_1(t)$ increases from $5.0 \times 10^{-4}$ to $1.0 \times 10^{-3}$, the

Table 1: Amplitude settings of the detection signal in different cases

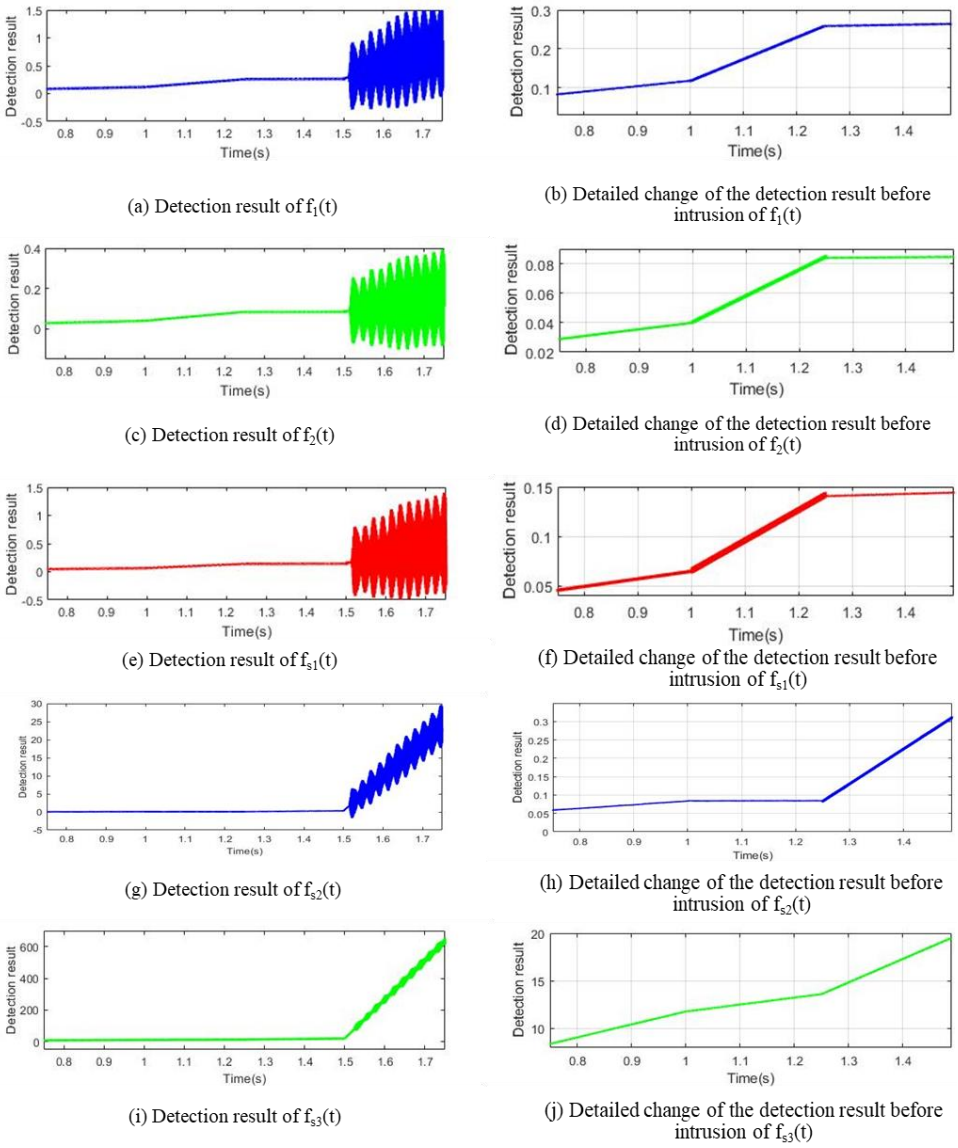
| Case | Figure Number | Detection Signal | Frequency(Hz) | Interval(s) | Amplitude |
|---|---|---|---|---|---|
| $A_1$ | Fig. 4(a)(b) | $f_1(t)$ (Square) | 3000 | [0 1] | $5 \times 10^{-4}$ |
| | | | | [1 1.25] | $1 \times 10^{-3}$ |
| | | | | [1.25 2] | $2 \times 10^{-4}$ |
| $A_2$ | Fig. 4(c)(d) | $f_2(t)$ (Sinusoidal) | 3000 | [0 1] | $4 \times 10^{-4}$ |
| | | | | [1 1.25] | $8 \times 10^{-4}$ |
| | | | | [1.25 2] | $1 \times 10^{-4}$ |
| $A_3$ | Fig. 4(e)(f) | $f_{s1}(t) = 2 * f_1(t) + 4 * f_2(t)$ | | | |
| | | $D_1(t)$ (Square) | 3000 | [0 1] | $8 \times 10^{-4}$ |
| | | | | [1 1.25] | $1 \times 10^{-3}$ |
| | | | | [1.25 2] | $1.5 \times 10^{-3}$ |
| | | $D_2(t)$ (Sinusoidal) | 3000 | [0 1] | $6 \times 10^{-4}$ |
| | | | | [1 1.25] | $2 \times 10^{-4}$ |
| | | | | [1.25 2] | $3 \times 10^{-4}$ |
| $A_4$ | Fig. 4(g)(h) | $f_{s2}(t) = D_1(t) + D_2(t)$ | | | |
| | | $D_3(t)$ (Square) | 3000 | [0 1] | $9 \times 10^{-4}$ |
| | | | | [1 1.25] | $6 \times 10^{-4}$ |
| | | | | [1.25 2] | $1.2 \times 10^{-3}$ |
| | | $D_4(t)$ (Sinusoidal) | 3000 | [0 1] | $7 \times 10^{-4}$ |
| | | | | [1 1.25] | $3 \times 10^{-4}$ |
| | | | | [1.25 2] | $9 \times 10^{-4}$ |
| $A_5$ | Fig. 4(i)(j) | $f_{s3}(t) = 7 * D_3(t) + 3 * D_4(t)$ | | | |

increment rate of the detection result at $[1.00s, 1.25s]$ is four times of that at $[0.80s, 1.00s]$, as shown in Figure 4 (b). It validates the detection result is proportional to the amplitude square of $f_1(t)$.

*4.1.2. Case $A_2$: $\alpha_1 = 0$ and $\alpha_2 = 1$*

In Case $A_2$, $\alpha_1 = 0$, the detection signal is equivalent to the sinusoidal wave $f_2$. The amplitude of $f_2(t)$ is $4 \times 10^{-4}$. At 1.00 s, the amplitude changes to $8 \times 10^{-4}$, and then changes to $1 \times 10^{-4}$ at 1.25 s. Figure 4 (c) and (d) show the outer loop detection results, from which it can be observed that:

- During normal operations, the detection result is linearly increasing as the time $t$ increases, as shown by the results during $[0.80s, 1.00s]$ and $[1.00s, 1.25s]$ in Figure 4 (d). It demonstrates the detection rule in (15).
- When the amplitude of $f_2(t)$ increases from $4.0 \times 10^{-4}$ to $8.0 \times 10^{-4}$, the increment rate of the detection result at $[1.00s, 1.25s]$ is about four times of




(a) Detection result of $f_1(t)$

(b) Detailed change of the detection result before intrusion of $f_1(t)$

(c) Detection result of $f_2(t)$

(d) Detailed change of the detection result before intrusion of $f_2(t)$

(e) Detection result of $f_{s1}(t)$

(f) Detailed change of the detection result before intrusion of $f_{s1}(t)$

(g) Detection result of $f_{s2}(t)$

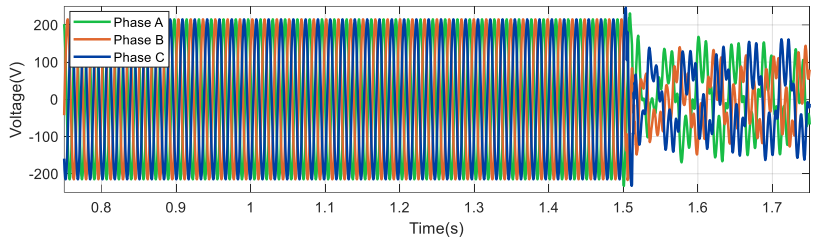
(h) Detailed change of the detection result before intrusion of $f_{s2}(t)$

(i) Detection result of $f_{s3}(t)$

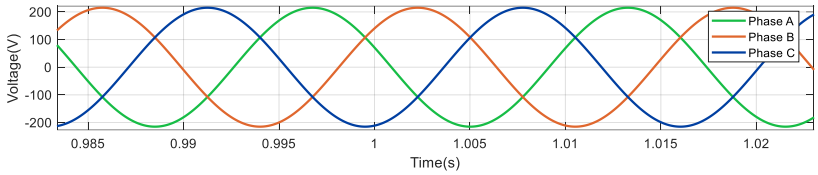
(j) Detailed change of the detection result before intrusion of $f_{s3}(t)$

Figure 4: Detection results when adjusting the amplitude of the detection signal

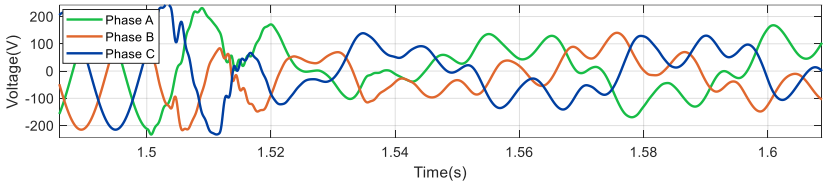
that at $[0.80s, 1.00s]$, as shown in Figure 4 (d). It validates the detection result is proportional to the amplitude square of $f_2(t)$ when sinusoidal wave is adopted as a detection signal.




(a) Dynamics of three-phase voltage




(b) Detailed dynamics of three-phase voltage before intrusion occurs




(c) Detailed dynamics of three-phase voltage after intrusion occurs

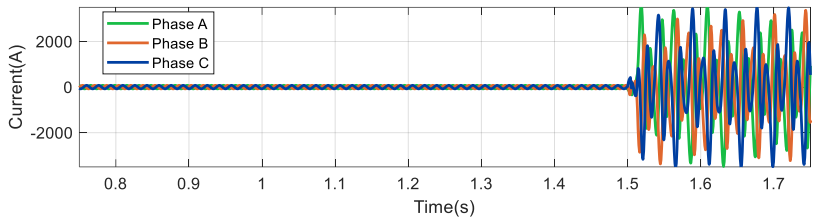
Figure 5: Voltage dynamics at bus 20 in Case A and Case B

*4.1.3. Case $A_3$: $\alpha_1 = 2$ and $\alpha_2 = 4$*

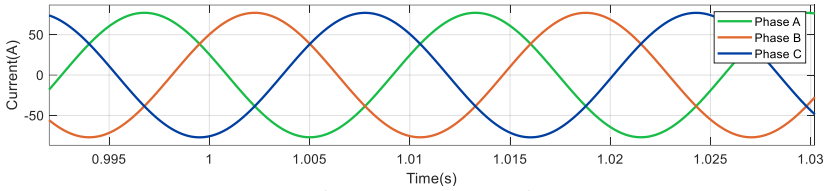
In Case $A_3$, the detection signal $f_{s1}(t)$ is the combination of the $f_1(t)$ and $f_2(t)$, where $f_{s1}(t) = 2*f_1(t) + 4*f_2(t)$. Figure 4 (e) and (f) show the outer loop detection results, from which we can see that: During normal operations, the detection result is linearly increasing as the time $t$ increases, which verifies the detection rule in (22). The increment rate of the detection result at $[1.00s, 1.25s]$ is four times of that at $[0.80s, 1.00s]$, as shown in Figure 4 (f). It validates the detection result is proportional to $\alpha_1 f_1(t) + \alpha_2 f_2(t)$.

*4.1.4. Case $A_4$: $\alpha_1 = 1$ and $\alpha_2 = 1$*

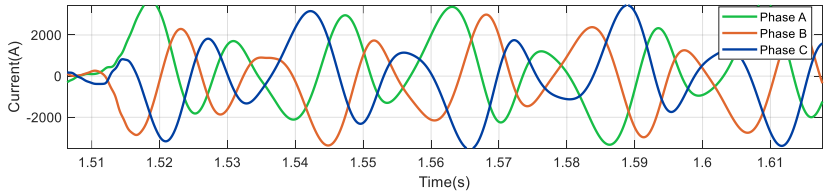
In Case $A_4$, setting a second hybrid signal by using square and sinusoidal signals, $D_1(t)$ and $D_2(t)$, which are shown in Table 1. The detection signal $f_{s2}(t)$ is the combination of $D_1(t)$ and $D_2(t)$, where $f_{s2}(t) = D_1(t) + D_2(t)$. Figure 4 (g) and (h) show the outer loop detection results. From Figure 4 (g)




(a) Dynamics of three-phase current




(b) Detailed dynamics of three-phase current before intrusion occurs




(c) Detailed dynamics of three-phase current after intrusion occurs

Figure 6: Current dynamics at bus 20 in Case A and Case B

and (h), it can be observed that: During normal operations, the detection result is linearly increasing as the time $t$ increases, through which the detection rule in (22) can be verified. The increment rate of the detection result at $[1.25s, 1.50s]$ is 2.25 times of that at $[1.00s, 1.25s]$, as shown in Figure 4(h). It also validates the detection result is proportional to $\alpha_1 f_1(t) + \alpha_2 f_2(t)$.

*4.1.5. Case $A_5$: $D_3(t)$ and $D_4(t)$, $\alpha_1 = 7$ and $\alpha_2 = 3$*

In Case $A_5$, setting a third hybrid signal by using square and sinusoidal signals, $D_3(t)$ and $D_4(t)$, as shown in Table 1. The detection signal $f_{s3}(t)$ is the combination of $D_3(t)$ and $D_4(t)$, wherer $f_{s3}(t) = 7 * D_3(t) + 3 * D_4(t)$. Figure 4 (i) and (j) show the outer loop detection results, from which we can observe that: The detection result is linearly increasing as the time $t$ increases without attacks, which verifies the detection rule in (22). The increment rate of the detection result at $[1.00s, 1.25s]$ is 0.5 times of that at $[0.80s, 1.00s]$, as

shown in Figure 4 (j). It further validates the detection result is proportional to $\alpha_1 f_1(t) + \alpha_2 f_2(t)$.

To conclude the results from the tests of changing amplitude of the detection signal, we can see from Figures 4, 5, and 6 that:

- Based on the detection rules (1), the detection result is a function of the detection time $t$.
- The increment rate of the detection result validates the detection result is proportional to $\alpha_1 f_1(t)+\alpha_2 f_2(t)$. When $\alpha_1$ and $\alpha_2$ are programmable, the overall detection results will also be different. This salient feature makes it efficient to monitor the system.
- The amplitude adjustments of the detection signal do not cause changes to the system normal operations, as shown in Figure 5(a)(b) and Figure 6(a)(b) . It indicates the programmable function of the presented method will not impact system's operations during normal conditions.
- When the intrusion occurs at $1.50s$ as shown in Figure 5(c) and Figure 6(c), the detection result shows a significant change which can bee seen in Figure 4 (a), (c), (e), (g), and (i). It demonstrates the intrusion can be effectively detected through the presented method.
- The simulation results also demonstrate attacks can be immediately detected when they occur rather than severe damages have been caused by attacks. Therefore, the simulation results also assess the novelty of the presented method.

In summary, when there is a significant difference in the detection result, as shown in Figure 4 (a), (c), (e), (g), and (i) after 1.50s, alarm will be triggered in the control center because the abnormal behavior causes the responses react very differently.

### *4.2. Validation When Adjusting the Frequency of the Detection Signal*

The test system is secure before 1.50 s. The same intrusion attack is introduced to the system at 1.50 s. Therefore, Figure 5 and Figure 6 also show the

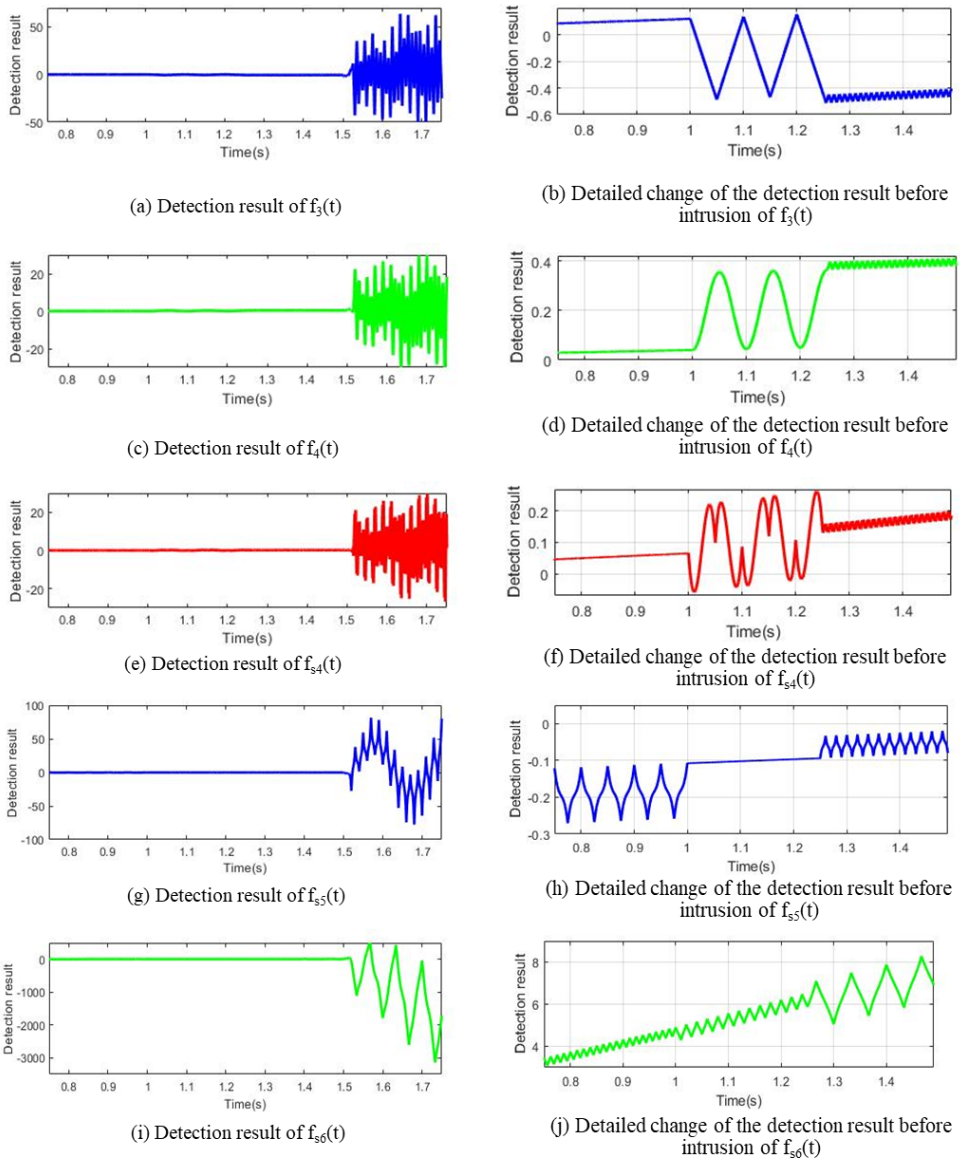
transient dynamics of the test system under the intrusion. Five test cases are carried out and their settings are summarized in Table 2. Figure 7 demonstrates the corresponding detection results of the system.

Table 2: Frequency settings of the detection signal in different cases

| Case | Figure Number | Detection Signal | Amplitude | Interval | Frequency(Hz) |
|---|---|---|---|---|---|
| $B_1$ | Fig. 7(a)(b) | $f_3(t)$ (Square) | $5 \times 10^{-4}$ | [0 1] | 3000 |
| | | | | [1 1.25] | 10 |
| | | | | [1.25 2] | 100 |
| $B_2$ | Fig. 7(c)(d) | $f_4(t)$ (Sinusoidal) | $4 \times 10^{-4}$ | [0 1] | 3000 |
| | | | | [1 1.25] | 10 |
| | | | | [1.25 2] | 100 |
| $B_3$ | Fig. 7(e)(f) | $f_{s4}(t) = 2 * f_3(t) + 4 * f_4(t)$ | | | |
| | | $D_5(t)$ (Square) | $5 \times 10^{-4}$ | [0 1] | 20 |
| | | | | [1 1.25] | 1000 |
| | | | | [1.25 2] | 50 |
| | | $D_6(t)$ (Sinusoidal) | $4 \times 10^{-4}$ | [0 1] | 20 |
| | | | | [1 1.25] | 1000 |
| | | | | [1.25 2] | 50 |
| $B_4$ | Fig. 7(g)(h) | $f_{s5}(t) = D_5(t) + D_6(t)$ | | | |
| | | $D_7(t)$ (Square) | $5 \times 10^{-4}$ | [0 1] | 80 |
| | | | | [1 1.25] | 50 |
| | | | | [1.25 2] | 15 |
| | | $D_8(t)$ (Sinusoidal) | $4 \times 10^{-4}$ | [0 1] | 80 |
| | | | | [1 1.25] | 50 |
| | | | | [1.25 2] | 15 |
| $B_5$ | Fig. 7(i)(j) | $f_{s6}(t) = 7 * D_7(t) + 3 * D_8(t)$ | | | |

*4.2.1. Case $B_1$: $\alpha_1 = 0$ and $\alpha_2 = 1$*

In Case $B_1$, the amplitude of $f_3(t)$ is set at $5.0 \times 10^{-4}$ and the frequency is $3,000$ Hz. At 1.00 s, the frequency changes to 10 Hz, and then changes to 100 Hz at 1.25 s. Figure 7(a) and (b) show the detection results under the above settings. From Figure 7(a) and (b), it can be seen that: When the frequency of the detection signal is relatively small (e.g., 10 Hz), the detection result is observed as a periodical signal with the same frequency as the detection signal. For example, Figure 7 (b) shows during $[1.00s, 1.25s]$, the detection result's frequency is 10 Hz which is equal to the detection signal's frequency. During $[1.25s, 1.50s]$, the detection result's frequency becomes 100 Hz which is also




(a) Detection result of $f_3(t)$

(b) Detailed change of the detection result before intrusion of $f_3(t)$

(c) Detection result of $f_4(t)$

(d) Detailed change of the detection result before intrusion of $f_4(t)$

(e) Detection result of $f_{s4}(t)$

(f) Detailed change of the detection result before intrusion of $f_{s4}(t)$

(g) Detection result of $f_{s5}(t)$

(h) Detailed change of the detection result before intrusion of $f_{s5}(t)$

(i) Detection result of $f_{s6}(t)$

(j) Detailed change of the detection result before intrusion of $f_{s6}(t)$

Figure 7: Detection results when adjusting the frequency of the detection signal

equal to the detection signal's frequency. It also shows the detection result is a triangle wave which can be validated through (10).

*4.2.2. Case $B_2$: $\alpha_1 = 0$ and $\alpha_2 = 1$*

In Case $B_2$, the amplitude of $f_2(t)$ is set at $4.0 \times 10^{-4}$ and the frequency is $3,000$ Hz. At 1.00 s, the frequency changes to 10 Hz, and then changes to 100 Hz at 1.25 s. Figure 7(c) and (d) show the detection results. From the results, we can see that: During normal operations, the detection result is a periodical signal with the same frequency as the detection signal. Because a sinusoidal wave is used to monitor the system, according to (17), the detection result is also a sinusoidal wave with the same frequency as the detection signal.

*4.2.3. Case $B_3$: $\alpha_1 = 2$ and $\alpha_2 = 4$*

In Case $B_3$, the detection signal $f_{s4}(t)$ is the combination of the $f_3(t)$ and $f_4(t)$, where $f_{s4}(t) = 2{*}f_3(t) + 4{*}f_4(t)$. Figure 7 (e) and (f) show the corresponding detection results, which also verifies the detection result is a periodical signal with the same frequency as the detection signal. But the shape of the detection wave is very different from the aforementioned two ones. Further analysis shows it is corresponding to the derivation given in (24).

*4.2.4. Case $B_4$: $\alpha_1 = 1$ and $\alpha_2 = 1$*

In Case $B_4$, the amplitude of the square detection signal, $D_5(t)$, is set as $5.0 \times 10^{-4}$ and its frequency is 20 Hz. At 1.00 s, the frequency changes to $1,000$ Hz, and then changes to 50 Hz at 1.25 s. The amplitude of the sinusoidal detection signal, $D_6(t)$, is $4.0 \times 10^{-4}$ and the frequency is 20 Hz. At 1.00 s, the frequency changes to $1,000$ Hz, and then changes to 50 Hz at 1.25 s. The detection signal $f_{s5}(t)$ is the combination of $D_5(t)$ and $D_6(t)$, namely $f_{s5}(t) = D_5(t) + D_6(t)$. Figure 7(g) and (h) show the detection results in the above scenario. From Figure 7(g) and (h), it can be seen that: The detection result is a periodical signal with the same frequency as the detection signal. But its shape changes again because we actively change the combination of the detection signals. When we substitute the above settings to (24), we can get the same detection results, which verifies the simulation is correct.

*4.2.5. Case $B_5$: $\alpha_1 = 7$ and $\alpha_2 = 3$*

In Case $B_5$, the amplitude of the square detection signal, $D_7(t)$ is $5.0 \times 10^{-4}$ and the frequency is 80 Hz. At 1.00 s, the frequency changes to 50 Hz, and then changes to 100 Hz at 1.25 s. The amplitude of the sinusoidal detection signal, $D_8(t)$ is $4.0 \times 10^{-4}$ and the frequency is 80 Hz. At 1.00 s, the frequency changes to 50 Hz, and then changes to 15 Hz at 1.25 s. The detection signal $f_{s6}(t)$ is the combination of the $D_7(t)$ and $D_8(t)$, namely $f_{s6}(t) = 7 * D_7(t) + 3 * D_8(t)$. Figure 7(i) and (j) show the detection results, which shows a different periodical signal with the same frequency as the detection signal..

To conclude the results from the tests of changing frequency of the detection signal, we can see from Figures 5, 6, and 7 that:

- During normal operations, the detection result is observed as a periodical signal with the same frequency as the detection signal.
- When the frequency of the detection signal is adjusted, only the frequency of the detection results need to be monitored, which makes it easy for system operators to capture the signs of attacks.
- The frequency adjustments do not cause changes to the system's operation, which proves the method is a lightweight approach for monitoring a dynamic system.
- When the intrusion occurs at 1.50 s, the detection results in Figure 7 (a), (c), (e), (g), and (i) show significant changes, which demonstrate the intrusion can be effectively detected through the presented method.

Considering the attacks will propagate through and affect multiple interconnected grid components, the detection results of PV 35 are also shown in Figure 8, where (a)-(e) illustrate the detection results when the amplitude of the detection signal changes and (f)-(i) illustrate the detection results when the frequency of the detection signal changes.

From Figure 8(a)-(e), there is no obvious change in the detection results of PV 35 while a significant difference immediately shows up in the detection result of Fuel Cell 20 as shown in Figure 4 after attack occurs at 1.50s. So, the attack

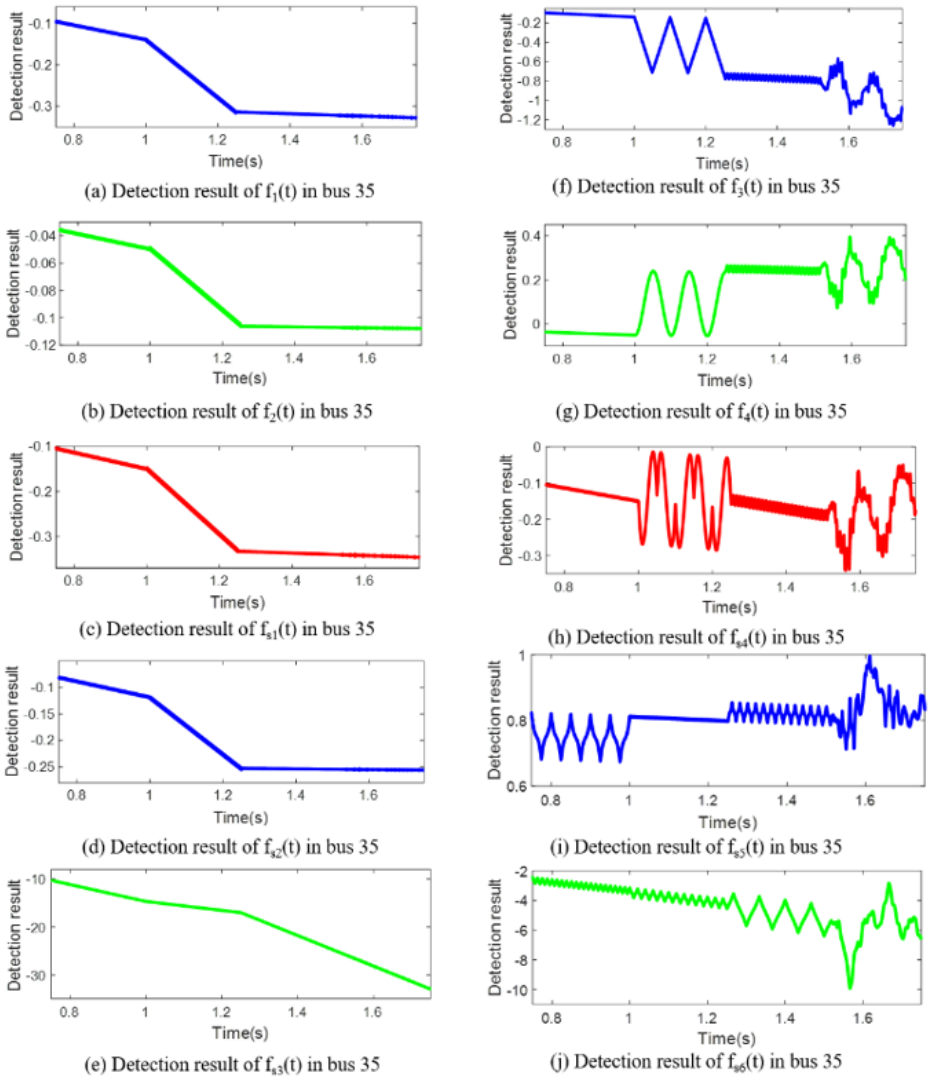



Figure 8: Detection results from bus 35 for each case

can be quickly located attack based on the detection results. Figure 8(f)-(i) also show that after the attack, the detection results of PV 35 do not change much when the detection signal's frequency changes; however, a significant difference immediately shows up in the detection result of Fuel Cell 20 after attack occurs

as shown in Figure 7. So, based on the difference of detection results of each DER unit, the attacks can be quickly located.

The above test cases verify the feasibility of the presented detection method. Note that one shortcoming of the method is that the detection signals need to be continuously sent to the physical system and then the response of the physical system is sent back to the control center for monitoring and analysis. It might put a certain pressure on the communication network. For instance, it could increase latency to communication network due to the intensive traffic. This drawback can be overcome by leveraging the advanced communication network or signal process technique, such as 5G network [26] and compressive sensing [27].

## 5. Conclusions

A programmable intrusions detection method is presented and performed in this paper to identify malicious intrusions into DERs in microgrids. The detection signals are designed to be programmable to make it difficult for attack actors to gain the knowledge of the detection rules for avoiding being detected. Theoretical analysis is provided to discuss the changes of two different detection rules for DER power-electronic interfaces, i.e., programming the amplitude of the detection signal and programming its frequency. Numerical tests are performed on a typical networked microgrids system, which validate the presented method can be used to proactively monitor the system to locate attacks. Those features make it a potent tool for detection intrusions and defending dynamic systems in a precise way.

## References

[1] R. Madurai Elavarasan, R. Pugazhendhi, T. Jamal, J. Dyduch, M. Arif, N. Manoj Kumar, G. Shafiullah, S. S. Chopra, M. Nadarajah, Envisioning the un sustainable development goals (sdgs) through the lens of energy sustainability (sdg 7) in the post-covid-19 world, Applied Energy 292 (2021) 116665.

[2] J. D. Fonseca, J.-M. Commenge, M. Camargo, L. Falk, I. D. Gil, Sustainability analysis for the design of distributed energy systems: A multi-objective optimization approach, Applied Energy 290 (2021) 116746.

[3] M. Roslan, M. Hannan, P. J. Ker, M. Uddin, Microgrid control methods toward achieving sustainable energy management, Applied Energy 240 (2019) 583–607.

[4] Y. Li, P. Zhang, M. Yue, Networked microgrid stability through distributed formal analysis, Applied Energy 228 (2018) 279–288.

[5] C. Wang, Y. Li, K. Peng, B. Hong, Z. Wu, C. Sun, Coordinated optimal design of inverter controllers in a micro-grid with multiple distributed generation units, IEEE Transactions on Power Systems 28 (3) (2013) 2679–2687.

[6] V. Shahbazbegian, S.-M. Hosseini-Motlagh, A. Haeri, Integrated forward/reverse logistics thin-film photovoltaic power plant supply chain network design with uncertain data, Applied Energy 277 (2020) 115538.

[7] M. Quashie, C. Marnay, F. Bouffard, G. Joós, Optimal planning of microgrid power and operating reserve capacity, Applied Energy 210 (2018) 1229–1236.

[8] J. Nelson, N. G. Johnson, K. Fahy, T. A. Hansen, Statistical development of microgrid resilience during islanding operations, Applied Energy 279 (2020) 115724.

[9] N. Soni, S. Doolla, M. C. Chandorkar, Improvement of transient response in microgrids using virtual inertia, IEEE Transactions on Power Delivery 28 (3) (2013) 1830–1838.

[10] Y. Zhang, Y. Li, K. Tomsovic, S. M. Djouadi, M. Yue, Review on set-theoretic methods for safety verification and control of power system, IET Energy Systems Integration 2 (3) (2020) 226–234.

[11] Y. Li, W. Gao, J. Jiang, Stability analysis of microgrids with multiple der units and variable loads based on mpt, in: PES General Meeting—Conference & Exposition, 2014 IEEE, IEEE, 2014, pp. 1–5.

[12] K. Lai, M. Illindala, K. Subramaniam, A tri-level optimization model to mitigate coordinated attacks on electric power systems in a cyber-physical environment, Applied Energy 235 (2019) 204–218.

[13] X. Luo, X. Wang, M. Zhang, X. Guan, Distributed detection and isolation of bias injection attack in smart energy grid via interval observer, Applied Energy 256 (2019) 113703.

[14] G. Liang, S. R. Weller, J. Zhao, F. Luo, Z. Y. Dong, The 2015 ukraine blackout: Implications for false data injection attacks, IEEE Transactions on Power Systems 32 (4) (2016) 3317–3318.

[15] Y. Li, Y. Zhang, D. Zhao, L. Du, Scalable distributed reachability analysis for cyber-physical networked microgrids with communication latency, in: 2021 IEEE Transportation Electrification Conference and Expo (ITEC), IEEE, 2021, pp. 1–5.

[16] O. T. Soyoye, K. C. Stefferud, Cybersecurity risk assessment for california's smart inverter functions, in: 2019 IEEE CyberPELS (CyberPELS), IEEE, 2019, pp. 1–5.

[17] B. Yang, L. Guo, F. Li, J. Ye, W. Song, Impact analysis of data integrity attacks on power electronics and electric drives, in: 2019 IEEE Transportation Electrification Conference and Expo (ITEC), IEEE, 2019, pp. 1–6.

[18] I. N. Fovino, A. Carcano, M. Masera, A. Trombetta, An experimental investigation of malware attacks on scada systems, International Journal of Critical Infrastructure Protection 2 (4) (2009) 139–145.

[19] R. G. Bace, Intrusion detection, Sams Publishing, 2000.

[20] A. A. Saad, S. Faddel, O. Mohammed, A secured distributed control system for future interconnected smart grids, Applied Energy 243 (2019) 57–70.

[21] P. Garcia-Teodoro, J. Diaz-Verdejo, G. Maciá-Fernández, E. Vázquez, Anomaly-based network intrusion detection: Techniques, systems and challenges, computers & security 28 (1-2) (2009) 18–28.

[22] S. Axelsson, Intrusion detection systems: A survey and taxonomy, Tech. rep., Technical report (2000).

[23] A. Khraisat, I. Gondal, P. Vamplew, J. Kamruzzaman, Survey of intrusion detection systems: techniques, datasets and challenges, Cybersecurity 2 (1) (2019) 1–22.

[24] Y. Li, P. Zhang, L. Zhang, B. Wang, Active synchronous detection of deception attacks in microgrid control systems, IEEE Transactions on Smart Grid 8 (1) (2017) 373–375.

[25] Y. Li, Y. Qin, P. Zhang, A. Herzberg, SDN-enabled cyber-physical security in networked microgrids, IEEE Transactions on Sustainable Energy 10 (3) (2018) 1613–1622.

[26] A. Gupta, R. K. Jha, A survey of 5g network: Architecture and emerging technologies, IEEE access 3 (2015) 1206–1232.

[27] R. G. Baraniuk, Compressive sensing [lecture notes], IEEE signal processing magazine 24 (4) (2007) 118–121.